Oracle Utilities Customer Care and Billing Integration to Oracle E-Business Suite Financials for General Ledger and Accounts Payable

Installation Guide

Release 12.1

E24601-03

June 2017 (Updated)

ORACLE®

Oracle Utilities Customer Care and Billing Integration to Oracle E-Business Suite Financials for General Ledger and Accounts Payable, Release 12.1 Installation Guide

Contents

Chapter 5

Chapter 6

Chapter 7

Contents - ii

Oracle Utilities Customer Care and Billing Integration to Oracle E-Business Suite Financials for General Ledger and Accounts Payable Installation Guide

Preface

This document is intended for anyone implementing the Oracle Utilities Customer Care and Billing Integration to Oracle E-Business Suite 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 E-Business Suite Financials for General Ledger and Accounts Payable Release Notes	
Oracle Utilities Customer Care and Billing Integration to Oracle E-Business Suite 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 E-Business Suite Financials for General Ledger and Accounts Payable Installation Guide	
Edge application documentation:	
Oracle Utilities Customer Care and Billing	
Oracle E-Business Suite 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/webservicestasks.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 For additional information on the type of database to use.	http://docs.oracle.com/middleware/1221/wls/NOTES/toc.htm
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.
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.

Abbreviations

The following table lists the commonly used abbreviations in this guide.

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
DVM	Domain Value Map
EBF	Enterprise Business Flow
EBS	Oracle E-Business Suite
EM	Enterprise Manager
FT	Financial Transactions
GL	General Ledger
MDS	Meta Data Store
OHS	Oracle HTTP Server

OUCCB or CCB	Oracle Utilities Customer Care and Billing
SOA	Service Oriented Architecture
UMS	User Messaging Service

Chapter 1

Overview

This section provides information on prerequisites for installation of the Oracle Utilities Customer Care and Billing Integration to Oracle E-Business Suite 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 version v2.3.1 or v2.4.x or v2.5.0x installed on an Oracle database with the latest supported service pack.

- Oracle E-Business Suite Financials for General Ledger and Accounts Payable version v12.1 or v12.2.2 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 E-Business Suite 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 s**erver 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 Integration Product CCB-EBS.zip file from Oracle Software Delivery Cloud (http://edelivery.oracle.com/).

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

2. Extract the CCB-EBS.zip file to get the installation folder.

    This folder includes the subfolders such as bin, config, install, MDS-Artifacts, and services.
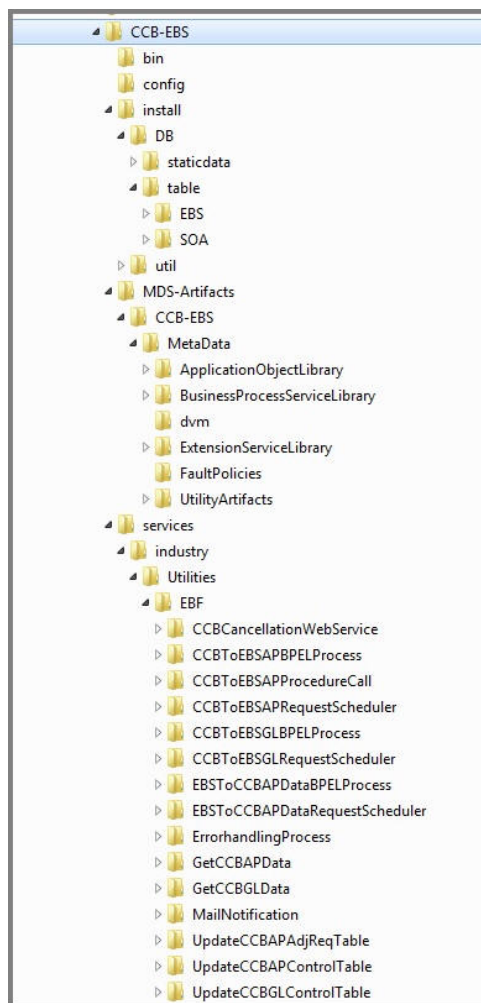
CCB-EBS Product Home Directory

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-EBS

c. 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 to set up environment variables in a typical installation:

   Linux
```
export MW_HOME=/Oracle/Middleware/soa
export SOA_HOME=$MW_HOME/soa
export PRODUCT_HOME=/Product_Homes/CCB-EBS
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-EBS
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-EBS integration code.

   • PRODUCT_HOME/bin/UnInstallBuild.xml is used to uninstall CCB-EBS 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 Integration 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 ErrorHandling Module.
- Create an outbound connection pool instance for the database by updating the DBAdapter_CCB-EBS.rar file.
- Create the CCBEBS_CCB 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-EBS.
- Compile and deploy all composites.

Post-Installation Checklist

After running the installation scripts, follow these steps to complete the installation:

1. Verify that all the JDBC resources were created.
   Refer to Verify JDBC Configuration for the instructions.

2. Verify that the csf-keys are generated.
   Refer to Verifying the csf-Key for the instructions.

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 all the composites in Enterprise Manager are deployed.
   Refer to Verifying Composites in Enterprise Manager for the steps.

5. Configure the Oracle Utilities Customer Care and Billing Key Store Certificate.
   Refer to Configuring the Oracle Utilities Customer Care and Billing Key Store Certificate for more details.

6. Verify that the user messaging service is active.
Refer to Verifying the User Messaging Service List for more details.

Verify JDBC Configuration

To verify the JDBC configuration, follow these steps:

1. Navigate to **Home > Deployments**.

2. Verify that DbAdapter_CCBEBS.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_CCBEBS** 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/CCBEBS-CCBDS

      • eis/DB/CCBEBS-EBSDS

      • eis/DB/CCBEBS-SOADS

4. Ensure the database details are as required:

   a. On the left pane, navigate to **Services > Data Sources**.

   b. Click the CCBEBS-CCBDS data source to check the JNDI Name: jdbc/CCBEBS-CCBDS.

   c. Click the CCBEBS-EBSDS data source to check the JNDI Name: jdbc/CCBEBS-EBSDS.

   d. Click the CCBEBS-SOADS data source to check the JNDI Name: jdbc/CCBEBS-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 that the CCB-EBS partition was created with all the composites deployed. Perform the following steps to verify composites in Enterprise Manager:

1. Login to the Enterprise Manager.

2. Expand **SOA> soa-infra > CCB-EBS partition**.

3. Verify that all the composites are deployed and are in an active state.

   Composites List:

      • CCBCancellationWebService

      • CCBToEBSAPBPELProcess

      • CCBToEBSAPProcedureCall

- CCBToEBSAPRequestScheduler
- CCBToEBSGLBPELProcess
- CCBToEBSGLRequestScheduler
- EBSToCCBAPDataBPELProcess
- EBSToCCBAPDataRequestScheduler
- ErrorhandlingProcess
- GetCCBAPData
- GetCCBGLData
- MailNotification
- UpdateCCBAPAdjReqTable
- UpdateCCBAPControlTable
- UpdateCCBGLControlTable

Verifying the csf-Key

To verify that the csf-key is created successfully, complete the following:

1. Login to the Enterprise Manager console.
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 CCBEBS_CCB key is available.

Configuring the 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 CCBEBSIntegration.jks for importing the certificates.

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

   Windows:
   ```
   keytool -genkey -keystore
   %MW_HOME%\wlserver\server\lib\CCBEBSIntegration.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/CCBEBSIntegration.jks -storepass
   <keystore password>
   ```

   Windows:
   ```
   keytool -import -file c:\ccbcert.cer -alias RootCA -keystore
   %MW_HOME%\wlserver\server\lib\CCBEBSIntegration.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/
   CCBEBSIntegration.jks
   ```

   Windows:
   ```
   keytool -list -v -keystore
   %MW_HOME%\wlserver\server\lib\CCBEBSIntegration.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/ CCBEBSIntegration.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 a clustered environment, managed servers should have their own keystore configured.

If the services in Oracle Utilities Customer Care and Billing are SSL enabled, import the Oracle Utilities Customer Care and Billing certificates into the WebLogic Managed server to enable secure communication between the integration layer and Oracle Utilities Customer Care and Billing.

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 the 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 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.

7. Click **Configure Driver** to check the e-mail driver properties and view the specific configuration details as shown in the figure below.

Configuring Edge Applications

Configure Oracle Utilities Customer Care and Billing Integration and Oracle E-Business Suite Financials for General Ledger and Accounts Payable installation according to the guidelines in the *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 section describes how to deploy/ undeploy individual composites for incremental builds or patches. It includes the following sections:

- Undeploying Individual Composites

- Deploying Individual Composites

    Note: Refer to Verifying Composites in Enterprise Manager to see the composites for this integration

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

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

2. Validate the following parameters when prompted with default values during deployment. Press ENTER to use the default value.

