## Contents

### Preface

- Audience ............................................................... vii
- Documentation Accessibility ........................................ vii
- Related Documentation .............................................. vii

### 1 Unified Inventory Management System Administration Overview

- Overview of UIM Administration Tasks .............................. 1-1
- Directory Placeholders Used in This Guide .............................. 1-1

### 2 Starting and Stopping UIM

- About Starting and Stopping UIM ................................. 2-1
- Starting the UIM Server ............................................. 2-1
- Verifying the UIM Server Started .................................. 2-1
- Stopping the UIM Server .......................................... 2-2
- Verifying the UIM Server Stopped .............................. 2-3

### 3 Working with Cartridges and Technology Packs

- Managing UIM Cartridges and Technology Packs .......... 3-1
  - Using the Cartridge Deployer Tool .......................... 3-2
  - Deploying Cartridges ......................................... 3-2
  - Deploying Cartridges on/from a Remote Server ........ 3-4
  - Viewing Deployed Cartridges .............................. 3-5
  - Migrating Cartridges ........................................... 3-6
    - Migrating UIM Base Cartridges ..................... 3-6
    - Migrating UIM Sample and Custom Cartridges ... 3-6
  - Grouping andDeploying Multiple Cartridges ........... 3-7
- Guidelines and Recommended Cartridge and Technology Pack Deployment ................................. 3-9

### 4 Understanding UIM Security

- UIM Security Overview ............................................. 4-1
  - Authentication ...................................................... 4-3
    - Setting the Session Timeout .............................. 4-4
    - Authenticating Web Services .............................. 4-4
  - Authorization ....................................................... 4-5
5 Monitoring and Managing Unified Inventory Management

Monitoring and Managing Overview ................................................................. 5-1
Sharing JAR Files ................................................................................................. 5-1
Disabling the HTTP Port ...................................................................................... 5-3
Setting the Database RowPrefetch Size ............................................................ 5-3
Modifying the Default File Encoding ............................................................... 5-4
Modifying the Time Zone ................................................................................... 5-4
Configuring Your Server's Timers ..................................................................... 5-5
Registering Entities to the LifeCycle Listener .................................................. 5-5
Configuring Exception-Type-to-Error-Code Mappings .................................. 5-5
Localizing UIM Error Messages ........................................................................ 5-5
Localizing the UIM Server and the Application Server ...................................... 5-7
Shutting Down an Application Server ............................................................... 5-7
Configuring the SSL Policy/Certificate ........................................................... 5-7
Resetting/Changing the WebLogic Server’s Database Connections................ 5-9
Setting the Default Telephone Number Edit Mask ............................................ 5-10
Load Balancing a Clustered Server ................................................................... 5-10
Configuring the Load Balancer ......................................................................... 5-11
F5 BIG-IP Configuration Example ..................................................................... 5-11
Cisco CSS 1150X Configuration Example .......................................................... 5-11
Configuring the Proxy Server ............................................................................ 5-12
Configuring Topology Updates ......................................................................... 5-12
Configuring Asynchronous Topology Updates ............................................... 5-12
Turning Off Topology Updates ......................................................................... 5-12
Rebuilding Topology ......................................................................................... 5-12

6 Improving Unified Inventory Management Performance

Improving UIM Performance Overview ............................................................ 6-1
Configuring a Shared Index Directory................................................................. 6-1
Changing the Logging Level .............................................................................. 6-1
  Appender Configuration.................................................................................... 6-1
  Logger Configuration.......................................................................................... 6-3
  Connecting debugger to UIM........................................................................... 6-4
Enabling SQL and Other EclipseLink Logging.................................................. 6-5
Updating the System Configuration Files.......................................................... 6-6
  Updating the castor.properties File............................................................... 6-7
  Updating the config-reload.properties File..................................................... 6-7
  Updating the consumer.properties File.......................................................... 6-8
  Updating the reference.properties File........................................................... 6-9
  Updating the ruleProcess.properties File....................................................... 6-11
  Updating the system-config.properties File.................................................. 6-11
  Updating the timers.properties File............................................................... 6-14
  Updating the topologyProcess.properties File.............................................. 6-15
Setting Timeout Values for UIM........................................................................ 6-17
  Setting the Oracle Database Timeout............................................................. 6-17
  Setting the JTA Timeout.................................................................................. 6-18
Changing the Query Behavior and Row Limit Parameters............................... 6-18

7 Unified Inventory Management Backup and Restore

  WebLogic Server Related Artifacts................................................................. 7-1
  Static Artifacts................................................................................................. 7-1
  Runtime Artifacts............................................................................................. 7-1
  Persistent Stores............................................................................................... 7-1
    Using a Shared File System to Backup the Artifacts...................................... 7-2
    Using the WebLogic Backup Utility.............................................................. 7-2
    Using the Pack and Unpack Utility............................................................... 7-2
  Restoring WebLogic Related Configurations and Artifacts.......................... 7-2
  Embedded LDAP.............................................................................................. 7-2
    Restoring Embedded LDAP Server File...................................................... 7-3
    Export and Import of LDAP Data............................................................... 7-4
    Database Backup and Restore...................................................................... 7-4
    Backup SerializedSystemIni.dat and Security Certificates........................ 7-4

8 Managing the Unified Inventory Management Database

  Overview of Managing the UIM Database...................................................... 8-1
  Tuning the Database......................................................................................... 8-1
Preface

This guide contains information about administering Oracle Communications Unified Inventory Management (UIM). This guide includes information about how to start and stop UIM, working with cartridges and technology packs, an overview of security for UIM, and how to manage and monitor UIM. It also includes information about improving UIM performance, backing up and restoring UIM data, and managing the UIM database.

Note: Documentation on third-party software products is limited to the information needed to use UIM. If you need additional information on a third-party software application, consult the documentation provided by the product’s manufacturer.

Audience

This guide is intended for system administrators and other individuals who are responsible for ensuring that UIM is operating in the manner required for your business.

This document assumes that you have a good working knowledge of Sun Solaris, Windows, UNIX, IBM AIX, Oracle Fusion Middleware 11gR1, Oracle WebLogic, and Java J2EE software.

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 through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documentation

For more information, see the following documents in the Oracle Communications Unified Inventory Management Release 7.2 documentation set:
- **UIM Concepts**: Provides an overview of important concepts and an introduction to using both UIM and Oracle Communications Design Studio.

- **UIM Installation Guide**: Describes the requirements and procedures for installing UIM.

- **UIM Migration Guide**: Provides information about migrating from previous releases of UIM to the current release.

- **UIM Developer’s Guide**: Explains how to customize and extend many aspects of UIM, including the schema, user interface, rule sets, Web services, life-cycle management, topology, security, and localization.

- **UIM Information Model Reference**: Describes the UIM information model entities and data attributes, and explains patterns that are common across all entities.

- **Oracle Communications Information Model Reference**: Describes the Oracle Communications information model entities and data attributes, and explains patterns that are common across all entities. The information described in this reference is common across all Oracle Communications products.

- **UIM Base Cartridges Guide**: Provides descriptions of entities included in base cartridges. These entities are used for all technology domains. Examples include telephone numbers, units of measure, and base rule sets.

- **UIM technology pack implementation guides**: Describe the content of product technology packs as well as configuration guidelines and implementation considerations.

For step-by-step instructions for performing tasks, log in to each application to see the following:


- **UIM Help**: Provides step-by-step instructions for tasks you perform in UIM.
Unified Inventory Management System Administration Overview

This chapter provides an overview of Oracle Communications Unified Inventory Management (UIM) basic administration tasks and the tools to perform those tasks.

Overview of UIM Administration Tasks

A UIM administrator is responsible for the day-to-day tasks of maintaining and managing UIM and its users. The tasks also include managing UIM components and database.

You perform the following tasks as a UIM administrator:

- Starting and stopping the UIM server. See "Starting and Stopping UIM" for more information.
- Managing UIM cartridges and technology packs. See "Working with Cartridges and Technology Packs" for more information.
- Managing UIM security. See "Understanding UIM Security" for more information.
- Monitoring and managing UIM. See "Monitoring and Managing Unified Inventory Management" for more information.
- Improving UIM performance. See "Improving Unified Inventory Management Performance" for more information.
- Backing up and restoring UIM data. See "Unified Inventory Management Backup and Restore" for more information.
- Managing the UIM database. See "Managing the Unified Inventory Management Database" for more information.

Directory Placeholders Used in This Guide

Table 1–1 lists the placeholders that are used in this guide to refer to directories related to the UIM application.
### Table 1–1  Directory Placeholders

<table>
<thead>
<tr>
<th>Placeholder</th>
<th>Default Directory Path</th>
<th>Directory Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MW_Home</td>
<td>/opt/Oracle/Middleware</td>
<td>The location where the Oracle Middleware product was installed. This directory contains the base directory for the WebLogic Server, a utilities directory, and other files and directories.</td>
</tr>
<tr>
<td>WL_Home</td>
<td>/opt/Oracle/Middleware/wlserver_10.3</td>
<td>The base directory for the WebLogic Server core files. It is located in the MW_Home directory.</td>
</tr>
<tr>
<td>Domain_Home</td>
<td>/opt/Oracle/Middleware/user_projects/domains/domain_name</td>
<td>The directory that contains the configuration for the domain into which UIM is typically installed, but it is frequently set to some other directory at installation.</td>
</tr>
<tr>
<td></td>
<td>where domain_name is the name assigned to the domain at installation</td>
<td></td>
</tr>
<tr>
<td>UIM_Home</td>
<td>/opt/Oracle/Middleware/user_projects/domains/domain_name/UIM</td>
<td>The directory into which UIM was installed. This directory contains various installation-related files.</td>
</tr>
<tr>
<td></td>
<td>where domain_name is the name assigned to the domain at installation</td>
<td></td>
</tr>
</tbody>
</table>
This chapter describes how to start and stop Oracle Communications Unified Inventory Management (UIM).

About Starting and Stopping UIM

Because UIM resides on a WebLogic server, starting or stopping the WebLogic server also starts and stops UIM.

---

**Note:** If the UIM environment is in a WebLogic cluster, consult the Oracle WebLogic Server documentation for information about how to start and stop the cluster servers.

---

Starting the UIM Server

To start the UIM server:

1. Open a command window.
2. Navigate to the `Domain_Home/bin` directory.
3. Run the following command:
   ```
   ./startUIM.sh
   ```

**Note:** For managed servers in a cluster, run the following command for each managed server:

```
./startUIM.sh managed_server_name admin_url
```

For example: `./startUIM.sh uim_ms1 machine1.oracle.com:7001`

---

Verifying the UIM Server Started

To verify that the UIM server started:

1. In a Web browser, enter:
   ```
   http://ServerName:Port/console
   ```
2. Enter the WebLogic server administration user name and password.
3. In the Domain Structure tree, expand Environment, and click Servers.
Stopping the UIM Server

The Summary of Servers screen appears.

4. View the state of the AdminServer and see RUNNING.

   If the State is not RUNNING, you may need to wait a short period and refresh the page.

5. In the Domain Structure tree, click Deployments.

   The Summary of Deployments screen appears.

6. Verify that the state of the deployments for the UIM related applications are ACTIVE. The following is a list of the UIM related applications and libraries:
   - oracle.communications.inventory
   - oracle.communications.inventory.cartridgeadapter
   - oracle.communications.inventory.corelib(7.2, 7.2.0.0.0)
   - oracle.communications.inventory.corelib(7.2, 7.2.0.0.0)
   - oracle.communications.inventory.customlib(7.2, 7.2.0.0.0)
   - oracle.communications.inventory.externallib(7.2, 7.2.0.0.0)
   - oracle.communications.inventory.javadoc
   - oracle.communications.inventory.mapviewer

**Note:** If any of the deployments are not in the status you expected, you can use the buttons in this window to start and stop individual deployments, if necessary.

### Stopping the UIM Server

To stop the UIM server:

1. Navigate to the Domain_Home/bin directory.

2. Run the following command:

   ./stopWebLogic.sh

**Note:** You can also stop the UIM server from the WebLogic console, by doing the following:

1. In a Web browser, enter:

   http://ServerName:Port/console

2. Enter the WebLogic server administration user name and password.

3. In the Domain Structure tree, expand Environment, and click Servers.

   The Summary of Servers screen appears.

4. Click the Control tab and select AdminServer.

5. Click Shutdown and select Force Shutdown Now.

   The Server Life Cycle Assistant screen appears.

6. Click Yes.
Verifying the UIM Server Stopped

To verify that UIM has stopped, do one of the following:

- Try connecting to the WebLogic console. If you cannot, WebLogic is probably not running.

- Look at the process list for the user who started the server. If WebLogic is running, there will probably be at least one process with `startUIM.sh` in its description. Look in the user’s process list for a java process that was started out of the Java directory for WebLogic. Process descriptions vary from platform to platform, so look at the process list when you know UIM is running to see what the entries look like on your platform. You can later use this information to confirm that the WebLogic server has shut down completely.

**Note:** The procedure above stops UIM by stopping the Administration server for the WebLogic Server. If the WebLogic Server does not shut down completely, you will not be able to start it again due to a port conflict. If the procedure above has completed, but some WebLogic Server processes are still running for the domain, you can use the `kill` command to stop them. See “Verifying the UIM Server Stopped” for information about verifying whether UIM and WebLogic have stopped completely.
This chapter provides an overview of how you can use cartridges, technology packs, and sample packs to extend Oracle Communications Unified Inventory Management (UIM) with specifications, rules, and other content developed in Oracle Communications Design Studio. You can install the following into UIM:

- **Cartridges**: Cartridges contain UIM extensions, such as specifications, characteristic data elements, rule sets, and extended code. When extending UIM, you can create one or more cartridges, depending on how you choose to organize the extensions. Everything you create in Design Studio (data elements, specifications, and rule sets) resides in a cartridge. The name you choose for the cartridge in Design Studio becomes the name of a JAR file.

- **Technology packs**: A technology pack is a collection of one or more cartridges that addresses a particular technology domain. Oracle provides technology packs as separately licensed products. You can extend technology packs or deploy them directly into UIM. You can also create your own technology packs, which is essentially a cartridge that addresses a particular domain.

- **Sample packs**: Sample packs are cartridges that include sample specifications, extensions, rule sets, and code. Sample packs need to be configured for your environment before they can be deployed into UIM. You configure sample packs by changing environment information within various files. These files may be provided by the sample pack, or by the UIM installation.

### Managing UIM Cartridges and Technology Packs

Managing UIM cartridges includes deploying cartridges, viewing deployed and available cartridges, and migrating older cartridges to the latest version of UIM. This section explains how you manage cartridges and technology packs in a UIM production environment using the Cartridge Deployer Tool.

For more information about managing cartridges and technology packs in a UIM test environment, see the Design Studio Help.

In some cases, cartridges are grouped together to make deployment simpler. See "Grouping and Deploying Multiple Cartridges" for more information.
Managing UIM Cartridges and Technology Packs

Using the Cartridge Deployer Tool

The Cartridge Deployer Tool is a component of UIM. The Oracle Universal Installer installs the Cartridge Deployer Tool as part of the installation process in a location selected by the customer.

Deploying Cartridges

To deploy cartridges:

1. Navigate to $CDT_Home/CartridgeDeployerClients/CartridgeDeployer$ directory.

   where $CDT_Home$ is the directory where the Cartridge Deployer Tool was installed.

2. Run the following command:
   ```
   ./runCartridgeDeployer.sh
   ```

   The Cartridge Deployer Welcome page appears.

3. Select the Deploy Cartridge option and click Next.

   The Select Cartridge Type page appears.

4. From the Cartridge Type list, select Inventory and click Next.

   The Cartridge Location page appears.

5. Click Browse to search for and select the cartridges you want to deploy.

   You can select multiple cartridges from a single directory by holding down the Ctrl key.

   The Cartridge Deployer Tool does not validate cartridge dependencies. If any selected cartridge is dependent upon another cartridge, you must ensure that the cartridge upon which the dependency is based is already deployed or is selected first in the list for deployment.

   **Note:** The customized file browser shows only predefined cartridge extensions. UIM supports cartridges with only the .jar extension.

6. Click Next.
The Configure Deployment Queue page appears.

7. View the details of the selected cartridges and click **Next**.

---

**Note:** To add Deploy property or Model property, under Details for that cartridge, right-click on Properties and select the respective options for related menus.

---

The WebLogic Connection Information page displays.

8. Do the following:

   a. In the **Host name or IP address** field, enter the host name or IP address of the WebLogic Administration Server.

   b. In the **Port number** field, enter the port number of the WebLogic Administration Server.

   c. Select **Use SSL (if enabled) while connecting to WebLogic Admin server**

   d. In the **Keystore location** field, enter the path or click **Browse** to search for the Keystore location.

   e. In the **CMWS User** field, enter the user name of the Cartridge Management Web service (CMWS) user.

---

**Note:** Use your WebLogic administrator or CMWS user name.

The CMWS user is a WebLogic server user belonging to the Cartridge_Management_Webservice group. The Cartridge_Management_Webservice group is also a member of the Administrators group.

---

f. In the **Password** field, enter the password for the CMWS user.

---

**Note:** Use your WebLogic administrator user password.

---

g. Click **Next**.

The Select WebLogic Target page displays.

9. In the list, select the managed server where the CMWS is deployed and click **Next**.

If the Secure Sockets Layer (SSL) is not configured correctly, the following message displays:

SSL Handshaking failed. You can proceed without SSL by unchecking SSL options on the bottom of this screen.

---

**Note:** The SSL handshake fails when the Cartridge Deployer Tool connects to the CMWS using HTTPS.

---

10. If you receive this message, click **OK** in the message dialog box, and deselect the **Use SSL (if enabled) while connecting to Cartridge Management Web service** check box located at the bottom of the page.

11. Click **Next**.
The Review Deployment page displays.

12. Review and confirm your selections and click **Next**.

The Cartridge Deployment page displays.

**Note:** The Cartridge Deployer Tool rejects cartridges if a higher versions already exist. You can view rejected cartridges in the **Cartridges rejected for this deployment session** list.

13. Click **Start Deployment**.

You can view the deployment progress.

Logs returned by the Cartridge Deployer Tool are displayed at the end of each cartridge deployment operation. The logs display whether the cartridge deployment succeeds or fails.

**Note:** If the UIM server goes down during cartridge deployment, the cartridge is recovered after the UIM server is up again, or during the next cartridge deployment session, with the cartridge deployment request showing Failed.

If a cartridge requires redeployment only, the CMWS will redeploy automatically. For more information on redeployment, see the WebLogic server administration console Help.

If a cartridge requires a redeployment and a restart, then you must deploy the cartridge, redeploy the **inventory.ear** file using the WebLogic administration server console, and then restart the server.

**Deploying Cartridges on/from a Remote Server**

**Note:** Oracle recommends that you deploy cartridges onto the server on which UIM is deployed.

To deploy cartridges from a remote server:

**Note:** If the **UIM_Home** directory is located in a shared location, then steps 1 - 4 are not required to be performed.

1. Copy the **uim_custom_lib.ear** file from the administration server to the remote managed server before starting the cartridge deployment.
2. On the remote server, deploy cartridges using the steps provided in the section "Deploying Cartridges".
3. Copy the **uim_custom_lib.ear** file from the remote managed server back to the administration server.
4. Redeploy the **uim_custom_lib.ear** file.

The cartridges are deployed in UIM from the remote managed server.
Managing UIM Cartridges and Technology Packs

Viewing Deployed Cartridges
To view deployed cartridges:

1. Locate the `UIM_home/CartridgeDeployer` directory.
2. From a command line, run the following command to run the Cartridge Deployer Tool executable:

   ```bash
   ./runCartridgeDeployer.sh
   ```
   
The Cartridge Deployer Welcome page displays.
3. Select the **View Deployed Cartridges** option, and click **Next**.

   The Select Cartridge Type page displays.
4. Select **Inventory** in the Cartridge Type list, and click **Next**.

   The WebLogic Connection Information page displays.
5. Do the following:
   a. In the **Host name or IP address** field, enter the host name or IP address of the WebLogic Administration Server.
   b. In the **Port number** field, enter the port number of the WebLogic Administration Server.
   c. In the **CMWS User** field, enter the user name of the Cartridge Management Web service (CMWS) user.
   d. In the **Password** field, enter the password for the CMWS user.
   e. Click **Next**.

   The Select WebLogic Target page displays.
6. Select the WebLogic targets where the Cartridge Management Web service is installed and click **Next**.

   If the SSL is not configured correctly, the following message displays:

   **SSL Handshaking failed. You can proceed without SSL by unchecking SSL options on the bottom of this screen.**

   **Note:** The SSL handshake fails when the Cartridge Deployer Tool connects to the CMWS using HTTPS.
7. Click **OK** in the message dialog box, and deselect the **Use SSL (if enabled) while connecting to Cartridge Management Web service** check box located at the bottom of the page.

