

**Oracle Utilities Customer Care and Billing
Integration to Oracle PeopleSoft
Financials for General Ledger and
Accounts Payable**

Installation Guide

Release 12.1

E21390-04

June 2017 (Updated)

Oracle Utilities Customer Care and Billing Integration to Oracle PeopleSoft Financials for General Ledger and Accounts Payable, Release 12.1 Installation Guide

Copyright ©2009, 2017 Oracle and/or its affiliates. All rights reserved.

Primary Author: Oracle Corporation UGBU Documentation

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

Installation Guide

Preface	i
Documentation and Resources	i
Documentation Accessibility	iii
Conventions.....	iii
Abbreviations	iii

Chapter 1

Overview	1-1
Integration Pack Software Requirements.....	1-1

Chapter 2

Installation	2-1
Pre-Installation Tasks.....	2-1
Installation Steps.....	2-2
Installing the Integration	2-4
Post-Installation Checklist.....	2-4
Verifying JDBC Configuration.....	2-5
Verifying Composites in Enterprise Manager.....	2-5
Verifying CSF-Key Generation	2-6
Configuring Oracle Utilities Customer Care and Billing Key Store Certificate	2-6
Verifying User Messaging Service List	2-8
Configuring Edge Applications	2-9
Security Policies	2-9

Chapter 3

Individual Composites	3-1
Undeploying Individual Composites	3-1
Deploying Individual Composites.....	3-2

Chapter 4

Metadata Store (MDS) Artifacts	4-1
Undeploying the MDS Folder	4-2
Deploying the MDS Folder.....	4-2
Update MDS.....	4-3

Chapter 5

Installation Properties.....	5-1
------------------------------	-----

Chapter 6

Troubleshooting.....	6-1
Password Expiry for Database	6-1

Chapter 7

Uninstalling the Integration	7-1
Uninstalling the Integration	7-1
Uninstalling the UsageMessagingDriver-Email	7-2

Preface

This document is intended for anyone implementing the Oracle Utilities Customer Care and Billing Integration to Oracle PeopleSoft Financials for General Ledger and Accounts Payable.

Documentation and Resources

For more information regarding this integration, foundation technology and the edge applications, refer to the following documents:

Product Documentation

Topic	Description
Integration documentation:	
Oracle Utilities Customer Care and Billing Integration to Oracle PeopleSoft Financials for General Ledger and Accounts Payable Release Notes	
Oracle Utilities Customer Care and Billing Integration to Oracle PeopleSoft Financials for General Ledger and Accounts Payable Implementation Guide	Refer to the Oracle Utilities applications documentation page: http://docs.oracle.com/cd/E72219_01/documentation.html
Oracle Utilities Customer Care and Billing Integration to Oracle PeopleSoft Financials for General Ledger and Accounts Payable Installation Guide	
Edge application documentation:	
Oracle Utilities Customer Care and Billing	
Oracle PeopleSoft Financials for General Ledger and Accounts Payable	

Additional Documentation

Resource	Location
SOA Suite 12c documentation	Refer to the SOA documentation at: http://www.oracle.com/technetwork/middleware/soasuite/documentation/index.html
Oracle Support	Visit My Oracle Support at https://support.oracle.com regularly to stay informed about updates and patches. Access the support site for the Edge Application Certification Matrix for Oracle Utilities Products (Doc ID 1454143.1) or refer to the Oracle Utilities Integrations page at http://my.oracle.com/site/tugbu/productsindustry/productinfo/utilities/integration/index.htm
Oracle Technology Network (OTN) Latest versions of documents	http://www.oracle.com/technetwork/index.html
Oracle University for training opportunities	http://education.oracle.com/
Web Services Security	For more information about Web services security using Oracle Fusion Middleware 12c refer to https://docs.oracle.com/middleware/12211/cross/webservicetasks.htm .
Oracle Fusion Middleware 12c documentation	Refer to the Oracle applications documentation page: http://docs.oracle.com/en/middleware/
Oracle Fusion Middleware “What's New In Oracle WebLogic Server” Section: Standards Support, Supported Configurations and WebLogic Server Compatibility, Database Interoperability	http://docs.oracle.com/middleware/1221/wls/NOTES/toc.htm
For additional information on the type of database to use.	
Instructions on installing this integration on non-Windows/ Linux platforms	Refer to Oracle Support Knowledge Article ID 1349320.1.

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 for the hearing impaired. Visit: <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs>

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.

Abbreviations

The following table lists the commonly used abbreviations in these guides

Abbreviation	Expanded Form
AIA	Application Integration Architecture
AP	Accounts Payable
AP data	Accounts Payable Data
AP Request	Accounts Payable Request
BPEL	Business Process Execution language
CCB or OUCCB	Oracle Utilities Customer Care and Billing
EBF	Enterprise Business Flow
EM	Enterprise Manager
FT	Financial Transaction
GL	General Ledger
MDS	Meta Data Store
PS	Oracle PeopleSoft Financials
SOA	Service Oriented Architecture

Chapter 1

Overview

This section provides information on prerequisites for installation of the Oracle Utilities Customer Care and Billing Integration to Oracle PeopleSoft Financials for General Ledger and Accounts Payable.

Integration Pack Software Requirements

The following software and platforms must be installed and configured before the integration package can be installed.

Participating Applications

- Oracle Utilities Customer Care and Billing v2.3.1 or v2.4.x or v2.5.0.x installed on an Oracle database with the latest supported service pack.
- Oracle PeopleSoft Financials for General Ledger and Accounts Payable v 9.2 installed on an Oracle database with the latest supported service pack.

