Oracle Utilities Network Management System Integration to Oracle Utilities Mobile Workforce Management

Installation Guide

Release 12.1

E63258-02

February 2017
(Updated July 2017)

ORACLE

Oracle Utilities Network Management System Integration to Oracle Utilities Mobile Workforce Management, Release 12.1 Installation Guide

Contents

Installation Guide

Chapter 5

Chapter 6

Chapter 7

Preface

This document is intended for anyone implementing the Oracle Utilities Network Management System 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 Network Management System Integration to Oracle Utilities Mobile Workforce Management Release Notes	Refer to the Oracle Utilities applications documentation page: http://docs.oracle.com/cd/E72219_01/documentation.html
Oracle Utilities Network Management System Integration to Oracle Utilities Mobile Workforce Management Implementation Guide	
Oracle Utilities Network Management System Integration to Oracle Utilities Mobile Workforce Management Installation Guide	
Edge application documentation:	
Oracle Utilities Network Management System	
Oracle Utilities Mobile Workforce Management	

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 terms are used in this document:

- AIA - Application Integration Architecture
- AVL - Automatic Vehicle Location
- BPEL - Business Process Execution Language
- EBF - Enterprise Business Flow
- EM - Enterprise Manager
- ERT - Estimated Restoration Time
- FMW - Fusion Middleware
- JMS - Java Message Service
- MDS - Meta Data Services
- MDT - Mobile Data Terminal
- MWM - Oracle Utilities Mobile Workforce Management
- NMS - Oracle Utilities Network Management System
- OHS - Oracle HTTP Server
- SOA - Service Oriented Architecture

Chapter 1

Overview

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

Integration Pack Software Requirements

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

> **Note**: For complete details, refer to the product specific installation instructions.

Participating Applications

- Oracle Utilities Network Management System - Application version 1.12.0.3 installed on an Oracle database with the latest supported service pack
- Oracle Utilities Mobile Workforce Management - Application version 2.2.0.3 installed on an Oracle database with the latest supported service pack

Oracle SOA/ Weblogic Server

- Oracle SOA Suite 12c with Enterprise Manager 12.1.3 on Weblogic Server 12c (12.1.3)

  Note: This integration is an AIA direct integration and does not require to install the AIA Foundation Pack.

> **Note**: Refer to the Oracle Utilities product Certification Matrix (referenced in the Additional Documentation 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 Network Management System 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.

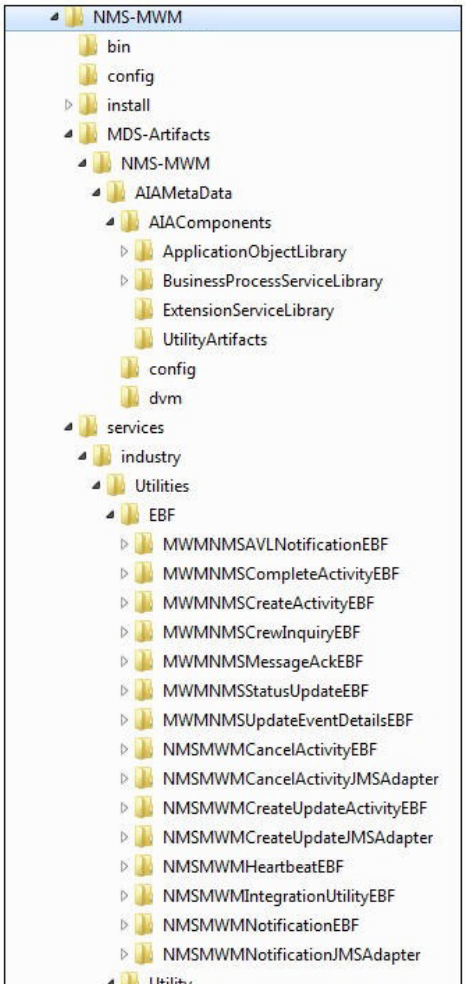
Installation Steps

To install the integration follow these steps:

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.

