**Oracle Utilities Service Order
Management Integration to Oracle
Utilities Mobile Workforce Management**

Installation Guide

Release 12.1

E63566-03

June 2017 (Updated)

ORACLE®

Oracle Utilities Service Order Management Integration to Oracle Utilities Mobile Workforce Management, Release 12.1 Installation Guide

Contents

Installation Guide

Chapter 1

Chapter 2

Chapter 3

Chapter 4

Chapter 5

Chapter 6

Chapter 7

Preface

This document is intended for anyone implementing the Oracle Utilities Service Order Management Integration to Oracle Utilities Mobile Workforce Management.

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 Service Order Management Integration to Oracle Utilities Mobile Workforce Management Release Notes	
Oracle Utilities Service Order Management Integration to Oracle Utilities Mobile Workforce Management Implementation Guide	Refer to the Oracle Utilities applications documentation page: http://docs.oracle.com/cd/E72219_01/documentation.html
Oracle Utilities Service Order Management Integration to Oracle Utilities Mobile Workforce Management Installation Guide	
Edge application documentation:	
Oracle Utilities Mobile Workforce Management	
Oracle Utilities Service Order Management	

Preface - i

Oracle Utilities Service Order Management Integration to Oracle Utilities Mobile Workforce Management Installation Guide

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 used in this document.

Abbreviation	Expanded Form
AIA	Application Integration Architecture
EBF	Enterprise Business Flow
MDS	Metadata Store
MWM	Oracle Utilities Mobile Workforce Management
OHS	Oracle HTTP Server
SOA	Service-Oriented Architecture
SOM	Oracle Utilities Service Order Management

Chapter 1

Overview

This section provides information on prerequisites for installation of the Oracle Utilities Service Order Management Integration to Oracle Utilities Mobile Workforce Management.

Integration Pack Software Requirements

The following software and applications must be installed and configured before installing the integration pack.

Participating Applications

- Oracle Utilities Service Order Management - Application version v2.2.0 installed on an Oracle database with the latest supported service pack.

- Oracle Utilities Mobile Workforce Management - Application version v2.3.0 installed on an Oracle database with the latest supported service pack.

Oracle SOA / Weblogic Server

- Oracle SOA Suite 12c with Enterprise Manager 12.2.x on Weblogic Server 12c (12.2.x).

    Note: This integration does not require the 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 Service Order Management Integration to Oracle Utilities Mobile Workforce Management 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 **installation zip** file from Oracle Software Delivery Cloud (https://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.
   > (The process described refers specifically to the CCB-MDM integration, however it applies any integration being installed on alternate platforms).

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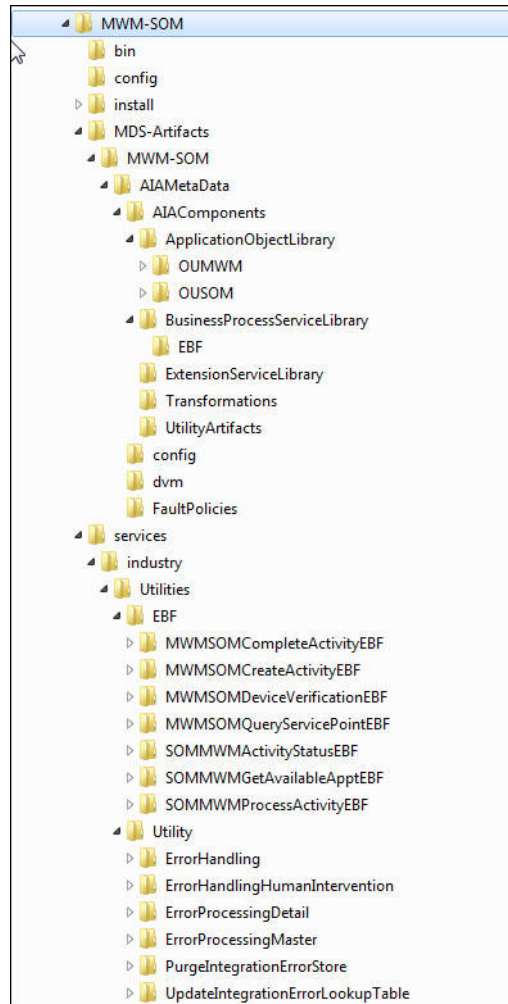
MWM-SOM Product Home Directory

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 chapter for information about individual properties.