Oracle SOA / Weblogic Server

- Oracle SOA suite 12c with Oracle Enterprise Manager 12.2.x on WebLogic Server 12.2.x.

Note: This integration does not require AIA Foundation Pack to be installed.

Note: Refer to the Oracle Utilities product Certification Matrix (referenced in the [Documentation and Resources](#) section) for the most up to date supported edge application versions.

Chapter 2

Installation

This section describes the settings and requirements for a successful installation of the Oracle Utilities Customer Care and Billing Integration to Oracle PeopleSoft Financials for General Ledger and Accounts Payable including:

- [Pre-Installation Tasks](#)
- [Installation Steps](#)
- [Post-Installation Checklist](#)
- [Configuring Edge Applications](#)
- [Security Policies](#)

Pre-Installation Tasks

The following tasks should be completed before you install the integration package:

1. Verify that Oracle SOA Suite 12c is installed and running.
For more information, refer to the documentation at <http://www.oracle.com/technetwork/middleware/soasuite/documentation/index.html>.
2. Login to the **WebLogic Server Administration** console to confirm there are no changes in **Pending Activation** status.

Complete this step to verify that the WebLogic Server is in a healthy state. If any items are in **Pending Activation** status, then there is likely an issue on the server. All issues must be resolved before you can proceed with the installation.
3. Start **Node Manager**, if not already running.
4. Restart the **WebLogic Managed** server and the **WebLogic Admin** server.
5. Verify that the **Weblogic Admin Server**, **Managed Server**, and **Node Manager** are up and running.

Note: The syntax for PRODUCT_HOME changes depending on whether you are installing on Linux or Windows. The following sections refer to this as \$PRODUCT_HOME/ in Linux and as %PRODUCT_HOME%\ in Windows. In general, note that the forward slash (/) is used as the path separator on Linux and the back slash (\) is used on Windows.

Excusing any inadvertent syntax errors in this guide, these conventions should be followed for all commands depending on your operating system.

Also, as installation commands and arguments are lengthy, please copy the installation commands in a text file and verify that the command is formatted correctly without any syntax or formatting errors.

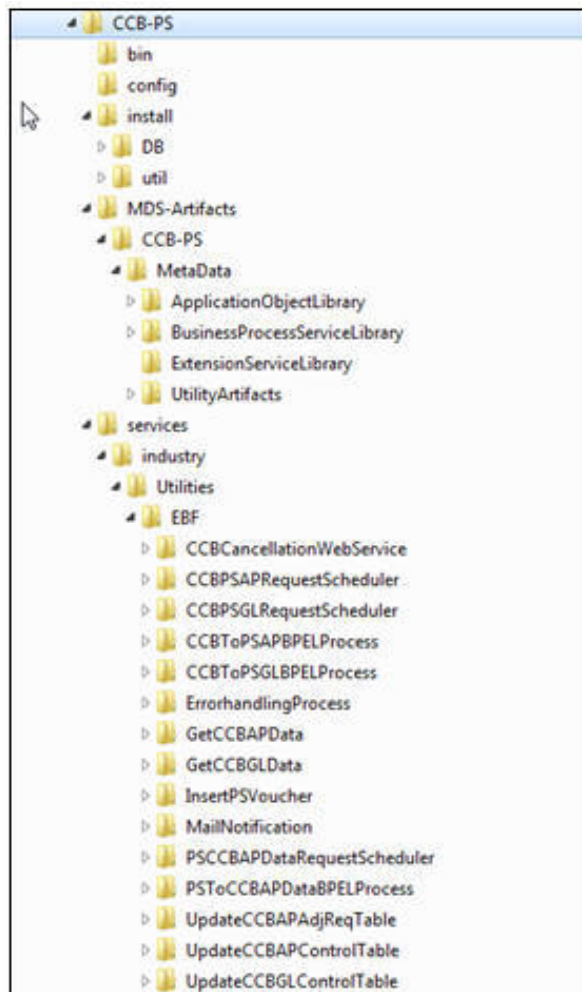
Installation Steps

Complete the following to install:

1. Download the installation CCB-PS.zip file from Oracle Software Delivery Cloud (<http://edelivery.oracle.com/>).

Note: For specific instructions about installing this integration on non-Windows/ Linux platforms see Oracle Support Knowledge article ID 1349320.1.

2. Extract the zip file to get the installation folder. This folder includes subfolders such as bin, config, install, MDS-Artifacts, and services.



CCB-PS Product Home Directory

3. Download and apply patch 23295348.

- a. Refer to the **Readme.txt** file and **PatchInstallInstructions.txt** files included with the patch for more information and installation instructions. The following sub-steps provide more information related to the steps included in the Readme file.

Note: As indicated in the Readme.txt file, you must define or populate the values in the Install Properties xml file prior to installing the integration. Refer to Step 1 in the **PatchInstallInstructions.txt** file included in the patch download.

Refer to the [Installation Properties](#) section for information about individual properties.

- b. Set the following environment variables for Linux and Windows OS:

Variable	Example
Linux and Windows OS	
PATCH_HOME	XXX/23295348
MW_HOME	XXX/Middleware
SOA_HOME	XXX/Middleware/soa
PRODUCT_HOME	The product installation folder. Example: PRODUCT_HOME=/scratch/PRODUCT_HOMES/ CCB-PS

The commands indicated in the readme file (setWLSEnv.sh on Linux and setWLSEnv.bat on Windows) set the environment variables used for executing the installation scripts.