    - **Composite Name**: Name of the composite to be undeployed to SOA server. This parameter does not have a default value.

    - **Composite Folder Location**: The folder name should be an absolute path, beginning with <PRODUCT_HOME>/services/industry/Utilities/<EBF>.

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

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

  - **SOA Partition Name**: The SOA partition name from where the composite
  should be undeployed.

3. Press Enter to use the default value.

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 above in the installation steps.

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

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

2. Validate the following parameters when prompted with default values during
deployment. Press ENTER to use the default value.

   - **Composite Name:** Name of the composite to be deployed to SOA server. This
   parameter does not have a default value. For example:
   CCBToEBSAPBPELProcess

   - **Composite Folder Location**: The folder name should be an absolute path
   beginning with %PRODUCT_HOME%/services/industry/Utilities/<EBF>.

     For example: Deploy the composite from%PRODUCT_HOME%/services/
     industry/Utilities/EBF, then pass %PRODUCT_HOME%/services/industry/
     Utilities/EBF to this property.

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

   - **SOA Partition Name**: The SOA partition name to which the composite should
   be deployed.

3. Press Enter to use the default value.

   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-EBS. Refer to the CCB-EBS Home Directory image in the Installation chapter for a reference.

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

  For example: To undeploy <PRODUCT_HOME>/MDS-Artifacts/CCB-EBS/AIAMetaData/dvm pass CCB-EBS/AIAMetaData/dvm as the **MDS Folder Name**.

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.

DVM Changes

When new DVM values are added to a DVM file, the DVM folder must be updated in MDS. This command will not only deploy the files that were changed but the whole DVM folder.

- Pass CCB-EBS**/AIAMetaData/dvm** as the **MDS Folder Name** and the entire DVM folder will deploy to MDS.

- **W**hen the DVMs are updated from the SOA composer, verify that the values are updated in the /MDS-Artifacts/CCB-EBS/AIAMetaData/dvm folder.
  If not, the changes made from the composer will be overridden by the PRODUCT_HOME values.

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-EBS**/MetaData/ApplicationObjectLibrary** to deploy the schema folders, or

- Pass CCB-EBS**/MetaData/ApplicationObjectLibrary/**OUCCB to deploy only the CCB schema folder, or

- Replace OUCCB with EBS to deploy only the EBS 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-EBS**/MetaData/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-SOM/MDS-Artifacts/CCB-SOM/AIAMetaData/AIAComponents/ApplicationObjectLibrary/OUCCB/V1/wsdls

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

Oracle Utilities Customer Care and Billing Integration to Oracle E-Business Suite Financials for General Ledger and Accounts Payable Installation Guide

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.	CCB-EBS
<CCB-EBS>		
<jdbc_driver_class>	JDBC Driver class	oracle.jdbc.OracleDriver
<jdbc_xa_driver_class>	JDBC XA Driver class	oracle.jdbc.xa.client.OracleXADataSource
Workflow Notification Properties		
<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

Property (XPath Representation)	Description	Example
CCB Application Information		
<CCB>		
<ApplicationUsername>	CCB Application login username	CCBUSER
<ApplicationPassword>	CCB Application login password	CCBPWD
<dbhostname>	CCB Database host name	CCBDB_HOST.yourdomain.com
<dbport>	CCB Database port number	CCBDB_PORT_NO
<dbsid>	CCB Database SID	CCBSID
<dbuser>	CCB Database username	CCBDBUSER
<dbpwd>	CCB Database password	CCBDBPWD
<ApplicationHost>	Host name of the CCB application/ server	CCB_HOST.yourdomain.com
<ApplicationPort>	Port number of the CCB application/ server	CCB_PORT_NO
<contextRoot>	CCB service context root	CCB_CONTEXT_ROOT _NAME • ouaf/XAIApp/xaiserver (for XAI services) • ouaf/webservices (for IWS services)
<protocol>	CCB Service Protocol	http
<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.
EBS Application Information		
<EBS>		
<ApplicationUsername>	EBS Application login username	EBSUSER
<ApplicationPassword>	EBS Application login password	EBSPWD
<dbhostname>	EBS Database host name	EBSDB_HOST.yourdomain.com
<dbport>	EBS Database port number	EBSDB_PORT_NO
<dbsid>	EBS Database SID	EBSSID
<dbuser>	EBS Database username	EBSDBUSER
<dbpwd>	EBS Database password	EBSDBPWD
SOA Information		