8. Click **Next**.

   The Deployed Cartridges page displays.

   This page lists all of the cartridges that are currently deployed in UIM.

**Migrating Cartridges**

If you developed or extended cartridges for a previous version of UIM, you need to migrate them to the current version of UIM so that you can continue to use them.

Follow the correct procedure for each of your cartridges:

- **Migrating UIM Base Cartridges**
- **Migrating UIM Sample and Custom Cartridges**

**Migrating UIM Base Cartridges**

UIM base cartridges are already compatible with the latest version of UIM. Deploy the cartridge into the latest installation of UIM. See "Deploying Cartridges" for more information.

**Migrating UIM Sample and Custom Cartridges**

Sample and custom cartridges (cartridges with binaries not supplied by Oracle) must be migrated to the latest version of UIM. This section assumes that you have two Design Studio environments: one for the previous release and another for the current release.

---

**Note:** Ensure that Design Studio is up to date with the correct plug-ins. See *Oracle Communications Design Studio Installation Guide* for more information.

---

To migrate the cartridge:

1. Using the old installation of Design Studio for UIM, do the following:

---

**Note:** It is recommended that any project dependencies be imported first, before importing the migration cartridge.

---

a. Select the Design Studio perspective.

b. Select the Cartridge view.

c. Select the cartridge project and, from the **Project** menu, deselect **Build Automatically**.

d. From the **Project** menu, select **Clean**.

e. Select the Navigator view.

f. Delete all files and folders from the **cartridgeBuild** and **cartirdgeBin** directories.

  
g. Right-click the cartridge project folder and select **Close Project**.
2. Using the new installation of Design Studio for UIM, do the following:
   a. Select the Design Studio perspective.
   b. Select the Cartridge view.
   c. Right-click anywhere in the Cartridge view and select **Import**.
      
      The Import Project dialog box displays.
   d. Locate the cartridge project and import it.
   e. Double-click the cartridge project folder.
      
      The cartridge properties appear.
   f. In the **Target Version** field, enter 7.2.

   **Note:** If the **Target Version** field is not editable, it may mean that the cartridge is sealed, read-only, or under source control.

   g. Using Windows Explorer, navigate to the cartridge directory.
   h. Open the `.classpath` file and delete all entries that contain the text `kind="lib" path="generated"`. Design Studio generates new entries in the file when the project is built.

   **Note:** If the `.classpath` file is read only, it may mean that it is under source control.

   i. From the **Project** menu, select **Build Automatically**.
   j. From the **Project** menu, select **Clean**.
      
      The cartridge project is automatically built. The JAR file is created and placed in the `cartridgeBin` directory.
   k. Deploy the cartridge into UIM.
      
      See "Deploying Cartridges" for more information.

**Grouping and Deploying Multiple Cartridges**

You can group multiple cartridges into one deployable archive file and then deploy the file into UIM.

The cartridges in a group work together to provide a full domain of capabilities for a functional area of communications inventory. The group of cartridges are deployed as a unit, thus requiring, at most, only one redeployment of the `inventory.ear` file in the WebLogic server administration console.

Your grouping of multiple cartridges is a JAR file that contains individual cartridges that are located in a specific path within that JAR file. For example, the bundled JAR file may contain:

```
meta-inf/cartridges/
custom-cartridge-1.jar
custom-cartridge-2.jar
custom-cartridge-3.jar
```
To group multiple cartridges:

2. Place the Design Studio-built cartridge JAR files into the `meta-inf/cartridges` directory.
3. Create a `MANIFEST.MF` file and include the following properties:
   - Bundle-Name: `<Unique name for this bundle>`
   - Bundle-Version: `<5 digit version number>`
   - Bundle-BuildTime: `<yyy-mm-dd hh:mm:ss>`
   - Bundle-BuildNumber: `<Build Number>`
   - Bundle-Category: `Inventory` (Optional)
   - Bundle-RequiredExecutionEnvironment:
     Oracle-Communications/Inventory-7.2.0, JavaSE-1.6 (Optional)
   - Bundle-RequiredTargetVersion: `7.2.0` (Optional)
4. Place the file into the `meta-inf` directory.
5. Navigate to the parent folder of `meta-inf`.
6. Open a command window.
7. Run the following command:

   `jar cfM your-bundle-name.jar *.*`

   where `your-bundle-name` is the name of the bundle to be created.

The group is deployed into UIM in the same manner as a single cartridge.

---

**Note:** A group can only be managed using the Cartridge Deployer Tool; A group cannot be managed using Design Studio. If you are using Design Studio to manage cartridges in a test environment, and you need to manage a group in that test environment, you need to use the Cartridge Deployer Tool. You can use Design Studio and the Cartridge Deployer Tool together in a test environment. That is, you can manage single cartridges using Design Studio and manage group cartridges using the Cartridge Deployer Tool.

---

If the group of cartridges is successfully deployed, the message `your-bundle-name has been installed` appears.

The list of cartridges that are contained in the group is displayed in the Installed Cartridges table, in the Cartridge Management page.

The Cartridge Deployer Tool determines the appropriate order in which the cartridges are deployed, based on the dependencies of each cartridge.

To automate this process, use an Ant script to create the group. See *UIM Developer’s Guide* for more information.
Guidelines and Recommended Cartridge and Technology Pack Deployment

If unexpected issues occur while you deploy a cartridge, or when you are accessing data through the UIM user interface, read the message that displays to troubleshoot the cause of the issue.

Common deployment errors occur for the following reasons:

- The Design Studio project from which the cartridge was built has an error. Check the Problems view in Design Studio for error information, and then correct any problems before redeploying the cartridge into UIM. See the Design Studio Help for more information.

- The UIM database data model does not match the version of the data model that Design Studio used to build the cartridge.

  If you build a cartridge that relies on features found in an older version of the data model, deploying the cartridge into a UIM instance with a newer data model can result in deployment errors. Ensure that the data model that you use is the same version in both Design Studio and UIM.

- The UIM version is not compatible with the version of Design Studio used to build the cartridge.

  In this situation, the UIM cartridge reader encounters information it cannot handle and throws an error. Make sure you use the version of Design Studio and the Inventory plug-in that corresponds to your UIM version. If necessary, rebuild cartridges with the correct Design Studio version.

  Design Studio operates without a connection to the UIM database, so it is possible to create cartridges that are structured correctly in Design Studio but do not deploy properly into UIM. Ensure that the target UIM environment is configured with the correct schema, parameters, and base data that match the version of Design Studio being used.

- The cartridge being deployed is dependent on another cartridge that has not yet been deployed.

  Correct this by deploying the base or parent cartridge and then redeploying the cartridge that is dependent on the parent cartridge. A message displays telling you which cartridges are required if you try to deploy a child cartridge without the base.

- There have been intermittent instances where technology pack deployment was causing the policy store to be corrupted (especially when permgen out of memory error is encountered when redeploying the UIM application as part of a technology pack deployment). Oracle recommends that before deploying any technology packs, a backup is taken of the policy store file located at:

  Domain_Home/config/fmwconfig/system-jazn-data.xml

  Upon deployment of the technology pack, when the user is not able to login or upon login if the user is not able to see the links in the application, copy the backed up policy store to Domain_Home/config/fmwconfig, replacing the existing policy store and then restart the managed servers.

In some cases, cartridges can be deployed with errors and you experience inconsistencies or unexpected behavior of the UIM data after the deployment. These issues can be avoided by following the recommended guides for upgrading and extending cartridges and technology packs. See UIM Concepts for more information.
This chapter provides an overview of security in Oracle Communications Unified Inventory Management (UIM). You manage most aspects of UIM security externally rather than in the application itself. This chapter does not provide detailed information about how you perform application security tasks in external systems. Consult the documentation for these systems for more information.

UIM Security Overview

UIM supports two categories of application security:

- Authentication is the process of identifying users (including computer processes) by user name and password to ensure that they are allowed to access the system. See "Authentication" for more information.

- Authorization controls access to specific parts of UIM, such as pages, actions, and data entities. Users are granted access as the result of being assigned to security roles, which are in turn associated with security policies. For example, when an authenticated user logs in to UIM, the content of the main UIM work area depends on their level of access. Users with unrestricted access see links to all pages in the Tasks pane; others see only links to the pages they are authorized to access. See "Authorization" for more information.

Figure 4–1 illustrates a simple authentication and authorization flow. A user logs in to UIM, searches for an entity (in this case, a Network entity), views the Summary work area of that entity, and then opens the Network Information work area to edit data.
By default, you use two external systems to manage most aspects of UIM security:

- WebLogic Server Administration Console enables you to manage users and groups. You create and delete users and assign passwords in this application.
- Oracle Enterprise Manager enables you to create security roles and security policies that define what pages users can access and what actions they can take.
The default systems provide a low-cost, basic set of security features. You can use the following tools, which provide additional security functionality.

- Oracle Internet Directory is an LDAP-compliant security directory that runs on the Oracle database. It is fully integrated into Oracle Fusion Middleware.
- Oracle Identity Management is an enterprise-scale tool for managing the end-to-end life cycle of user identities across all resources. Oracle Identity Management is a member of the Oracle Fusion Middleware family of products.

The use of non-default systems requires configuration of both WebLogic Server and the systems themselves. See the WebLogic Server and the third-party documentation for information.

Entity security is performed by the application itself. API security must be implemented through the extensibility framework. See UIM Developer’s Guide for more information about implementing these kinds of security.

**Authentication**

Authentication verifies that you are who you claim to be. UIM requires authentication by user name and password before allowing you access to the application. Login name and password are required for access to the application home page or via direct URL to a specific work area.

---

**Note:** UIM requires a separate sign on from other Oracle Communications applications. Single Sign On (SSO) is not enabled.

---

The UIM login page is configured to not allow auto-completion of user names and passwords. Password text is not echoed to the field as you type. If you enter an invalid user name or password, an error message is displayed.

A configurable period of user inactivity results in a session timeout. The user must provide a user name and password to resume activity. The default session timeout is 30 minutes, but you can configure a different one. See "Setting the Session Timeout".

Access to UIM from Web services also requires a user name and password. The user name and password are passed into the system in the Simple Object Access Protocol (SOAP) header of each message.

---

**Note:** Web services are delivered over unencrypted channels, such as HTTP and Java message service (JMS) transports. The user name and password are included in the SOAP headers of the Web service messages. When transported over an unencrypted channel, passwords must not be passed as clear text. To avoid this vulnerability, use a digest password (encrypted hash) instead.

---

You manage user names and passwords in the WebLogic Server Administration Console (or another application of your choice). The actual authentication process is performed by the Default Authentication provider or the authentication provider provided by the chosen LDAP. The WebLogic Server Administration Console uses embedded LDAP by default.

Password requirements are determined by the authentication provider. In the case of WebLogic Server Embedded LDAP, passwords must be a minimum of eight
characters and include at least one numerical and one alphabetic character. Password expiration policies are also determined by the authentication provider.

You can create groups that include similar users. Grouping users makes it easier to set up authorization. You can assign a group to a role, which automatically grants all permissions associated with the role to all members of the group.

See the WebLogic Server Administration Console documentation and Help for information about creating, deleting, and managing users, groups, and passwords.

To grant access to individual pages and actions in UIM, you associate users and groups with security roles, which are in turn associated with security policies. See “Authorization” for more information.

Setting the Session Timeout

By default, a user session times out after 30 minutes of inactivity. The user must log back in to UIM if the session times out.

You can modify the session timeout in WebLogic Server Administration Console. Enter the new value in the Session Timeout (in seconds) value in the Configuration tab for the oracle.communications.uimapp application.

See the WebLogic Server Administration Console documentation and online Help for additional information.

Authenticating Web Services

Web service operations require authentication to ensure that the Web service operations have the correct permissions to access the application.

You use the WebLogic Server Administration Console to configure authorization for Web services. You configure authentication by associating a Web service to one or more Web service policies. Web service policies specify the details of the message-level security (digital signatures and encryption) and reliable SOAP messaging capabilities of a Web service.

Policies can be attached to the Web service endpoint, which means that the policy assertions apply to the entire Web service, or at the operation level, which means that the policy assertions apply only to the specific operation.

Web services are defined and stored in one or more Web service policy files. A sample Web service policy file (UIM_Home/webservices/reference_webservice.zip/security/SampleAuth.xml) is shipped with UIM. You can use that file or create additional files. See UIM Developer’s Guide for information about how to create Web service policy files.

You associate Web services and Web service policies in the WebLogic Server Administration Console. The following procedure describes at a high level how to make this association. See the WebLogic Server Administration Console documentation and online Help for detailed instructions.

You can associate a policy to a Web service without having to restart the server.

1. In the WebLogic Server Administration Console, open the Settings page for the UIM deployment (oracle.communications.uimapp).

2. In the Modules and Components area, select the Web service you want to configure.

   For example, to configure the Service Fulfillment Web service, click the oracle.communications.inventory.sfws.ws.UIMServiceFulfillmentPortImpl link.
3. Click the Configuration tab.
   The Settings page for the Web service appears.

4. Click the WS-Policy tab.
   The table of Web service endpoints and operations appears. The table also displays current Web service policies.

5. Click Lock & Edit.

6. Select a Web service endpoint or operation.
   The Configure a Web service policy page appears.

7. Select a pre-packaged or a custom Web service policy file and then click the right arrow.

8. Click OK.
   The Save Deployment Plan Assistant page appears.

9. Click the link next to Location.


11. Click Finish.

Note: Refer to Developing Custom Web Services in the UIM Developer’s Guide for more detail.

Authorization

Authorization determines whether an authenticated user has permission to view a work area or to take an action. For example, if an authenticated user does not have permission to view or change telephone number information, the link to the Telephone Number Search work area does not appear in the Tasks panel of the UIM home page. Similarly, the user would be denied access from a direct URL to a Telephone Number Summary work area.

There are two types of authorization in UIM:

- Taskflow authorization controls the ability to view UIM work areas, such as entity Summary work areas. See "Taskflow Permissions" for a complete list.
- Resource authorization controls the ability to take actions, such as deleting or validating an entity. These actions are triggered by clicking a button or making selections from the Actions menu. See "Resource Permissions" for a complete list.

Users are granted permissions by their assignment to security roles and security policies.

- Security roles define groups of users that require particular kinds of access. For example, you can define a role for users who must be able to view but not change telephone number information. You could define another role for users who need to be able make changes to telephone numbers.
- Security policies are groups of permissions that grant access to pages and actions. You associate security roles to security policies to define the access granted to users who are assigned to those roles. For example, to grant view access for telephone numbers, you can create a policy that includes permissions to view the Telephone Number Summary and Telephone Number Search Results pages.
You use Oracle Enterprise Manager (or another system of your choice) to administer roles and policies for UIM. Changes you make are applied immediately without the need to restart the server. User permission changes require that the user log out and log in again.

UIM provides the ability to extend its security so that customers can create their own custom ways of authorizing what users see. See *UIM Developer’s Guide* for more information.

**Using Security Roles**

You create security roles that define the access levels appropriate for users performing particular functions. You can create as many roles as you need and you can assign as many or as few roles to a user as is necessary.

For example, you can assign Jaime to a **Number_Admin** role, allowing him to both view and edit telephone number entities. You can assign Jagdeep to both **Number_Admin** and **Service_Admin** roles, allowing her to view and edit telephone number entities and service entities.

The actual permissions associated with any role are the result of the role being associated with security policies. Each policy defines access to a work area or action in UIM. See "Using Security Policies".

All users are assigned to a default role called **authenticated-role**. This role grants no access except the ability to log in to UIM. A user with only this level of access can view the UIM home page, but cannot view any other UIM pages or take any actions.

Another default role, **uimuser**, grants super user permissions. Users assigned to this role can access all UIM pages and actions. In some cases, such as in testing or development environments, this may be the only role that is required.

You use Oracle Enterprise Manager to create roles and to assign users to them. You can assign users when you create roles. You can also update existing roles by adding and removing users. See the Oracle Enterprise Manager documentation and online Help for more information.

**Using Security Policies**

You use security policies to associate specific permissions, such as the ability to view the Logical Device Search Results work areas or make changes to Equipment entities, with roles. Policies are groupings of specific permissions that you grant to users assigned to roles.

---

**Note:** It is possible to associate policies directly with users, but using roles reduces duplicative work and is therefore recommended.

---

Because there are separate permissions for each UIM work area and for the ability to make changes on those work areas, there are a large number of specific permissions that can be assigned. As a result, you can tailor policies to grant exactly the permissions required for a role.

For example, suppose you have two roles associated with telephone numbers. One role (**Number_User**) is associated with a policy that includes permissions for viewing Telephone Number Summary and Search Results work areas. Another role (**Number_Admin**) is associated with a policy that includes those same permissions as well as permission to edit telephone number information.
You use Oracle Enterprise Manager to manage policies. To create policies, you gather together the permissions that apply to a role or roles and then associate those permissions to the roles.

**Figure 4–2** shows a portion of the Oracle Enterprise Manager Application Policies page. The highlighted area represents the permissions associated with **Number_Admin_Role**. The full names of the three permissions associated with that role are:

- `/WEB-INF/oracle/communications/inventory/ui/number/flow/TelephoneNumberSearchResultsFlow.xml#TelephoneNumberSearchResultsFlow`
- `/WEB-INF/oracle/communications/inventory/ui/number/flow/TelephoneNumberSummaryFlow.xml#TelephoneNumberSummaryFlow`
- `/WEB-INF/oracle/communications/inventory/ui/number/flow/TelephoneNumberEditFlow.xml#TelephoneNumberEditFlow`

**Note:** The permission strings are too long to be fully visible in Oracle Enterprise Manager Application Policies page. See “Taskflow Permissions” and “Resource Permissions” for a list of all of the permissions at full length.

The Oracle Enterprise Manager Application Policies page lists all the policies defined for the application, including the policies for the default **authenticated-role** and **uim_user** roles.

See the Oracle Enterprise Manager documentation and online Help for detailed information about working with policies.

**Figure 4–2  Security Policies in Oracle Enterprise Manager**

<table>
<thead>
<tr>
<th>Principal</th>
<th>Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number_Admin_Role</td>
<td>oracle.adf.controller.security.TaskFlowPermission ()</td>
</tr>
<tr>
<td></td>
<td>/WEB-INF/oracle/communications/inventory/ui/number/flow/TelephoneNumberSearchResultsFlow</td>
</tr>
<tr>
<td></td>
<td>/WEB-INF/oracle/communications/inventory/ui/number/flow/TelephoneNumberSummaryFlow</td>
</tr>
<tr>
<td></td>
<td>/WEB-INF/oracle/communications/inventory/ui/number/flow/TelephoneNumberEditFlow</td>
</tr>
<tr>
<td>Network_Admin_Role</td>
<td>oracle.adf.controller.security.TaskFlowPermission ()</td>
</tr>
<tr>
<td></td>
<td>/WEB-INF/oracle/communications/inventory/ui/network/flow/MapPage</td>
</tr>
<tr>
<td></td>
<td>/WEB-INF/oracle/communications/inventory/ui/network/flow/MapWeb</td>
</tr>
<tr>
<td></td>
<td>/WEB-INF/oracle/communications/inventory/ui/network/flow/Network</td>
</tr>
<tr>
<td></td>
<td>/WEB-INF/oracle/communications/inventory/ui/network/flow/Network1</td>
</tr>
<tr>
<td></td>
<td>/WEB-INF/oracle/communications/inventory/ui/network/flow/Network2</td>
</tr>
<tr>
<td></td>
<td>/WEB-INF/oracle/communications/inventory/ui/network/flow/Network3</td>
</tr>
<tr>
<td></td>
<td>/WEB-INF/oracle/communications/inventory/ui/network/flow/Network4</td>
</tr>
<tr>
<td></td>
<td>/WEB-INF/oracle/communications/inventory/ui/network/flow/Network5</td>
</tr>
<tr>
<td></td>
<td>/WEB-INF/oracle/communications/inventory/ui/network/flow/Network6</td>
</tr>
<tr>
<td></td>
<td>/WEB-INF/oracle/communications/inventory/ui/network/flow/Network7</td>
</tr>
<tr>
<td></td>
<td>/WEB-INF/oracle/communications/inventory/ui/network/flow/Network8</td>
</tr>
<tr>
<td></td>
<td>/WEB-INF/oracle/communications/inventory/ui/network/flow/Network9</td>
</tr>
</tbody>
</table>

**Changing Security Policy Providers**

By default, Oracle Enterprise Manager uses an XML file as the security policy store. This file, `Domain_home/config/fmwconfig/system-jazn-data.xml`, is installed automatically during the WebLogic and UIM installations.
You can configure Oracle Enterprise Manager to use a different policy store instead of the default XML file. For example, you may have a pre-existing LDAP server that you want to use for this purpose.