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



NMS-MWM 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.

b. Verify the 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
ORACLE_HOME	XXX/Middleware/soa
PRODUCT_HOME	The product installation folder. Example: PRODUCT_HOME=/scratch/PRODUCT_HOMES/NMS-MWM

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/NMS-MWM
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\NMS-MWM
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 NMS-MWM integration code.
- PRODUCT_HOME/bin/UnInstallBuild.xml is used to uninstall NMS-MWM 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.

4. Install the Integration.

   Follow the guidelines in step 4 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_NMS-MWM .rar file.
   - Create JMS server/JMS module/JMS connection pool/JMS persistence store/JMS queues and assigns the error queues to the interface queues.
   - Create JMS outbound connections to both Oracle Utilities Network Management System and Oracle Utilities Mobile Workforce Management by updating the JMSAdapter_NMS-MWM .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: NMS-MWM .
   - Compile and deploy all composites.

Post-Installation Checklist

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

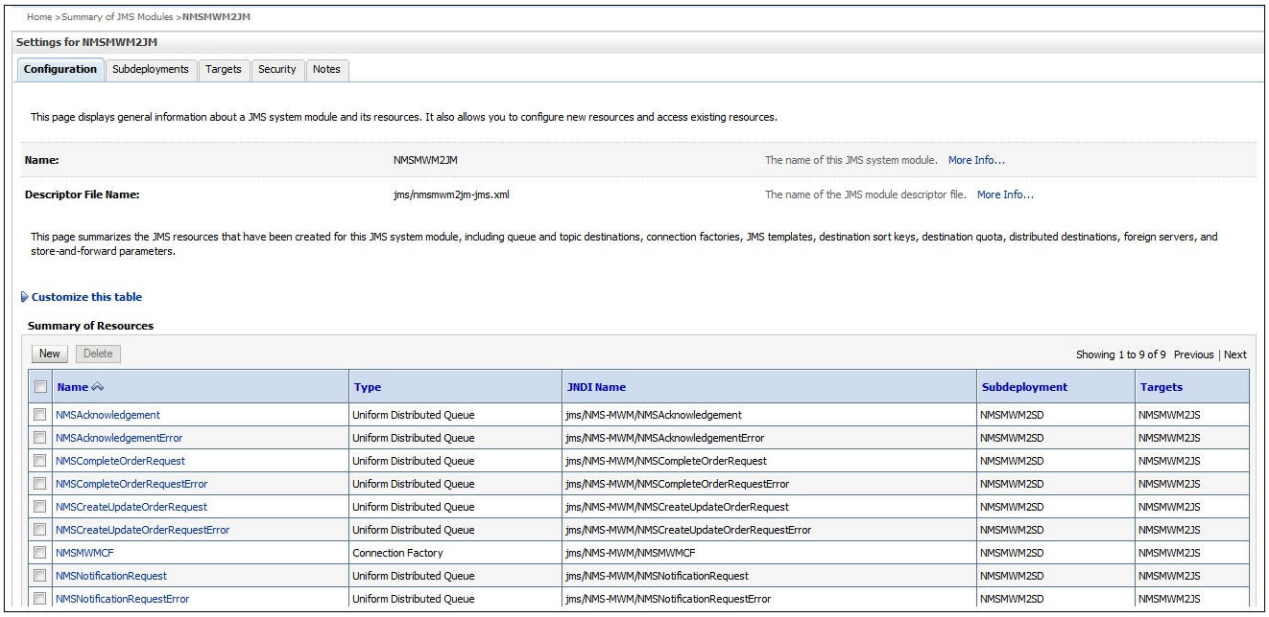
1. Verify that all the JMS and JDBC resources were created. Refer to Verifying JMS and JDBC Configurations for the instructions.
2. Verify that the csf-keys are generated. Refer to Verifying the csf-key Generation for the instructions.
3. Review the logs under $WL_HOME/user_projects/domains/soa_domain/servers/ /<managed-server-name>/logs to check for any 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 Network Management System and Oracle Utilities Mobile Workforce Management applications. Refer to Importing Security Certificates into KeyStore for more details.
6. Add the Oracle Utilities Network Management System Key Store Certificate. Refer to Importing Security Certificates into KeyStore for the steps.
7. Verify that the user messaging service is active. Refer to Verifying the User Messaging Service List for more details.

