Oracle Utilities Smart Grid Gateway Integration for Outage Operations

Installation Guide

Release 12.1

E40672-04

May 2015
(Updated December 2021)

ORACLE®

Oracle Utilities Smart Grid Gateway Integration for Outage Operations, Release 12.1 Installation Guide

Contents

Chapter 1

Chapter 2

Chapter 3

Chapter 4

Chapter 5

Chapter 6

Chapter 7

Preface

Welcome to the Oracle Utilities Smart Grid Gateway Integration for Outage Operations Installation Guide.

The preface includes the following:

- Audience
- Documentation and Resources
- Documentation Accessibility
- Conventions
- Abbreviations

Audience

This document is intended for anyone implementing the Oracle Utilities Smart Grid Gateway Integration for Outage Operations.

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 Smart Grid Gateway Integration for Outage Operations Release Notes	
Oracle Utilities Smart Grid Gateway Integration for Outage Operations Implementation Guide	Refer to the Oracle Utilities applications documentation page: http://docs.oracle.com/cd/E72219_01/documentation.html
Oracle Utilities Smart Grid Gateway Integration for Outage Operations Installation Guide	
Edge application documentation:	
Oracle Utilities Network Management System	
Oracle Utilities Smart Grid Gateway	

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

Resource	Location
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.

Convention	Meaning
`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	Oracle Application Integration Architecture
DVM	Domain Value Map
EBF	Enterprise Business Flow
NMS	Oracle Utilities Network Management System
MDS	Metadata Store
SGG	Oracle Utilities Smart Grid Gateway
SOA	Service-Oriented Architecture
UMS	User Messaging Service

Chapter 1

Overview

This chapter provides information about the prerequisites for installing the Oracle Utilities Smart Grid Gateway Integration for Outage Operations.

Integration Pack Software Requirements

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

Participating Applications

- Oracle Utilities Network Management System installed on an Oracle database with the latest supported media pack.

- Oracle Utilities Smart Grid Gateway installed on an Oracle database with the latest supported media pack.

Refer to the *Certification Matrix for Oracle Utilities Products* (Document ID 1454143.1) on My Oracle Support for current/supported application version details.

Oracle SOA/WebLogic Server

- Oracle SOA suite 12c with Oracle Enterprise Manager 12.2.1.1 on WebLogic Server 12.2.1.1.

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

Chapter 2

Installing the Integration

This section describes the settings and requirements for a successful installation of the Oracle Utilities Smart Grid Gateway Integration for Outage Operations 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 complete the following:

1. Download the installation NMS-SGG.zip file from Oracle Software Delivery Cloud (http://edelivery.oracle.com/).

   > **Note**: For specific instructions about installing this integration on non-Windows/ Linux platforms, see Oracle Support Knowledge article ID 1349320.1 (The process described refers specifically to the CCB-MDM integration; however it applies to 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.
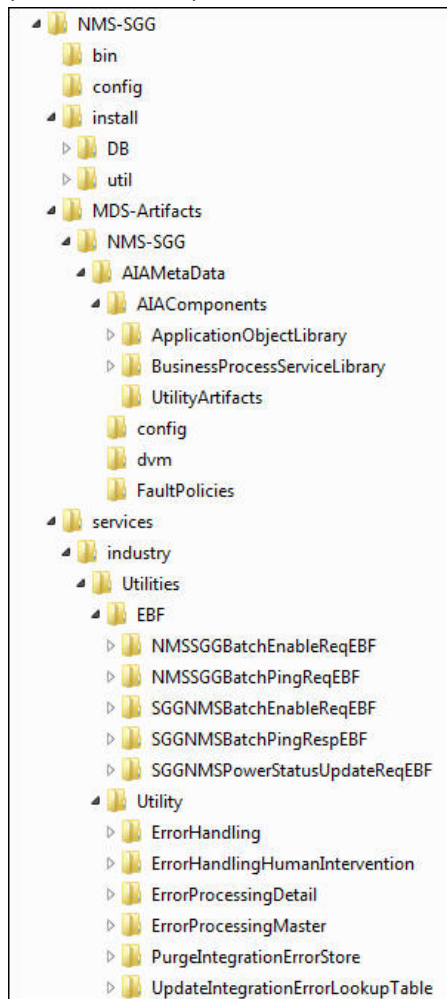
3. Set the following environment variables for Unix and Windows operating systems:

Variable	Example
MW_HOME	XXX/Middleware
SOA_HOME	XXX/Middleware/soa
ORACLE_HOME	XXX/Middleware/soa
PRODUCT_HOME	The product installation folder. Example: **Linux**: PRODUCT_HOME=/scratch/PRODUCT_HOMES/ NMS-SGG **Windows**: PRODUCT_HOME=D:\PRODUCT_HOMES\NMS-SGG

4. Run the following commands (setWLSEnv.sh on Linux and setWLSEnv.bat on Windows) to set the environment variables used for executing the installation scripts:

Linux

```
source ${MW_HOME}/wlserver/server/bin/setWLSEnv.sh"
```

Windows

Change the directory:

```
cd %MW_HOME%\wlserver\server\bin\
```

Execute the following command:

```
setWLSEnv.cmd
```

Example:

Linux

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

Windows

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

5. Modify the $PRODUCT_HOME/config/InstallProperties.xml file and ensure that the values entered are relevant to the server where the integration product has to be installed. Use a text editor to update the InstallProperties.xml file. Login to the WebLogic console to cross verify the values being entered for these properties, as the build may fail due to inappropriate values.

Refer to the Installation Properties chapter for information about individual properties.

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-SGG integration code.

*   PRODUCT_HOME/bin/UnInstallBuild.xml is used to uninstall NMS- SGG 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. Please stand by until the install or uninstall process is completed.

Installing the Integration

After setting the environment variables, open the Command prompt window and execute the following installation scripts in Linux and Windows respectively. Note that the installation process is divided into three steps.

1. Execute the following commands to create the database objects required for the Error Handling module and the database artifacts required for the integration.

    Linux

    ```
    cd $PRODUCT_HOME/bin
    ant -f InstallBuild.xml installDB -
    DInstallProperties=$PRODUCT_HOME/ config/InstallProperties.xml -l
    InstallDB.log
    ```

    Windows

    ```
    cd %PRODUCT_HOME%\bin
    ant -f InstallBuild.xml installDB -
    DInstallProperties=%PRODUCT_HOME%/ config/InstallProperties.xml -l
    InstallDB.log
    ```

    The `installDB` commands perform the followings tasks:

    1. Create Error Handling user for the integration.

    2. Create Error Handling tables and Error Lookup tables.

    3. Insert the seed data that is used for Error Handling scenarios that occur during the BPEL flow instances.

2. Execute the following commands at the Command prompt:

    Linux

    ```
    cd $PRODUCT_HOME/bin
    ant -f InstallBuild.xml installWL -
    DInstallProperties=$PRODUCT_HOME/config/InstallProperties.xml -l
    InstallWL.log
    ```

    Windows

    ```
    cd %PRODUCT_HOME%\bin
    ant -f InstallBuild.xml installWL -
    DInstallProperties=%PRODUCT_HOME%/config/InstallProperties.xml -l
    InstallWL.log
    ```

The `installWL` commands perform the following tasks:

1. Create JDBC DataSource for the ErrorHandling module.

2. Create an outbound connection pool instance for the database by updating the DBAdapter_NMS-SGG.rar file.

3. Create the csf key for the integration NMS-SGG_NMS, NMS-SGG_SGG_XAI and NMS-SGG_SGG_BPEL.

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

3. Execute these commands at the command prompt:

    Linux

    ```
    cd $PRODUCT_HOME/bin
    ```

```
ant -f InstallBuild.xml installSOA -
DInstallProperties=$PRODUCT_HOME/config/InstallProperties.xml -l
InstallSOA.log
```

Windows

```
cd %PRODUCT_HOME%\bin
ant -f InstallBuild.xml installSOA -
DInstallProperties=%PRODUCT_HOME%/config/InstallProperties.xml -l
InstallSOA.log
```

The `installSOA` commands perform the following tasks:

1. Update the MDS repository with all artifacts.

2. Create the application partition where the composites are deployed.
   For example: NMS-SGG

3. Compile and deploy all composites.

Post-Installation Checklist

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

1. Review InstallDB.log, InstallWL.log, and InstallSOA.log files for any deployment errors.

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

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

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

5. Verify that the CSF-Keys are created.Refer to Verifying the CSF-Keys Generation for the steps.

6. Import Oracle Utilities Network Management System certificates into the key store if required. Refer to for the steps.