You specify the security policy store in the Enterprise Manager Security Provider Configuration page. See the Oracle Enterprise Manager Help and documentation for detailed instructions.

**Taskflow Permissions**

Table 4-1 lists all of the UIM taskflow permissions, sorted by component name.

<table>
<thead>
<tr>
<th>Component</th>
<th>Access Type</th>
<th>Permission String</th>
<th>Controls the Ability to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Interaction</td>
<td>Edit</td>
<td>/WEB-INF/oracle/communications/inventory/ui/businessinteraction/flow/BusinessInteractionEditFlow.xml#BusinessInteractionEditFlow</td>
<td>Edit a business interaction from search results or the Summary work area.</td>
</tr>
<tr>
<td>Business Interaction</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/businessinteraction/flow/BusinessInteractionSearchResultsFlow.xml#BusinessInteractionSearchResultsFlow</td>
<td>Open a Search work area for business interactions by clicking the Business Interactions link in the Tasks panel.</td>
</tr>
<tr>
<td>Custom Network Address</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/customnetworkaddress/flow/CustomNetworkAddressSearchResultsFlow.xml#CustomNetworkAddressSearchResultsFlow</td>
<td>Open a Search work area for custom network addresses by clicking the Custom Network Address link in the Tasks panel.</td>
</tr>
<tr>
<td>Custom Network Address</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/customnetworkaddress/flow/CustomNetworkAddressSummaryFlow.xml#CustomNetworkAddressSummaryFlow</td>
<td>Open a Custom Network Address Summary work area.</td>
</tr>
<tr>
<td>Custom Network Address</td>
<td>Edit</td>
<td>/WEB-INF/oracle/communications/inventory/ui/customnetworkaddress/flow/CustomNetworkAddressEditFlow.xml#CustomNetworkAddressEditFlow</td>
<td>Edit a custom network address from search results or a Summary work area.</td>
</tr>
<tr>
<td>Condition</td>
<td>Edit</td>
<td>/WEB-INF/oracle/communications/inventory/ui/condition/flow/ConditionEditFlow.xml#ConditionEditFlow</td>
<td>Edit a condition by opening its work area from the Related Pages menu in an entity work area.</td>
</tr>
<tr>
<td>Condition</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/condition/flow/ConditionListFlow.xml#ConditionListFlow</td>
<td>Open the list of conditions associated by using the Related Pages menu in an entity work area.</td>
</tr>
<tr>
<td>Configuration</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/configuration/flow/ConfigurationSummaryFlow.xml#ConfigurationSummaryFlow</td>
<td>Open a Configuration Summary work area. (For all configurations except Pipe.)</td>
</tr>
</tbody>
</table>
Table 4–1 (Cont.) Taskflow Permissions

<table>
<thead>
<tr>
<th>Component</th>
<th>Access Type</th>
<th>Permission String</th>
<th>Controls the Ability to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>Edit</td>
<td>/WEB-INF/oracle/communications/inventory/ui/configuration/flow/...</td>
<td>Edit an entity configuration. (For all configurations except Pipe.)</td>
</tr>
<tr>
<td>Configuration</td>
<td>Edit</td>
<td>/WEB-INF/oracle/communications/inventory/ui/configuration/flow/...</td>
<td>Add a configuration item from a Configuration Summary work area. (For all configurations, except Pipe.)</td>
</tr>
<tr>
<td>Configuration</td>
<td>Edit</td>
<td>/WEB-INF/oracle/communications/inventory/ui/configuration/flow/...</td>
<td>Rename a configuration item in a Configuration Summary work area</td>
</tr>
<tr>
<td>Configuration</td>
<td>Edit</td>
<td>/WEB-INF/oracle/communications/inventory/ui/configuration/flow/...</td>
<td>Edit configuration characteristics.</td>
</tr>
<tr>
<td>Consumer</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/consumer/flow/...</td>
<td>View telephone number assignments in a Telephone Number Summary work area.</td>
</tr>
<tr>
<td>Custom Object</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/customobject/flow/...</td>
<td>Open a Search work area for custom objects by clicking the Custom Objects link in the Tasks panel.</td>
</tr>
<tr>
<td>Custom Object</td>
<td>Edit</td>
<td>/WEB-INF/oracle/communications/inventory/ui/customobject/flow/...</td>
<td>Edit a custom object from search results or a Summary work area.</td>
</tr>
<tr>
<td>Device Interface</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/deviceinterface/flow/...</td>
<td>Open a Search work area for device interfaces by clicking the Device Interface link in the Tasks panel.</td>
</tr>
<tr>
<td>Device Interface</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/deviceinterface/flow/...</td>
<td>Open a Device Interface Summary work area.</td>
</tr>
<tr>
<td>Device Interface</td>
<td>Edit</td>
<td>/WEB-INF/oracle/communications/inventory/ui/deviceinterface/flow/...</td>
<td>Edit a device interface from a device interface hierarchy.</td>
</tr>
<tr>
<td>Device Interface</td>
<td>Edit</td>
<td>/WEB-INF/oracle/communications/inventory/ui/deviceinterface/flow/...</td>
<td>Open a Search work area for equipment by clicking the Equipment link in the Tasks panel.</td>
</tr>
<tr>
<td>Equipment</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/equipment/flow/...</td>
<td>Open an Equipment Summary work area.</td>
</tr>
<tr>
<td>Equipment</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/equipment/flow/...</td>
<td>Open an Equipment Visual work area.</td>
</tr>
<tr>
<td>Equipment</td>
<td>Edit</td>
<td>/WEB-INF/oracle/communications/inventory/ui/equipment/flow/...</td>
<td>Edit an Equipment entity from search results or a Summary work area.</td>
</tr>
</tbody>
</table>
### Table 4–1 (Cont.) Taskflow Permissions

<table>
<thead>
<tr>
<th>Component</th>
<th>Access Type</th>
<th>Permission String</th>
<th>Controls the Ability to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equipment Holder</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/equipmentholder/flow/EquipmentHolderSearchResultsFlow</td>
<td>Open a Search work area for device interfaces by clicking the Device Interface link in the Tasks panel.</td>
</tr>
<tr>
<td>Favorite Items</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/platform/cui/flow/FavoriteItemsFlow.xml#FavoriteItemsFlow</td>
<td>View the Favorites menu in the UIM main page.</td>
</tr>
<tr>
<td>Favorite Items</td>
<td>Edit</td>
<td>/WEB-INF/oracle/communications/platform/cui/flow/ManageFavoritesFlow.xml#ManageFavoritesFlow</td>
<td>Edit the contents of the Favorites menu in the UIM main page.</td>
</tr>
<tr>
<td>Import</td>
<td>Edit</td>
<td>/WEB-INF/oracle/communications/inventory/ui/admin/flow/ExecuteRuleFlow.xml#ExecuteRuleFlow</td>
<td>View the Inventory Import work area.</td>
</tr>
<tr>
<td>Inventory Group</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/inventorygroup/flow/InventoryGroupSearchResultsFlow.xml#InventoryGroupSearchResultsFlow</td>
<td>Open a Search work area for inventory groups by clicking the Inventory Group link in the Tasks panel.</td>
</tr>
<tr>
<td>Inventory Group</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/inventorygroup/flow/InventoryGroupSummaryFlow.xml#InventoryGroupSummaryFlow</td>
<td>View an Inventory Group Summary work area.</td>
</tr>
<tr>
<td>Inventory Group</td>
<td>Edit</td>
<td>/WEB-INF/oracle/communications/inventory/ui/inventorygroup/flow/InventoryGroupEditFlow.xml#InventoryGroupEditFlow</td>
<td>Edit an inventory group from search results or a Summary work area.</td>
</tr>
<tr>
<td>Involvement</td>
<td>Edit</td>
<td>/WEB-INF/oracle/communications/inventory/ui/custominvolvement/flow/CustomInvolvementEditFlow.xml#CustomInvolvementEditFlow</td>
<td>Edit a custom involvement from an entity Summary page. The user can edit the custom involvement by clicking Edit in the Custom Involvement list in the entity Summary page.</td>
</tr>
<tr>
<td>Logical Device</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/logicaldevice/flow/LogicalDeviceSearchResultsFlow.xml#LogicalDeviceSearchResultsFlow</td>
<td>Open a Search work area for logical devices by clicking the Logical Device link in the Tasks panel.</td>
</tr>
<tr>
<td>Logical Device</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/logicaldevice/flow/LogicalDeviceSummaryFlow.xml#LogicalDeviceSummaryFlow</td>
<td>Open a Logical Device Summary work area.</td>
</tr>
<tr>
<td>Logical Device</td>
<td>Edit</td>
<td>/WEB-INF/oracle/communications/inventory/ui/logicaldevice/flow/LogicalDeviceEditFlow.xml#LogicalDeviceEditFlow</td>
<td>Edit a logical device from search results or a Summary work area.</td>
</tr>
<tr>
<td>Logical Device</td>
<td>Edit</td>
<td>/WEB-INF/oracle/communications/inventory/ui/device/MaintainMappingsFlow.xml#MaintainMappingsFlow</td>
<td>Map a device interface to a physical connector or physical port.</td>
</tr>
<tr>
<td>Logical Device Account</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/logicaldeviceaccount/flow/LogicalDeviceAccountSearchResultsFlow.xml#LogicalDeviceAccountSearchResultsFlow</td>
<td>Open a Search work area for logical device accounts by clicking the Logical Device Account link in the Tasks panel.</td>
</tr>
<tr>
<td>Logical Device Account</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/logicaldeviceaccount/flow/LogicalDeviceAccountSummaryFlow.xml#LogicalDeviceAccountSummaryFlow</td>
<td>Open a Logical Device Account Summary work area.</td>
</tr>
</tbody>
</table>
### Table 4–1 (Cont.) Taskflow Permissions

<table>
<thead>
<tr>
<th>Component</th>
<th>Access Type</th>
<th>Permission String</th>
<th>Controls the Ability to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical Device Account</td>
<td>Edit</td>
<td>/WEB-INF/oracle.communications/inventory/ui/logicaldeviceaccount/flow/LogicalDeviceAccountEditFlow.xml#LogicalDeviceAccountEditFlow</td>
<td>Edit a logical device account from search results or a Summary work area.</td>
</tr>
<tr>
<td>Map Profile</td>
<td>Edit</td>
<td>/WEB-INF/oracle.communications/inventory/ui/network/flow/MapProfileEditFlow.xml#MapProfileEditFlow</td>
<td>Edit a the map profile from a Network Summary work area.</td>
</tr>
<tr>
<td>Map Viewer</td>
<td>View</td>
<td>/WEB-INF/oracle.communications/inventory/ui/network/flow/MapViewFlow.xml#MapViewFlow</td>
<td>Open the Map Viewer application.</td>
</tr>
<tr>
<td>Media Resource View</td>
<td>View</td>
<td>/WEB-INF/oracle.communications/inventory/ui/mediaresource/flow/MediaResourceLogicalDeviceListFlow.xml#MediaResourceLogicalDeviceListFlow</td>
<td>Open a list of media resources in a Logical Device or Media Stream Summary work area.</td>
</tr>
<tr>
<td>Media Stream</td>
<td>View</td>
<td>/WEB-INF/oracle.communications/inventory/ui/mediaresource/flow/MediaStreamSearchResultsFlow.xml#MediaStreamSearchResultsFlow</td>
<td>Open a Search work area for media streams by clicking the Media Streams link in the Tasks panel.</td>
</tr>
<tr>
<td>Media Stream</td>
<td>View</td>
<td>/WEB-INF/oracle.communications/inventory/ui/mediaresource/flow/MediaStreamSummaryFlow.xml#MediaStreamSummaryFlow</td>
<td>Open a Media Stream Summary work area.</td>
</tr>
<tr>
<td>Media Stream</td>
<td>Edit</td>
<td>/WEB-INF/oracle.communications/inventory/ui/mediaresource/flow/MediaStreamEditFlow.xml#MediaStreamEditFlow</td>
<td>Edit a Media Stream entity from search results or a Summary work area.</td>
</tr>
<tr>
<td>Network</td>
<td>View</td>
<td>/WEB-INF/oracle.communications/inventory/ui/networknode/flow/NetworkNodeSearchResultsFlow.xml#NetworkNodeSearchResultsFlow</td>
<td>Open a Search work area for network nodes. The work area is opened from the topology visualization.</td>
</tr>
<tr>
<td>Network</td>
<td>View</td>
<td>/WEB-INF/oracle.communications/inventory/ui/network/flow/NetworkSearchResultsFlow.xml#NetworkSearchResults</td>
<td>Open a Search work area for Network entities by clicking the Network link in the Tasks panel.</td>
</tr>
<tr>
<td>Network</td>
<td>Edit</td>
<td>/WEB-INF/oracle.communications/inventory/ui/networkedge/flow/NetworkEdgeEditFlow.xml#NetworkEdgeEditFlow</td>
<td>Edit a network edge from Network canvas.</td>
</tr>
<tr>
<td>Network</td>
<td>Edit</td>
<td>/WEB-INF/oracle.communications/inventory/ui/network/flow/NetworkEditFlow.xml#NetworkEditFlow</td>
<td>Edit a Network entity from search results or a Summary work area.</td>
</tr>
<tr>
<td>Party</td>
<td>View</td>
<td>/WEB-INF/oracle.communications/inventory/ui/party/flow/PartySearchResultsFlow.xml#PartySearchResultsFlow</td>
<td>Open a Search work area for parties by clicking the Party link in the Tasks panel.</td>
</tr>
<tr>
<td>Party</td>
<td>View</td>
<td>/WEB-INF/oracle.communications/inventory/ui/party/flow/PartySummaryFlow.xml#PartySummaryFlow</td>
<td>Open a Party Summary work area.</td>
</tr>
<tr>
<td>Party</td>
<td>Edit</td>
<td>/WEB-INF/oracle.communications/inventory/ui/party/flow/PartyEditFlow.xml#PartyEditFlow</td>
<td>Edit a party from search results or a Summary work area.</td>
</tr>
</tbody>
</table>
### Table 4-1 (Cont.) Taskflow Permissions

<table>
<thead>
<tr>
<th>Component</th>
<th>Access Type</th>
<th>Permission String</th>
<th>Controls the Ability to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path Analysis</td>
<td>Edit</td>
<td>/WEB-INF/oracle/communications/inventory/ui/communications/flow/PathAnalysisFlow.xml#PathAnalysisFlow</td>
<td>Open a Path Analysis work area from a Pipe or Pipe Configuration work area.</td>
</tr>
<tr>
<td>Physical Connector</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/physicalconnector/flow/PhysicalConnectorSearchResultsFlow.xml#PhysicalConnectorSearchResultsFlow</td>
<td>Open a Search work area for physical connectors from a Physical Device or Equipment Summary work area.</td>
</tr>
<tr>
<td>Physical Connector</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/physicalconnector/flow/PhysicalConnectorSummaryFlow.xml#PhysicalConnectorSummaryFlow</td>
<td>Open a Physical Connector Summary work area from a Physical Device or Equipment Summary work area.</td>
</tr>
<tr>
<td>Physical Connector</td>
<td>Edit</td>
<td>/WEB-INF/oracle/communications/inventory/ui/physicalconnector/flow/PhysicalConnectorEditFlow.xml#PhysicalConnectorEditFlow</td>
<td>Edit a physical connector from a Physical Device or Equipment Summary work area.</td>
</tr>
<tr>
<td>Physical Device</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/physicaldevice/flow/PhysicalDeviceSearchResultsFlow.xml#PhysicalDeviceSearchResultsFlow</td>
<td>Open a Search work area for physical devices by clicking the Physical Device link in the Tasks panel.</td>
</tr>
<tr>
<td>Physical Device</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/physicaldevice/flow/PhysicalDeviceSummaryFlow.xml#PhysicalDeviceSummaryFlow</td>
<td>Open a Physical Device Summary work area.</td>
</tr>
<tr>
<td>Physical Device</td>
<td>Edit</td>
<td>/WEB-INF/oracle/communications/inventory/ui/physicaldevice/flow/PhysicalDeviceEditFlow.xml#PhysicalDeviceEditFlow</td>
<td>Edit a physical device from search results or a Summary work area.</td>
</tr>
<tr>
<td>Physical Port</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/physicalport/flow/PhysicalPortSearchResultsFlow.xml#PhysicalPortSearchResultsFlow</td>
<td>Open a Search work area for physical ports from a Physical Device or Equipment Summary work area.</td>
</tr>
<tr>
<td>Physical Port</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/physicalport/flow/PhysicalPortSummaryFlow.xml#PhysicalPortSummaryFlow</td>
<td>Open a Physical Port Summary page from a Physical Device or Equipment Summary work area.</td>
</tr>
<tr>
<td>Physical Port</td>
<td>Edit</td>
<td>/WEB-INF/oracle/communications/inventory/ui/physicalport/flow/PhysicalPortEditFlow.xml#PhysicalPortEditFlow</td>
<td>Edit a physical port from a Physical Device or Equipment Summary work area.</td>
</tr>
<tr>
<td>Pipe</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/communications/flow/EnabledbyViewFlow.xml#EnabledbyViewFlow</td>
<td>Open an Enabled by Visualization work area from a Pipe Summary work area.</td>
</tr>
<tr>
<td>Pipe</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/configuration/flow/PipeConfigurationTrailListFlow.xml#PipeConfigurationTrailListFlow</td>
<td>Open an Enabled By Visualization work area in a Pipe Configuration Summary work area.</td>
</tr>
<tr>
<td>Pipe</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/communications/flow/PipeSearchResultsFlow.xml#PipeSearchResultsFlow</td>
<td>Open a Search work area for pipes by clicking the Pipe link in the Tasks panel.</td>
</tr>
<tr>
<td>Pipe</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/communications/flow/PipeSummaryFlow.xml#PipeSummaryFlow</td>
<td>Open a Pipe Summary work area.</td>
</tr>
<tr>
<td>Pipe</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/communications/flow/PipeTerminationPointSearchResultsFlow.xml#PipeTerminationPointSearchResultsFlow</td>
<td>Open a Search work area for pipe termination points.</td>
</tr>
</tbody>
</table>
**Table 4–1 (Cont.) Taskflow Permissions**

<table>
<thead>
<tr>
<th>Component</th>
<th>Access Type</th>
<th>Permission String</th>
<th>Controls the Ability to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pipe</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/connectivity/flow/PipeTerminationPointSummaryFlow.xml#PipeTerminationPointSummaryFlow</td>
<td>Open a Pipe Termination Point Summary work area from a Pipe Summary work area.</td>
</tr>
<tr>
<td>Pipe</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/configuration/flow/PipeConfigurationSummaryFlow.xml#PipeConfigurationSummaryFlow</td>
<td>Open a Pipe Configuration Summary work area.</td>
</tr>
<tr>
<td>Pipe</td>
<td>Edit</td>
<td>/WEB-INF/oracle/communications/inventory/ui/connectivity/flow/PipeEditFlow.xml#PipeEditFlow</td>
<td>Edit a pipe from search results or a Summary work area.</td>
</tr>
<tr>
<td>Pipe</td>
<td>Edit</td>
<td>/WEB-INF/oracle/communications/inventory/ui/connectivity/flow/PipeTPDirectionEditPopupFlow.xml#PipeTPDirectionEditPopupFlow</td>
<td>Edit pipe directionality from a Pipe Summary work area.</td>
</tr>
<tr>
<td>Pipe</td>
<td>Edit</td>
<td>/WEB-INF/oracle/communications/inventory/ui/connectivity/flow/PipeTerminationPointEditFlow.xml#PipeTerminationPointEditFlow</td>
<td>Edit a pipe termination point from a Pipe Summary work area.</td>
</tr>
<tr>
<td>Place</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/place/flow/PlaceSearchResultsFlow.xml#PlaceSearchResultsFlow</td>
<td>Open a Search work area for places by clicking the Place link in the Tasks panel.</td>
</tr>
<tr>
<td>Place</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/place/flow/PlaceSummaryFlow.xml#PlaceSummaryFlow</td>
<td>Open a Place Summary work area.</td>
</tr>
<tr>
<td>Place</td>
<td>Edit</td>
<td>/WEB-INF/oracle/communications/inventory/ui/place/flow/PlaceEditFlow.xml#PlaceEditFlow</td>
<td>Edit a place from search results or a Summary page.</td>
</tr>
<tr>
<td>Product</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/product/flow/ProductSearchResultsFlow.xml#ProductSearchResultsFlow</td>
<td>Open a Search work area for products by clicking the Product link in the Tasks panel.</td>
</tr>
<tr>
<td>Product</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/product/flow/ProductSummaryFlow.xml#ProductSummaryFlow</td>
<td>Open a Product Summary work area.</td>
</tr>
<tr>
<td>Product</td>
<td>Edit</td>
<td>/WEB-INF/oracle/communications/inventory/ui/product/flow/ProductEditFlow.xml#ProductEditFlow</td>
<td>Edit a product from search results or a Summary work area.</td>
</tr>
<tr>
<td>Reservation</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/consumer/flow/ReservationListFlow.xml#ReservationListFlow</td>
<td>View the reservation list for an entity by selecting from the Related Pages menu in an entity Summary page.</td>
</tr>
<tr>
<td>Reservation</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/consumer/flow/ReservationSearchResultsFlow.xml#ReservationSearchResultsFlow</td>
<td>Open a Search work area for reservations by clicking the Reservation link in the Tasks panel.</td>
</tr>
<tr>
<td>Reservation</td>
<td>Edit</td>
<td>/WEB-INF/oracle/communications/inventory/ui/consumer/flow/RedeemReservationFlow.xml#RedeemReservationFlow</td>
<td>Open the Redeem Reservation work area.</td>
</tr>
<tr>
<td>Role</td>
<td>Edit</td>
<td>/WEB-INF/oracle/communications/inventory/ui/role/flow/InventoryRoleEditFlow.xml#InventoryRoleEditFlow</td>
<td>Edit a role from an entity Summary work area.</td>
</tr>
<tr>
<td>RuleSet</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/rule/flow/RuleSearchResultsFlow.xml#RuleSearchResultsFlow</td>
<td>Open a Search work area for rulesets by clicking the Rule Set link in the Tasks panel.</td>
</tr>
<tr>
<td>RuleSet</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/rule/flow/RuleSummaryFlow.xml#RuleSummaryFlow</td>
<td>Open a RuleSet Summary work area.</td>
</tr>
</tbody>
</table>
Table 4–1 (Cont.) Taskflow Permissions

