Oracle® Communications Unified Inventory Management

System Administrator's Guide

Release 7.2.2

E36044-01

January 2013

Oracle Communications Unified Inventory Management System Administrator's Guide, Release 7.2.2

E36044-01

Contents

5 Improving Unified Inventory Management Performance

6 Unified Inventory Management Backup and Restore

7 Managing the Unified Inventory Management Database

Preface

This guide contains information about administering Oracle Communications Unified Inventory Management (UIM). This guide includes information about how to start and stop UIM, 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 11*g*R1, Oracle WebLogic, and Java J2EE software.

Related Documentation

For more information, see the following documents in the Oracle Communications Unified Inventory Management Release 7.2.2 documentation set:

- *UIM Installation Guide*: Describes the requirements for installing UIM, installation procedures, and post-installation tasks.
- *UIM Security Guide*: Provides guidelines and recommendations for setting up UIM in a secure configuration.
- *UIM Concepts*: Provides an overview of important concepts and an introduction to using both UIM and Design Studio.
- *UIM Developer's Guide*: Explains how to customize and extend many aspects of UIM, including the data model, life-cycle management, topology, security, rulesets, Web services, user interface, 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 Cartridge and Technology Pack Guide*: Provides information about how you use cartridges and technology packs with UIM. Describes the content of the base cartridges.
- 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:

- Design Studio Help: Provides step-by-step instructions for tasks you perform in Design Studio.
- UIM Help: Provides step-by-step instructions for tasks you perform in UIM.

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.

1

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 adminstrator:

- Starting and stopping the UIM server. See "Starting and Stopping UIM" 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

Placeholder	Default Directory Path	Directory Description
MW_Home	**/opt/Oracle/Middleware**	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.
WL_Home	**/opt/Oracle/Middleware/wlserver_10.3**	The base directory for the WebLogic Server core files. It is located in the *MW_Home* directory.
Domain_Home	**/opt/Oracle/Middleware/user_projects/domains/***domain_name* where *domain_name* is the name assigned to the domain at installation	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.
UIM_Home	**/opt/Oracle/Middleware/user_projects/domains/***domain_name***/UIM** where *domain_name* is the name assigned to the domain at installation	The directory into which UIM was installed. This directory contains various installation-related files.

2 Starting and Stopping UIM

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**.

   The Summary of Servers screen appears.

4. View the state of the Administration Server and and verify that the state is 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, 7.2.2.0.0)

   oracle.communications.inventory.customlib(7.2, 7.2.2.0.0)

   oracle.communications.inventory.externallib(7.2, 7.2.2.0.0)

   oracle.communications.inventory.javadoc

   oracle.communications.inventory.mapviewer

   oracle.communications.platform.poms(11.1.1.6.0, 1.2.0.0.0)

   oracle.communications.platform.ies(11.1.1.6.0, 1.2.0.0.0)

   oracle.communications.platform.cui.webapp(11.1.1.6.0, 1.2.0.0.0)

   oracle.communications.platform.WsFramework(11.1.1.6.0, 1.2.0.0.0)

   cartridge_management_ws(1.2.0.0.0)