Installation 2 - 3

Oracle Utilities Service Order Management Integration to Oracle Utilities Mobile Workforce Management Installation Guide

b. Set the following environment variables for Linux and Windows operating system:

Variable	Example
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/ MWM-SOM

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 of how 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/MWM-SOM
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\MWM-SOM
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 MWM-SOM integration code.

• PRODUCT_HOME/bin/UnInstallBuild.xml is used to uninstall MWM-SOM 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 & 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 ErrorHandling Module.
  - Create an outbound connection pool instance for the database by updating the DbAdapter_MWMSOM.rar file.
  - Create the csf key for the integration.Oracle Utilities Service Order Data Management and Oracle Utilities Meter Data Management.
    - MWM-SOM_SOM
    - MWM-SOM_MWM
- 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: MWM-SOM.
  - Compile and deploy all composites

Post-Installation Checklist

Post-installation checklist includes the following:

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

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

3. Review the logs. Refer to Reviewing the Logs for instructions.

4. Verify that the csf-keys are generated. Refer to Verifying CSF-Key Generation for the instructions.

5. Verify the user messaging service list. Refer to Verifying the User Messaging Service List for the steps.

Verifying the JDBC Configuration

To verify the JDBC configuration, follow these steps:

1. Login to Weblogic Administration console.

2. Navigate to **Home** > **Deployments**.

3. Verify that **DbAdapter_MWMSOM.rar** is deployed, and is in **Active** state.

4. Verify the **eis/DB/MWM-SOMErrorHandling** connection factory details to ensure the connection-factory location matches with that defined in the JCA files. Follow these steps:

   a. Click "DbAdapter_MWMSOM" on the **Deployments** table.

   b. On the **Configuration** tab, click **Outbound Connection Pools**.

   c. Expand **javax.resource.cci.ConnectionFactory** to check the eis/DB/MWM-SOMErrorHandling connection factory instance.

5. Verify that the database details are as required:

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

   b. Click the **MWM-SOMEHDS** data source to check the JNDI Name. The JNDI name should be "jdbc/MWM-SOMEHDS".

6. Click **Connection Pool** to check the URL and properties.

7. 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 the Enterprise Manager

Verify that the MWM-SOM partition is created with all the composites deployed. Perform the following steps to verify the composites in the Enterprise Manager:

1. Login to the **Enterprise Manager**.

2. Expand **soa_domain soa/soa-infra/SOA Folder/MWM-SOM Deployed Composites**.

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

   • ErrorHandling

   • ErrorHandlingHumanIntervention

   • ErrorProcessingDetail

   • ErrorProcessingMaster

   • MWMSOMCompleteActivityEBF

   • MWMSOMCreateActivityEBF

   • MWMSOMQueryServicePointEBF

   • PurgeIntegrationErrorStore

   • SOMMWMActivityStatusEBF

   • SOMMWMGetAvailableApptEBF

   • SOMMWMProcessActivityEBF

   • UpdateIntegrationErrorLookupTable

Reviewing the Logs

Review the logs under $MW_HOME/user_projects/domains/soa_domain/servers/ <managed_server>/logs to check for deployment errors.

For example: $MW_HOME/user_projects/domains/soa_domain/servers/ soa_server1/logs.

Verifying CSF-Key Generation

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

1. Login to the **Enterprise Manager**.

2. Navigate to **soa_domain** > **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 following keys are available:

   • MWM-SOM_SOM

   • MWM-SOM_MWM

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 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.

7. Click **Configure Driver** to check the email driver properties and view the specific configuration details as shown in the image below.

Configuring Edge Applications

Configure Oracle Utilities Mobile Workforce Management and Oracle Utilities Service Order Management installation according to the guidelines in the *Oracle Utilities Service Order Management Integration to Oracle Utilities Mobile Workforce Management Implementation Guide*.

