

Oracle® Fusion Middleware

Release Notes for Oracle SOA Suite



14c (14.1.2.0.0)

F80752-01

December 2024

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Oracle Fusion Middleware Release Notes for Oracle SOA Suite, 14c (14.1.2.0.0)

F80752-01

Copyright © 2006, 2024, Oracle and/or its affiliates.

Primary Author: Oracle Corporation

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, software documentation, data (as defined in the Federal Acquisition Regulation), 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 embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. 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®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside 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, Epyc, and the AMD 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

Documentation Accessibility	iv
Related Documents	iv
Conventions	v

1 New Features

New Features in Oracle SOA Suite	1-1
Updates in Oracle B2B	1-1

2 Known Issues and Workarounds

SOA Core Known Issues and Workarounds	2-1
Secure Mode Disabled by Default in Upgraded Environment	2-1
Restart in High Availability Secure Mode May Fail	2-2
Managed Server Created in Secure Clustered Environment Fails to Start	2-2
java.lang.reflect.UndeclaredThrowableException in Deployed Composite Tab	2-4
Plan Creation in SOAINFRA Fails with JAVA.LANG.ILEGALSTATEEXCEPTION Error	2-4
SOA Users with Application Roles Require Special Permissions to Perform Operations in Secure Mode	2-5
14.1.2.0.0 Post Upgrade CQs Related to Alerts and KPIs are Deregistered	2-6
Unable to Deploy SOA Composite Using the Application Server Connection Created with Hostname as Localhost	2-6

Preface

Release Notes for Oracle SOA Suite describes new features for Release 14c (14.1.2.0.0) of Oracle SOA Suite, and also includes information about known issues and workarounds.

For release notes for earlier releases not covered here, refer to the Oracle Fusion Middleware library on the Oracle Help Center for the release you need.

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>.

Accessible Access to Oracle Support

Oracle customers who 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

Refer to the [Oracle Fusion Middleware library on the Oracle Help Center](#) for additional information.

- For Oracle SOA Suite information, see Oracle SOA Suite.
- For adapters information, see On-Premises and Cloud SOA Adapters.
- For Oracle BAM information, see Oracle Business Activity Monitoring.
- For Oracle B2B information, see Oracle B2B.
- For Oracle Business Process Management information, see Oracle Business Process Management.
- For Oracle Enterprise Scheduler information, see Oracle Enterprise Scheduler.
- For Oracle Managed File Transfer information, see Oracle Managed File Transfer.
- For Oracle Service Bus information, see Oracle Service Bus.
- For Oracle SOA Suite for healthcare integration information, see Oracle SOA Suite for Healthcare Integration.
- For versions of platforms and related software for which Oracle products are certified and supported, review the [Certification Matrix on OTN](#).
- For cloud adapters information, see :
 - *Using Ariba Adapter*
 - *Using Oracle Eloqua Cloud Adapter*

- *Using Oracle ERP Cloud Adapter*
- *Using the NetSuite Adapter*
- *Using Oracle RightNow Cloud Adapter*
- *Using Salesforce Adapter*
- *Using Oracle Sales Cloud Adapter*
- *Using ServiceNow Adapter*
- *Oracle Cloud Adapters Postinstallation Configuration Guide*

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.
<i>italic</i>	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

New Features

Oracle SOA Suite 14c (14.1.2.0.0) is available on-premises and in the cloud. To use Oracle SOA Suite in the cloud, see:

- [Using Oracle SOA Suite on Marketplace in Oracle Cloud Infrastructure](#)
- [Oracle SOA Cloud Service](#)

New Features in Oracle SOA Suite

Here are the new features for Release 14c (14.1.2.0.0) of Oracle SOA Suite on-premises:

- The new Apache Kafka adapter enables you to create an integration that connects to an Apache Kafka messaging system. See [Apache Kafka Adapter](#).
- Hybrid integrations that enable you to connect your Oracle SOA Suite on-premises applications with cloud applications through Oracle Integration Cloud. See:
 - [How to Invoke OAuth-Protected Oracle Integration REST Endpoints from a SOA Composite Application in *Developing SOA Applications with Oracle SOA Suite*](#).
 - [See *Track Oracle Integrations Invoked from Oracle SOA Suite* in *Initiating a Test Instance of a Business Flow in Administering Oracle SOA Suite and Oracle Business Process Management Suite*](#).
 - [Copy Between JSON and XML Variables in a BPEL Process in *Developing SOA Applications with Oracle SOA Suite*](#).
 - [See *Create a REST binding using the OpenAPI Document URL* in *Create a REST Binding in Developing SOA Applications with Oracle SOA Suite*](#).
- A REST enhancement that enables you to configure proxy port and port host for an external REST endpoint. See [Configure Proxy Host and Proxy Port for an External REST Endpoint in *Developing SOA Applications with Oracle SOA Suite*](#).
- An option to add multipart form data in REST binding. See [REST Method Definition Dialog in *Developing SOA Applications with Oracle SOA Suite*](#).
- An option to view the auto purge job execution history in Oracle Enterprise Manager. See [View Purge History in *Administering Oracle SOA Suite and Oracle Business Process Management Suite*](#).
- When the payload size for a SOA composite exceeds the maximum limit, the payload is rejected, and a notification email is sent to the configured users. See [Configured Reference Configuration Domain Settings in *Administering Oracle SOA Suite and Oracle Business Process Management Suite*](#).

Updates in Oracle B2B

Release 14c (14.1.2.0.0) of Oracle SOA Suite does not support EDI, EDIFACT, HL7, and PFF document protocols. Customers using these document protocols are suggested to remain on Release 12c (12.2.1.4.0).

2

Known Issues and Workarounds

This chapter describes known issues and workarounds for Release 14c (14.1.2.0.0) of Oracle SOA Suite:

- [SOA Core Known Issues and Workarounds](#).



Note:

To apply patches noted in this guide, sign in to [My Oracle Support](#) and search for the patch numbers to locate and download the patches.

SOA Core Known Issues and Workarounds

Known issues and workarounds for Release 14c (14.1.2.0.0) of SOA Core are:

- [Secure Mode Disabled by Default in Upgraded Environment](#)
- [Restart in High Availability Secure Mode May Fail](#)
- [Managed Server Created in Secure Clustered Environment Fails to Start](#)
- [java.lang.reflect.UndeclaredThrowableException in Deployed Composite Tab](#)
- [Plan Creation in SOAINFRA Fails with JAVA.LANG.ILEGALSTATEEXCEPTION Error](#)
- [SOA Users with Application Roles Require Special Permissions to Perform Operations in Secure Mode](#)
- [Post Upgrade CQs Related to Alerts are Deregistered](#)
- [Unable to Deploy SOA Composite Using the Application Server Connection Created with Hostname as Localhost](#)

Secure Mode Disabled by Default in Upgraded Environment

Issue

Bug Number: 36735609

Impacted Releases: 14.1.2.0.0

Impacted Platforms: All

When you upgrade from 12.2.1.4 to 14.1.2.0.0, the secure mode is disabled by default in the upgraded Oracle SOA Suite environment. If you choose to enable secure mode, and as a result, if the protocol, host, and port combination changes, it might cause issues in the existing Oracle SOA Suite flow instances created before the migration.

The existing Oracle SOA Suite instances created before the migration might be impacted in the following cases.

- If SSL is disabled in the source environment before the migration.

- If there is an external reference from a SOA composite to another SOA composite WSDL or service using a non-SSL URL, which changes.
Workaround:
For this case, the SOA composite must be updated to avoid the usage of hard coded URL using a token or a Load Balancer URL, which remains valid after the upgrade.
- All the call backs from external systems for the instances created before the upgrade might fail if the call back is made to the SOA instance with an old SOA server URL, which gets modified as part of the upgrade.
Workaround:
For this case, you can temporarily enable the non-SSL URL to recover call back of instances. However, this might not work for all the cases. Ensure that there are no open instances expecting call backs from external systems before the upgrade.