   > **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
   ```

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**.

> **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

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.

3

Understanding UIM Security

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.

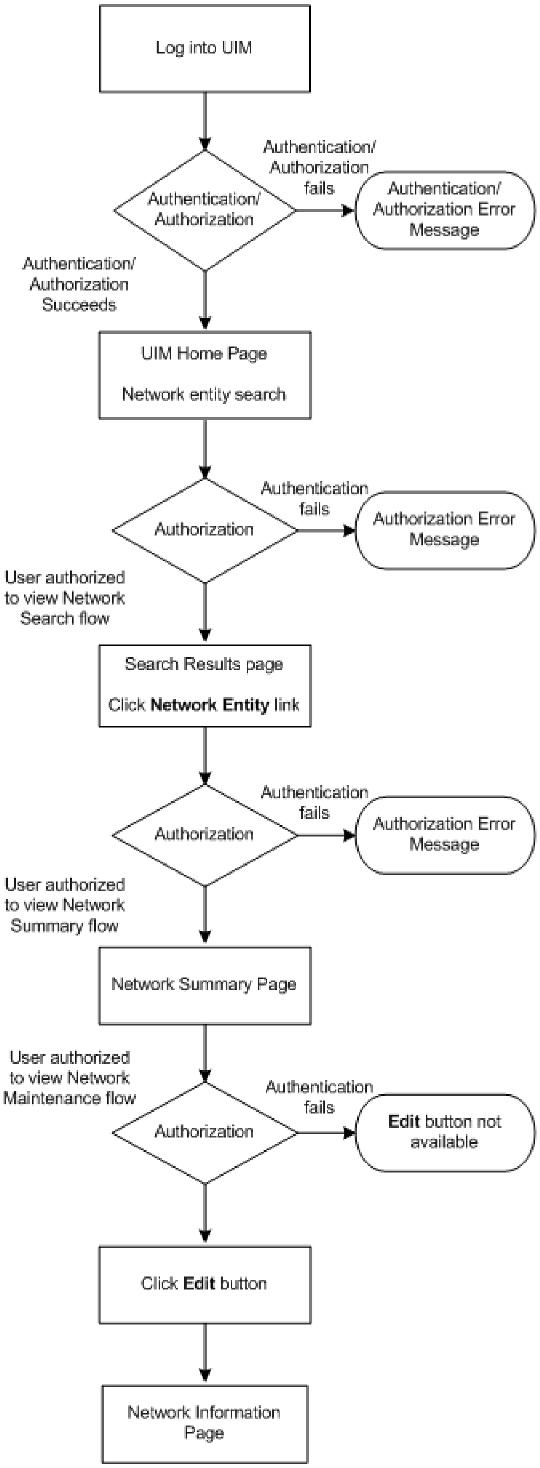
UIM Security Overview

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 3–1 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.

Figure 3–1 Authentication and Authorization Flow


Log into UIM
Authentication/ Authorization
Authentication/ Authorization fails
Authentication/ Authorization Error Message
Authentication/ Authorization Succeeds
UIM Home Page
Network entity search
Authorization
Authentication fails
Authorization Error Message
User authorized to view Network Search flow
Search Results page
Click **Network Entity** link
Authorization
Authentication fails
Authorization Error Message
User authorized to view Network Summary flow
Network Summary Page
User authorized to view Network Maintenance flow
Authorization
Authentication fails
Edit button not available
Click **Edit** button
Network Information Page

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 Web Logic 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.inventory**).
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**.

10. Navigate to the *Domain_Home*/**UIM/app/plan** directory.

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. You can retrieve user information, including the roles assigned to a user, through the **UserEnvironment** class. See *UIM Developer's Guide* for an example.

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 3–2 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:

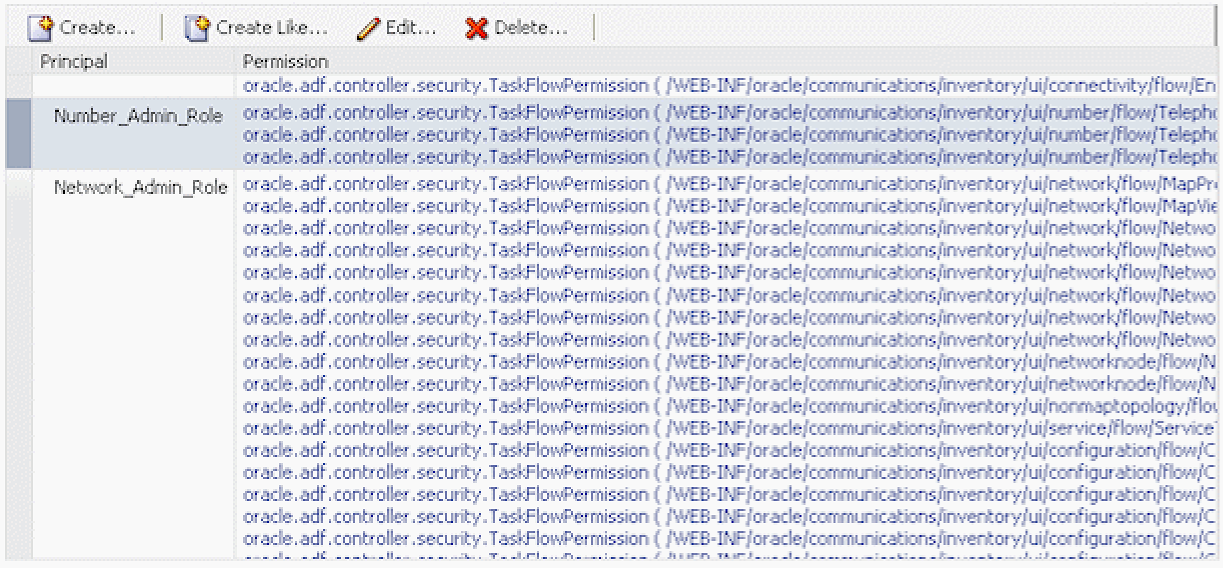
- /WEB-INF/oracle/communications/inventory/ui/number/flow/TelephoneNumberSearchResultsFlow.xml#TelephoneNumberSearchResultsFlow
- /WEB-INF/oracle/communications/inventory/ui/number/flow/TelephoneNumberSummaryFlow.xml#TelephoneNumberSummaryFlow
- /WEB-INF/oracle/communications/inventory/ui/number/flow/TelephoneNumberEditFlow.xml#TelephoneNumberEditFlow

> **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 3–2 Security Policies in Oracle Enterprise Manager



Principal	Permission
	oracle.adf.controller.security.TaskFlowPermission (/WEB-INF/oracle/communications/inventory/ui/connectivity/flow/En
Number_Admin_Role	oracle.adf.controller.security.TaskFlowPermission (/WEB-INF/oracle/communications/inventory/ui/number/flow/Telepho oracle.adf.controller.security.TaskFlowPermission (/WEB-INF/oracle/communications/inventory/ui/number/flow/Telepho oracle.adf.controller.security.TaskFlowPermission (/WEB-INF/oracle/communications/inventory/ui/number/flow/Telepho