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 and undeploy individual composites for incremental builds or patches and includes the following:

- Undeploying Individual Composites
- Deploying Individual Composites

Undeploying Individual Composites

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

Perform the following steps to undeploy the composites:

1. Open a Command prompt and execute the following commands for Linux and Windows respectively:

    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 the composite to be undeployed to SOA server. This parameter does not have a default value. Enter the composite name to be undeployed.
      For example: MWMSOMCompleteActivityEBF

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

Individual Composites 3 - 1

Oracle Utilities Service Order Management Integration to Oracle Utilities Mobile Workforce Management Installation Guide

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

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

Deploying Individual Composites

Deploy individual composites by performing the following steps:

Note: Refer to Verifying Composites in the Enterprise Manager section to review the composites.

1. Open a Command prompt and execute the following commands for Linux and Windows respectively:

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 the composite to be deployed to SOA server. This parameter does not have a default value. Enter the composite name to be deployed.
  For example: MWMSOMCompleteActivityEBF

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

  For example: If you are planning to 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.

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

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 MWM-SOM. Refer to the MWM-SOM Home Directory image in the Installation chapter for a reference.

- The MWM-SOM 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/MWM-SOM/AIAMetaData/dvm pass MWM-SOM/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
    ```

Metadata Store (MDS) Artifacts 4 - 1

Oracle Utilities Service Order Management Integration to Oracle Utilities Mobile Workforce Management Installation Guide

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 MWM-SOM**/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/MWM-SOM/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 MWM-SOM**/AIAMetaData/ApplicationObjectLibrary** to deploy the
  schema folders, or

- Pass MWM-SOM**/AIAMetaData/ApplicationObjectLibrary/**OUMWM to
  deploy only the MWM schema folder, or

• Replace OUMWM with OUSOM to deploy only the SOM 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.

Do one of the following:

• Pass MWM-SOM**/AIAMetaData/ExtensionServiceLibrary** to deploy the extension service library folders, or

• Pass MWM-SOM**/AIAMetaData/ApplicationObjectLibrary/**OUMWM to deploy only the MWM extension library folder, or

• Replace OUMWM with OUSOM to deploy only the MWM extension service library.

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:

   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/OUMWM/AIAMetaData/AIAComponents/ApplicationObjectLibrary/<ApplicationFolder>

     Example: MWM-SOM/MDS-Artifacts/MWM-SOM/AIAMetaData/AIAComponents/ApplicationObjectLibrary/OUMWM/V1/wsdls

2. Restart the managed server.
   You must restart 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 intregration module	Deafult: MWM-SOM Do not change this value
Oracle Utilities Mobile Workforce Management Application Information		
<MWM>		
<MWM><ApplicationUsername>	Application login username.	MWMUSER
<MWM><ApplicationPassword>	Application login password.	MWMPWD
<MWM-SOM><MWM><policy>	The security policy that MWM 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.
<AppointmentService>		
<MWM-SOM><Protocol>	AppointmentService protocol	http

Property (XPath Representation)	Description	Example
<MWM-SOM><Host>	AppointmentService Host	MWM_HOST.yourdomain.com
<MWM-SOM><Port>	AppointmentService Port	MWM_SERVICE_PORT_NO
<MWM-SOM><ContextRoot>	AppointmentService ContextRoot	MWM_CONTEXT_ROOT_NAME • ouaf/XAIApp/xaiserver (for XAI services) • ouaf/webservices (for IWS services)
<ASService>		
<Protocol>	ASService protocol	http
<Host>	ASService Host	MWM_HOST.yourdomain.com
<Port>	ASService Port	MWM_SERVICE_PORT_NO
<ContextRoot>	ASService ContextRoot	MWM_CONTEXT_ROOT_NAME • ouaf/XAIApp/xaiserver (for XAI services) • ouaf/webservices (for IWS services)
<PAService>		
<Protocol>	PAService protocol	http
<Host>	PAService Host	MWM_HOST.yourdomain.com
<Port>	PAService Port	MWM_SERVICE_PORT_NO
<ContextRoot>	PAService ContextRoot	MWM_CONTEXT_ROOT_NAME • ouaf/XAIApp/xaiserver (for XAI services) • ouaf/webservices (for IWS services)
Service Order Management Application Information		
<SOM>		
<SOM><ApplicationUsername>	Application login username.	SOMUSER
<SOM><ApplicationPassword>	Application login password.	SOMPWD
<SOM><policy>	The security policy that MWM 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.
<QuerySPService>		
<Protocol>	QuerySPService protocol	http
<Host>	QuerySPService Host	MWM_HOST.yourdomain.com
<Port>	QuerySPService Port	MWM_SERVICE_PORT_NO