Below is an example of environment variables set up in a typical installation:

Linux

```
export MW_HOME=/Oracle/Middleware/soa
export SOA_HOME=$MW_HOME/soa
export PRODUCT_HOME=/Product_Homes/CCB-PS
source $MW_HOME/wlserver/server/bin/setWLSEnv.sh
```

Windows

```
SET MW_HOME=C:\Oracle\Middleware\soa
SET SOA_HOME=%MW_HOME%\soa
SET PRODUCT_HOME=C:\Product_Homes\CCB-PS
cd %MW_HOME%\wlserver\server\bin/
setWLSEnv.cmd
```

Also note the following:

- PRODUCT_HOME/install/util/ant folder contains all the ant build scripts.
- PRODUCT_HOME/bin/InstallBuild.xml is used to install CCB-PS integration code.
- PRODUCT_HOME/bin/UnInstallBuild.xml is used to uninstall CCB-PS integration code.

- `PRODUCT_HOME/bin/DeployUndeployUtility.xml` is used to deploy/undeploy individual composite/ MDS folder and then restart the managed server.

Note: The installation process may take several minutes to complete.

Installing the Integration

After setting the environment variables, open a command prompt and execute the installation scripts (steps 3 and 4) mentioned in the “Installing the Patch” section in the **PatchInstallInstructions.txt** file included in the patch download.

This section provides additional detail to supplement those steps.

The `installDB` commands perform the followings tasks:

- Create the Error Handling user for the integration.
- Create the Error Handling tables and Error Lookup tables.
- Insert the seed data that is used for Error Handling scenarios that occur during the BPEL flow instances.

The `installWL` commands perform the following tasks:

- Create the JDBC DataSource for the ErrorHandler Module.
- Create an outbound connection pool instance for the database by updating the `DBAdapter_CCBPS.rar` file.
- Create the csf key for the integration.

The `installSOA` commands perform the following tasks:

- Update the MDS repository with all artifacts.
- Create the application partition where the composites are deployed. For example: CCB-PS.
- Compile and deploy all composites.

Post-Installation Checklist

After running the installation scripts, complete the following tasks to complete the installation:

1. Verify that all the JDBC resources were created.
Refer to [Verifying JDBC Configuration](#) for the instructions.
2. Verify that all the composites in Enterprise Manager are deployed.
Refer to [Verifying Composites in Enterprise Manager](#) for the steps.
3. Review the logs under `$MW_HOME/user_projects/domains/soa_domain/servers/<managed-server-name>/logs` to check for deployment errors
4. Verify that the csf-keys are generated.
Refer to [Verifying CSF-Key Generation](#) for the instructions.
5. Configure the Oracle Utilities Customer Care and Billing certificate.
Refer to [Configuring Oracle Utilities Customer Care and Billing Key Store Certificate](#) for the instructions.

6. Verify the user messaging service list.
Refer to [Verifying User Messaging Service List](#) for the steps.

Verifying JDBC Configuration

To verify the JDBC configuration, follow these steps:

1. Navigate to **Home > Deployments**.
2. Verify that DbAdapter_CCBPS.rar is deployed, and is in **Active** state.
3. Verify the connection factory details to ensure the **connection-factory** location matches with that defined in the JCA files. Follow these steps:
 - a. Click **DbAdapter_CCBPS** on the Deployments table.
 - b. On the **Configuration** tab, click **Outbound Connection Pools**.
 - c. Expand **javax.resource.cci.ConnectionFactory** to check the following connection factory instances.
 - eis/DB/CCBPS-CCBDS
 - eis/DB/CCBPS-PSDS
 - eis/DB/CCBPS-SOADS
4. Ensure the database details are as required:
 - a. On the left pane, navigate to **Services > Data Sources**.
 - b. Click the CCBPS-CCBDS data source to check the JNDI Name: jdbc/CCBPS-CCBDS.
 - c. Click the CCBPS-PSDS data source to check the JNDI Name: jdbc/CCBPS-PSDS.
 - d. Click the CCBPS-SOADS data source to check the JNDI Name: jdbc/CCBPS-SOADS.
5. Click **Connection Pool** to check the URL and properties.
6. Click **Monitoring**, click **Testing**, select the target server, and then click **Test Data Source**.
Verify that the data source has been configured successfully.

Verifying Composites in Enterprise Manager

Verify whether or not the CCB-PS partition was created with all the composites deployed by completing the following in Enterprise Manager:

1. Login to the **Enterprise Manager**.
2. Expand **SOA> soa-infra > CCB-PS partition**.
3. Verify that all the composites are deployed and are in an active state.

Composites List:

- CCBCancellationWebService
- CCBPSAPRequestScheduler
- CCBPSGLRequestScheduler
- CCBToPSAPBPELProcess

- CCBToPSGLBPELProcess
- ErrorhandlingProcess
- GetCCBAPData
- GetCCBGLData
- InsertPSVoucher
- MailNotification
- PSCCBAPDataRequestScheduler
- PSToCCBAPDataBPELProcess
- UpdateCCBAPAdjReqTable
- UpdateCCBAPControlTable
- UpdateCCBGLControlTable

Verifying CSF-Key Generation

To verify that the csf-keys are generated, complete the following:

1. Login to the **Enterprise Manager**.
2. Navigate to **WebLogic_Domain > soa_domain**.
3. Right-click **soa_domain**, and then select **Security > Credentials**.
4. Expand the **oracle.wsm.security map**.
5. Verify that the OUCCBPS_CCB key is available.