Network_Admin_Role	oracle.adf.controller.security.TaskFlowPermission (/WEB-INF/oracle/communications/inventory/ui/network/flow/MapPr oracle.adf.controller.security.TaskFlowPermission (/WEB-INF/oracle/communications/inventory/ui/network/flow/MapVie oracle.adf.controller.security.TaskFlowPermission (/WEB-INF/oracle/communications/inventory/ui/network/flow/Netwo oracle.adf.controller.security.TaskFlowPermission (/WEB-INF/oracle/communications/inventory/ui/network/flow/Netwo oracle.adf.controller.security.TaskFlowPermission (/WEB-INF/oracle/communications/inventory/ui/network/flow/Netwo oracle.adf.controller.security.TaskFlowPermission (/WEB-INF/oracle/communications/inventory/ui/network/flow/Netwo oracle.adf.controller.security.TaskFlowPermission (/WEB-INF/oracle/communications/inventory/ui/network/flow/Netwo oracle.adf.controller.security.TaskFlowPermission (/WEB-INF/oracle/communications/inventory/ui/network/flow/Netwo oracle.adf.controller.security.TaskFlowPermission (/WEB-INF/oracle/communications/inventory/ui/networknode/flow/N oracle.adf.controller.security.TaskFlowPermission (/WEB-INF/oracle/communications/inventory/ui/networknode/flow/N oracle.adf.controller.security.TaskFlowPermission (/WEB-INF/oracle/communications/inventory/ui/nonmaptopology/flo oracle.adf.controller.security.TaskFlowPermission (/WEB-INF/oracle/communications/inventory/ui/service/flow/Service oracle.adf.controller.security.TaskFlowPermission (/WEB-INF/oracle/communications/inventory/ui/configuration/flow/C oracle.adf.controller.security.TaskFlowPermission (/WEB-INF/oracle/communications/inventory/ui/configuration/flow/C oracle.adf.controller.security.TaskFlowPermission (/WEB-INF/oracle/communications/inventory/ui/configuration/flow/C oracle.adf.controller.security.TaskFlowPermission (/WEB-INF/oracle/communications/inventory/ui/configuration/flow/C oracle.adf.controller.security.TaskFlowPermission (/WEB-INF/oracle/communications/inventory/ui/configuration/flow/C

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 3–1 lists all of the UIM taskflow permissions, sorted by component name.

Table 3–1 Taskflow Permissions

Component	Access Type	Permission String	Controls the Ability to:
Business Interaction	Edit	/WEB-INF/oracle/communications/inventory/ui/businessinteraction/flow/BusinessInteractionEditFlow.xml#BusinessInteractionEditFlow	Edit a business interaction from search results or the Summary work area.
Business Interaction	View	/WEB-INF/oracle/communications/inventory/ui/businessinteraction/flow/BusinessInteractionSearchResultsFlow.xml#BusinessInteractionSearchResultsFlow	Open a Search work area for business interactions by clicking the **Business Interactions** link in the **Tasks** panel.
Business Interaction	View	/WEB-INF/oracle/communications/inventory/ui/businessinteraction/flow/BusinessInteractionSummaryFlow.xml#BusinessInteractionSummaryFlow	Open a Business Interaction Summary by clicking on the id (hyperlink) in the **Business Interactions** search results.
Business Interaction	View	/WEB-INF/oracle/communications/inventory/ui/businessinteraction/flow/BusinessInteractionAttachmentSummaryFlow.xml#BusinessInteractionAttachmentSummaryFlow	Open a Business Interaction Attachment Summary work area, which displays the XML payload.