<table>
<thead>
<tr>
<th>Component</th>
<th>Access Type</th>
<th>Permission String</th>
<th>Controls the Ability to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/service/flow/ServiceSearchResultsFlow.xml#ServiceSearchResultsFlow</td>
<td>Open a Search work area for services by clicking the Service link in the Tasks panel.</td>
</tr>
<tr>
<td>Service</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/service/flow/ServiceSummaryFlow.xml#ServiceSummaryFlow</td>
<td>Open a Service Summary work area.</td>
</tr>
<tr>
<td>Service</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/service/flow/ServiceTopologyViewFlow.xml#ServiceTopologyViewFlow</td>
<td>Open the topology view for a service.</td>
</tr>
<tr>
<td>Service</td>
<td>Edit</td>
<td>/WEB-INF/oracle/communications/inventory/ui/service/flow/ServiceEditFlow.xml#ServiceEditFlow</td>
<td>Edit a service from search results or a Summary page.</td>
</tr>
<tr>
<td>Signal Structure</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/connectivity/flow/SignalTPSpecificationSearchResultsFlow.xml#SignalTPSpecificationSearchResultsFlow</td>
<td>Open a Search work area for Signal Termination Point specifications by selecting Map Signal Structure from the Related Pages menu of a Pipe Summary work area.</td>
</tr>
<tr>
<td>Telephone Number</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/number/flow/TelephoneNumberSearchResultsFlow.xml#TelephoneNumberSearchResultsFlow</td>
<td>Open a Search work area for telephone numbers by clicking the Telephone Number link in the Tasks panel.</td>
</tr>
<tr>
<td>Telephone Number</td>
<td>View</td>
<td>/WEB-INF/oracle/communications/inventory/ui/number/flow/TelephoneNumberSummaryFlow.xml#TelephoneNumberSummaryFlow</td>
<td>Open the Telephone Number Summary work area.</td>
</tr>
<tr>
<td>Telephone Number</td>
<td>Edit</td>
<td>/WEB-INF/oracle/communications/inventory/ui/number/flow/TelephoneNumberEditFlow.xml#TelephoneNumberEditFlow</td>
<td>Edit a telephone number.</td>
</tr>
</tbody>
</table>

**Resource Permissions**

Table 4–2 lists all the UIM resource permissions, sorted by component.
<table>
<thead>
<tr>
<th>Component</th>
<th>Type</th>
<th>Permission Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Interaction</td>
<td>Button Action</td>
<td>BusinessInteraction.DELETE</td>
<td>Delete a business interaction from the search results.</td>
</tr>
<tr>
<td>Business Interaction</td>
<td>Button Action</td>
<td>BusinessInteractionItem.DELETE</td>
<td>Delete a business interaction item from the Business Interaction Summary work area.</td>
</tr>
<tr>
<td>Business Interaction</td>
<td>Menu Action</td>
<td>BusinessInteraction.ACTIVATE</td>
<td>Activate a business interaction from the Business Interaction Summary work area.</td>
</tr>
<tr>
<td>Business Interaction</td>
<td>Menu Action</td>
<td>BusinessInteraction.APPROVE_CONFIGURATIONS</td>
<td>Approve a business interaction from the Business Interaction Summary work area.</td>
</tr>
<tr>
<td>Business Interaction</td>
<td>Menu Action</td>
<td>BusinessInteraction.CANCEL</td>
<td>Cancel a business interaction from the Business Interaction Summary work area.</td>
</tr>
<tr>
<td>Business Interaction</td>
<td>Menu Action</td>
<td>BusinessInteraction.CANCEL_HIERARCHY</td>
<td>Cancel a business interaction hierarchy from the Business Interaction Summary work area.</td>
</tr>
<tr>
<td>Business Interaction</td>
<td>Menu Action</td>
<td>BusinessInteraction.COMPLETE</td>
<td>Complete a business interaction from the Business Interaction Summary work area.</td>
</tr>
<tr>
<td>Business Interaction</td>
<td>Menu Action</td>
<td>BusinessInteraction.COMPLETE_HIERARCHY</td>
<td>Complete a business interaction hierarchy from the Business Interaction Summary work area.</td>
</tr>
<tr>
<td>Business Interaction</td>
<td>Menu Action</td>
<td>BusinessInteraction.DEACTIVATE</td>
<td>Deactivate a business interaction from the Business Interaction Summary work area.</td>
</tr>
<tr>
<td>Business Interaction</td>
<td>Menu Action</td>
<td>BusinessInteraction.ISSUE_CONFIGURATIONS</td>
<td>Issue a service configuration from the Business Interaction Summary work area.</td>
</tr>
<tr>
<td>Business Interaction</td>
<td>Menu Action</td>
<td>BusinessInteraction.SEND_REQUEST</td>
<td>Send a request from the Business Interaction Summary work area.</td>
</tr>
<tr>
<td>Business Interaction</td>
<td>Menu Action</td>
<td>BusinessInteraction.VALIDATE</td>
<td>Validate a business interaction from the Business Interaction Summary work area.</td>
</tr>
<tr>
<td>Condition</td>
<td>Button Action</td>
<td>CONDITION.DELETE</td>
<td>Delete a condition from the Condition List work area.</td>
</tr>
<tr>
<td>Custom Network Address</td>
<td>Button Action</td>
<td>CustomNetworkAddress.DELETE</td>
<td>Delete a custom network address from search results.</td>
</tr>
<tr>
<td>Custom Network Address</td>
<td>Menu Action</td>
<td>CustomNetworkAddress.ACTIVATE</td>
<td>Activate a custom network address from the Custom Network Address Summary work area.</td>
</tr>
<tr>
<td>Custom Network Address</td>
<td>Menu Action</td>
<td>CustomNetworkAddress.DEACTIVATE</td>
<td>Deactivate a custom network address from the Custom Network Address Summary work area.</td>
</tr>
<tr>
<td>Custom Network Address</td>
<td>Menu Action</td>
<td>CustomNetworkAddress.VALIDATE</td>
<td>Validate a custom network address from the Custom Network Address Summary work area.</td>
</tr>
<tr>
<td>Custom Object</td>
<td>Button Action</td>
<td>CustomObject.DELETE</td>
<td>Delete a custom object from search results.</td>
</tr>
<tr>
<td>Custom Object</td>
<td>Menu Action</td>
<td>CustomObject.ACTIVATE</td>
<td>Activate a custom object from the Custom Object Summary work area.</td>
</tr>
<tr>
<td>Custom Object</td>
<td>Menu Action</td>
<td>CustomObject.DEACTIVATE</td>
<td>Deactivate a custom object from the Custom Object Summary work area.</td>
</tr>
<tr>
<td>Component</td>
<td>Type</td>
<td>Permission Name</td>
<td>Purpose</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------</td>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Custom Object</td>
<td>Menu Action</td>
<td>CustomObject.VALIDATE</td>
<td>Validate a custom object from the Custom Object Summary work area.</td>
</tr>
<tr>
<td>Equipment</td>
<td>Button Action</td>
<td>EquipmentHolder.DELETE</td>
<td>Delete an equipment holder from search results.</td>
</tr>
<tr>
<td>Equipment</td>
<td>Button Action</td>
<td>Equipment.DELETE</td>
<td>Delete an Equipment entity from search results.</td>
</tr>
<tr>
<td>Equipment</td>
<td>Button Action</td>
<td>EQUIPMENT.DUPLICATE</td>
<td>Duplicate an Equipment entity from search results.</td>
</tr>
<tr>
<td>Equipment</td>
<td>Menu Action</td>
<td>Equipment.ACTIVATE</td>
<td>Activate an Equipment entity from the Equipment Summary work area.</td>
</tr>
<tr>
<td>Equipment</td>
<td>Menu Action</td>
<td>Equipment.DEACTIVATE</td>
<td>Deactivate an Equipment entity from the Equipment Summary work area.</td>
</tr>
<tr>
<td>Equipment</td>
<td>Menu Action</td>
<td>Equipment.VALIDATE</td>
<td>Validate an Equipment entity from the Equipment Summary work area.</td>
</tr>
<tr>
<td>Inventory Group</td>
<td>Button Action</td>
<td>InventoryGroup.DELETE</td>
<td>Delete an inventory group from search results.</td>
</tr>
<tr>
<td>Inventory Group</td>
<td>Button Action</td>
<td>INVENTORYGROUPITEMS.DELETE</td>
<td>Delete an inventory group from search results.</td>
</tr>
<tr>
<td>Inventory Group</td>
<td>Menu Action</td>
<td>InventoryGroup.ACTIVATE</td>
<td>Activate an inventory group from the Inventory Group Summary work area.</td>
</tr>
<tr>
<td>Inventory Group</td>
<td>Menu Action</td>
<td>InventoryGroup.DEACTIVATE</td>
<td>Deactivate an inventory group from the Inventory Group Summary work area.</td>
</tr>
<tr>
<td>Inventory Group</td>
<td>Menu Action</td>
<td>InventoryGroup.VALIDATE</td>
<td>Validate an inventory group from the Inventory Group Summary work area.</td>
</tr>
<tr>
<td>Involvement</td>
<td>Button Action</td>
<td>INVOLVEMENT.DELETE</td>
<td>Delete an involvement from an entity Summary work area.</td>
</tr>
<tr>
<td>Logical Device</td>
<td>Button Action</td>
<td>LogicalDevice.DELETE</td>
<td>Delete a logical device from search results.</td>
</tr>
<tr>
<td>Logical Device</td>
<td>Button Action</td>
<td>DEVICEMAPPING.DELETE</td>
<td>Map a physical port or connector to a device interface from the Device Interface Summary work area.</td>
</tr>
<tr>
<td>Logical Device</td>
<td>Menu Action</td>
<td>LogicalDevice.ACTIVATE</td>
<td>Activate a logical device from the Logical Device Summary work area.</td>
</tr>
<tr>
<td>Logical Device</td>
<td>Menu Action</td>
<td>LogicalDevice.DEACTIVATE</td>
<td>Deactivate a logical device from the Logical Device Summary work area.</td>
</tr>
<tr>
<td>Logical Device</td>
<td>Menu Action</td>
<td>LogicalDevice.VALIDATE</td>
<td>Validate a logical device from the Logical Device Summary work area.</td>
</tr>
<tr>
<td>Logical Device Account</td>
<td>Button Action</td>
<td>LogicalDeviceAccount.DELETE</td>
<td>Delete a logical device account from search results.</td>
</tr>
<tr>
<td>Logical Device Account</td>
<td>Menu Action</td>
<td>LogicalDeviceAccount.ACTIVATE</td>
<td>Activate a logical device account from the Logical Device Account Summary work area.</td>
</tr>
<tr>
<td>Logical Device Account</td>
<td>Menu Action</td>
<td>LogicalDeviceAccount.DEACTIVATE</td>
<td>Deactivate a logical device account from the Logical Device Account Summary work area.</td>
</tr>
<tr>
<td>Logical Device Account</td>
<td>Menu Action</td>
<td>LogicalDeviceAccount.VALIDATE</td>
<td>Validate the logical device account from the Logical Device Account Summary work area.</td>
</tr>
<tr>
<td>Logical Device</td>
<td>Menu Action</td>
<td>LogicalDeviceConfigurationVersion.APPROVE</td>
<td>Approve a configuration from the Logical Device Configuration Summary work area.</td>
</tr>
<tr>
<td>Component</td>
<td>Type</td>
<td>Permission Name</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------</td>
<td>-----------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Logical Device Configuration</td>
<td>Menu Action</td>
<td>LogicalDeviceConfigurationVersion.AutoConfigure</td>
<td>Auto-configure a configuration from the Logical Device Configuration Summary work area.</td>
</tr>
<tr>
<td>Logical Device Configuration</td>
<td>Menu Action</td>
<td>LogicalDeviceConfigurationVersion.CANCEL</td>
<td>Cancel a configuration from the Logical Device Configuration Summary work area.</td>
</tr>
<tr>
<td>Logical Device Configuration</td>
<td>Menu Action</td>
<td>LogicalDeviceConfigurationVersion.COMPLETE</td>
<td>Complete a configuration from the Logical Device Configuration Summary work area.</td>
</tr>
<tr>
<td>Logical Device Configuration</td>
<td>Menu Action</td>
<td>LogicalDeviceConfigurationVersion.CreateNewVersion</td>
<td>Create a new configuration from the Logical Device Configuration Summary work area.</td>
</tr>
<tr>
<td>Logical Device Configuration</td>
<td>Menu Action</td>
<td>LogicalDeviceConfigurationVersion.ISSUE</td>
<td>Issue a configuration from the Logical Device Configuration Summary work area.</td>
</tr>
<tr>
<td>Logical Device Configuration</td>
<td>Menu Action</td>
<td>LogicalDeviceConfigurationVersion.RESUME</td>
<td>Resume a configuration from the Logical Device Configuration Summary work area.</td>
</tr>
<tr>
<td>Logical Device Configuration</td>
<td>Menu Action</td>
<td>LogicalDeviceConfigurationVersion.SUSPEND</td>
<td>Suspend a configuration from the Logical Device Configuration Summary work area.</td>
</tr>
<tr>
<td>Logical Device Configuration</td>
<td>Menu Action</td>
<td>LogicalDeviceConfigurationVersion.validate</td>
<td>Validate a configuration from the Logical Device Configuration Summary work area.</td>
</tr>
<tr>
<td>Logical Device</td>
<td>Button Action</td>
<td>LOGICAL_DEVICE.DUPLICATE</td>
<td>Duplicate a logical device from search results.</td>
</tr>
<tr>
<td>Media</td>
<td>Button Action</td>
<td>Media.DELETE</td>
<td>Delete a media file from search results.</td>
</tr>
<tr>
<td>Media Stream</td>
<td>Button Action</td>
<td>MediaStream.DELETE</td>
<td>Delete a media stream from search results.</td>
</tr>
<tr>
<td>Media Stream</td>
<td>Button Action</td>
<td>MEDIA_STREAM.DUPLICATE</td>
<td>Duplicate a media stream from search results.</td>
</tr>
<tr>
<td>Media Stream</td>
<td>Menu Action</td>
<td>MediaStream.ACTIVATE</td>
<td>Activate a media stream from the Media Stream Summary work area.</td>
</tr>
<tr>
<td>Media Stream</td>
<td>Menu Action</td>
<td>MediaStream.DEACTIVATE</td>
<td>Deactivate a media stream from the Media Stream Summary work area.</td>
</tr>
<tr>
<td>Media Stream</td>
<td>Menu Action</td>
<td>MediaStream.VALIDATE</td>
<td>Validate a media stream from the Media Stream Summary work area.</td>
</tr>
<tr>
<td>Network</td>
<td>Button Action</td>
<td>Network.DELETE</td>
<td>Delete a network from search results.</td>
</tr>
<tr>
<td>Network</td>
<td>Menu Action</td>
<td>Network.ACTIVATE</td>
<td>Activate a network from the Network Summary work area.</td>
</tr>
<tr>
<td>Network</td>
<td>Menu Action</td>
<td>Network.DEACTIVATE</td>
<td>Deactivate a network from the Network Summary work area.</td>
</tr>
<tr>
<td>Network</td>
<td>Menu Action</td>
<td>Network.VALIDATE</td>
<td>Validate a network from the Network Summary work area.</td>
</tr>
<tr>
<td>Network</td>
<td>Menu Action</td>
<td>NetworkEdge.ADD</td>
<td>Add a network edge from the Network Summary work area.</td>
</tr>
<tr>
<td>Network</td>
<td>Menu Action</td>
<td>NetworkEdge.DELETE</td>
<td>Delete a network edge from the Network Summary work area.</td>
</tr>
<tr>
<td>Network</td>
<td>Menu Action</td>
<td>NetworkNode.ADD</td>
<td>Add a network node from the Network Summary work area.</td>
</tr>
<tr>
<td>Network</td>
<td>Menu Action</td>
<td>NetworkNode.DELETE</td>
<td>Delete a network node from the Network Summary work area.</td>
</tr>
</tbody>
</table>
Table 4–2 (Cont.) Resource Permissions

<table>
<thead>
<tr>
<th>Component</th>
<th>Type</th>
<th>Permission Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Configuration</td>
<td>Menu Action</td>
<td>NetworkConfigurationVersion.APPROVE</td>
<td>Approve a configuration from the Network Configuration Summary work area.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NetworkConfigurationVersion.AutoConfigure</td>
<td>Auto-configure a configuration from the Network Configuration Summary work area.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NetworkConfigurationVersion.CANCEL</td>
<td>Cancel a configuration from the Network Configuration Summary work area.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NetworkConfigurationVersion.COMPLETE</td>
<td>Complete a configuration from the Network Configuration Summary work area.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NetworkConfigurationVersion.CREATEVERSION</td>
<td>Create a new configuration from the Network Configuration Summary work area.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NetworkConfigurationVersion.ISSUE</td>
<td>Issue a configuration from the Network Configuration Summary work area.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NetworkConfigurationVersion.RESUME</td>
<td>Resume a configuration from the Network Configuration Summary work area.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NetworkConfigurationVersion.SUSPEND</td>
<td>Suspend a configuration from the Network Configuration Summary work area.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NetworkConfigurationVersion.validate</td>
<td>Validate a configuration from the Network Configuration Summary work area.</td>
</tr>
<tr>
<td>Party</td>
<td>Button Action</td>
<td>Party.DELETE</td>
<td>Delete a party from search results.</td>
</tr>
<tr>
<td>Party</td>
<td>Button Action</td>
<td>Party.EDIT</td>
<td>Edit a party from Party search results or the Service Summary work area.</td>
</tr>
<tr>
<td>Party</td>
<td>Menu Action</td>
<td>Party.ACTIVATE</td>
<td>Activate a party from the Party Summary work area.</td>
</tr>
<tr>
<td>Party</td>
<td>Menu Action</td>
<td>Party.DEACTIVATE</td>
<td>Deactivate a party from the Party Summary work area.</td>
</tr>
<tr>
<td>Physical Device</td>
<td>Button Action</td>
<td>PhysicalDevice.DELETE</td>
<td>Delete a physical device from search results.</td>
</tr>
<tr>
<td>Physical Device</td>
<td>Button Action</td>
<td>PHYSICAL_DEDUPLICATE</td>
<td>Duplicate a physical device from search results.</td>
</tr>
<tr>
<td>Physical Device</td>
<td>Menu Action</td>
<td>PhysicalDevice.ACTIVATE</td>
<td>Activate physical device from the Physical Device Summary work area.</td>
</tr>
<tr>
<td>Physical Device</td>
<td>Menu Action</td>
<td>PhysicalDevice.DEACTIVATE</td>
<td>Deactivate a physical device from the Physical Device Summary work area.</td>
</tr>
<tr>
<td>Physical Device</td>
<td>Menu Action</td>
<td>PhysicalDevice.VALIDATE</td>
<td>Validate a physical device from the Physical Device Summary work area.</td>
</tr>
<tr>
<td>Pipe</td>
<td>Button Action</td>
<td>Pipe.DELETE</td>
<td>Delete a pipe from search results.</td>
</tr>
<tr>
<td>Pipe</td>
<td>Button Action</td>
<td>PIPE.DUPLICATE</td>
<td>Duplicate a pipe from search results.</td>
</tr>
<tr>
<td>Pipe</td>
<td>Menu Action</td>
<td>Pipe.ACTIVATE</td>
<td>Activate a pipe from the Pipe Summary work area.</td>
</tr>
<tr>
<td>Pipe</td>
<td>Menu Action</td>
<td>Pipe.AutoConfigure</td>
<td>TBD</td>
</tr>
<tr>
<td>Pipe</td>
<td>Menu Action</td>
<td>Pipe.DEACTIVATE</td>
<td>Deactivate a pipe from the Pipe Summary work area.</td>
</tr>
</tbody>
</table>
### Table 4–2 (Cont.) Resource Permissions