Configuring Oracle Utilities Customer Care and Billing Key Store Certificate

To import and configure the Oracle Utilities Customer Care and Billing certificate, complete the following:

1. Export the certificate and ensure it is available on the server to add it to the key store.

The certificate import and export operations support four file formats. Choose the format that meets your specific requirements.

If the Base64-encoded X.509 format is chosen, it supports the storage of a single certificate. It does not support the storage of private key or certification path. For example: /tmp/ccbcert.cer

2. Create a keystore CCBPSIntegration.jks for importing the certificates.

Linux:

```
keytool -genkey -keystore $MW_HOME/wlserver/server/lib/
CCBPSIntegration.jks -storepass <keystore password>
```

Windows:

```
keytool -genkey -keystore
%MW_HOME%\wlserver\server\lib\CCBPSIntegration.jks -storepass
<keystore password>
```

3. Import the certificates into the trust store created in Step 2.

Linux:

```
keytool -import -file /tmp/ccbcert.cer -alias RootCA -keystore
$MW_HOME/wlserver/server/lib/CCBPSIntegration.jks -storepass
<keystore password>
```

Windows:

```
keytool -import -file c:\ccbcert.cer -alias RootCA -keystore
%MW_HOME%\wlserver\server\lib\CCBPSIntegration.jks -storepass
<keystore password>
```

4. Verify that the certificate is added to the store using the following command.

Linux:

```
keytool -list -v -keystore $MW_HOME/wlserver/server/lib/
CCBPSIntegration.jks
```

Windows:

```
keytool -list -v -keystore
%MW_HOME%\wlserver\server\lib\CCBPSIntegration.jks
```

Note: When prompted for a password, enter <password>.

5. Edit the setDomainEnv.cmd for Windows or setDomainEnv.sh file for Linux and replace the existing javax.net.ssl.trustStore property. It is located at `{MW_HOME}/user_projects/domains/<domain_name>/bin`
6. Search for -Djavax.net.ssl.trustStore in the file and replace it with `Djavax.net.ssl.trustStore=${MW_HOME}/wlserver/server/lib/CCBEBSIntegration.jks - Djavax.net.ssl.trustStorePassword=<keystore password>`
7. In the WebLogic console, navigate to **Home > Servers > [managed server] > Keystores** and configure the details there.
8. Click **Lock & Edit** to change the keystore details.
9. Click **Change** and then select **Custom Identity and Java Standard Trust** from the drop-down list.
10. Enter the following values in the respective fields:
 - **Custom Identity Keystore:** /Oracle/Middleware/Oracle_Home/wlserver/server/lib/CCBPSIntegration.jks
 - **Custom Identity Keystore Type:** jks
 - **Custom Identity Keystore Passphrase:** <keystore password>

For example: welcome1

 - **Confirm Custom Identity Keystore Passphrase:** <keystore password>

For example: welcome1
11. Click **Activate Changes** to release the configuration and bounce the managed server to bring the changes into effect.

Note: In cluster support, all the managed servers configured in each node need to have key store and the same reference should be

configured for the respective managed servers from the host server WebLogic console.

Restart the server before using the system to ensure all the processes are activated as some of the artifacts used by the processes require restart of admin and managed servers after the complete installation.

Verifying User Messaging Service List

To verify the user messaging service list, follow these steps:

1. In the **WebLogic Administration** console, navigate to **Deployments**.
2. Verify that the **usermessagingdriver-email email driver** is **Active**.
If not, click **usermessagingdriver-email > Targets > <managed server>**.
For example, `soa_server1`
Then, select **Yes** and click **Activate Changes**.
3. In the **WebLogic Enterprise Manager** console, navigate to **soa-infra** [managed server].
4. Right-click the **soa-infra** [managed server] node, select **SOA Administration**, and then select **Workflow Properties**.
5. Verify that the **Notification Mode** under **Workflow Notification Properties** is set to **Email**.
6. Navigate to the **User Messaging Service** node, and select the **usermessagingserver** [managed server] entry.
For example: **usermessagingserver (soa_server1)**
Notice that the email driver is already enabled.

- Click **Configure Driver** to check the email driver properties and view the specific configuration details as shown in the screenshot given below:

Edit Driver Properties

Common Configuration

Name: usermessagingdriver-CCBPS
 Driver Type: User Messaging Email Driver
 Configuration Level: Domain
 Supported Delivery Types: EMAIL
 Capability: SEND, RECEIVE
 Supported Content Types: *
 Supported Status Types: DELIVERY_TO_GATEWAY_SUCCESS, DELIVERY_TO_GATEWAY_FAILURE, USER_REPLY_ACKNOWLEDGEMENT_SUCCESS, USER_REPLY_ACKNOWLEDGEMENT_FAILURE

Supported Protocols: SMTP
 Supported Carriers:
 Sender Address:
 Cost:
 Speed:
 Supports Cancel
 Supports Replace
 Supports Status Polling
 Supports Tracking