Verifying JMS and JDBC Configurations

To verify the JMS configuration, follow these steps:

1. Open a WebLogic Admin console and navigate to Home /JMS Modules/ NMSMWM2JM.
2. Verify that the queues and connection factory are created successfully by navigating to one of the queues.



Note: If JMSMODULENAME!JMSQUEUENAME does not exist in the rows of the **Destinations** table, it means there are no problems with the installation.

3. Navigate to **Services** > **Persistent Stores** > **NMSMWM2FS**.
4. Verify that the JMSFileStorePath is correct and the directory has 'write' permissions.

To verify the JDBC configuration, follow these steps:

1. Navigate to **Home** > **Deployments**.
2. Verify that DbAdapter_NMSMWM.rar is deployed, and is in **Active** state.
3. Verify the eis/DB/NMS-MWMErrorHandling connection factory details to ensure the connection-factory location matches with that defined in the JCA files. Follow these steps:

a. Click **DbAdapter_NMSMWM** on the **Deployments** table.

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

c. Expand javax.resource.cci.ConnectionFactory to check the eis/DB/NMS-MWMErrorHandling connection factory instance.

4. Verify the database details:

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

   b. Click the **NMS-MWMEHDS** data source to check the JNDI Name.

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

To verify that the NMS-MWM partition was created with all the composites deployed, follow these steps:

1. Login to the Enterprise Manager console.
2. Navigate to the **Expand SOA > soa-infra** > **NMS-MWM** partition.
3. Verify that the composites listed below are deployed and are in 'active' state.
   - ErrorHandling [1.0]
   - ErrorHandlingHumanIntervention [1.0]
   - ErrorProcessingDetail [1.0]
   - ErrorProcessingMaster [1.0]
   - MWMNMSAVLNotificationEBF [1.0]
   - MWMNMSCompleteActivityEBF [1.0]
   - MWMNMSCreateActivityEBF [1.0]
   - MWMNMSCrewInquiryEBF [1.0]
   - MWMNMSMessageAckEBF [1.0]
   - MWMNMSStatusUpdateEBF [1.0]
   - MWMNMSUpdateEventDetailsEBF [1.0]
   - NMSMWMCancelActivityEBF [1.0]
   - NMSMWMCancelActivityJMSAdapter [1.0]
   - NMSMWMCreateUpdateActivityEBF [1.0]
   - NMSMWMCreateUpdateJMSAdapter [1.0]
   - NMSMWMHeartbeatEBF [1.0]
   - NMSMWMIntegrationUtilityEBF [1.0]
   - NMSMWMNotificationEBF [1.0]
   - NMSMWMNotificationJMSAdapter [1.0]
   - PurgeIntegrationErrorStore [1.0]

- UpdateIntegrationErrorLookupTable [1.0]

Verifying the csf-key Generation

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

1. Login to the Enterprise Manager console.
2. Navigate to **Expand SOA** > **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:
   - NMS-MWM_NMS
   - NMS-MWM_MWM

Importing Security Certificates into KeyStore

To import and configure the security certificate (for example: Oracle Utilities Network Management System certificate), follow these steps:

> **Important**: Copy/paste the commands in a text editor to remove extra spaces, if any.