The existing Oracle SOA Suite instances created before the migration are not impacted in the following cases.

- If SSL is enabled in the source environment before the migration, and the protocol, host, and port remain unchanged as part of the upgrade.
- If the customer is using Oracle HTTP Server or Load Balancer URL as the SOA Server URL, which is used to route calls and if all the external interactions occur through the SOA Server URL (assuming that the URL remains unchanged).

When you switch from non-secure mode to secure mode for the first time, ensure that you update the external client with the new endpoint URL. The call back requests are then routed to the new call back composite endpoint URL. For subsequent switches between secure mode and non-secure mode, the endpoint URL remains unchanged and the call backs function seamlessly.

Restart in High Availability Secure Mode May Fail

Issue

Bug Number: 36733624

Impacted Releases: 14.1.2.0.0

Impacted Platforms: All

When you restart Oracle SOA Suite in high availability and secure mode, the Enterprise Manager Fusion Middleware Control may throw an error. This is an intermittent issue.

- `errorPage.jspx` error is thrown when you access Enterprise Manager Fusion Middleware Control (`https://hostname:port/em`).
- Failure of Web Server bridge: No backend server available for connection error is thrown when you access soa-infra node (`https://hostname:port/soa-infra`).

Workaround

None.

Managed Server Created in Secure Clustered Environment Fails to Start

Issue

Bug Number: 36735609

Impacted Releases: 14.1.2.0.0

Impacted Platforms: All

The managed server fails to start when created through remote console in 14.1.2.0.0 and throws "Keystore password was incorrect" error.

Workaround

To create and start a managed server through WebLogic Remote Console, log in to your WebLogic Remote Console and perform the following steps.

1. Navigate to **Edit Tree**, under **Environment** select **Servers**.
2. Click **New**.
3. Specify a name for the managed server.
4. From **Copy settings from another server** drop-down, select an existing managed server.
5. Click **Create**.
6. In Edit Tree, navigate to the newly created server. For example, WLS_SOA5.
7. In the General tab, update and specify a unique number in the **Local Administration Port Override** field. Ensure that all the managed servers in the domain on the same machine have unique administration port values (≥ 1024).
8. Click **Save**.
A message confirms that the changes are added to the shopping cart.
9. Navigate to the **Security** tab, and then select **Keystores**.
10. In the Keystores tab, specify the **Custom Identity Key Store Pass Phrase** and **Custom Trust Key Store Pass Phrase**.
11. Click **Save**.
A message confirms that the changes are added to the shopping cart.
12. Navigate to the **SSL** tab and specify the **Server Private Key Pass Phrase**.
13. Click **Save**.
A message confirms that the changes are added to the shopping cart.
14. Navigate to the Shopping Cart in the top-right corner of the WebLogic Remote Console window and click **Commit Changes**.
15. Start the managed server.
Sample Command:

```
cd /u02/oracle/config/domains/base_domain_1/bin
./startManagedWebLogic.sh WLS_SOA5
https://soaexternal.oraclevcn.com:9002
-Djavax.net.ssl.trustStore=/u01/oracle/config/keystores/soahost1/
trust.p12

-Djavax.net.ssl.trustStorePassword=WELCOME1_1_
```

java.lang.reflect.UndeclaredThrowableException in Deployed Composite Tab

Issue

Bug Number: 36733516

Impacted Releases: 14.1.2.0.0

Impacted Platforms: All

Description of the issue and when it might occur.

1. Log in to Enterprise Manager Fusion Middleware Control.
2. Navigate to **SOA Infrastructure** and select **SOA Folder**.
3. Select **Default** and then navigate to the **Deployed Composite** tab.
The following error message is displayed in the browser: Retrieval failed with error java.lang.reflect.UndeclaredThrowableException. Please view the log file for details.