Driver-Specific Configuration

Name	Description	Mandatory	Encoded Credential	Value
Outgoing Mail Server Security	Possible values are None, TLS and SSL. Default value is None.			SSL
Default From Address	Deprecated. Use Default Sender Address instead. The default FROM address (if one is not provided in the outgoing message).			jane.eyre@abc.com
Outgoing Username	The username used for SMTP authentication. Required only if SMTP authentication is supported by the SMTP server.			jane.eyre@abc.com
Outgoing Password	The password used for SMTP authentication. Required only if SMTP authentication is supported by the SMTP server.		<input checked="" type="checkbox"/>	Type of Password: Use Cleartext Password Password: *****
Incoming Mail Server	The host name of the incoming mail server. Required only if e-mail receiving is supported on the driver instance.			<input type="text"/>
Incoming Mail Server Port	Port number of IMAP4 (i.e. 143 or 993) or POP3 (i.e. 110 or 995) server.			143

Configuring Edge Applications

Configure Oracle Utilities Customer Care and Billing and Oracle PeopleSoft Financials for General Ledger and Accounts Payable installation according to the guidelines in the Oracle Utilities Customer Care and Billing Integration to *Oracle PeopleSoft Financials for General Ledger and Accounts Payable Implementation Guide* for this integration package.

Security Policies

When a composite needs to invoke an edge application web service, an appropriate security policy should be attached to the reference web service of the composite.

- Invoking edge application XAI Service

When calling an edge application XAI service, the security policy to attach to the reference web service of the composite is oracle/wss_http_token_client_policy.

- Invoking edge application Inbound Web Service (IWS)

When calling an edge application Inbound Web Service (IWS), the security policy to attach to the reference web service of the composite is dependent on the annotation specified in the IWS wsdl.

- If a security policy annotation is specified in the edge application's Inbound Web Service, use the policy specified.

Example 1: The policy defined in the IWS wsdl is UsernameToken, meaning that oracle/wss_username_token_client_policy should be attached to the composite's reference web service.

```
<wsp:UsingPolicy wssutil:Required="true"/>
- <ns0:Policy wssutil:Id="UsernameToken">
- <ns1:SupportingTokens>
- <ns0:Policy>
- <ns1:UsernameToken ns1:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200512/IncludeToken/AlwaysToRecipient">
- <ns0:Policy>
- <ns1:WssUsernameToken10/>
</ns0:Policy>
</ns1:UsernameToken>
</ns0:Policy>
</ns1:SupportingTokens>
</ns0:Policy>
```

Example 2: The policy defined in the IWS wsdl is Https-BasicAuth xml meaning that HTTP Basic Authentication over SSL Including Timestamp is required. The oracle/wss_http_token_over_ssl_client_policy should be attached to the composite's reference web service.

```
<wsp:UsingPolicy wssutil:Required="true"/>
- <ns0:Policy wssutil:Id="Wssp1.2-2007-Https-BasicAuth.xml">
- <ns1:TransportBinding>
- <ns0:Policy>
- <ns1:TransportToken>
```

- If no security policy annotation is specified in the edge application's Inbound Web Service and the edge application is using Framework 4.3.0.2.0, a default security policy oracle/wss_http_token_over_ssl_client_policy will be used by the edge application's Inbound Web Service. The default policy can be changed in the edge application's Feature Configuration Menu.

Refer to the specific edge application implementation guide for more information.

- If the edge application is using Framework 4.2.0, a security policy annotation has to be specified in the edge application's Inbound Web Service. In this version of framework, there is no default security policy specified. oracle/wss_http_token_client_policy has to be specified in the edge application's Inbound Web Service security policy annotation.

Chapter 3

Individual Composites

This chapter describes how to deploy/ undeploy individual composites for incremental builds or patches. It includes the following sections:

- [Undeploying Individual Composites](#)
- [Deploying Individual Composites](#)

Undeploying Individual Composites

If the composite being deployed involves changes made to the MDS artifacts, you must first undeploy the composite.

1. Open a Command prompt and execute the following commands for Linux and Windows respectively. Set the environment variables as described in the installation steps.

Linux:

```
cd $PRODUCT_HOME/bin
ant -f DeployUndeployUtility.xml UnDeployComposite -
DInstallProperties=$PRODUCT_HOME/config/InstallProperties.xml
```

Windows:

```
cd %PRODUCT_HOME%/bin
ant -f DeployUndeployUtility.xml UnDeployComposite -
DInstallProperties=%PRODUCT_HOME%/config/InstallProperties.xml
```

2. Validate the following parameters when prompted with default values during deployment. Press **ENTER** to use the default value.
 - **Composite Name** - The name of composite which needs to be undeployed to the SOA server. There is no default value for this parameter.
 - **Composite Folder Location** - The folder name should be absolute path starting <PRODUCT_HOME>/services/industry/Utilities/<EBF/utility>.

For example, if you are planning to undeploy composite from <PRODUCT_HOME>/services/industry/Utilities/EBF then pass <PRODUCT_HOME>/services/industry/Utilities/EBF for this property.

The default value is %PRODUCT_HOME%/services/industry/Utilities/EBF, as most of the business specific composites reside in this folder.

- **SOA Partition Name** - This is the SOA partition name to which this composite should be undeployed.

Deploying Individual Composites

Perform the following steps to deploy individual composites:

1. Execute the following commands in the Command prompt for Linux and Windows respectively. Set the environment variables as described in the installation steps.

Linux:

```
cd $PRODUCT_HOME/bin
ant -f DeployUndeployUtility.xml DeployComposite -
DInstallProperties=$PRODUCT_HOME/config/InstallProperties.xml
```

Windows:

```
cd %PRODUCT_HOME%/bin
ant -f DeployUndeployUtility.xml DeployComposite -
DInstallProperties=%PRODUCT_HOME%/
config/InstallProperties.xml
```

2. Validate the following parameters when prompted with default values during deployment. Press **ENTER** to use the default value.
 - **Composite Name** - The name of composite which needs to be deployed to SOA server. There is no default value for this parameter.
 - **Composite Folder Location** - The folder name should be absolute path starting %PRODUCT_HOME%/services/industry/Utilities/<EBF/utility>.