Property (XPath Representation)	Description	Example
<ContextRoot>	QuerySPService ContextRoot	MWM_CONTEXT_ROOT_NAME
		• ouaf/XAIApp/xaiserver (for XAI services)
		• ouaf/webservices (for IWS services)
<CreateActivityService>		
<Protocol>	CreateActivityService protocol	http
<Host>	CreateActivityService Host	MWM_HOST.yourdomain.com
<Port>	CreateActivityService Port	MWM_SERVICE_PORT_NO
<ContextRoot>	CreateActivityService ContextRoot	MWM_CONTEXT_ROOT_NAME
		• ouaf/XAIApp/xaiserver (for XAI services)
		• ouaf/webservices (for IWS services)
<DVService>		
<Protocol>	DVService protocol	http
<Host>	DVService Host	MWM_HOST.yourdomain.com
<Port>	DVService Port	MWM_SERVICE_PORT_NO
<ContextRoot>	DVService ContextRoot	MWM_CONTEXT_ROOT_NAME
		• ouaf/XAIApp/xaiserver (for XAI services)
		• ouaf/webservices (for IWS services)
<CAService>		
<Protocol>	CAService protocol	http
<Host>	CAService Host	MWM_HOST.yourdomain.com
<Port>	CAService Port	MWM_SERVICE_PORT_NO
<ContextRoot>	CAService ContextRoot	MWM_CONTEXT_ROOT_NAME
		• ouaf/XAIApp/xaiserver (for XAI services)
		• ouaf/webservices (for IWS services)
WorkFlow Notification Properties		
<WorkFlow.Notification>		
<from.emailid>	The valid email address.	Admin.user@yourdomain.com
<mode>	The type of mode such as email or sms.	EMAIL

Property (XPath Representation)	Description	Example
SOA Information		
<SOA>		
Admin Server Information		
<AdminServer>		
<hostname>	The host name of the server where admin server hosting SOA suite is installed.	SOA_Admin.yourdomain.com
<portnumber>	The port number the admin server (hosting SOA suite) is referring to.	7001
<servername>	The admin server name (hosting SOA suite).	AdminServer
<username>	The user name used to log in as an Admin server (hosting SOA suite) administrator.	webLogic
<password>	The password used to log in as an Admin server (hosting SOA suite) administrator.	XX_PWD
<domainname>	The WebLogic domain name hosting SOA suite.	soa_domain
Managed Server Information		
<ManagedServer>		
<hostname>	The host name of the server where managed server (hosting SOA suite) is installed.	SOA_MS.yourdomain.com
<portnumber>	The port number, the managed server (hosting SOA suite) is referring to.	8001
<servername>	The managed server name (hosting SOA suite).	soa_server1
<username>	The user name used to login to managed server (hosting SOA suite) as an administrator.	webLogic
<password>	The password used to login to managed server (hosting SOA suite) as an administrator.	XX_PWD
OHS (Oracle HTTP Server Information)		
<OHS>		Cluster Support Properties: Oracle HTTP Server host, port & server name. In case of the non-cluster environment, these properties would be same as <ManagedServer> values.