7. Verify that the user messaging service is active. Refer to Verifying the User Messaging Service List for instructions.

Verifying JDBC Configuration

To verify the JDBC configuration:

1. Open the **Weblogic Admin** console.

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

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

4. Verify the eis/DB/NMS-SGGErrorHandling connection factory details to ensure the connection-factory location matches with the one defined in the JCA files by following these steps:

   a. Click the **DBAdapter_NMSSGG** link on the **Deployments** table.

     b. Click the **Configuration** tab, and then click **Outbound Connection Pools**.

         a. Expand **javax.resource.cci.ConnectionFactory** to check eis/DB/NMS-SGGErrorHandling connection factory instance.

5. Check to ensure the database details are correct:

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

     b. Click the **NMS-SGGEHDS** data source link to verify that the **JNDI Name** is jdbc/NMS-SGGEHDS.

     c. Click the **Connection Pool** subtab to check the **URL** and **Properties**.

     d. 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-SGG partition was created with all the composites deployed:

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

2. Navigate to the **Farm_soa_domain > SOA > soa-infra > SOA Folders> NMS-SGG** partition.

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

   The composite list is as below:

   - ErrorHandling

   - ErrorHandlingHumanIntervention

   - ErrorProcessingDetail

   - ErrorProcessingMaster

   - NMSSGGBatchEnableReqEBF

   - NMSSGGBatchPingReqEBF

   - PurgeIntegrationErrorStore

   - SGGNMSBatchEnableReqEBF

   - SGGNMSBatchPingRespEBF

   - SGGNMSPowerStatusUpdateReqEBF

   - UpdateIntegrationErrorLookupTable

Verifying the CSF-Keys Generation

To verify that all of the CSF-Keys are created successfully:

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

2. Navigate to **Farm_soa_domain > WebLogic_Domain** > **soa_domain**.

3. Right-click **soa_domain,** and navigate to **Security** > **Credentials**.

4. Expand **oracle.wsm.security Map**.

5. Verify that the following keys are available:

   • NMS-SGG_SGG_BPEL

   • NMS-SGG_SGG_XAI

   • NMS-SGG_NMS

Verifying the User Messaging Service List

To verify the user messaging service list:

1. In the WebLogic Administration console, navigate to **Deployments**.

2. Verify that the **usermessagingdriver-email** email driver is **Active**.

3. If not, navigate to **usermessagingdriver-email** > **Targets** and then click **<managed server>**. For example: soa_server1

   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 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. 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 Network Management System and Oracle Utilities Smart Grid Gateway to point to the integration as per the guidelines in the *Oracle Utilities Smart Grid Gateway Integration for Outage Operations 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

Deploying/Undeploying Individual Composites

This chapter describes how to deploy/ undeploy individual composites for incremental builds or patches.

- Undeploying Composites
- Deploying Individual Composites

Undeploying Composites

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

To undeploy the composite:

1. Open a **Command** prompt, and execute the following commands 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 deployment. Press ENTER to use the default value.

    • **Composite Name**: Indicates 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 from the partition.

    • **Composite Folder Location**: Indicates that 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.

    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**: Indicates that the SOA partition name from where the composite should be undeployed.

3. Press ENTER to use the default value.

Deploying Individual Composites

To deploy individual composites:

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

    Linux

    ```
    cd $PRODUCT_HOME/bin
    ant -f DeployUndeployUtility.xml
    -DInstallProperties=$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**: Indicates the name of composite to be deployed to SOA server. This parameter does not have a default value.

   - **Composite folder location**: Indicates the folder name should be an absolute path beginning with %PRODUCT_HOME%/services/industry/Utilities/EBF.

     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.

     If you are planning to deploy the composite from Error Handling then **%PRODUCT_HOME%/services/industry/Utilities/Utility,** then pass **%PRODUCT_HOME%/services/industry/Utilities/Utility** to this property.