For Example: If you are planning to deploy composite from %PRODUCT_HOME%/services/industry/Utilities/EBF, then pass %PRODUCT_HOME%/services/industry/Utilities/EBF for this property.

The default value for this property is %PRODUCT_HOME%/services/industry/Utilities/EBF, as most of business specific composite reside in this folder.

- **SOA Partition Name** - This is the SOA partition name to which this composite should be deployed.

Note: Refer to [Verifying Composites in Enterprise Manager](#) to see the composites for this integration.

Chapter 4

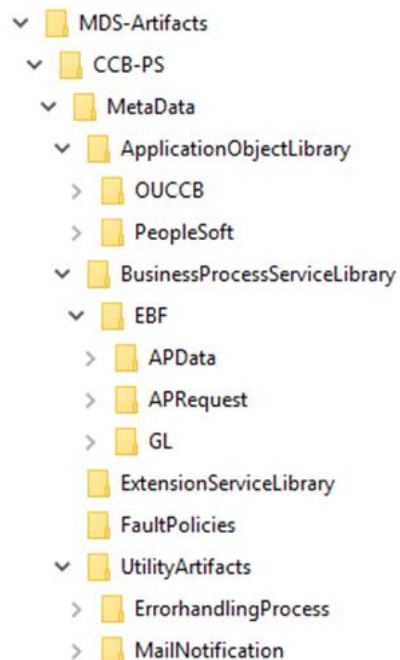
Metadata Store (MDS) Artifacts

Individual Metadata Store (MDS) folders may need to be undeployed, deployed or updated for incremental builds or patches. This section describes the following:

- [Undeploying the MDS Folder](#)
- [Deploying the MDS Folder](#)
- [Update MDS](#)

Please note the following:

- You can only use the indicated commands to perform folder-level undeployment, deployment or update. The commands do not support file-level actions.
- Validate the **MDS Folder Name** parameter when prompted with default values during undeployment or deployment. Press ENTER to use the default value.
- The **MDS Folder Name** represents the name of the folder to be deployed or undeployed from MDS repository. The folder name should be a relative path inside **<PRODUCT_HOME>/MDS-Artifacts** beginning with CCB-PS.



MDS Artifacts Folder Structure

- The folder includes an MDS-Artifacts subfolder which contains all the files that can be deployed to MDS.

Undeploying the MDS Folder

To undeploy a particular folder from MDS:

1. Open a command prompt and execute the following commands for Linux and Windows respectively. These commands undeploy a folder under `PRODUCT_HOME/MDS-Artifacts` from the MDS repository.

Linux

```
cd $PRODUCT_HOME/bin
ant -f DeployUndeployUtility.xml -DInstallProperties=$PRODUCT_HOME/
config/InstallProperties.xml UnDeployMDS
```

Windows

```
cd %PRODUCT_HOME%\bin
ant -f DeployUndeployUtility.xml -
DInstallProperties=%PRODUCT_HOME%\
config\InstallProperties.xml UnDeployMDS
```

2. Pass the folder name to be undeployed.
Validate the **MDS Folder Name** parameter when prompted with default values during deployment. Press ENTER to use the default value.

Deploying the MDS Folder

Perform the following steps to deploy the MDS folder:

1. Open a command prompt and execute the following commands in Linux and Windows respectively:

Linux

```
cd $PRODUCT_HOME/bin
ant -f DeployUndeployUtility.xml -DInstallProperties=$PRODUCT_HOME/
config/InstallProperties.xml DeployMDS
```

Windows

```
cd %PRODUCT_HOME%\bin
ant -f DeployUndeployUtility.xml -
DInstallProperties=%PRODUCT_HOME%\config\InstallProperties.xml
DeployMDS
```

2. Validate the **MDS Folder Name** parameter when prompted with default values during deployment. Press ENTER to use the default value.

Custom Schema Changes

If custom elements are added to either or both of the edge application schemas, the ApplicationObjectLibrary folder must be updated in MDS.

Do one of the following:

- Pass CCB-PS/**MetaData/ApplicationObjectLibrary** to deploy the schema folders, or
- Pass CCB-PS/**MetaData/ApplicationObjectLibrary** OUCCB to deploy only the CCB schema folder, or
- Replace with to deploy only the schema folder.

Concrete WSDL changes for Extensions

If an extension service needs to be called by a process and the concrete WSDL is updated, the ExtensionServiceLibrary folder must be updated in MDS.

Pass CCB-PS/**AIAMetaData/AIAComponents/ExtensionServiceLibrary** to deploy the extension service.

Update MDS

If there is any change in the endpoints of the participating applications, references of those endpoints in the integration have to be updated to point to the correct URIs. In order to make the changes, update the \$PRODUCT_HOME/config/InstallProperties.xml file with the correct edge application details and updateMDS.