<table>
<thead>
<tr>
<th>Component</th>
<th>Type</th>
<th>Permission Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pipe</td>
<td>Menu Action</td>
<td>Pipe.MAP_SIGNAL_STRUCTURE</td>
<td>Associate a signal structure to a pipe from the Pipe Summary work area.</td>
</tr>
<tr>
<td>Pipe</td>
<td>Menu Action</td>
<td>Pipe.REMOVE_SIGNAL_STRUCTURE</td>
<td>Disassociate a signal structure from a pipe from the Pipe Summary work area.</td>
</tr>
<tr>
<td>Pipe</td>
<td>Menu Action</td>
<td>Pipe.VALIDATE</td>
<td>Validate a pipe from the Pipe Summary work area.</td>
</tr>
<tr>
<td>Pipe Configuration</td>
<td>Menu Action</td>
<td>PipeConfigurationVersion.APPROVE</td>
<td>Approve a configuration from the Pipe Configuration Summary work area.</td>
</tr>
<tr>
<td>Pipe Configuration</td>
<td>Menu Action</td>
<td>PipeConfigurationVersion.AutoConfigure</td>
<td>Auto-configure a configuration from the Pipe Configuration Summary work area.</td>
</tr>
<tr>
<td>Pipe Configuration</td>
<td>Menu Action</td>
<td>PipeConfigurationVersion.CANCEL</td>
<td>Cancel a configuration from the Pipe Configuration Summary work area.</td>
</tr>
<tr>
<td>Pipe Configuration</td>
<td>Menu Action</td>
<td>PipeConfigurationVersion.COMPLETE</td>
<td>Complete a configuration from the Pipe Configuration Summary work area.</td>
</tr>
<tr>
<td>Pipe Configuration</td>
<td>Menu Action</td>
<td>PipeConfigurationVersion.CreateNewVersion</td>
<td>Create a new configuration from the Pipe Configuration Summary work area.</td>
</tr>
<tr>
<td>Pipe Configuration</td>
<td>Menu Action</td>
<td>PipeConfigurationVersion.ISSUE</td>
<td>Issue a configuration from the Pipe Configuration Summary work area.</td>
</tr>
<tr>
<td>Pipe Configuration</td>
<td>Menu Action</td>
<td>PipeConfigurationVersion.RESUME</td>
<td>Resume a configuration from the Pipe Configuration Summary work area.</td>
</tr>
<tr>
<td>Pipe Configuration</td>
<td>Menu Action</td>
<td>PipeConfigurationVersion.SUSPEND</td>
<td>Suspend a configuration from the Pipe Configuration Summary work area.</td>
</tr>
<tr>
<td>Place</td>
<td>Button Action</td>
<td>Place.DELETE</td>
<td>Delete a place from search results.</td>
</tr>
<tr>
<td>Place</td>
<td>Button Action</td>
<td>Place.EDIT</td>
<td>Edit a place from search results or an entity Summary work area.</td>
</tr>
<tr>
<td>Place Configuration</td>
<td>Menu Action</td>
<td>PlaceConfigurationVersion.APPROVE</td>
<td>Approve a configuration from the Place Configuration Summary work area.</td>
</tr>
<tr>
<td>Place Configuration</td>
<td>Menu Action</td>
<td>PlaceConfigurationVersion.AutoConfigure</td>
<td>Auto-configure a configuration from the Place Configuration Summary work area.</td>
</tr>
<tr>
<td>Place Configuration</td>
<td>Menu Action</td>
<td>PlaceConfigurationVersion.CANCEL</td>
<td>Cancel a configuration from the Place Configuration Summary work area.</td>
</tr>
<tr>
<td>Place Configuration</td>
<td>Menu Action</td>
<td>PlaceConfigurationVersion.COMPLETE</td>
<td>Complete a configuration from the Place Configuration Summary work area.</td>
</tr>
<tr>
<td>Place Configuration</td>
<td>Menu Action</td>
<td>PlaceConfigurationVersion.CreateNewVersion</td>
<td>Create a new configuration from the Place Configuration Summary work area.</td>
</tr>
<tr>
<td>Place Configuration</td>
<td>Menu Action</td>
<td>PlaceConfigurationVersion.ISSUE</td>
<td>Issue a configuration from the Place Configuration Summary work area.</td>
</tr>
<tr>
<td>Place Configuration</td>
<td>Menu Action</td>
<td>PlaceConfigurationVersion.RESUME</td>
<td>Resume a configuration from the Place Configuration Summary work area.</td>
</tr>
<tr>
<td>Place Configuration</td>
<td>Menu Action</td>
<td>PlaceConfigurationVersion.SUSPEND</td>
<td>Suspend a configuration from the Place Configuration Summary work area.</td>
</tr>
</tbody>
</table>
Table 4–2 (Cont.) Resource Permissions

<table>
<thead>
<tr>
<th>Component</th>
<th>Type</th>
<th>Permission Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Place Configuration</td>
<td>Menu Action</td>
<td>PlaceConfigurationVersion.validate</td>
<td>Validate a configuration from the Place Configuration Summary work area.</td>
</tr>
<tr>
<td>Product</td>
<td>Button Action</td>
<td>Product.DELETE</td>
<td>Delete a product from search results.</td>
</tr>
<tr>
<td>Product</td>
<td>Menu Action</td>
<td>Product.ACTIVATE</td>
<td>Activate a product from the Product Summary work area.</td>
</tr>
<tr>
<td>Product</td>
<td>Menu Action</td>
<td>Product.DEACTIVATE</td>
<td>Deactivate a product from the Product Summary work area.</td>
</tr>
<tr>
<td>Product</td>
<td>Menu Action</td>
<td>Product.VALIDATE</td>
<td>TBD</td>
</tr>
<tr>
<td>Product</td>
<td>Menu Action</td>
<td>Product.VALIDATE_PRODUCT</td>
<td>Validate a product from the Product Summary work area.</td>
</tr>
<tr>
<td>Reservation</td>
<td>Button Action</td>
<td>RESERVATION.DELETE</td>
<td>Delete a reservation from the Reservations list.</td>
</tr>
<tr>
<td>Role</td>
<td>Button Action</td>
<td>ROLE.DELETE</td>
<td>Delete a role from the Roles list in an entity Summary work area.</td>
</tr>
<tr>
<td>Role</td>
<td>Button Action</td>
<td>ROLE.EDIT</td>
<td>Edit a role from the Roles list in an entity Summary work area.</td>
</tr>
<tr>
<td>Ruleset</td>
<td>Button Action</td>
<td>Rule.DELETE</td>
<td>Delete a ruleset.</td>
</tr>
<tr>
<td>Service</td>
<td>Button Action</td>
<td>Service.DELETE</td>
<td>Delete a service from search results.</td>
</tr>
<tr>
<td>Service</td>
<td>Menu Action</td>
<td>Service.ACTIVATE</td>
<td>Activate a service from the Service Summary work area.</td>
</tr>
<tr>
<td>Service</td>
<td>Menu Action</td>
<td>Service.CANCEL</td>
<td>Cancel a service from the Service Summary work area.</td>
</tr>
<tr>
<td>Service</td>
<td>Menu Action</td>
<td>Service.COMPLETE</td>
<td>Complete a service from the Service Summary work area.</td>
</tr>
<tr>
<td>Service</td>
<td>Menu Action</td>
<td>Service.DEACTIVATE</td>
<td>Deactivate a service from the Service Summary work area.</td>
</tr>
<tr>
<td>Service</td>
<td>Menu Action</td>
<td>Service.DISCONNECT</td>
<td>Disconnect a service from the Service Summary work area.</td>
</tr>
<tr>
<td>Service</td>
<td>Menu Action</td>
<td>Service.RESUME</td>
<td>Resume a service from the Service Summary work area.</td>
</tr>
<tr>
<td>Service</td>
<td>Menu Action</td>
<td>Service.SUSPEND</td>
<td>Suspend a service from the Service Summary work area.</td>
</tr>
<tr>
<td>Service</td>
<td>Menu Action</td>
<td>Service.VALIDATE</td>
<td>Validate a service from the Service Summary work area.</td>
</tr>
<tr>
<td>Service Configuration</td>
<td>Menu Action</td>
<td>ServiceConfigurationVersion.APPROVE</td>
<td>Approve a configuration from the Service Configuration Summary work area.</td>
</tr>
<tr>
<td>Service Configuration</td>
<td>Menu Action</td>
<td>ServiceConfigurationVersion.AutoConfigure</td>
<td>Auto-configure a configuration from the Service Configuration Summary work area.</td>
</tr>
<tr>
<td>Service Configuration</td>
<td>Menu Action</td>
<td>ServiceConfigurationVersion.CANCEL</td>
<td>Cancel a configuration from the Service Configuration Summary work area.</td>
</tr>
<tr>
<td>Service Configuration</td>
<td>Menu Action</td>
<td>ServiceConfigurationVersion.COMPLETED</td>
<td>Complete a configuration from the Service Configuration Summary work area.</td>
</tr>
<tr>
<td>Service Configuration</td>
<td>Menu Action</td>
<td>ServiceConfigurationVersion.ISSUE</td>
<td>Issue a configuration from the Service Configuration Summary work area.</td>
</tr>
</tbody>
</table>

Table 4–2 (Cont.) Resource Permissions
Application Role Management

For any administrative tasks related to Application Roles using EM Console, it is recommended to take a backup of `system-jaxn-data.xml` located in the `Domain_home/config/fmwconfig/` directory. All the changes made to Application Roles will be in effect immediately, without a restarting the application server.

Creating the Application Role

To create Application Role, perform the following,

1. Login to Enterprise Manager Console.
2. Navigate to Inventory Application on the left navigation bar.
4. Click the Create button to create a new Application Role.
5. In the New Application Role page, enter the role details.
6. To associate a user to the application role, click the Add User button. Click the Search button, of the User Name field, to view the available users in the mapping page.
7. From the Available Users field, select the user to be assigned to the new application role and click the Move button to move the user to the Selected Users field.

Table 4-2 (Cont.) Resource Permissions

<table>
<thead>
<tr>
<th>Component</th>
<th>Type</th>
<th>Permission Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Configuration</td>
<td>Menu Action</td>
<td>ServiceConfigurationVersion.RESUME</td>
<td>Resume a configuration from the Service Configuration Summary work area.</td>
</tr>
<tr>
<td>Service Configuration</td>
<td>Menu Action</td>
<td>ServiceConfigurationVersion.SUSPEND</td>
<td>Suspend a configuration from the Service Configuration Summary work area.</td>
</tr>
<tr>
<td>Service Configuration</td>
<td>Menu Action</td>
<td>ServiceConfigurationVersion.validate</td>
<td>Validate a configuration from the Service Configuration Summary work area.</td>
</tr>
<tr>
<td>Telephone Number</td>
<td>Button Action</td>
<td>TelephoneNumber.DELETE</td>
<td>Delete a telephone number from search results.</td>
</tr>
<tr>
<td>Telephone Number</td>
<td>Menu Action</td>
<td>TelephoneNumber.ACTIVATE</td>
<td>Activate a telephone number from the Telephone Number Summary work area.</td>
</tr>
<tr>
<td>Telephone Number</td>
<td>Menu Action</td>
<td>TelephoneNumber.DEACTIVATE</td>
<td>Deactivate a telephone number from the Telephone Number Summary work area.</td>
</tr>
<tr>
<td>Telephone Number</td>
<td>Menu Action</td>
<td>TelephoneNumber.SNAPBACK</td>
<td>Configure the Snapback action on a telephone number from the Telephone Number Summary work area.</td>
</tr>
<tr>
<td>Telephone Number</td>
<td>Menu Action</td>
<td>TelephoneNumber.VALIDATE</td>
<td>Validate a telephone number from the Telephone Number Summary work area.</td>
</tr>
</tbody>
</table>
8. Click OK.

9. On the Application Role Creation page, click the OK button to complete the association of a user to an application role.

Updating the Application Role
To update the Application Role, perform the following:
1. Login to Enterprise Manager Console.
2. Navigate to Inventory Application on the left navigation bar.
4. In the Application Roles page, click the search button, of the Role Name field, to view a list of existing application roles.
5. Click the application role you want to update and click the Edit button to navigate to the Edit Application Role page.

From the Edit Application Role page, you can add an existing Application Role/User/Group to an application role.

6. In this case, we shall add a new user to resourceAdmin application Role. Click on Add User button to view a popup.
7. Select a user, click the Move button to move the user to the Select Users box and click OK.
8. Click OK in the Edit Application Role page to add the user to Application Role.

Deleting the Application Role
To delete the Application Role, perform the following:
1. Login to Enterprise Manager Console.
2. Navigate to Inventory Application on the left navigation bar
4. In the Application Roles page, click the search button to view a list of existing application roles.
5. Click on the application role you want to delete and click Delete.
6. In the confirmation popup page click Yes to delete the application role.

The role is deleted.

Application Policy Management
For any administrative tasks related to Application Policies using EM Console, it is recommended to take a backup of system-jaxn-data.xml located under Domain_Home/Config/fmwconfig/.

All the changes made to Application Policies will be in effect immediately, without restarting the application server.

Creating the Policy
A Policy can be created by adding User Interface page permissions and Action permissions to an existing policy.
Adding User Interface (UI) Page Permissions to an Existing Policy

To add User Interface (UI) page permissions to an existing policy, perform the following:

1. Login to Enterprise Manager Console.
2. Navigate to Inventory Application on the left navigation bar.
   
   The Application Policies List page appears.
4. Click the Create button to create a new Application Policy.
   
   The Create Application Grant page appears.
5. Click the Add button, in the Grant Details section.

   The Add Permission popup appears.
6. Enter the resource_name in the Resource Name field and click the search button, of the Resource Name field, to list all the resources that start with resource_name.

   
   Note: The search is NOT cases sensitive.

   7. From the Search results section, all the resources that start with resource_name are displayed. Select a resource to see details in the Customize section.

   If customization is required, enter the custom information and click OK.

   If customization is not required, click OK.
8. The resource is added to the Permissions list.
9. Repeat steps 7. and 8. for the remaining resources that start with resource_name.
10. Click the Add Application Role button in the Grantee section.
   
   The Add Application Role popup page appears.
11. Select the applicationrole_name and click Move, to move the application role to the Selected Roles section.
12. Click OK to complete the Application Grant Creation process.

Adding Action Permissions to an Existing Policy

To add Action permissions to an existing policy, perform the following:

1. Login to Enterprise Manager Console.
2. Navigate to Inventory Application on the left navigation bar.
   
   The Application Policies List page appears.
4. Click the Search button, of the Permissions field, to search for existing policies.
   
   The Edit Application Grant page appears.
5. Select the Policy to be modified and click the Edit button.
   
   The Applications Grant page appears.
6. Click the **Add** button to add a new Permission.
The Add Permission popup page appears.

7. In the **Customize** section, enter customized data in the following fields:
   - Permission Class
   - Resource Name
   - Permission Actions
   Click **OK** to add the permissions.

8. Click **OK** to complete the Add Application Permissions process.

### Updating the Policy Role
To update the Policy Role, perform the following:

1. Login to Enterprise Manager Console.

2. Navigate to **Inventory Application** on the left navigation bar.

3. Navigate to **Security Policies** page. Right-click the `oracle.communications.inventory` and select **Security>Application Policies**.

4. In the **Application Policies** page, click the search button, of the Permission field, to view a list of existing application policies.

5. Select the application policy you want to edit and click the **Edit** button to navigate to the **Edit Application Grant Page** page.

   From the **Edit Application Role** page, you can add/remove the following aspects of a policy:
   - **Permissions** (TaskFlow permissions or Resource Permissions). TaskFlow Permissions are used for UI pages whereas Resource Permissions are used for UI Actions.
   - **Grantee** (User/Group/Role). Note that if multiple Roles/Groups are associated to a Policy, the Application Policy will be applicable to the user only if the user is part of all Roles/Groups.

6. Click the **Add** button to add Permissions.
The Add Permissions page appears.

7. Enter **TelephoneNumber** in the **Resource Name** section and click the **Search** button to view all the UI resources having TelephoneNumber in their name.

8. Select the first row (TelephoneNumberEditFlow) and click **OK** to add the Permission to the role.

9. Repeat steps 7. and 8. to add **TelephoneNumberSearchResultsFlow** and **TelephoneNumberSummaryFlow**.

10. Click **OK** to update the policy.

### Deleting the Policy Role
To delete the Application Role, perform the following:

1. Login to Enterprise Manager Console.

2. Navigate to **Inventory Application** on the left navigation bar
4. In the Application Policies page, click the search button, of the Permission field, to view a list of existing application policies.
5. Select the application role you want to delete and click Delete.
6. In the confirmation popup, click Yes to delete the application policy.
   The policy is deleted.

Enabling Web Service Authentication at Runtime

Web Service policies can be associated with deployed web services using the Admin Console.

---

**Note:** Each time the application is deployed, the WS_Policies will have to be reconfigured.

---

This approach is better suited for applications that do not need frequent deployments.

Creating the Application Role

To create Application Role, perform the following.

1. Login to Admin Console.
2. In the left pane, select Deployments and click the deployed application to expand it as shown below (in this example DemoWS). Click on the deployed web service as highlighted below.
3. Select Configuration tab and WS-Policy sub-tab. Click on the + sign next to the Service End point listed to see all the operations that the web service supports.
4. Click on the service Endpoint to configure the policy type for the web service.
5. Select the policy for this end point and click Finish.
6. To attach a policy to an operation, click the operation. On the next screen select the policy that you would like to associate with the operation and click on the ‘>’ sign. The selected policy or policies get moved over to the Chosen Message Policies list. Click on Next.
7. To use the same policy for inbound (i.e. requests) and outbound(i.e. response) message, click Next on: Configure the WS-Policy for the Inbound SOAP Message of an Operation & Configure the WS-Policy for the outbound SOAP Message of an Operation pages.
8. Click Finish.

Partitioning the Database

This section explains how to partition your UIM database by using user groups, within a security realm, to represent data partitions. Partitioning allows the user to control data access to an entity.

The UIM database management tasks include:

- Creating Partitions in the UIM Database
Updating the system-config.properties File

Creating Partitions in the UIM Database
To create partitions in the UIM database, do the following:

1. Ensure you are logged into the WebLogic server administration console.
2. Click Lock and Edit.
   The Summary of Security Realms page appears.
4. Select the security_realm.
   The Settings for security_realm page appears.
5. Click the Users and Groups tab.
6. Click the Groups tab.
7. Click on New.
   The Create a New Group page appears.
8. Enter the name for the new group. Use the following format for the new group:
   ora_uim_partition#name
   
   **Note:** If you do not use the ora_uim_partition#name prefix, UIM will not recognize the group as a partition and the partitioning will not work.

9. Click Ok.
   Repeat steps 8. and 9. for each partition that is to be created.
   The Settings for security_realm page appears.
10. Click the Users tab.
11. Click on the user name that you want to add to the new group.
    The Settings for user_name page appears.
12. Click the Groups tab.
13. From the Parents Groups Available: list, select the group or groups that you want to add the user to and then click on the single arrow to move the group or groups to the Chosen: list.
14. Click Save.
15. Click Release Configuration.

**Note:** Changes made to groups in WebLogic Server are immediate, but you must log out/log back into UIM to pick up the changes.

Updating the system-config.properties File
To update the system-config.properties file, do the following:

1. In the UIM_Home/config directory, open the system-config.properties file.
2. Set the uim.security.filter.enabled property value to True.
uim.security.filter.enabled=true
Monitoring and Managing Unified Inventory Management

This chapter provides monitoring and managing activities that you may need to perform after installing or upgrading the Oracle Communications Unified Inventory Management (UIM) software.