1. Export the certificate and save it on the integration server to add it to the key store.

   For example: /tmp/nmsdemocert.cer

2. Create a new keystore (for example: UtilitiesIntegration.jks for importing the certificates.

   Linux
   ```
   keytool -genkey -keystore /Oracle/Middleware/Oracle_Home/wlserver/
   server/lib/UtilitiesIntegration.jks -storepass <keystore password>
   ```

   Windows
   ```
   keytool -genkey -keystore
   C:\Oracle\Middleware\Oracle_Home\wlserver\UtilitiesIntegration.
   jks -storepass <keystore password>
   ```

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

   Linux
   ```
   keytool -import -file /tmp/nmsdemocert.cer -alias RootCA - keystore
   /Oracle/Middleware/Oracle_Home/wlserver/server/lib/
   UtilitiesIntegration.jks -storepass <keystore password>
   ```

   Windows
   ```
   keytool -import -file C:\nmsdemocert.cer -alias RootCA - keystore
   C:\Oracle\Middleware\Oracle_Home\wlserver\UtilitiesIntegration.jks
   -storepass <keystore password>
   ```

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

Linux

```
keytool -list -v -keystore /Oracle/Middleware/Oracle_Home/wlserver/
server/lib/UtilitiesIntegration.jks
```

Windows

```
keytool -list -v -keystore
C:\Oracle\Middleware\Oracle_Home\wlserver\UtilitiesIntegration.jks
```

Note: Enter the password when prompted.

5. Edit the setDomainEnv.sh file for Linux or setDomainEnv.cmd for Windows 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/UtilitiesIntegration.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/UtilitiesIntegration.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 Network Management System are SSL enabled, import the Oracle Utilities Network Management System certificates into the Weblogic Managed server to enable secure communication between the integration layer and Oracle Utilities Network Management System.

    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.

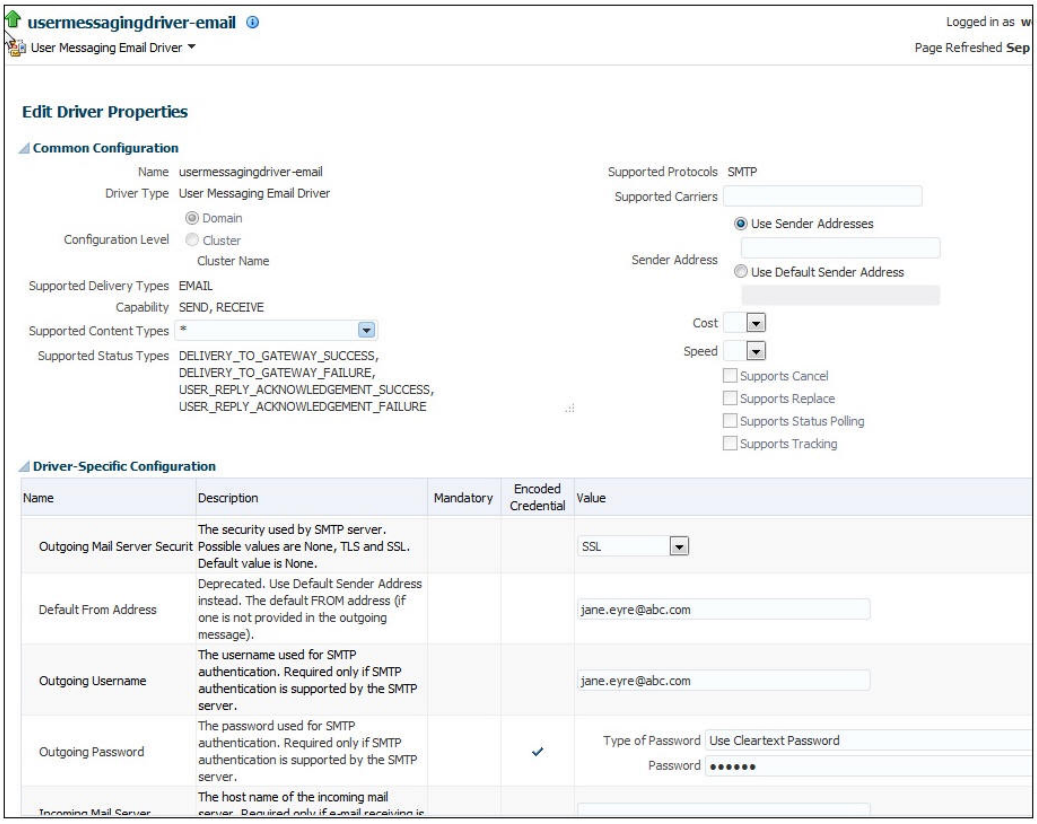
    The composite PurgeIntegrationErrorStore gets deployed only when purge.process.deploy=true in deploy.properties. If this is set to false, then the process is not deployed.