1. Open a command prompt and execute the following commands to update MDS.

Linux

```
ant -f InstallBuild.xml updateMDS -
DInstallProperties=$PRODUCT_HOME/config/InstallProperties.xml |
tee $PRODUCT_HOME/bin/updatemds.log
```

Windows

```
ant -f InstallBuild.xml updateMDS -
DInstallProperties=%PRODUCT_HOME%/config/InstallProperties.xml -l
%PRODUCT_HOME%/bin/updatemds.log
```

This command performs the following tasks:

- Updates the edge application endpoint URIs in ConfigurationProperties.xml file
- Updates the edge application endpoint URIs in Application Object Library directory \$PRODUCT_HOME/MDS-Artifacts/OUCCB/AIAMetaData/AIAComponents/ApplicationObjectLibrary/<ApplicationFolder>

Example: CCB-PS/MDS-Artifacts/CCB-PS/AIAMetaData/AIAComponents/ApplicationObjectLibrary/OUCCB/V1/wsdl

2. Restart the managed server to see the changes take effect.

Chapter 5

Installation Properties

This section includes a listing of applicable installation properties.

Make sure that you follow XML editing standards while editing the InstallProperties.xml file. All XML elements need to be closed properly. The XML element in the InstallProperties.xml file does not contain any attribute.

Login to the WebLogic console to cross verify the values being entered for these properties. Also ensure that the values are relevant to the server where the integration product is to be installed. The build may fail due to inappropriate values.

Note: If the dbuser.createflag is set to false, the schema needed for integration error handling will not be automatically created by the install and will need to be created manually prior to running the installation. When creating the user manually, grant connect and resource to the user.

The table below lists the properties available in the InstallProperties.xml file along with their usage. The default values are specified wherever applicable.

Installation Properties

Property (XPath Representation)	Description	Example
<config>		
<modulename>	Name of the integration module.	Default: CCB-PS Do not change this value.
<CCB>		
<ApplicationHost>	Application host	CCB_HOST.yourdomain.com
<ApplicationPort>	Application port	CCB_PORT_NO
<contextRoot>	Application context root	CCB_CONTEXT_ROOT _NAME <ul style="list-style-type: none">• ouaf/XAIApp/xaiserver (for XAI services)• ouaf/webservices (for IWS services)
<protocol>	Application protocol	http

Property (XPath Representation)	Description	Example
<dbhostname>	CCB Application DB hostname	CCBDB_HOST.yourdomain.com
<dbport>	CCB Application DB port	CCBDB_PORT_NO
<dbsid>	CCB Application DB sid	CCBSID
<dbuser>	CCB Application DB username	CCBDBUSER
<dbpwd>	CCB Application DB password	CCBDBPWD
<ApplicationUsername>	Application login username	CCBUSER
<ApplicationPassword>	Application login password	CCBPWD
<policy>	The security policy that CCB accepts when invoking it's webservice.	Use oracle/ wss_http_token_client_policy for XAI services or refer to the Security Policies section for more information when invoking IWS services.
<PS>		
<dbhostname>	PS Application DB hostname	PSDB_HOST.yourdomian.com
<dbport>	PS Application DB port	PSDB_PORT_NO
<dbsid>	PS Application DB sid	PSSID
<dbuser>	PS Application DB username	PSDBUSER
<dbpwd>	PS Application DB password	PSDBPWD
<ApplicationUsername>	Application login username	PSUSER
<ApplicationPassword>	Application login password	PSPWD
<WorkFlow.Notification>		
<from.emailid>	Email ID which should be set in the "From" property of Workflow Notification bean.	Admin.user@yourdomain.com
<mode>	Type of notification mode	EMAIL
<jdbc_driver_class>	JDBC Driver class	oracle.jdbc.OracleDriver
<jdbc_xa_driver_class>	JDBC Driver class	oracle.jdbc.xa.client.OracleXADataSource
<SOA>		
<db>		
<adminusername>	Database admin user name	ADMIN_USERNAME
<adminpassword>	Database admin password	ADMIN_PWD
<username>	Database username	ccbpsuser
<password>	Database password	ccbpspwd
<user.createflag>	User create flag	true
<hostname>	Database host name	Db.sample.oracle.com

Property (XPath Representation)	Description	Example
<portnumber>	Database port number	1521
<sid>	Database sid	SID
<AdminServer>		
<hostname>	The host name of the server where admin server is installed	adminserver.example.oracle.com
<portnumber>	The port number admin server is listening to	7001
<servername>	Admin server's name	AdminServer
<username>	Admin server username	weblogic
<password>	Admin server password	weblogic
<domainname>	Admin server domain name	soa_domain
<ManagedServer>		
<hostname>	The host name of managed server	managedserver.example.oracle.com
<portnumber>	The port number of managed server	8001
<servername>	Server name of managed server	Soa_Managedserver1
<username>	Username of managed server	Weblogic
<password>	Password of managed server	Weblogic1
<OHS>		
		Cluster support properties: Oracle HTTP Server host name, port number, server name and protocol ; in case of non-cluster environment these properties would be same as <ManagedServer> values
<hostname>	Oracle HTTP server host name	xxx.example.oracle.com
<portnumber>	Oracle HTTP server port number	7777
<servernames>	SOA server names	Soa_cluster
<Protocol>	The protocol on which Oracle HTTP Server can be accessed.	http or https
<mdsconfig>		
<mdsdbusername>	MDS username	XXX_MDS
<mdsdbuserpassword>	MDS user password	XXX_MDSPWD
<mdsdbhostname>	MDS hostname	Db.hostname.oracle.com
<mdsdbportnumber>	MDS port number	1521
<mdsdbsid>	MDS sid	SID