Characteristics	View	/WEB-INF/oracle/communications/inventory/ui/characteristic/flow/CharacteristicSpecificationSearchResultsFlow.xml#CharacteristicSearchResultsFlow	View characteristics search results.
Characteristics	View	/WEB-INF/oracle/communications/inventory/ui/characteristic/flow/CharacteristicSpecificationSummaryFlow.xml#CharacteristicSpecificationSummaryFlow	Open a Characteristic Specification Summary work area.
Custom Network Address	View	/WEB-INF/oracle/communications/inventory/ui/customnetworkaddress/flow/CustomNetworkAddressSearchResultsFlow.xml#CustomNetworkAddressSearchResultsFlow	Open a Search work area for custom network addresses by clicking the **Custom Network Address** link in the **Tasks** panel.
Custom Network Address	View	/WEB-INF/oracle/communications/inventory/ui/customnetworkaddress/flow/CustomNetworkAddressSummaryFlow.xml#CustomNetworkAddressSummaryFlow	Open a Custom Network Address Summary work area.

Table 3–1 (Cont.) Taskflow Permissions

Component	Access Type	Permission String	Controls the Ability to:
Custom Network Address	Edit	/WEB-INF/oracle/communications/inventory/ui/customnetworkaddress/flow/CustomNetworkAddressEditFlow.xml#CustomNetworkAddressEditFlow	Edit a custom network address from search results or a Summary work area.
Condition	Edit	/WEB-INF/oracle/communications/inventory/ui/consumer/flow/ConditionEditFlow.xml#ConditionEditFlow	Edit a condition by opening its work area from the **Related Pages** menu in an entity work area.
Condition	View	/WEB-INF/oracle/communications/inventory/ui/consumer/flow/ConditionListFlow.xml#ConditionListFlow	Open the list of conditions associated by using the **Related Pages** menu in an entity work area.
Configuration	View	/WEB-INF/oracle/communications/inventory/ui/configuration/flow/ConfigurationSummaryFlow.xml#ConfigurationSummaryFlow	Open a Configuration Summary work area. (For all configurations except Pipe.)
Configuration	Edit	/WEB-INF/oracle/communications/inventory/ui/configuration/flow/ConfigurationEditFlow.xml#ConfigurationEditFlow	Edit an entity configuration. (For all configurations except Pipe.)
Configuration	Edit	/WEB-INF/oracle/communications/inventory/ui/configuration/flow/ConfigurationItemAddFlow.xml#ConfigurationItemAddFlow	Add a configuration item from a Configuration Summary work area. (For all configurations, except Pipe.)
Configuration	Edit	/WEB-INF/oracle/communications/inventory/ui/configuration/flow/ConfigurationItemRenameFlow.xml#ConfigurationItemRenameFlow	Rename a configuration item in a Configuration Summary work area
Configuration	Edit	/WEB-INF/oracle/communications/inventory/ui/configuration/flow/ConfigurationMaintainCharacteristicsFlow.xml#ConfigurationMaintainCharacteristicsFlow	Edit configuration characteristics.
Connectivity	View	/WEB-INF/oracle/communications/inventory/ui/connectivity/flow/ConnectivityGapAnalysisFlow.xml	View Gap Analysis.