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**.
3. If not, click **usermessagingdriver-email** > **Targets** > <managed server>. For example: soa_server1
   Then, select **Yes** and click **Activate Changes**.
4. In the WebLogic Enterprise Manager console, navigate to **soa-infra [managed server]**.
5. Right-click the **soa-infra [managed server]** node, select **SOA Administration**, and then select **Workflow Properties**.
6. Verify that the **Notification Mode** under **Workflow Notification Properties** is set to **Email**.
7. 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.
8. In the **Driver Properties** drop-down list select **usermessagingdriver-NMSMWM**, and then click **Edit**. The configuration details as are shown in the figure below.



Configuring Edge Applications

To configure the Oracle Utilities Mobile Workforce Management and Oracle Utilities Network Management System installation, refer to the instructions in the *Oracle Utilities Network Management System 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 chapter describes how to deploy and undeploy individual composites for incremental builds or patches. It includes the following sections:

3.1 Undeploying Composites

To undeploy a composite, follow these steps:

Important: Copy/paste the commands in a text editor to remove extra spaces, if any.

1. Execute the following commands in the Command prompt for Linux and Windows respectively:

   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 the deployment.

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

     For example: MWMNMSCompleteActivityEBF

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

  For example: To undeploy the composite from <PRODUCT_HOME>/services/industry/Utilities/EBF, pass <PRODUCT_HOME>/services/industry/Utilities/EBF to this property.

  Note: 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.

3.2 Deploying Individual Composites

To deploy the individual composites, follow these steps:

Note: Refer to Verifying Composites in Enterprise Manager for the composites for Oracle Utilities Network Management System integration to Oracle Utilities Mobile Workforce Management.

Important: Copy/paste the commands in a text editor to remove extra spaces, if any.

1. Execute the following commands in the Command prompt for Linux and Windows respectively:

   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 the deployment.

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

     For example: MWMNMSCompleteActivityEBF

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

     For example: To deploy the composite from %PRODUCT_HOME%/services/industry/Utilities/EBF, 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.

3.3 Connection Mapping

All connections are mapped/ grouped by the edge applications in the <PRODUCT_HOME>/config/ConnectionMappings.xml file.

The ConnectionMapping.xml file is used for internal reference purposes only and hence the entries should not be modified. This helps to de-tokenize the Oracle Utilities Network Management System/ Oracle Utilities Mobile Workforce Management URLs in the ${PRODUCT_HOME}/MDS-Artifacts/NMS-MWM/AIAMetaData/config/ConfigurationProperties.xml file.

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 NMS-MWM. Refer to the Home Directory image in the Installation chapter for a reference.
- The 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/NMS-MWM/AIAMetaData/dvm pass NMS-MWM/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. 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 **/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/NMS-MWM/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 NMS-MWM**/AIAMetaData/AIAComponents/ApplicationObjectLibrary** to deploy the schema folders, or
- Pass NMS-MWM**/AIAMetaData/AIAComponents/ApplicationObjectLibrary/**OUNMS to deploy only the xxx 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.

Do one of the following:

- Pass NMS-MWM**/AIAMetaData/ApplicationObjectLibrary/ExtensionServiceLibrary** to deploy the extension service library folders, or
- Pass **/AIAMetaData/ApplicationObjectLibrary/** to deploy only the extension library folder, or
- Replace with to deploy only the 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 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/OUNMS/AIAMetaData/AIAComponents/ApplicationObjectLibrary/<ApplicationFolder>

  Example: NMS-MWM/MDS-Artifacts/NMS-MWM/AIAMetaData/AIAComponents/ApplicationObjectLibrary/OUNMS/V1/wsdls