Monitoring and Managing Overview

The following list includes tasks that you may need to perform on both a single server environment and a clustered server environment:

- Sharing JAR Files
- Disabling the HTTP Port
- Setting the Database RowPrefetch Size
- Modifying the Default File Encoding
- Modifying the Time Zone
- Configuring Your Server’s Timers
- Registering Entities to the LifeCycle Listener
- Configuring Exception-Type-to-Error-Code Mappings
- Localizing UIM Error Messages
- Localizing the UIM Server and the Application Server
- Shutting Down an Application Server
- Configuring the SSL Policy/Certificate
- Resetting/Changing the WebLogic Server’s Database Connections
- Setting the Default Telephone Number Edit Mask
- Load Balancing a Clustered Server
- Configuring Topology Updates

Sharing JAR Files

After you install UIM, you need to share specific JAR files with Design Studio (DS) for use with tech packs. Each individual UIM System Administrator must determine the best method for sharing these JAR files, based on your company’s standard practices. The following is a list of directories, with the JAR files that need to be shared:
- **UIM_Home/lib**
  - capacity_caps.jar
  - characteristic_caps.jar
  - consumable_caps.jar
  - core_caps.jar
  - groupenabled_caps.jar
  - ora_uim_commonLib.jar
  - persistence.jar
  - platform-persistence.jar
  - poms.jar
  - uim-api-framework.jar
  - uim-caps.jar
  - uim-entities.jar
  - uim-entity-xmlbean.jar
  - uim-managers.jar
  - uim-tools.jar
  - uim-webservices-framework.jar

- **POMSClient/lib**
  - platformWsFramework.jar

- **WL_Home/server/lib**
  - log4j.jar
  - weblogic.jar
  - webservices.jar
  - wlclient.jar
  - xbean.jar

- **UIM_Home/cartirdges/base**
  - ora_uim_baseextpts
  - ora_uim_basemeasurements
  - ora_uim_basephone_mgmt
  - ora_uim_baserulesets
  - ora_uim_basespecifications
  - ora_uim_canada_tn
  - ora_uim_mds
  - ora_uim_model
  - ora_uim_norway_tn
  - ora_uim_saudi_arabia_tn
  - ora_uim_uk_tn
Disabling the HTTP Port

After you install UIM, you can disable the HTTP (non-SSL) port if it was enabled during installation.

To disable the HTTP port:
1. Ensure you are logged into the WebLogic Administration Console.
2. Click Lock & Edit.
3. In the Domain Structure tree, expand Environment, and then click Servers.
   The Summary of Servers page appears.
4. Select the AdminServer.
   The Settings for AdminServer page appears.
5. Deselect the Listen Port Enabled setting.

   Note: If you disable this port, then you must enable the SSL port.

6. Click Save.
7. Click Activate Changes.

Setting the Database RowPrefetch Size

You can specify the number of result set rows to prefetch.
1. Ensure you are logged into the WebLogic Administration Console.
2. Click Lock & Edit.
3. In the Domain Structure tree, expand Services, then expand JDBC and then click Data Sources.
   The Summary of JDBC Data Sources page appears.
4. Click the InventoryDataSource data source.
   The Settings for InventoryDataSource page appears.
5. Under Configuration, click the Connection Pool tab.
6. In the Properties field, enter the following:
   defaultRowPrefetch=50
7. Click Save.
8. Repeat steps 3. through 7. for InventoryTxDataSource.
9. Click Activate Changes.
10. Restart the WebLogic Application Server.

Note: These JAR files will change with each new patchset or maintenance release. The JAR files will need to be re-distributed each time UIM is upgraded with a patchset or maintenance release and the DS Administrator will need to be notified.

Note: If you disable this port, then you must enable the SSL port.
Modifying the Default File Encoding

The UIM installer automatically sets the default file encoding to UTF8 for both full installations and upgrades. Check the startup script to verify that the default file encoding is set to UTF8. If this setting is incorrect, you can manually change the default file encoding setting in the CUSTOM SECTION segment of the startup script.

The following example shows the correct command syntax:

```
JAVA_OPTIONS="${JAVA_OPTIONS}-Dfile.encoding=UTF-8"
```

Modifying the Time Zone

For full installations and upgrades, the UIM installer automatically sets the time zone for your locale. You should check your startup script to verify that the time zone setting for your locale is correct. If this setting is incorrect, add a line to the CUSTOM SECTION segment of your startup script. Enter the time zone ID in a format that is recognizable by the `java.util.TimeZone` object. The following example shows the command syntax:

```
JAVA_OPTIONS="${JAVA_OPTIONS} -Duser.timezone=Asia/Shanghai"
```

To view a list of valid time zone values, run the following command:

```java
import java.util.*;
public class TimeZoneList {
    public static void main(String[] args) {
        String[] sZoneIds = TimeZone.getAvailableIDs();
        List<String> lZoneIdList = Arrays.asList(sZoneIds);
        Collections.sort(lZoneIdList);
        System.out.println(lZoneIdList);
    }
}
```

**Note:** If your application server and database server are located in different time zones, set the application server’s `user.timezone` value to match the database server’s time zone. The application server and database server time zones must match.

**Note:** The application server time zone is defaulted to the underlying operating system time zone. To configure a different time zone for the application server, add the following value to the startup script at `Domain_Home/bin/setUIMenv.sh`. The valid time zone values are defined in `java.util.TimeZone`.

```
JAVA_OPTIONS="${JAVA_OPTIONS} -Duser.timezone=timezone"
```

where `timezone` is a valid string value defining the time zone ID such as GMT or EST.
Configuring Your Server’s Timers

You can create and configure timers for:

- Monitoring whether the server that manages the cluster-aware timers is still running
- Custom extensions
- Cleaning up expired reservations
- Detecting telephone number jeopardy and publishing notification events

You configure the timers for your servers in the `UIM_Home/config/timers.properties` file. For more information, see the comments in the `timers.properties` file.

Registering Entities to the LifeCycle Listener

You can register all or a subset of entities for create, retrieve, update, and delete (CRUD) events. For example, you can specify that create events are generated when any entity is created. Likewise, you can specify that update events are generated only when Equipment and TelephoneNumber entities are updated.

You register entities to the lifecycle listener by using the `UIM_Home/config/events.properties` file. For more information, see the comments in the `events.properties` file.

Configuring Exception-Type-to-Error-Code Mappings

You can map error codes to exception types to help the persistence framework manage validation exceptions. For example, you can map error codes to `DuplicateEntityException` or to `AttributeRequiredException`.

You map error codes to exception types by using the `UIM_Home/config/resources/logging/exception.properties` file. For more information, see the comments in the `exception.properties` file.

Localizing UIM Error Messages

You can localize UIM error messages and items by modifying properties files in the `UIM_Home/config/resources/logging` directory.

Table 5–1 lists each property’s file name, error ID range, and the error messages or items it localizes.

<table>
<thead>
<tr>
<th>Property File Name</th>
<th>Error ID Range</th>
<th>Error Message or Item It Localizes</th>
</tr>
</thead>
<tbody>
<tr>
<td>addressrange.properties</td>
<td>N/A</td>
<td>Property names for the address range cartridge</td>
</tr>
<tr>
<td>businessInteraction.properties</td>
<td>270000-279999</td>
<td>Error messages generated by the business interaction module</td>
</tr>
<tr>
<td>capacity.properties</td>
<td>320000-329999</td>
<td>Error messages generated by the capacity module</td>
</tr>
<tr>
<td>configaction.properties</td>
<td>240000-249999</td>
<td>Error messages generated by the configuration actions</td>
</tr>
<tr>
<td>configuration.properties</td>
<td>240000-249999</td>
<td>Tree node label names</td>
</tr>
<tr>
<td>Property File Name</td>
<td>Error ID Range</td>
<td>Error Message or Item It Localizes</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>connectivity.properties</td>
<td>260000-269999</td>
<td>Error messages generated by the connectivity module</td>
</tr>
<tr>
<td>consumer.properties</td>
<td>220000-229999</td>
<td>Error messages generated by the consumer module</td>
</tr>
<tr>
<td>custom.properties</td>
<td>280000-289999</td>
<td>Error messages generated by the custom module</td>
</tr>
<tr>
<td>enum.properties</td>
<td>N/A</td>
<td>Error messages generated by enumeration</td>
</tr>
<tr>
<td>equipment.properties</td>
<td>210000-219999</td>
<td>Error messages generated by the equipment module</td>
</tr>
<tr>
<td>extensibility.properties</td>
<td>180000-189999</td>
<td>Error messages generated by the extensibility module</td>
</tr>
<tr>
<td>inventoryGroup.properties</td>
<td>190000-199999</td>
<td>Error messages generated by the inventory group module</td>
</tr>
<tr>
<td>logicaldevice.properties</td>
<td>290000-299999</td>
<td>Error messages generated by the logical device module</td>
</tr>
<tr>
<td>media.properties</td>
<td>350000-359999</td>
<td>Error messages generated by the media module</td>
</tr>
<tr>
<td>network.properties</td>
<td>300000-309999</td>
<td>Error messages generated by the network module</td>
</tr>
<tr>
<td>number.properties</td>
<td>120000-129999</td>
<td>Error messages generated by the number module</td>
</tr>
<tr>
<td>party.properties</td>
<td>230000-239999</td>
<td>Error messages generated by the party role module</td>
</tr>
<tr>
<td>place.properties</td>
<td>250000-259999</td>
<td>Error messages generated by the place module</td>
</tr>
<tr>
<td>product.properties</td>
<td>390000-399999</td>
<td>Error messages generated by the product module</td>
</tr>
<tr>
<td>project.properties</td>
<td>140000-149999</td>
<td>Error messages generated by the project module</td>
</tr>
<tr>
<td>resource.properties</td>
<td>330000-339999</td>
<td>Resource entity names and resource-related error messages</td>
</tr>
<tr>
<td>role.properties</td>
<td>90000-99999</td>
<td>Error messages generated by the role module</td>
</tr>
<tr>
<td>service.properties</td>
<td>110000-119999</td>
<td>Error messages generated by the service module</td>
</tr>
<tr>
<td>signal.properties</td>
<td>310000-319999</td>
<td>Error messages generated by the connectivity signal module</td>
</tr>
<tr>
<td>specification.properties</td>
<td>130000-139999</td>
<td>Error messages generated by the specification module</td>
</tr>
<tr>
<td>status.properties</td>
<td>N/A</td>
<td>Error messages generated by the status module</td>
</tr>
<tr>
<td>subscriber.properties</td>
<td>150000-159999</td>
<td>Error messages generated by the subscriber module</td>
</tr>
<tr>
<td>system.properties</td>
<td>100000-109999</td>
<td>Error messages generated by the framework module</td>
</tr>
</tbody>
</table>
Localizing the UIM Server and the Application Server

By default, the UIM and application server software display information in English. You can set the software to display information in another language by localizing text strings in the UIM properties files. For more information, see UIM Developer’s Guide.

Shutting Down an Application Server

UIM provides a script to shut down an application server. Use the following command or the kill command on the machine running the server to be shut down:

```
stopWebLogic.sh AdminUserID AdminPassword ServerName
AdminServerURL
```

where `AdminServerURL` is in the format: `t3://ServerName:PortNumber`

For example:

```
stopWebLogic.sh weblogic password server03 t3://wplsnroyall:7101
```

Configuring the SSL Policy/Certificate

This section describes the configuration of SSL with Oracle WebLogic server. You must configure the new self-signed certificate in the WebLogic Administration Console.

To generate a new private key and self-signed certificate:

1. Navigate to the `WL_home/server/lib` directory and run the following command:

   ```
   keytool -alias alias -genkey -keypass keypass -keystore keystore.jks -storepass
   keystorepass
   ```

   where:
   - `alias` is the name
   - `keypass` is the password
   - `keystore.jks` is the key store name
   - `keystorepass` is the key store password

2. For What is your first and last name?, enter the application server IP address.

3. Provide relevant information for the following prompts:
   - What is the name of your organizational unit?
   - What is the name of your organization?
   - What is the name of your City or Locality?
   - What is the name of your State or Province?
   - What is the two-letter country code for this unit?
A summary is displayed showing the information you entered, as shown in the example below:

Is CN=IPAddressProvided, OU=OrganizationalUnit, O=Organization, L=Locality, ST=State, C=CountryCode correct?

- Enter Yes.
  The keystore keystore.jks file is created.

To configure the new self-signed certificate in the WebLogic Administration Console:
1. Log in to the WebLogic server Administration Console using the Administrator credentials.
  The Home screen appears.
2. Click Lock & Edit.
3. In the Domain Structure tree, expand Environment and then click Servers.
  The Summary of Servers screen appears.
4. In the Servers table, click AdminServer.
  The Settings for AdminServer screen appears.
  The General tab is displayed by default.
5. Select SSL Listen Port Enabled.
6. In the SSL Listen Port field, update the value as appropriate.
7. Click Save.
8. Click the Keystores tab.
9. Click Change and then from the Keystores list, select Custom Identity and Java Standard Trust.
10. Do the following:
    - In the Custom Identity Keystore field, enter the full path to your JKS file as follows:
      WL_Home/server/lib/keystore.jks
    - In the Custom Identity Keystore Type field, enter jks.
    - In the Custom Identity Keystore Passphrase field, enter the keystore password.
    - Leave the Java standard trust key as the default.
    - Click Save.
11. Click the SSL tab.
12. Do the following:
    - From the Identity and Trust Locations list, select Keystores.
    - In the Private Key Alias field, enter the alias name.
    - In the Private Key Passphrase field, enter the private key password.
    - Click Save.
    - Click Advanced.
From the Two Way Client Cert Behavior list, select Client Certs Requested But Not Enforced.

Click Save.

13. Click Activate Changes in the Change Center in the left pane.

For more information on SSL configuration, see the Administration Console Help.

---

**Note:** To replace a self-signed certificate with a production-quality certificate, or to import a trusted CA certificate into a keystore, run the following command:

```
keytool -import -alias alias -file cert.pem -keypass keypass -keystore keystore.jks -storepass keystorepass
```

---

**Note:** If you import a trusted CA certificate, no existing entry for alias should be in the keystore.

While accessing the application, the browser asks to install the certificate. Install the certificate in Trusted Root Certification Authorities.

### Resetting/Changing the WebLogic Server’s Database Connections

You may need to reset the WebLogic server’s database connections when the following occurs:

- The database goes down while UIM is active
- UIM is started when the database is down

You reset the database connections by resetting the following JDBC data sources in the WebLogic server administration console: InventoryDataSource, InventoryTxDataSource, CMDSInventoryPersistentDataSource, InventoryMapDataSource, InvJMSPersistentDataSource, mds-commsRepository, and UIMAdapterDataSource.

To reset/change the database connections:

1. Log in to the WebLogic server administration console at:
   
   `http://ServerName:PortNumber/console`

2. Click Lock & Edit.

3. In the Domain Structure tree, expand Services and then click Data Sources.
   
   The Summary of JDBC Data Sources page appears.

4. Click InventoryDataSource.
   
   The Settings for InventoryDataSource page appears.

5. Click the Control tab.

6. Select the check box next to the data source instance that you want to reset.

7. Click Reset.

8. Click Yes.
9. Click the Connection Pool tab.

10. Modify the following fields to match your environment:
   - URL
   - Properties
   - Password
   - Confirm Password

11. Repeat steps 4. through 10. for all the remaining data sources.

Setting the Default Telephone Number Edit Mask

The default telephone number edit mask defines the length format for telephone numbers entered into the UIM system. This value is used when a Telephone Number specification fails to specify the extension point rule set Formatting - SpecManager.getEditMask.

The initial value is ######## (eight digits).

When the rule, the properties file, or both the rule and the properties file fail to provide a default edit mask, the UIM application forces the edit mask to the value in the number.properties file.

To modify the default telephone number edit mask:

1. Open UIM_Home/config/resources/logging.
2. Find the following entry:
   ```
   number.defaultEditMask=##########
   ```
3. Change ########## to the desired length.
   - For example, enter ########## to set the telephone number length to 10 digits.
   - Each pound sign symbol (#) represents one digit.

Load Balancing a Clustered Server

The two methods for load balancing a clustered server include a hardware-based load balancer and a software-based proxy server.

Note: Oracle recommends using the hardware-based load balancer in production environments. Use either the hardware-based load balancer or the software-based proxy server in test or development environments.

Depending on the type of environment being deployed, do one of the following:
   - Configure the load balancer
   - Configure the proxy server
Configuring the Load Balancer

The requirement for the load balancer service is server affinity, also known as a sticky session. For example, a user starts a new session and it is load balanced to server #2. The subsequent HTTP requests in this session will be always routed to server #2 until server #2 fails.

For information on load balancer requirements, refer to the WebLogic document: Using WebLogic Server Clusters (see Load Balancing in a Cluster).

F5 BIG-IP Configuration Example


Model: BIG-IP LTM 6400
Software version: 9.4.0 Build 517.5

The following were configured in the BIG-IP load balancer:

Monitor, HTTP profile with rechunk, persistence profile with HTTP cookie insert, stream profile, OneConnect, TCP profile, pools, and a virtual server.

Cisco CSS 1150X Configuration Example

The following is an example configuration using Cisco CSS 1150X machines.

```plaintext
service uim01
  port 8026
  protocol tcp
  string uim01
  keepalive type http
  keepalive maxfailure 2
  keepalive retryperiod 2
  keepalive uri '/inv'
  ip address 10.143.34.53 (uim01 listening ip address)
  active

service uim02
  port 8026
  protocol tcp
  string uim02
  keepalive type http
  keepalive maxfailure 2
  keepalive retryperiod 2
  keepalive uri '/inv'
  ip address 10.143.34.56 (uim02 listening ip address)
  active

Owner test
content UIMCluster
  ip address 10.143.36.12
  protocol tcp
  port 8026
  add service uim01
  add service uim02
  advanced-balance arrowpoint-cookie
  balance leastconn
  param-bypass enable
  no persistentactive
```
Configuring the Proxy Server

There are several options available for the proxy server, refer to Oracle WebLogic Server documentation for information on configuring the various proxy server options.

Configuring Topology Updates

To configure topology updates, see the following topics:

- Configuring Asynchronous Topology Updates
- Turning Off Topology Updates
- Rebuilding Topology

Configuring Asynchronous Topology Updates

By default, the UIM topology is updated synchronously with business model changes. The topology and the business model are updated in single transaction to reflect new, changed, and deleted entities. See UIM Concepts and UIM Developer’s Guide for more information about topology.

You can configure UIM to update the topology asynchronously from business model updates. In this scenario, topology updates are performed in a separate transaction from business model updates. Configuring UIM to update the topology asynchronously can improve performance by reducing the system overhead associated with business model changes.

To configure UIM for asynchronous topology updates:

1. Stop the UIM application server.
2. Open the $UIM_home/config/topologyProcess.properties$ file.
3. Change the value of the processSynchronous entry to false.
4. Save the file.

Turning Off Topology Updates

If you use topology infrequently or want to optimize UIM performance, you can turn off topology updates entirely. If updates are turned off and you want to use topology-related features, such as path analysis, you must first rebuild the topology. See "Rebuilding Topology".

To turn off topology updates:

1. Stop the UIM application server.
2. Open the $UIM_home/config/topologyProcess.properties$ file.
3. Change the value of the disableTopology entry to true.
4. Save the file.

Rebuilding Topology

If you have turned off topology updates, you must rebuild the topology before you can use any topology-related features, such as path analysis or visualization. You should schedule this as a maintenance task during time when no changes to the inventory will take place.
If UIM is installed in a cluster environment, only one instance can be rebuilt at a time. When a rebuild is in progress on one instance, the rebuild operation is disabled for other instances.

You should schedule topology rebuilds during times when no changes to the inventory will take place.

To rebuild the UIM topology:

1. Log in to the Enterprise Management Console.
2. In the Tasks panel, click Rebuild Topology.
   The Rebuild Topology work area appears.
3. Click the Rebuild Topology button.
   The topology begins to be rebuilt. You can refresh the work area to see status updates. When the process is complete, the work area reverts to its original appearance and the Rebuild Topology button becomes available.

   You can check on the success of the rebuild by consulting the log at:

   WLServer_Home\user_projects\domains\Domain_Home\ui\logs\****Server_uim_rebuild.log

---

**Caution:** When you rebuild, the old topology is deleted and a new one created. You should back up your old topology to ensure that you can return to it if necessary.
This chapter describes ways to improve UIM performance.

**Improving UIM Performance Overview**

The following list includes tasks that you may need to perform to improve UIM performance.

- Configuring a Shared Index Directory
- Changing the Logging Level
- Enabling SQL and Other EclipseLink Logging
- Updating the System Configuration Files
- Setting Timeout Values for UIM
- Changing the Query Behavior and Row Limit Parameters

**Configuring a Shared Index Directory**

For multiserver deployment environments (including configurations for multiple single servers, admin/managed servers, and admin/clustered servers), you must deploy a common shared storage, such as a storage area network (SAN), for all UIM WebLogic application servers. Without a SAN, results may vary on different servers because some servers may have different domains.