Connectivity	View	/WEB-INF/oracle/communications/inventory/ui/connectivity/flow/MultiplexedFacilityCapacityConfigurationFlow.xml	View Capacity Configuration Page.
Connectivity	View	/WEB-INF/oracle/communications/inventory/ui/connectivity/flow/TDMConnectivityChannelFlow.xml	View Connectivity Channel page.
Connectivity	Edit	/WEB-INF/oracle/communications/inventory/ui/connectivity/flow/TDMConnectivityCreateFlow.xml	Create Connectivity.
Connectivity	View	/WEB-INF/oracle/communications/inventory/ui/connectivity/flow/TDMConnectivityDesignFlow.xml	View Connectivity Design Page.
Connectivity	View	/WEB-INF/oracle/communications/inventory/ui/connectivity/flow/TDMConnectivityDetailsFlow.xml	View Connectivity Details Page.

Table 3–1 (Cont.) Taskflow Permissions

Component	Access Type	Permission String	Controls the Ability to:
Connectivity	View	/WEB-INF/oracle/communications/inventory/ui/connectivity/flow/TDMConnectivitySearchResultsFlow.xml	View Connectivity Search Page.
Connectivity	View	/WEB-INF/oracle/communications/inventory/ui/connectivity/interconnection/visualization/flow/CrossConnectsViewFlow.xml	View Cross Connect Visualization Page.
Consumer	View	/WEB-INF/oracle/communications/inventory/ui/consumer/flow/ConsumerListFlow.xml#ConsumerListFlow	View telephone number assignments in a Telephone Number Summary work area.
Custom Object	View	/WEB-INF/oracle/communications/inventory/ui/customobject/flow/CustomObjectSearchResultsFlow.xml#CustomObjectSearchResultsFlow	Open a Search work area for custom objects by clicking the **Custom Objects** link in the **Tasks** panel.
Custom Object	View	/WEB-INF/oracle/communications/inventory/ui/customobject/flow/CustomObjectSummaryFlow.xml#CustomObjectSummaryFlow	Open a Custom Object Summary work area.
Custom Object	Edit	/WEB-INF/oracle/communications/inventory/ui/customobject/flow/CustomObjectEditFlow.xml#CustomObjectEditFlow	Edit a custom object from search results or a Summary work area.
Device Interface	View	/WEB-INF/oracle/communications/inventory/ui/deviceinterface/flow/DeviceInterfaceSearchResultsFlow.xml#DeviceInterfaceSearchResultsFlow	Open a Search work area for device interfaces by clicking the **Device Interface** link in the **Tasks** panel.
Device Interface	View	/WEB-INF/oracle/communications/inventory/ui/deviceinterface/flow/DeviceInterfaceSummaryFlow.xml#DeviceInterfaceSummaryFlow	Open a Device Interface Summary work area.
Device Interface	Edit	/WEB-INF/oracle/communications/inventory/ui/deviceinterface/flow/DeviceInterfaceEditPopupFlow.xml#DeviceInterfaceEditFlow	Edit a device interface from a device interface hierarchy.
Device Interface	Edit	/WEB-INF/oracle/communications/inventory/ui/deviceinterface/flow/DeviceInterfaceEditFlow.xml#DeviceInterfaceEditFlow	Edit a device interface from a Device Interface Summary work area
Equipment	View	/WEB-INF/oracle/communications/inventory/ui/equipment/flow/EquipmentSearchResultsFlow.xml#EquipmentSearchResultsFlow	Open a Search work area for equipment by clicking the **Equipment** link in the **Tasks** panel.