Property (XPath Representation)	Description	Example
<config> <SOA>		
Admin Server Information		
<AdminServer>		
<hostname>	Host name of the server where admin server hosting SOA suite is installed.	adminserver.example.oracle.com
<portnumber>	Port number the admin server (hosting SOA suite) is listening to.	7001
<servername>	Admin server name (hosting SOA suite)	AdminServer
<username>	User name used to log in as an Admin server (hosting SOA suite) administrator.	weblogic
<password>	Password used to log in as an Admin server (hosting SOA suite) administrator.	weblogic
<domainname>	WebLogic domain name hosting SOA suite.	soa_domain
Managed Server Information		
<ManagedServer>		
<hostname>	Host name of the server where managed server (hosting SOA suite) is installed.	managedserver.example.oracle.com
<portnumber>	Port number the managed server (hosting SOA suite) is listening to.	8001
<servername>	Managed server name (hosting SOA suite)	Managedserver1
<username>	User name used to log in to managed server (hosting SOA suite) as an administrator.	weblogic
<password>	Password used to log in to managed server (hosting SOA suite) as an administrator.	
Oracle HTTP Server Information		
<OHS>		In case of non-cluster environment these properties would be same as <ManagedServer> values
<hostname>	Oracle HTTP server host name	Oracle http server where cluster is managed
<portnumber>	Oracle HTTP server port number	Port number of the Oracle http server
<servernames>	Provide the list of managed server(s)	In case of multiple managed servers, provide comma separated values. Example: soa_server1, soa_server2
<Protocol>	Oracle HTTP Server Protocol. The protocol on which Oracle HTTP Server can be accessed.	http or https

Property (XPath Representation)	Description	Example
MDS DB Information		
<mdsconfig>		
<mdsdbusername>	User name used to log in to MDS schema.	XXX_MDS
<mdsdbuserpassword>	Password used to log in to MDS schema.	XXX_MDSPWD
<mdsdbhostname>	Host name of the server hosting the database containing MDS schema.	Db.hostname.oracle.com
<mdsdbportnumber>	Port number of the database containing MDS schema.	1521
<mdsdbsid>	SID of the database containing MDS schema.	SID
Integration DB Information		
<db>		
<adminusername>	SOA Database admin user name	system
<adminpassword>	SOA Database admin password	manager
<username>	Integration schema name to access SOA database for CCB-EBS Lookup tables etc	ccbebsuser
<password>	Integration schema password	ccbebspwd
<user.createflag>	This flag controls whether an Integration schema user is created. If the user is already created then this will be set to false for the next installation.	true
<hostname>	SOA Database host name	Db.sample.oracle.com
<portnumber>	SOA Database port number	1521
<sid>	SOA Database SID	SID
Email Information		
<EMAIL>		
<MailAccessProtocol>	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

Property (XPath Representation)	Description	Example
<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	CCBEBS
<Capability>	Sets the driver's capability to send or receive messages.	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

To uninstall the integration, complete the following steps:

1. Restart the WebLogic Admin server and the SOA server.

2. Set the environment variables as mentioned above in the installation steps.

   The uninstallation process is divided into three steps. Execute the commands in each of those steps

   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
   ```

   These commands perform the following tasks:

   - Undeploys all the composites from the Enterprise Manager partition.

   - Deletes the partition.

   - Undeploys MDS artifacts.

   b. Execute the following commands at the command prompt:

   Linux
   ```
   cd $PRODUCT_HOME/bin
   ```

Uninstalling the Integration 7 - 1

Oracle Utilities Customer Care and Billing Integration to Oracle E-Business Suite Financials for General Ledger and Accounts Payable Installation Guide

```
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
```

These commands perform the following tasks:

- Undeploy the database outbound connection pool.

- Delete the JDBC data source for the CCBDS, EBSDS, SOADS modules.

- Remove the work flow notification that is created.

- Delete 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
```

These commands drop the database objects created for the Error Handling module created for the integration.

After a successful uninstall, all JDBC resources, and the CCB-EBS partition 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.