**Changing the Logging Level**

UIM is using log4j for the logging services. For details on log4j, refer to: [http://logging.apache.org/log4j/1.2/index.html](http://logging.apache.org/log4j/1.2/index.html)

The logging level is defined in the `loggingconfig.xml` file.

The file is located in `UIM_Home/config`.

**Appender Configuration**

Three default appenders are supplied by default:

- **Stdout**
  
  Console Appender - used to log messages to the standard output
- rollingFile
  Rolling File Appender - used to log messages to the rolling file
  \textit{UIM\_Home/\textit{logs/WebLogic\_Name\_uim.log}}

- rebuildRollingFile
  Rolling File Appender - used to log the rebuild topology messages to the rolling
  file \textit{UIM\_Home/\textit{logs/WebLogic\_Name\_uim\_rebuild.log}}

The following is an example of the layout of the \textit{appender} log message:
\begin{verbatim}
%d{yyyy-MM-dd HH:mm:ss,SSS} %-5p [%X{userName}] [%X{requestSession}] [%c{1}] %m%n
\end{verbatim}

where:
- \texttt{%d{yyyy-MM-dd HH:mm:ss,SSS}}
  is the Date in the format \texttt{yyyy-MM-dd HH:mm:ss,SSS})
- \texttt{%-5p}
  is the priority of the logging event
- \texttt{%X{userName}}
  is the user name associated with the thread that generated the logging event
- \texttt{%X{requestSession}}
  is the session ID associated with the thread that generated the logging event. Note
  that the \texttt{requestSession} is not included by default. The layout value needs to be
  modified to add the \texttt{requestSession}.
- \texttt{%c{1}}
  is the category of the logging event with the \textbf{precision specifier} (ie: the decimal
  constant in brackets). The precision specifier correspond to the right most
  components of the category name. For example, for the category name
  \textit{oracle.communications.inventory.techpack.video.impl.VideoManagerImpl} the pattern
  \texttt{%c{1}} will output \textit{VideoManagerImpl}.
- \texttt{%m}
  is the application supplied message associated with the logging event. For
  example: \texttt{[INV-801005] No subscriber is associated to the service.}
- \texttt{%n}
  is the platform dependent line separator character or characters

For all parameters, see:
\url{http://logging.apache.org/log4j/1.2/apidocs/org/apache/log4j/PatternLayout.html}

This is a localized logging output message example:
\begin{verbatim}
2012-01-03 15:20:22,087 ERROR [uimuser1] [VideoManagerImpl] [INV-801005] No
subscriber is associated to the service.
\end{verbatim}

It's possible to filter the logging messages by the UIM user. To enable the UIM user
filter, we need to add the following element to the default \textit{appender}:
\begin{verbatim}
<filter class="oracle.communications.inventory.api.logging.util.FilterUtil">
<param name="userName" value=""/>
\end{verbatim}
The filter is already available, but commented out, in the default appender. To enable the UIM user filter, we can uncomment the filter and add a value to the userName parameter. For example:

```xml
<filter class="oracle.communications.inventory.api.logging.util.FilterUtil">
  <param name="userName" value="Justin"/>
</filter>
```

We can list multiple users in the filter by repeating the param element. For example:

```xml
<filter class="oracle.communications.inventory.api.logging.util.FilterUtil">
  <param name="userName" value="Justin"/>
  <param name="userName" value="Lili-Mai"/>
  <param name="userName" value="Marilou"/>
</filter>
```

### Logger Configuration

By default the root logger is set to error and will log the messages to the standard output and the UIM rolling file:

```xml
<root>
  <priority value="error"/>
  <appender-ref ref="stdout"/>
  <appender-ref ref="rollingFile"/>
</root>
```

Loggers may be assigned levels. The set of possible levels are (in the order message logging rank):

- **all** - lowest possible rank and is intended to turn on all logging
- **trace** - finer-grained informational events than the debug
- **debug** - fine-grained informational events that are most useful to debug an application
- **info** - informational messages that highlight the progress of the application at coarse-grained level
- **warn** - potentially harmful situations
- **error** - error events that might still allow the application to continue running
- **fatal** - very severe error events that will presumably lead the application to abort
- **off** - highest possible rank and is intended to turn off logging

Several application loggers are also pre-configured in the loggingconfig.xml file. Additional ones may be added as needed. For example, if the root logger level is set to error, but we would like to set the UIM Tech Packs logger level to debug, then we would add the following to the loggingconfig.xml:

```xml
<logger name="oracle.communications.inventory.techpack" additivity="false">
</logger>
```
Connecting debugger to UIM

**Tip:** To enable debug logging for the UIM Ruleset Extension Point Framework, you can add the following to the `loggingconfig.xml` file:

```xml
<logger name="oracle.communications.inventory.extensibility.rules" additivity="false">
  <level value="debug"/>
  <appender-ref ref="stdout"/>
  <appender-ref ref="rollingFile"/>
</logger>

<logger name="RuleSetLogger" additivity="false">
  <level value="debug"/>
  <appender-ref ref="stdout"/>
  <appender-ref ref="rollingFile"/>
</logger>
```

If you add the above, then you can comment out or remove the logger for `oracle.communications.inventory.extensibility.rules.impl`. It'll become redundant because `debug` level is enable on its parent package.

If we need to connect a debugger to the UIM Weblogic server, then we would need to edit the file `Domain_Home/bin/setUIMEnv.sh` and add the following string to the `USER_MEM_ARGS` variable:

```
-Xdebug -Xnoagent -Xrunjdwp:transport=dt_socket,address=1234,server=y,suspend=n -Djava.compiler=NONE
```
Example:
Before change:
USER_MEM_ARGS="-Xms1024m -Xmx3000m -Xmn850m -XX:MaxPermSize=1024m
-Xrs -XX:+HeapDumpOnOutOfMemoryError -XX:+UseConcMarkSweepGC
-XX:+CMSClassUnloadingEnabled -XX:+CMSPermGenSweepingEnabled"

After change:
USER_MEM_ARGS="-Xms1024m -Xmx3000m -Xmn850m -XX:MaxPermSize=1024m
-Xrs -XX:+HeapDumpOnOutOfMemoryError -XX:+UseConcMarkSweepGC
-XX:+CMSClassUnloadingEnabled -XX:+CMSPermGenSweepingEnabled -Xdebug
-Xnoagent -Xrunjdwp:transport=dt_socket,address=1234,server=y,suspend=n
-Djava.compiler=NONE"

You can adjust the port by changing address=1234.

## Enabling SQL and Other EclipseLink Logging

To enable SQL and other EclipseLink logging, perform the following:

1. Open a command window.
2. Navigate to the `MW_Home/oracle_common/common/bin` directory.
3. Start the WebLogic Scripting Tool (WLST) using the following command:
   ```bash
   ./wlst.sh
   ```
4. Connect to the server on which you want to change the logging level, use the following command:
   ```bash
   connect(userid,password,'t3://hostname:port')
   ```
5. Go to Custom settings using the following command:
   ```bash
   custom()
   ```

   **Note:** `custom()` can take a while to execute, approximately 5 minutes or more.

6. Go to TopLink using the following command:
   ```bash
   cd('TopLink')
   ```
7. List the sessions at this level using the following command:
   ```bash
   ls()
   ```

   **Note:** The following is an example of a TopLink session:
   ```bash
   TopLink:Name=Session(file/share/uimcluster/domains/clusterUim
   720b1357/servers/uim_ms1/tmp/_WL_user/oracle.communications.inventory/b0t675/APP-INF/lib/uim-entities.jar_default'
   ```

8. Copy the session and go to that session using the following command:
cd('session')

9. Change the EclipseLink logging level using the following command:

   set('CurrentEclipseLinkLogLevel',newLevel)

   **Note:** EclipseLink provides 9 logging levels, refer to Table 6–1 for a list of the different logging levels and a brief description of each.

### Table 6–1  EclipseLink Logging Levels

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OFF</td>
<td>This setting disables the generation of the log output. You may want to set logging to OFF during production to avoid the overhead of logging.</td>
</tr>
<tr>
<td>SEVERE</td>
<td>This level enables reporting of failure cases only. Usually, if the failure occurs, the application stops.</td>
</tr>
<tr>
<td>WARNING</td>
<td>This level enables logging of issues that have a potential to cause problems. For example, a setting that is picked by the application and not by the user.</td>
</tr>
<tr>
<td>INFO</td>
<td>This level enables the standard output. The contents of this output is very limited. It is the default logging level if a logging level is not set.</td>
</tr>
<tr>
<td>CONFIG</td>
<td>This level enables logging of such configuration details as your database login information and some metadata information. You may want to use the CONFIG log level at deployment time.</td>
</tr>
<tr>
<td>FINE</td>
<td>This level enables logging of the first level of the debugging information and SQL. You may want to use this log level during debugging and testing, but not at production.</td>
</tr>
<tr>
<td>FINER</td>
<td>This level enables logging of more debugging information than the FINE setting. For example, the transaction information is logged at this level. You may want to use this log level during debugging and testing, but not at production.</td>
</tr>
<tr>
<td>FINEST</td>
<td>This level enables logging of more debugging information than the FINER setting, such as a very detailed information about certain features (for example, sequencing). You may want to use this log level during debugging and testing, but not at production.</td>
</tr>
<tr>
<td>ALL</td>
<td>This level currently logs at the same level as FINEST.</td>
</tr>
</tbody>
</table>

10. To enable SQL logging use the following command:

   set('CurrentEclipseLinkLogLevel','FINE')

### Updating the System Configuration Files

The system configuration files located in UIM_Home/config are:

- castor.properties
- config-reload.properties
- consumer.properties
- reference.properties
- ruleProcess.properties
- system-config.properties
- timers.properties
- topologyProcess.properties

You may need to update these files depending on your environment.
If you are wanting to change telephone number again, see "Updating the consumer.properties File" and "Updating the timers.properties File".

See the next sections for property default values and examples.

**Updating the castor.properties File**

The *castor.properties* file is used to configure Castor. You can update the values in this file or leave the defaults.

- **1.** The *org.exolab.castor.indent* property of the *castor.properties* file is used to control if all documents should be indented on output by default.
  
  The default value is true.

  Example:

  org.exolab.castor.indent=true

- **2.** The *org.exolab.castor.xml.naming* property of the *castor.properties* file is used to preserve the Java mixed-case conventions. By default, all names are treated as the "lower" option. Uncomment the following line to preserve the Java mixed-case conventions:

  org.exolab.castor.xml.naming=mixed

- **3.** The *org.exolab.castor.parser* property of the *castor.properties* file is used to define the default XML parser to be used by Castor. The parser must implement org.xml.sax.Parsers.

  The default value is org.apache.xerces.parsers.SAXParser.

  Example:

  org.exolab.castor.parser=org.apache.xerces.parsers.SAXParser

- **4.** The *org.exolab.castor.xml.serializer.factory* property of the *castor.properties* file is used to define the (default) XML serializer factory to use by Castor, which must implement org.exolab.castor.xml.SerializerFactory.

  The default value is org.exolab.castor.xml.XercesXMLSerializerFactory.

  Example:

  org.exolab.castor.xml.serializer.factory=org.exolab.castor.xml.XercesXMLSerializerFactory

---

**Note:** When using Castor XML with JDK 5.0, you may switch to the XercesJDK5XMLSerializerFactory which will use the Xerces instance as shipped with the JDK itself; this avoids having to download another Xerces instance and installing it.

Example:

org.exolab.castor.xml.serializer.factory=org.exolab.castor.xml.XercesXMLSerializerFactory

---

**Updating the config-reload.properties File**

The *config-reload.properties* file is used to control inventory automatic reload. You can update the values in this file or leave the defaults.
1. The `inventory.auto.reload.enabled` property of the `config-reload.properties` file is used to enable/disable auto reload of System configuration properties.
   The default value is true.
   Example:
   ```properties
   inventory.auto.reload.enabled=true
   ```

2. The `inventory.auto.reload.interval` property of the `config-reload.properties` file is used to set the reload interval in milli seconds.
   The default value is 3000 milli seconds.
   Example:
   ```properties
   inventory.auto.reload.interval=3000
   ```

### Updating the consumer.properties File

The `consumer.properties` file is used to control consumption of entities. You can update the values in this file or leave the defaults.

1. The `deleteReservation.batchsize` property of the `consumer.properties` file is used to control the number of expired reservation records to be deleted for each execution of the Cleanup Expired Reservation timer process.
   The default value is 1000 records.
   Example:
   ```properties
   deleteReservation.batchSize=1000
   ```

2. The following pertain to telephone number (TN) aging and the TN lifecycle properties of the `consumer.properties` file.
   The `tn.defaultDisconnectedStateExpiry` property of the `consumer.properties` file is used to change the expiration period for transitional TN assignment state from Disconnected state to Transitional state.
   The default value is 30 days.
   Example:
   ```properties
   tn.defaultDisconnectedStateExpiry=30
   ```

3. The `tn.defaultTransitionalStateExpiry` property of the `consumer.properties` file is used to change the expiration period for transitional TN assignment state from Transitional state to Unassigned state.
   The default value is 30 days.
   Example:
   ```properties
   tn.defaultTransitionalStateExpiry=30
   ```

4. The `tn.recallTNSearchResultsLimit` property of the `consumer.properties` file is used to control the number of telephone number assignment records selected for the TN Aging and Recall Timer process.
   The default value is 500 records.
   Example:
   ```properties
   tn.recallTNSearchResultsLimit=500
   ```
5. The `tn.portabilityCharacteristicName` property of the `consumer.properties` file is used to specify the characteristic name of the TN which will be used in portability logic.
   
The default value is `tnType`.
   
Example:
   ```
   tn.portabilityCharacteristicName=tnType
   ```

6. The `tn.winbackCharacteristicName` property of the `consumer.properties` file is used to specify the characteristic name of the TN which will be used in winback (stealback) logic.
   
Example:
   ```
   tn.winbackCharacteristicName=winback
   ```

**Updating the reference.properties File**

The `reference.properties` file is used to control referenced properties. You can update the values in this file or leave the defaults.

1. The `AllowDeactivateReferencedCustomNetworkAddress` property of the `reference.properties` file is used to deactivate the ReferencedCustomNetworkAddress property.
   
The default value is false.
   
Example:
   ```
   AllowDeactivateReferencedCustomNetworkAddress=false
   ```

2. The `AllowDeactivateReferencedCustomObject` property of the `reference.properties` file is used to deactivate the ReferencedCustomObject property.
   
The default value is false.
   
Example:
   ```
   AllowDeactivateReferencedCustomObject=false
   ```

3. The `AllowDeactivateReferencedEquipment` property of the `reference.properties` file is used to deactivate the ReferencedCustomEquipment property.
   
The default value is false.
   
Example:
   ```
   AllowDeactivateReferencedEquipment=false
   ```

4. The `AllowedDeactivateReferencedLogicalDevice` property of the `reference.properties` file is used to deactivate the ReferencedLogicalDevice property.
   
The default value is false.
   
Example:
   ```
   AllowedDeactivateReferencedLogicalDevice=false
   ```

5. The `AllowDeactivateReferencedLogicalDeviceAccount` property of the `reference.properties` file is used to deactivate the ReferencedLogicalDeviceAccount property.
   
The default value is false.
Example:
AllowDeactivateReferencedLogicalDeviceAccount=false

6. The **AllowDeactivateReferencedNetwork** property of the **reference.properties** file is used to deactivate the ReferencedNetwork property.
The default value is false.
Example:
AllowDeactivateReferencedNetwork=false

7. The **AllowDeactivateReferencedPhysicalDevice** property of the **reference.properties** file is used to deactivate the ReferencedPhysicalDevice property.
The default value is false.
Example:
AllowDeactivateReferencedPhysicalDevice=false

8. The **AllowDeactivateReferencedPipe** property of the **reference.properties** file is used to deactivate the ReferencedPipe property.
The default value is false.
Example:
AllowDeactivateReferencedPipe=false

9. The **AllowDeactivateReferencedTelephoneNumber** property of the **reference.properties** file is used to deactivate the ReferencedTelephoneNumber property.
The default value is false.
Example:
AllowDeactivateReferencedTelephoneNumber=false

10. The **AllowSuspendReferencedService** property of the **reference.properties** file is used to suspend the ReferencedService property.
The default value is true.
Example:
AllowSuspendReferencedService=true

11. The **AllowDisconnectReferencedService** property of the **reference.properties** file is used to disconnect the ReferencedService property.
The default value is true.
Example:
AllowDisconnectReferencedService=true

12. The **AllowCancelReferencedService** property of the **reference.properties** file is used to cancel the ReferencedService property.
The default value is true.
Example:
AllowCancelReferencedService=true
13. The **AllowCancelReferencedBusinessInteraction** property of the **reference.properties** file is used to cancel the ReferencedBusinessInteraction property.

   The default value is true.
   
   Example:
   
   AllowCancelReferencedBusinessInteraction=true

**Updating the ruleProcess.properties File**

The **ruleProcess.properties** file is used to control the Work Manager. You can update the values in this file or leave the defaults.

1. The **WORK_MANAGER_JNDI** property of the **ruleProcess.properties** file is a setting only for WebLogic.

   Example:
   
   WORK_MANAGER_JNDI=java:comp/env/wm/ruleWorkManager

2. The **timeOutSec** property of the **ruleProcess.properties** file is used to set the timeout in WorkManager during cartridge Install.

   The default value is 10000 milli seconds.

   Example:
   
   timeOutSec=10000

**Updating the system-config.properties File**

1. The **createTN.flushSize** property of the **system-config.properties** file controls the number of telephone number entities to create before calling the flush transaction.

   Do not set the **createTN.flushSize** property to more than 500.

   Example:
   
   createTN.flushSize=500

2. The **securityViolationLoggingEnabled** property of the **system-config.properties** file is used for setting security access violation logging.

   Example:
   
   securityViolationLoggingEnabled=true

3. The following properties of the **system-config.properties** file are used for setting System specific settings.

   Examples:
   
   system.minDate=0
   
   system.maxDate=2147483647000
   
   system.lastModifiedDateThreshold=15

4. The **businessInteraction.allowCancelWithCompletedChild** property of the **system-config.properties** file is used to allow a business interaction to be canceled if it has completed children.

   Example:
   
   businessInteraction.allowCancelWithCompletedChild=false
5. The `businessInteraction.allowCancelWithCompletedConfiguration` property of the `system-config.properties` file is used to allow a business interaction to be canceled if it is associated to a completed configuration version.

   Example:
   
   ```
   businessInteraction.allowCancelWithCompletedConfiguration=false
   ```

6. The `lockPolicy.defaultRowLockExpirationDuration` property of the `system-config.properties` file is used for setting the default row lock expiration duration for the entity. The value is defined in milli seconds. This value should be defined as that it should be less than or equal to transaction time out.

   The default value is 30000.

   Example:
   
   ```
   lockPolicy.defaultRowLockExpirationDuration=30000
   ```

7. The `lockPolicy.MaxSupportedRowLocks` property of the `system-config.properties` file is used for setting the default maximum number of entities to be row locked. This should be in sync with the maximum number or range.

   The default value is 100.

   Example:
   
   ```
   lockPolicy.MaxSupportedRowLocks=100
   ```

8. The `system.auth.debug` property of the `system-config.properties` file is used to enable/disable the system authentication debug.

   Example:
   
   ```
   system.auth.debug=false
   ```

9. The `db.sequence.cacheSize` property of the `system-config.properties` file is used for setting the cache size for Oracle Sequence used for Auto ID generation.

   The default value is 20.

   Example:
   
   ```
   db.sequence.cacheSize=20
   ```

10. The `cmws.asynch.mode` property of the `system-config.properties` file is used for setting the Cartridge deployment mode to either synchronous or asynchronous.

    Example:
    
    ```
    cmws.asynch.mode=true
    ```

11. The `ui.search.pageSize` property of the `system-config.properties` file is used for setting the number of rows in a page in the UI. This number is applicable to the searches. When a Search is performed, only a page of data is brought back to the server. As the user scrolls beyond this page, next page is automatically retrieved from the database.

    The default value is 200.

    Example:
    
    ```
    ui.search.pageSize=200
    ```

12. The `ui.search.queryBehavior` property of the `system-config.properties` file is used for setting the query behavior. There are various choices presented to the system about how much data is queried from the database and whether the count is
retrieved for the UI. Based on performance evaluations, one of the following values can be picked:

FULL_COUNT_FULL_QUERY(1) (This is the default value)

NO_COUNT_FULL_QUERY(2)

LIMIT_COUNT_FULL_QUERY(3)

LIMIT_COUNT_LIMIT_QUERY(4)

Refer to the UIM System Administrator’s Guide about the details and pros and cons of these query behaviors.