Property (XPath Representation)	Description	Example
<EMAIL>		
<MailAccessProtocol>	The e-mail receiving protocol. The possible values are IMAP and POP3. Required only if e-mail is supported on the driver instance.	IMAP
<OutgoingDefaultFromAddr>	The default FROM address (if one is not provided in the outgoing message).	admin@yourcompany.com
<OutgoingMailServer>	The name of the SMTP server. Mandatory only if an e-mail needs to be sent.	host.yourdomain.com
<OutgoingMailServerPort>	The port number of SMTP server	465
<OutgoingMailServerSecurity>	The security used by SMTP server. Possible values are None, TLS, and SSL. Default value is None.	SSL
<OutgoingUsername>	The user name used for SMTP authentication. Required only if SMTP authentication is supported by the SMTP server.	admin@yourcompany.com
<Outgoingpassword>	The password used for SMTP authentication. Required only if SMTP authentication is supported by the SMTP server.	Yourpassword
<IncomingUserIDs>	The list of user names of the mail accounts the driver instance is polling from. Each name must be separated by a comma. Required only if e-mail receiving is supported on the driver instance.	admin@yourcompany.com
<IncomingUserPasswords>	The list of passwords corresponding to the user names. Each password is separated by a comma and must reside in the same position in the list as their corresponding user name appears on the user names list. Required only if e-mail receiving is supported on the driver instance.	Yourpassword
<applicationName>	This is the application name for the user messaging service.	usermessaging driver-email
<Capability>	Sets the driver's capability to send or receive messages.	For 12c, the values are SEND, RECEIVE, and BOTH.

Chapter 6

Troubleshooting

This section provides information regarding issues that may arise during installation.

Password Expiry for Database

If a password expires or is changed, credential issues may arise with the Meta Data Store (MDS) or with an integration specific database. To fix this issue, perform the following steps:

1. Reset or unlock the password for the corresponding database (MDS or integration specific database).
2. Change the password for the data source for which the password is changed/or locked from the Weblogic Administration Console.
3. Change the password in the **InstallationProperties.xml** for the database instance (this helps only while reinstalling).
4. Perform the following steps to find the **adf-config.xml** file that is generated during installation.

The file is generally located at \$PRODUCT_HOME/install/util/template/.

- a. Identify the correct “metadata-store-usage” from the “meta-data-namespaces” element by the path mentioned above.
- b. In the “metadata-store-usage” element, find the element property with the attribute value as “jdbc-password” for the “name” attribute.
- c. Change the password for the value attribute in the property element.

Chapter 7

Uninstalling the Integration

This section provides steps for:

- [Uninstalling the Integration](#)
- [Uninstalling the UsageMessagingDriver-Email](#)

Uninstalling the Integration

To uninstall the integration, perform the following steps:

1. Restart the WebLogic Admin server and the SOA server.
2. Set the environment variables as mentioned in the [Installation Steps](#) section.
3. Open a Command prompt window and execute the following three commands in Linux and Windows respectively:
 - a. Execute the following commands at the command prompt:

Linux:

```
cd $PRODUCT_HOME/bin
ant -f UnInstallBuild.xml uninstallSOA -
DInstallProperties=$PRODUCT_HOME/config/InstallProperties.xml -l
uninstallsoa.log
```

Windows:

```
cd %PRODUCT_HOME%\bin
ant -f UnInstallBuild.xml uninstallSOA -
DInstallProperties=%PRODUCT_HOME%/config/InstallProperties.xml -l
uninstallsoa.log
```

This command performs the following tasks.

- Undeploys all composites from the Enterprise Manager partition.
 - Deletes the partition.
 - Undeploys the MDS artifacts.
- b. Execute the following commands at the command prompt:

Linux:

```
cd $PRODUCT_HOME/bin
```

```
ant -f UnInstallBuild.xml uninstallWL -
DInstallProperties=$PRODUCT_HOME/config/InstallProperties.xml -l
uninstallwl.log
```

Windows:

```
cd %PRODUCT_HOME%\bin
ant -f UnInstallBuild.xml uninstallWL -
DInstallProperties=%PRODUCT_HOME%/config/InstallProperties.xml -l
uninstallwl.log
```

This command performs the following tasks:

- Undeploys the database outbound connection pool.
- Deletes the JDBC data source.
- Removes the workflow notification.
- Deletes the csf-keys generated.

After executing the commands mentioned above, bounce the managed server and admin server manually.

- c. Execute the following commands at the command prompt:

Linux:

```
cd $PRODUCT_HOME/bin
ant -f UnInstallBuild.xml uninstallDB -
DInstallProperties=$PRODUCT_HOME/config/InstallProperties.xml -l
uninstalldb.log
```

Windows:

```
cd %PRODUCT_HOME%\bin
ant -f UnInstallBuild.xml uninstallDB -
DInstallProperties=%PRODUCT_HOME%/config/InstallProperties.xml -l
uninstalldb.log
```

This command drops the database objects created for the integration.

Note: After a successful uninstall, all the JDBC resources and CCB-PS partitions created during installation are deleted.

Uninstalling the UsageMessagingDriver-Email

To uninstall the UsageMessagingDriver:

1. Open the **Enterprise Manager** console.
2. Expand the **Usage Message Service**.
3. Right-click on the **usermessagingdriver-email**.
4. Select the **Email Driver Properties** menu item.
5. In the **Email Driver Properties** table, find the row with the instance set as “usermessagingdriver-[integration]” or “usermessagingdriver-UGBUEMAIL”.
6. Click **Delete**.
7. Click **Yes** in the confirmation dialog box.