Equipment	View	/WEB-INF/oracle/communications/inventory/ui/equipment/flow/EquipmentSpecVisualFlow.xml#EquipmentSpecVisualFlow	Open an Equipment Specification Visual work area by using the **Related Pages** menu in the Equipment Specification Summary work area.
Equipment	View	/WEB-INF/oracle/communications/inventory/ui/equipment/flow/EquipmentSummaryFlow.xml#EquipmentSummaryFlow	Open an Equipment Summary work area.
Equipment	View	/WEB-INF/oracle/communications/inventory/ui/equipment/flow/EquipmentViewFlow.xml#EquipmentViewFlow	Open an Equipment Visual work area.

Table 3–1 (Cont.) Taskflow Permissions

Component	Access Type	Permission String	Controls the Ability to:
Equipment	Edit	/WEB-INF/oracle/communications/inventory/ui/equipment/flow/EquipmentEditFlow.xml#EquipmentEditFlow	Edit an Equipment entity from search results or a Summary work area.
Equipment	Edit	/WEB-INF/oracle/communications/inventory/ui/equipment/flow/EquipmentRangeEditFlow.xml#EquipmentRangeEditFlow	Edit a range of Equipment entities.
Equipment Holder	View	/WEB-INF/oracle/communications/inventory/ui/equipmentholder/flow/EquipmentHolderSearchResultsFlow.xml#EquipmentHolderSearchResultsFlow	Open a Search work area for device interfaces by clicking the **Device Interface** link in the **Tasks** panel.
Equipment Holder	View	/WEB-INF/oracle/communications/inventory/ui/equipmentholder/flow/EquipmentHolderSummaryFlow.xml#EquipmentHolderSummaryFlow	Open an Equipment Holder Summary work area.
Equipment Holder	Edit	/WEB-INF/oracle/communications/inventory/ui/equipmentholder/flow/EquipmentHolderEditFlow.xml#EquipmentHolderEditFlow	Edit an equipment holder.
Favorite Items	View	/WEB-INF/oracle/communications/platform/cui/flows/FavoriteItemsFlow.xml#FavoriteItemsFlow	View the **Favorites** menu in the UIM main page.
Favorite Items	Edit	/WEB-INF/oracle/communications/platform/cui/flows/ManageFavoritesFlow.xml#ManageFavoritesFlow	Edit the contents of the **Favorites** menu in the UIM main page.
Import	Edit	/WEB-INF/oracle/communications/inventory/ui/admin/flow/ExecuteRuleFlow.xml#ExecuteRuleFlow	View the Inventory Import work area.
Inventory Group	View	/WEB-INF/oracle/communications/inventory/ui/inventorygroup/flow/InventoryGroupSearchResultsFlow.xml#InventoryGroupSearchResultsFlow	Open a Search work area for inventory groups by clicking the **Inventory Group** link in the **Tasks** panel.
Inventory Group	View	/WEB-INF/oracle/communications/inventory/ui/inventorygroup/flow/InventoryGroupSummaryFlow.xml#InventoryGroupSummaryFlow	View an Inventory Group Summary work area.
Inventory Group	Edit	/WEB-INF/oracle/communications/inventory/ui/inventorygroup/flow/InventoryGroupEditFlow.xml#InventoryGroupEditFlow	Edit an inventory group from search results or a Summary work area.