The default value is 1.

Example:

ui.search.queryBehavior=1

13. The ui.search.queryLimit property of the system-config.properties file is used for setting the limit to be applied to the query and the count, through the UI. A -1 indicates that no limit is applied. Change this value if you want to apply a limit.

Refer to the UIM System Administrator’s Guide about the details on how this query limit is used.

Example:

ui.search.queryLimit=-1

14. The uim.default.paging.query.hint property of the system-config.properties file is used to improve performance of the finder APIs when invoked from Web Services. When a search query is fired from web service without SearchPolicy then the API will set this default query hint.

Example:

uim.defaultpaging.query.hint=FIRST_ROWS(25)

15. The uim.security.filter.enabled property of the system-config.properties file is used for setting security access to allow for the configuring of partitions.

Example:

uim.security.filter.enabled=false

16. The following properties of the system-config.properties file are used for setting Entity specific cache settings.

Examples:

uim.entitySpecificCache.enable=false

oracle.communications.platform.entity.impl.ServiceConfigurationVersionDAO.size=0

oracle.communications.platform.entity.impl.ServiceConfigurationVersionDAO.expiry=0

oracle.communications.platform.entity.impl.ServiceConfigurationVersionDAO.disableHits=true

oracle.communications.platform.entity.impl.BusinessInteractionDAO.size=0

oracle.communications.platform.entity.impl.BusinessInteractionDAO.expiry=0

oracle.communications.platform.entity.impl.BusinessInteractionDAO.disableHits=true
Updating the timers.properties File

Each timer can be defined by five properties: `firstTime`, `period`, `fixedRate`, `listener`, and `cluster`.

- **firstTime**: The first time to call the listener. If it is specified as relative time (without `:`), such as 600 (in seconds), then the listener will be called 10 minutes after the system is started.
  
  If it is specified as absolute time, such as 12:00:00 (noon), or 23:00:00 (11PM), then the listener will be called at the specified time after the system is started.

  If it is specified as "onTheHour", then the listener will be executed on the next hour (for example 08:00:00) after the system is started (for example 07:28:34).

  The default is 60 seconds in relative time.

- **period**: After the listener is called the first time, the number of seconds between repeating expiration intervals. The listener will be called when the timer expires.

  The default is 600 seconds.

- **fixedRate**: This is not used.

- **listener**: The listener’s class name. The listener’s `timerExpired(Timer timer)` method will be executed when the timer expired.

  There is no default. This property must be specified.

- **cluster**: The flag indicates whether this timer is cluster aware. If it is set to true, then there will only one instance of this timer running in the cluster. If it is set to false, then each server will have this timer instance running locally.

  Most of the timer should be cluster aware. An example of non-cluster aware timer is the timer which monitors whether the server which manages the cluster aware timers is still alive.

  The default value is true.

The `timers.properties` file is located in:

`UIM_Home/config/timers.properties`.

1. The `clusterTimerMonitor` timer of the `timers.properties` file is a timer to monitor if the current server which manages the cluster aware timers is still alive.

   This timer should be running on every server in the cluster.

   Examples:

   ```properties
   clusterTimerMonitor.firstTime=10
   clusterTimerMonitor.period=10
   clusterTimerMonitor.listener=oracle.communications.inventory.api.framework.timer.TimerController
   clusterTimerMonitor.cluster=false
   ```

2. The `customTimer` timer of the `timers.properties` file is a customer timer for custom extensions.
Updating the System Configuration Files

Updating the topologyProcess.properties File

The topologyProcess.properties file is used to control referenced properties. You can update the values in this file or leave the defaults.

1. The disableTopology property of the topologyProcess.properties file is used to turn Topology Refresh On or Off.
   The default value is false.
   Example:
   disableTopology=false

2. The processSynchronous property of the topologyProcess.properties file is used to refreshTopology as part of the transaction (true) or asynchronously in a separate transaction (false).
   The default value is true.
   Example:
processSynchronous=true

3. The `mapperClass` property of the `topologyProcess.properties` file is the Class Object that maps the business model to Topology.

Example:

mapperClass=com.metasolv.api.topology.mapper.impl.TopologyMapperImpl

4. The `WORK_MANAGER_CLASS`, `WORK_MANAGER_NAME`, and `WORK_MANAGER_THREADS` properties of the `topologyProcess.properties` file are settings only for oc4j.

Examples:

WORK_MANAGER_CLASS=com.tangosol.coherence.commonj.WorkManager
WORK_MANAGER_NAME=TopologyWorkManager
WORK_MANAGER_THREADS=20

5. The `WORK_MANAGER_JNDI` property of the `topologyProcess.properties` file is a setting only for WebLogic.

Example:

WORK_MANAGER_JNDI=java:comp/env/wm/TopologyWorkManager

6. The `defaultBaseMap`, `defaultApplicationDatasource`, `defaultMapTileServerUrl`, and `defaultMapCopyright` properties of the `topologyProcess.properties` file are used to set the default Map Profile settings.

Examples:

defaultBaseMap=elocation_mercator.world_map
defaultApplicationDatasource=UIMDATA
defaultMapTileServerUrl=http://elocation.oracle.com/mapviewer/mcserver
defaultMapCopyright=Copyright © 2007, 2012 Oracle Corp © 2010 NAVTEQ

7. The `MapViewerUrl` property of the `topologyProcess.properties` file is used if mapviewer is running in a separate domain. Uncomment the following line:

Example:

mapviewerUrl=http://hostname:port/mapviewer

8. The `simpleLinearMode`, `simpleLinearModeMaxCycles`, and `continueProcessingIndicator` properties of the `topologyProcess.properties` file are used to set the Path Analysis properties.

Examples:

simpleLinearMode=false
simpleLinearModeMaxCycles=5
continueProcessingIndicator=true

9. The following properties, used by Topology (rebuild/async) processing, are not to be modified. If modified, Topology may not work as expected.

Examples:

topology.threadedEntityList=LogicalDevice,PhysicalDevice,Equipment,GeographicPlace
topology.nonThreadedEntityList=Network,NetworkNode,Pipe,NetworkEdge
topology.placeRelList=LogicalDevice,PhysicalDevice,Equipment,NetworkNode,Network,GeographicPlace
topology.netNodeRelList=LogicalDevice,PhysicalDevice,Equipment,Network

10. The `rebuildServiceTopology` property of the `topologyProcess.properties` file is used for rebuilding service topology data.
    The default value is true.
    Example:
    ```
topology.rebuildServiceTopology=true
    ```

11. The `rebuildChunkSize` property of the `topologyProcess.properties` should be a number only.
    Example:
    ```
topology.rebuildChunkSize=100
    ```

12. The date format for the `topologyProcess.properties` file is `//EEE MMM d HH:mm:ss z yyyy`, for example - EST Jan19 22:14:07 2038.
    Examples:
    ```
topology.fromDate=EST Jan 29 22:14:07 2009
    topology.toDate=EST Jan 19 22:14:07 2038
    ```

### Setting Timeout Values for UIM

The WebLogic server supports distributed transactions, which are transactions that update multiple resource managers, such as an application server and a database, in a single transaction. This guarantees data integrity by ensuring that transactional updates are either committed or rolled back in all of the participating databases.

This section explains how to set transaction timeouts for the Oracle database, JTA, and XA. In general, the JTA timeout should be less than or equal to the XA timeout, and the XA timeout should be less than or equal to the Oracle database timeout:

JTA timeout <= XA timeout <= database timeout

Oracle recommends setting all three transaction timeouts to 1800 seconds.

### Setting the Oracle Database Timeout

The `DISTRIBUTED_LOCK_TIMEOUT` is a parameter of the database. There are two ways to change this parameter. You can use Oracle Enterprise Manager or use `sql`.

To change the `DISTRIBUTED_LOCK_TIMEOUT` parameter using `sql`:

1. Open `sqlplus`.
2. Connect to the database.
3. Enter:
   ```
   alter system set distributed_lock_timeout=1800 scope=spfile
   ```

   The default value for this parameter is 60 seconds, but Oracle recommends setting this parameter to 1800 seconds.
Setting the JTA Timeout

You specify how long a transaction can remain in the Active state until the transaction is rolled back by using the WebLogic server administration console.

To set the JTA timeout value:

1. Log in to the WebLogic server administration console at:
   
   `http://ServerName:PortNumber/console`

2. Click Lock & Edit.

3. In the Domain Structure tree, expand Services, and then click JTA.
   
   The Settings for Domain_Name pane appears.

4. Update the value in the Timeout Seconds field and then click Save.

5. Click Activate Changes.

Changing the Query Behavior and Row Limit Parameters

The query behavior and row limit parameters are defined in the `system-config.properties` file.

The file is located in the `UIM_Home/config/system-config.properties`.

The default options are as follows:

Example:

```
ui.search.queryLimit=-1 (-1 means do not limit)
ui.search.queryBehavior=1
ui.search.pageSize=200
```

Table 6–2 describes the options available for the Query Behavior and Row Limit parameters.
Changing the Query Behavior and Row Limit Parameters

To change the Query Behavior and Row Limit parameters, perform the following:

1. Open a command window.
2. Navigate to the `UIM_Home/config/system-config.properties` file.
3. Open the `system-config.properties` file and scroll down to the `ui.search.queryLimit`, `ui.search.queryBehavior` and `ui.search.pageSize` entries.
4. Change the parameters as required, to meet the specific needs of your deployment. Refer to Table 6–3 for a description of the pros and cons of the parameter options.
5. Save and close the `system-config.properties` file.

### Table 6–2  Query Behavior and Row Limit Parameters

<table>
<thead>
<tr>
<th>Behavior (option #)</th>
<th>Row Limit</th>
<th>Count</th>
<th>Scrolling</th>
</tr>
</thead>
<tbody>
<tr>
<td>FULL_COUNT_FULL_QUERY (1)</td>
<td>N/A</td>
<td>The exact count is displayed.</td>
<td>User can scroll through the entire result set.</td>
</tr>
<tr>
<td>NO_COUNT_FULL_QUERY (2)</td>
<td>N/A</td>
<td>Not displayed</td>
<td>User can scroll through the entire result set.</td>
</tr>
<tr>
<td>LIMIT_COUNT_FULL_QUERY (3)</td>
<td>Used for count only</td>
<td>If total count &lt; row limit, then total count is displayed else: Total count: row limit (Limit Reached) is displayed</td>
<td>User can scroll the results up to the row limit.</td>
</tr>
<tr>
<td>LIMIT_COUNT_LIMIT_QUERY (4)</td>
<td>Used for count and query</td>
<td>If total count &lt; row limit, then total count is displayed else Total count: row limit (Limit Reached) is displayed</td>
<td>User can scroll the results up to the row limit.</td>
</tr>
<tr>
<td>Behavior</td>
<td>Advantages</td>
<td>Disadvantages</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>FULL_COUNT_FULL_QUERY(1)</td>
<td>You know the exact count of rows satisfying the criteria. You can scroll through the entire result set.</td>
<td>If the user does not give meaningful criteria, and the number of rows matching the criteria is large, it may take a while to calculate the count. If the database is not tuned correctly, sorting the entire data set may take a while.</td>
<td></td>
</tr>
<tr>
<td>NO_COUNT_FULL_QUERY(2)</td>
<td>The query for finding the total count is not performed. So it will help the performance of the pages.</td>
<td>Usability of the page is not as good. The scrollbar in the page is not representative of the number of rows satisfying the data and so user never knows how much he needs to scroll. If the database is not tuned correctly, sorting the entire data set may take a while.</td>
<td></td>
</tr>
<tr>
<td>LIMIT_COUNT_FULL_QUERY(3)</td>
<td>If the criteria is meaningful, and the number of rows satisfying the criteria is less than the row limit, there is no difference in the results brought back and usability of the pages as compared to Behavior (1) or Behavior (4). Better performance as compared to Behavior (1), as the count query is limited. Results are more accurate as compared to Behavior (4).</td>
<td>User cannot scroll to the rows past the row limit.</td>
<td></td>
</tr>
<tr>
<td>LIMIT_COUNT_LIMIT_QUERY(4)</td>
<td>If the criteria is meaningful, and the number of rows satisfying the criteria is less than the row limit, there is no difference in the results brought back and usability of the pages as compared to Behavior (1) or Behavior (3). Better performance as compared to Behavior (1), as the count query is limited. Better performance as compared to Behavior (3), as the query is limited.</td>
<td>User cannot scroll to the rows past the row limit. If the number of rows matching the criteria is more than the row limit, the row limit is applied before the ordering, so the first rows displayed maybe not be the first in the sort order of the entire dataset.</td>
<td></td>
</tr>
</tbody>
</table>
This chapter describes how to backup and restore Oracle Communications Unified Inventory Management (UIM) data. It covers the following topics:

It is important to understand how to back up critical data to protect the system against different failures. You can save backup artifacts in various ways—by using periodic backups to tape or fault-tolerant disks, or by manually copying files to another machine.

**WebLogic Server Related Artifacts**

The following sections describe the artifacts that you should back up.

**Static Artifacts**

Static artifacts are those that change less frequently. These include:

- **MW_Home** (except `user_projects/domains/domain_name`) for the Administration Server and all the Managed Servers
- **WL_Home** (by default, it resides in **MW_Home** and it can be configured by the user to point to a different location) for the Administration Server and all the Managed Servers

This data is changed only while patching or upgrading the environment.

**Runtime Artifacts**

Runtime artifacts are those that change more frequently. These include:

- **Domain_Home** and **UIM_Home** directories in all the servers (By default, it resides in **Domain_Home**, but it can be configured by the user to point to a different location.)
- UIM Application artifacts (`.ear` files, `.war` files, `.properties` files) which reside outside of the domain directory on each of the servers (in case of nostage or external_stage application staging modes)

This data changes frequently while updating the domain configurations, deploying an application, and while performing other administrative changes.

**Persistent Stores**

A persistent store provides a built-in, high-performance storage solution for WebLogic Server subsystems and services that require persistence. For example, it can store
persistent JMS (Java Messaging Service) messages or durable subscriber information, as well as temporarily store messages sent to an unavailable destination using the Store-and-Forward feature. The persistent store supports persistence to a file-based store (File Store) or to a JDBC enabled database (JDBC Store). The default store maintains its data in the `Domain_Home/servers/AdminServer/data/store/default` directory inside the servername subdirectory of a domain’s root directory.

**Using a Shared File System to Backup the Artifacts**

The best practice is to store snapshots of the above artifacts either at the file system level, or using one of the models suggested below in “Using the WebLogic Backup Utility” and “Using the Pack and Unpack Utility”, onto a Storage Area Network (SAN). This would ensure the local machine failure at the physical level doesn’t impact the backups.

It is best to take backups before configuration changes are done.

**Using the WebLogic Backup Utility**

You can configure Oracle WebLogic Server to make backup copies of the configuration files. This facilitates recovery in cases where configuration changes need to be reversed or in the unlikely case that configuration files become corrupted. When the Administration Server starts up, it saves a JAR file named `config-booted.jar` that contains the configuration files. When you make changes to the configuration files, the old files are saved in the `configArchive` directory under the `Domain_Home` directory, in a JAR file with a sequentially numbered name such as `config-1.jar`. The configuration archive is always local to the Administration Server host. It is a best practice to back up the archives to an external location.

**Using the Pack and Unpack Utility**

This utility provides a way to define templates and use the template to pack a domain for unpacking later or to unpack in another node. Please note that the domain UIM is deployed in may contain other applications and the admin needs to ensure the UIM specific components are packed if the upgrade or patch is happening in UIM. You can use a template that contains a subset of a domain to create a Managed Server domain directory hierarchy on a remote machine. It would ensure that when unpacked only the UIM artifacts are restored.

Refer to the Oracle WebLogic Server documentation for more details.

**Restoring WebLogic Related Configurations and Artifacts**


The link above describes the different scenarios and what needs to be restored in each of the scenarios.

**Embedded LDAP**

If any of your security realms use the Default Authentication, Authorization, Credential Mapping, or Role Mapping providers, you should maintain an up-to-date backup of the following directory tree:

`Domain_Home/servers/AdminServer/data/ldap`
In the preceding directory, Domain_Home is the domain root directory and AdminServer is the directory in which the Administration Server stores run-time and security data.

For more information backing up the embedded LDAP server data, see the following topics:

- "Configure backups for embedded LDAP servers" in Oracle WebLogic Server Administration Console Help
- "Back Up LDAP Repository" in Managing Server Startup and Shutdown for Oracle WebLogic Server located at the following link:
  [http://docs.oracle.com/cd/E12840_01/wls/docs103/server_start/failures.html](http://docs.oracle.com/cd/E12840_01/wls/docs103/server_start/failures.html)

If the embedded LDAP server file becomes corrupt or unusable, the Administration Server will generate a NumberFormatException and fail to start. This situation is rare but can occur if the disk becomes full and causes the embedded LDAP file to enter into an invalid state.

Do not update the configuration of a security provider while a backup of LDAP data is in progress. If a change is made—for instance, if an administrator adds a user—while you are backing up the ldap directory tree, the backups in the ldapfiles subdirectory could become inconsistent. If this does occur, consistent, but potentially out-of-date, LDAP backups are available, because once a day, a server suspends write operations and creates its own backup of the LDAP data. It archives this backup in a ZIP file below the ldap/backup directory and then resumes write operations. This backup is guaranteed to be consistent, but it might not contain the latest security data.

### Restoring Embedded LDAP Server File

To recover from an unusable embedded LDAP server file, complete the following steps:

1. Change to the following directory:
   
   Domain_Home/servers/AdminServer/data

2. Rename the embedded LDAP server file, as in the following example:

   mv ldap ldap.old
   
   where mv is the Unix command used to rename the file.

   By renaming the file, and not deleting it completely, it remains available to you for analysis and potential data recovery.

3. Start the Administration Server.
   
   When the Administration Server starts, a new embedded LDAP server file is created.

4. Restore any data to the new embedded LDAP server that was added since the time the WebLogic domain was created.
   
   If you have configured a backup of the embedded LDAP server, you can restore the backed up data by importing it. For information, see Exporting and Importing Information in the Embedded LDAP Server.
   
   [http://download.oracle.com/docs/cd/E17904_01/web.1111/e13707/ldap.htm#SECMG543](http://download.oracle.com/docs/cd/E17904_01/web.1111/e13707/ldap.htm#SECMG543)
Export and Import of LDAP Data

Alternatively the export and import functions could also be used as described in Exporting and Importing Information in the Embedded LDAP Server.

Database Backup and Restore

Use Recovery Manager (RMAN) to back up, restore, and recover data files, control files, server parameter files (SPFILEs) and archived redo log files. You can use RMAN with a media manager to back up files to external storage. You can also configure parallelism when backing up or recovering Oracle RAC databases. In Oracle RAC, RMAN channels can be dynamically allocated across all of the Oracle RAC instances. Channel failover enables failed operations on one node to continue on another node. You can start RMAN from Oracle Enterprise Manager Backup Manager or from the command line.

For more information about using RMAN, see Configuring Recovery Manager and Archiving at the following link:

http://download.oracle.com/docs/cd/E11882_01/rac.112/e16795/rman.htm#g496102

---

**Note:** In addition to the UIM schema the MDS schema which was used in the installation process should also be backed up for failure handling.

---

Backup SerializedSystemIni.dat and Security Certificates

Each server instance creates a file named `SerializedSystemIni.dat` and locates it in the `Domain_Home/security` directory. This file contains encrypted security data that must be present to boot the server. You must back up this file.

If you configured a server to use SSL, you must also back up the security certificates and keys. The location of these files is user-configurable.
Managing the Unified Inventory Management Database

This chapter provides information about managing your Oracle Communications Unified Inventory Management (UIM) database and file system.

Overview of Managing the UIM Database

The UIM database management tasks include:

- Tuning the Database

Tuning the Database

This section explains how to tune your UIM database.

Table 8–1 and Table 8–2 provide recommended database parameters for tuning your database. These are the minimum requirements for UIM.

<table>
<thead>
<tr>
<th>Table 8–1  Database Creation Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>SGA+PGA</td>
</tr>
<tr>
<td>Processes</td>
</tr>
<tr>
<td>Connection mode</td>
</tr>
<tr>
<td>Redo log file size</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 8–2  Database Initialization Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>db_file_multiblock_read_count</td>
</tr>
<tr>
<td>distributed_lock_timeout</td>
</tr>
<tr>
<td>dml_locks</td>
</tr>
<tr>
<td>job_queue_processes</td>
</tr>
<tr>
<td>log_buffer</td>
</tr>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>-----------------------</td>
</tr>
<tr>
<td>open_cursors</td>
</tr>
<tr>
<td>parallel_max_servers</td>
</tr>
<tr>
<td>plsql_code_type</td>
</tr>
</tbody>
</table>