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

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

     For example: NMSSGGBatchPingReqEBF

3. Press ENTER to use the default value. 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 chapter describes the following:

- Undeploying the MDS Folder
- Deploying the MDS Folder
- Updating 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 xxx-xxx.

  Refer to Chapter 2: Installing the Integration for more information.

- 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/xxx-xxx/ AIAMetaData/dvm pass xxx-xxx/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

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.

- When the DVMs are updated from the SOA composer, verify that the values are updated in the /MDS-Artifacts/xxx-xxx/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 any of the following:

- Pass xxx-xxx**/AIAMetaData/AIAComponents/ApplicationObjectLibrary** to deploy the schema folders

- Pass xxx-xxx**/AIAMetaData/AIAComponents/ ApplicationObjectLibrary/**OUNMS to deploy only the NMS schema folder, or

- Replace OUNMS with OUSGG to deploy only the SGG 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 xxx-xxx**/AIAMetaData/ApplicationObjectLibrary/ ExtensionServiceLibrary** to deploy the extension service library folders, or

- Pass xxx-xxx**/AIAMetaData/ApplicationObjectLibrary** to deploy only the extension library folder, or

- Replace OUNMS with OUSGG to deploy only the SGG schema folder.

Updating 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-SGG/MDS-Artifacts/NMS-SGG/AIAMetaData/AIAComponents/ApplicationObjectLibrary/OUNMS/V1/wsdls

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

Chapter 5

Installation Properties

This chapter 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.

> **Note:** If install fails because of incorrect values defined in the installProperties.xml file, run uninstall, populate the correct values, and then run install again.

Installation Properties

Property (XPath Representation)	Description	Example
SOA Information		
<config>		
<modulename>	Name of the integration module	Default: NMS-SGG Do not change this value.
<config> <NMS-SGG>		
Workflow Notification Properties		
<WorkFlow.Notification>		
<from.emailid>	E-mail ID, which should be set in the "From" property of Workflow Notification bean.	Admin.user@yourdomain.com

Property (XPath Representation)	Description	Example
<mode>	Type of notification mode	EMAIL
Oracle Utilities Network Management System Application Information		
<NMS>		
<ApplicationUsername>	Application login username	NMSUSER
<ApplicationPassword>	Application login password	NMSPWD
<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.
<GenericService>		
<Protocol>	GenericService protocol	https
<Host>	GenericService Host	NMS_HOST.yourdomain.com
<Port>	GenericService Port	NMS_GENERICSERVICE_PORT _NO
<ContextRoot>	GenericService contextroot	NMS_CONTEXT_ROOT _NAME ouaf/XAIApp/xaiserver (for XAI services) ouaf/webservices (for IWS services)
Oracle Utilities Smart Grid Gateway Middleware Information		
<SGG>		
<ApplicationUsername>	Application login username	weblogic
<ApplicationPassword>	Application login password	
<policy>	The security policy that SGG 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.
<BatchPingReqService>		
<Protocol>	BatchPingRequest Service protocol	http
<Host>	BatchPingRequest Service host	SGG_SOA_HOST.yourdomain.com
<Port>	BatchPingRequest Service port	SGG_ BATCHPINGREQ SERVICE_PORT_NO

Property (XPath Representation)	Description	Example
<ContextRoot>	BatchPingRequest Service contextroot; This changes based on the partition where the SGG composite is deployed. Ex: soa-infra/services/D1	SGG_SOA_CONTEXTROOT_NAME ouaf/XAIApp/xaiserver (for XAI services) ouaf/webservices (for IWS services)
Oracle Utilities Smart Grid Gateway Application Information		
<SGG>		
<ApplicationUsername>	Application login username	SGGUSER
<ApplicationPassword>	Application login password	SGGPWD
<policy>	The security policy that SGG 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.
<EnableReqService>		
<Protocol>	EnableRequest Service protocol	http
<Host>	EnableRequest Service host	SGG_ HOST.yourdomain.com
<Port>	EnableRequest Service host	SGG_ENABLEREQ SERVICE_PORT_NO
<ContextRoot>	EnableRequest Service host	SGG_CONTEXT_ROOT_NAME
<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 login as an Admin server (hosting SOA suite) administrator.	webLogic
<password>	Password used to login as an Admin server (hosting SOA suite) administrator.	
<domainname>	WebLogic domain name hosting SOA suite.	soa_domain
Managed Server Information		
<ManagedServer>		