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
MWM Application Information		
<MWM>		
<ApplicationUsername>	Application login username	MWMUSER
<ApplicationPassword>	Application login password	MWMPWD
<CreateUpdateActivityService>		
<Protocol>	Create update activity service protocol	http
<Host>	CreateUpdateActivityService Host	MWM_HOST. yourdomain.com
<Port>	CreateUpdateActivityService Port	MWM_SERVICE_PORT_ NO

Property (XPath Representation)	Description	Example
<ContextRoot>	CreateUpdateActivityService contextroot	MWM_CONTEXT_ROOT_NAME • ouaf/XAIApp/xaiserver (for XAI services) • ouaf/webservices (for IWS services)
<HBService>		
<Protocol>	HBService protocol	http
<Host>	HBService Host	MWM_HOST. yourdomain.com
<Port>	HBService Port	MWM_SERVICE_PORT_NO
<ContextRoot>	HBService contextroot	MWM_CONTEXT_ROOT_NAME
<AVLService>		
<Protocol>	AVLService protocol	http
<Host>	AVLService Host	MWM_HOST. yourdomain.com
<Port>	AVLService Port	MWM_SERVICE_PORT_NO
<ContextRoot>	AVLService contextroot	MWM_CONTEXT_ROOT_NAME
<NotificationService>		
<Protocol>	NotificationService protocol	http
<Host>	NotificationService Host	MWM_HOST. yourdomain.com
<Port>	NotificationService Port	MWM_SERVICE_PORT_NO
<ContextRoot>	NotificationService contextroot	MWM_CONTEXT_ROOT_NAME
<CAService>		
<Protocol>	CAService protocol	http
<Host>	CAService Host	MWM_HOST. yourdomain.com
<Port>	CAService Port	MWM_SERVICE_PORT_NO

Property (XPath Representation)	Description	Example
<ContextRoot>	CAService contextroot	MWM_ CONTEXT_ ROOT_NAME
<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.
NMS Application Information		
<NMS>		
<ApplicationUsername>	Application login username	NMSUSER
<ApplicationPassword>	Application login password	NMSPWD
<GenericService>		
<Protocol>	GenericService protocol	https
<Host>	GenericService Host	NMS_HOST. yourdomain.com
<Port>	GenericService Port	NMS_GENERICSERVICE _ PORT_NO
<ContextRoot>	GenericService contextroot	nms-mwm
<DamageService>		
<Protocol>	DamageService protocol	https
<Host>	DamageService Host	NMS_HOST. yourdomain.com
<Port>	DamageService Port	NMS_GENERICSERVICE _PORT_NO
<ContextRoot>	DamageService contextroot	nms
<AVLService>		
<Protocol>	AVLService protocol	https
<Host>	AVLService Host	NMS_HOST. yourdomain.com
<Port>	AVLService Port	NMS_GENERICSERVICE _PORT_NO
<ContextRoot>	AVLService contextroot	nms-ms

Property (XPath Representation)	Description	Example
<policy>	The security policy that NMS 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.
WorkFlow Notification Properties		
<WorkFlow.Notification>		
<from.emailid>	Valid email address for work flow notifications	Admin.user@yourdomain.com
<mode>	Type of notification mode	EMAIL
SOA Information		
Admin Server Information		
<AdminServer>		
<hostname>	Host name of the server where admin server hosting SOA suite is installed.	SOA_Admin. yourdomain.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#1
<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.	SOA_MS. yourdomain.com
<portnumber>	Port number the managed server (hosting SOA suite) is listening to.	8001
<servername>	Managed server name (hosting SOA suite)	soa_server1
<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.	weblogic#1
Oracle HTTP Server Information		