Property (XPath Representation)	Description	Example
<hostname>	The Oracle HTTP server host name.	managedserver.example.oracle.com
<portnumber>	The Oracle HTTP server port name.	8001
<servernames>	The server names on cluster.	In case of multiple managed servers, provide comma to separate values. For example, soa_server1, soa_server2
<Protocol>	Oracle HTTP server protocol	http or https
MDS DB information		
<mdsconfig>		
<mdsdbusername>	The user name used to login to the MDS schema.	SOA_MDS
<mdsdbuserpassword>	The password used to login to the MDS schema.	XX_PWD
<mdsdbhostname>	The host name of the server hosting the database containing the MDS schema.	MDSDB_HOST.yourdomain.com
<mdsdbportnumber>	The port number of the database containing the MDS schema.	1521
<mdsdbsid>	The SID of the database containing the MDS schema.	MDSDBSID
Error Handling Schema Information		
<dba.dbusername>	The user name used to login as a Database Administrator (DBA). This database hosts the schema required for MWM-SOM integration.	System
<dba.dbuserpassword>	The password used to login as a Database Administrator (DBA). This database hosts the schema required for MWM-SOM integration.	XX_PWD
<dbusername>	The user name used to login to MWM-SOM schema for MWM-SOM integration. This user can be automatically created by the install (set dbuser.createflag to true) or manually outside the install process.	MWMSOMUSER
<dbuserpassword>	The password used to login to MWM-SOM schema for MWM-SOM integration.	XX_PWD

Property (XPath Representation)	Description	Example
<dbuser.createflag>	The flag specifying whether to create a new schema or use the existing schema for MWM-SOM integration. If the schema is created manually outside of the installation process, then set this value to "false". Else, set the value to "true", if the installation script should automatically create the schema. Valid values: true or false (this is case sensitive)	true
<dbhostname>	The database host name used for MWM-SOM integration.	DB_HOST.yourdomain.com
<dbportnumber>	The database port number used for MWM-SOM integration.	1521
<dbsid>	The database SID used for MWM-SOM integration.	DBSID
Email		
<MailAccessProtocol>	An e-mail receiving protocol. The possible values are IMAP and POP3. Required only if receiving of an email is supported on the driver instance.	IMAP
<OutgoingDefaultFromAddr>	The default FROM address (if one is not provided in the outgoing message).	Usr.login@company.com
<OutgoingMailServer>	The name of the SMTP server. Mandatory only if sending of email is required.	xxx.company.com
<OutgoingMailServerPort>	The port number of SMTP server. Typically 25.	456
<OutgoingMailServerSecurity>	The security used by SMTP server. The possible values are None, TLS and SSL. The default value is None.	SSL
<OutgoingUsername>	The username used for SMTP authentication. Required only if SMTP authentication is supported by the SMTP server.	Usr.login@company.com
<Outgoingpassword>	The password used for SMTP authentication. Required only if the SMTP authentication is supported by the SMTP server.	Password1
<Capability>	Sets the driver's capability to send or receive messages.	The values are SEND, RECEIVE, and BOTH. For 12c.

Property (XPath Representation)	Description	Example
<incomingMailServer>	The name of the SMTP server. Mandatory only if incoming of email is required.	host.yourdomain.com
<IncomingUserIDs>	The list of user names of the mail accounts the driver instance is polling from. Each name must be separated by a comma, for example, foo,bar. Required only if e-mail receiving is supported on the driver instance.	Usr.login@company.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 usernames list. Required only if e-mail receiving is supported on the driver instance.	Pasword1
<applicationName>	The application name for the user messaging service.	MWMSOM

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 section Installation Steps.

3. Open a Command prompt window and execute the following three commands in Linux and Windows respectively:

Step1: Execute the **UnInstallSOA** 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.

Step 2: Execute the **UnInstallWL** command 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.

- Deletes the JMS resources (JMS module/ JMS persistent store/ JMS server).

- Undeploys the JMS outbound connection pool.

- Undeploys the database outbound connection pool.

- Deletes the JDBC data source for the Error Handling module.

- Removes the workflow notification.

- Deletes the csf-keys generated.

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

Step 3: Execute the **UnInstallDB** command 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 Error Handling module and the artifacts created for the integration

> **Note**: After a successful uninstall, all the JDBC resources and MWM-SOM 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.