Property (XPath Representation)	Description	Example
<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 login to managed server (hosting SOA suite) as an administrator.	webLogic
<password>	Password used to login to managed server (hosting SOA suite) as an administrator.	
Oracle HTTP Server Information		
<OHS>		In case of cluster environment, these properties would be same as the OHS server.
<hostname>	Give a HTTP server host name	Oracle HTTP server where cluster is managed
<Portnumber>	Give a HTTP server port number	The 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. Ex: soa_server1, soa_server2
MDS DB Information		
<mdsconfig>		
<mdsdbusername>	User name used to login to MDS schema.	XXX_MDS
<mdsdbuserpassword>	Password used to login to MDS schema.	
<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
Email Information		
<MailAccessProtocol>	The E-mail receiving protocol. The possible values are IMAP and POP3. Required only if e-mail is supported on the driver instance.	IMAP
<OutgoingDefaultFromAddr>	The default FROM address (if one is not provided in the outgoing message).	mail.id@yourdomain.com
<OutgoingMailServer>	The name of the SMTP server. Mandatory only if an e-mail needs to be sent.	host.yourdomain.com

Property (XPath Representation)	Description	Example
<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
<incomingMailServer>	The name of the SMTP server. Mandatory only if e-mail sending is required.	host.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.	usermessagingdriver-email
<capability>	Sets the driver's capability to send or receive messages.	For 12c, the values are SEND, RECEIVE, and BOTH.
Error Handling Schema Information		
<config> <EH>		
<dba.dbusername>	User name used to log in as a Database Administrator (DBA). This database hosts the schema required for Oracle Utilities Network Management System and Oracle Utilities Smart Grid Gateway integration.	System
<dba.dbuserpassword>	Password used to log in as a Database Administrator (DBA). This database hosts the schema required for Oracle Utilities Network Management System and Oracle Utilities Smart Grid Gateway integration.	

Property (XPath Representation)	Description	Example
<dbusername>	User name used to login to NMS-SGG Error Handling schema for Oracle Utilities Network Management System and Oracle Utilities Smart Grid Gateway integration. This user can be automatically created by the install (set dbuser.createflag to true) or manually outside the install process.	Example: NMSSGGUser
<dbuserpassword>	Password used to log in to NMS-SGG Error Handling schema for Oracle Utilities Network Management System and Oracle Utilities Smart Grid Gateway integration.	
<dbuser.createflag>	Flag specifying whether to create a new schema or use the existing schema for Oracle Utilities Network Management System and Oracle Utilities Smart Grid Gateway 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 Oracle Utilities Network Management System and Oracle Utilities Smart Grid Gateway integration.	db.sample.oracle.com
<dbportnumber>	Database port number used for Oracle Utilities Network Management System and Oracle Utilities Smart Grid Gateway integration.	1521
<dbsid>	Database SID used for Oracle Utilities Network Management System and Oracle Utilities Smart Grid Gateway integration.	SID

Chapter 6

Troubleshooting

This chapter 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 chapter provides steps for:

- Uninstalling the Integration
- Uninstalling the UsageMessagingDriver-Email

Uninstalling the Integration

This section describes how to uninstall the integration.

> **Note**: It is recommended to take a back up of the NMS-SGG PRODUCT_HOME before uninstalling the product.

To uninstall the integration:

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

2. Set the environment variables as mentioned in the Installation Steps section in Chapter 2: Installing the Integration.

3. 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 to:

      • Undeploy all the composites from the Enterprise Manager partition.

      • Delete the partition.

      • Undeploy the MDS artifacts.

   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
   ```

   b. Execute the following commands at the Command prompt to:

      • Undeploy the database outbound connection pool.

      • Delete the JDBC data source for the Error Handling module.

      • Remove the work flow notification that is created.

      • Delete the csf-keys generated.

   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
   ```

   c. Execute the following commands at the Command prompt. These commands drop the database objects created for the Error Handling module and the artifacts created for the integration.

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
```

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