Property (XPath Representation)	Description	Example
<OHS>		In case of non-cluster environment these properties would be same as <ManagedServer> values
<hostname>	Give a HTTP server host name	Oracle http server where cluster is managed
<Portnumber>	Give a HTTP server port name	Port number of the Oracle http server
<servernames>		In case of multiple managed servers, provide comma separated values. Example: soa_server1
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.	MDSDB_HOST. yourdomain.com
<mdsdbportnumber>	Port number of the database containing MDS schema.	1521
<mdsdbsid>	SID of the database containing MDS schema.	MDSDBSID
JMS Information		
<serverName>	JMS server name **Note**: Do not change this value.	Default: NMSMWM2JS
<ModuleName>	JMS module name	Default: NMSMWM2JM **Note:** Do not change this value.
<SubDeploymentName>	Sub deployment name for JMS queues	Default: NMSMWM2SD **Note:** Do not change this value.
<PersistentStoreType>	JMS persistent store type (FileStores or DBStore). Deployment script supports a file based persistent store.	Default: FileStores
<TargetServerName>	WebLogic managed server name	soa_server1
<PersistentStoreName>	JMS persistent store name	Default: NMSMWM2FS
<JMSCFName>	JMS connection factory name	Default: NMSMWMCF

Property (XPath Representation)	Description	Example
<JMSCFJNDI>	JMS Connection factoy jndi name	Default: jms/NMS-MWM/NMSMWMCF
<PersistentStoreFilename>	Directory path name where the file based persistent store should be created.	/scratch/Oracle/Product_Homes/NMS-MWM/bin
Email Information		
<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).	mail.id@yourdomain.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.	mail.id@yourdomain.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.	mail.id@yourdomain.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	NMSMWM
<capability>	Sets the driver's capability to send or receive messages.	For 12c, the values are SEND, RECEIVE, and BOTH.
Error Handling Database Information		
<EH>		

Property (XPath Representation)	Description	Example
<dba.dbusername>	User name used to log in as a Database Administrator (DBA). This database hosts the schema required for integrating Oracle Utilities Network Management System and Oracle Utilities Mobile Workforce Management.	system
<dba.dbuserpassword>	Password used to log in as a Database Administrator (DBA). This database hosts the schema required for integrating Oracle Utilities Network Management System and Oracle Utilities Mobile Workforce Management.	DB_USER_PWD
<dbusername>	User name used to login to NMS-MWM Error Handling schema for integrating Oracle Utilities Network Management System and Oracle Utilities Mobile Workforce Management. This user can be automatically created by the install (set dbuser.createflag to true) or manually outside the install process.	Example: NMSMWMUser
<dbuserpassword>	Password used to log in to NMS-MWM Error Handling schema for integration Oracle Utilities Network Management System and Oracle Utilities Mobile Workforce Management.	NMSMWMPWD
<dbuser.createflag>	Flag specifying whether to create a new schema or use the existing schema for Oracle Utilities Network Management System and Oracle Utilities Mobile Workforce Management 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>	Database host name used for the Oracle Utilities Network Management System and Oracle Utilities Mobile Workforce Management integration.	DB_HOST. yourdomain.com
<dbportnumber>	Database port number used for the Oracle Utilities Network Management System and Oracle Utilities Mobile Workforce Management integration.	1521
<dbsid>	Database SID used for the Oracle Utilities Network Management System and Oracle Utilities Mobile Workforce Management integration.	DBSID

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, follow these steps:

1. Restart the WebLogic Admin server and the SOA server.
2. Set the environment variables as mentioned in the Installation Steps section.
3. The uninstallation process is divided into three steps. Execute the commands in each of those steps.

   Important: Copy/paste the commands in a text editor to remove extra spaces, if any.

   Step1: 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:

   a. Undeploys all the composites from the Enterprise Manager partition.

   b. Deletes the partition.

   c. Undeploys the MDS artifacts.

Step 2: 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
```

These commands perform the following tasks:

1. Delete the JMS resources (JMS module/ JMS persistent store/ JMS server).
2. Undeploy the JMS outbound connection pool.
3. Undeploy the database outbound connection pool.
4. Delete the JDBC data source for the Error Handling module.
5. Remove the work flow notification that is created.
6. Delete the csf-keys generated.

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

Step 3: 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 and the artifacts created for the integration.

After a successful uninstall, all JMS, JDBC resources, and the NMS-MWM 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.