Workaround

None.

Plan Creation in SOAINFRA Fails with JAVA.LANG.ILEGALSTATEEXCEPTION Error

Issue

Bug Number: 36907731

Impacted Releases: 14.1.2.0.0

Impacted Platforms: All

When you create a plan in SOAINFRA, the plan creation fails with the following error:

```
JAVA.LANG.ILEGALSTATEEXCEPTION: CANNOT CONVERT VALUE OF TYPE  
'JDK.PROXY7.$PROXY447'
```

This error is caused when you update the transaction timeout value for **FacadeFinderBean** property in the Oracle WebLogic Remote Console.

1. Navigate to the **Monitoring Tree**, and select **Deployments**.
2. Select **Subdeployments** and then choose **fabric-ejb.jar**.
3. Further, select **FacadeFinderBean** and then select **Transaction Descriptor**.
4. Update the value of **Transaction Timeout** field as 600.
5. **Save** and **Redeploy** the SOAINFRA application.

Workaround

You must manually modify the transaction timeout setting in your deployment archive.

1. Open the **fabric-ejb.jar** file in your deployment archive.
2. Increase the transaction timeout value in the **META-INF/weblogic-ejb-jar.xml** file to a larger value.
3. Update the jar file.
4. Restart the managed server that includes SOA infrastructure.

SOA Users with Application Roles Require Special Permissions to Perform Operations in Secure Mode

Issue

Bug Number: 36841322

Impacted Releases: 14.1.2.0.0

Impacted Platforms: All

Users with application roles such as `default_composer`, `SOAOperator`, `SOAMonitor`, and so on, face the following error when performing operations in secure mode.

```
[test_log] [INFO] [exec] Connecting to
    t3s://phxpffag40.dev2farmphx3.screvenfar02phx.oraclevcn.com:9002 with
userid
    partitioncomposeruser ...
    [test_log] [INFO] [exec] <Jul 10, 2024, 6:14:55â€AM Pacific Daylight
Time> <Info>
        <Security> <BEA-090908> <Using the default WebLogic SSL Wildcard
Hostname Verifier
    implementation.>
    [test_log] [ERROR] [exec] This Exception occurred at Wed Jul 10
06:14:55 PDT
    2024.
    [test_log] [ERROR] [exec] java.lang.SecurityException: User
partitioncomposeruser does
    not have access to the administrator port.
```

Workaround

When secure mode is enabled, all the admin traffic (including MBean Access) is directed to the admin channel. The admin channel is available only to users with an admin role. Thus, to perform operations in secure mode, users with application roles such as `default_composer`, `SOAOperator`, `SOAMonitor`, and so on, require access to **AdminChannel**. See [Users, Groups, And Security Roles](#). Below are the list of roles and their corresponding access privilege to the admin channel.

- Admin role : Read & Write Access
- Monitor role : Read Access
- App Tester role : Read Access

14.1.2.0.0 Post Upgrade CQs Related to Alerts and KPIs are Deregistered

Issue

Bug Number: 36907731

Impacted Releases: 14.1.2.0.0

Impacted Platforms: All

When you upgrade from 12.2.1.4 to 14.1.2.0.0, the previously registered CQs are deregistered after the upgrade is complete.

Workaround

After the upgrade process, register the CQs so that the KPIs start working.

Unable to Deploy SOA Composite Using the Application Server Connection Created with Hostname as Localhost

Issue

Bug Number: 37226467

Impacted Releases: 14.1.2.0.0

Impacted Platforms: All

If you create an application server connection by providing hostname as the localhost and try to deploy the SOA sample using this connection, the SOA servers are not listed in the deployment wizard.

Workaround

1. Remove the application server connection created using the localhost.
2. Remove the system file generated by the JDeveloper while starting the JDeveloper. For example : /home/<userid>/.jdeveloper.
3. Open the JDeveloper and create the application server connection using the hostname as, for example, myhost.com.
4. Now, deploy the SOA sample using the application server connection.