Involvement	Edit	/WEB-INF/oracle/communications/inventory/ui/custominvolvement/flow/CustomInvolvementEditFlow.xml#CustomInvolvementEditFlow	Edit a custom involvement from an entity Summary work area. The user can edit the custom involvement by clicking **Edit** in the **Custom Involvement** list in the entity Summary page.
Logical Device	View	/WEB-INF/oracle/communications/inventory/ui/logicaldevice/flow/LogicalDeviceSearchResultsFlow.xml#LogicalDeviceSearchResultsFlow	Open a Search work area for logical devices by clicking the **Logical Device** link in the **Tasks** panel.

Table 3–1 (Cont.) Taskflow Permissions

Component	Access Type	Permission String	Controls the Ability to:
Logical Device	View	/WEB-INF/oracle/communications/inventory/ui/logicaldevice/flow/LogicalDeviceSummaryFlow.xml#LogicalDeviceSummaryFlow	Open a Logical Device Summary work area.
Logical Device	Edit	/WEB-INF/oracle/communications/inventory/ui/logicaldevice/flow/LogicalDeviceEditFlow.xml#LogicalDeviceEditFlow	Edit a logical device from search results or a Summary work area.
Logical Device	Edit	/WEB-INF/oracle/communications/inventory/ui/device/MaintainMappingsFlow.xml#MaintainMappingsFlow	Map a device interface to a physical connector or physical port.
Logical Device Account	View	/WEB-INF/oracle/communications/inventory/ui/logicaldeviceaccount/flow/LogicalDeviceAccountSearchResultsFlow.xml#LogicalDeviceAccountSearchResultsFlow	Open a Search work area for logical device accounts by clicking the **Logical Device Account** link in the **Tasks** panel.
Logical Device Account	View	/WEB-INF/oracle/communications/inventory/ui/logicaldeviceaccount/flow/LogicalDeviceAccountSummaryFlow.xml#LogicalDeviceAccountSummaryFlow	Open a Logical Device Account Summary work area.
Logical Device Account	Edit	/WEB-INF/oracle/communications/inventory/ui/logicaldeviceaccount/flow/LogicalDeviceAccountEditFlow.xml#LogicalDeviceAccountEditFlow	Edit a logical device account from search results or a Summary work area.
Logical Device Account	Edit	/WEB-INF/oracle/communications/inventory/ui/logicaldeviceaccount/flow/LogicalDeviceAccountRangeEditFlow.xml#LogicalDeviceAccountRangeEditFlow	Edit a range of logical device accounts.
Map Profile	Edit	/WEB-INF/oracle/communications/inventory/ui/network/flow/MapProfileEditFlow.xml#MapProfileEditFlow	Edit a the map profile from a Network Summary work area.
Map Viewer	View	/WEB-INF/oracle/communications/inventory/ui/network/flow/MapViewFlow.xml#MapViewFlow	Open the Map Viewer application.
Media Resource	View	/WEB-INF/oracle/communications/inventory/ui/mediaresource/flow/MediaResourceLogicalDeviceListFlow.xml#MediaResourceLogicalDeviceListFlow	Open a list of media resources in a Logical Device or Media Stream Summary work area.
Media Stream	View	/WEB-INF/oracle/communications/inventory/ui/mediaresource/flow/MediaStreamSearchResultsFlow.xml#MediaStreamSearchResultsFlow	Open a Search work area for media streams by clicking the **Media Streams** link in the **Tasks** panel.
Media Stream	View	/WEB-INF/oracle/communications/inventory/ui/mediaresource/flow/MediaStreamSummaryFlow.xml#MediaStreamSummaryFlow	Open a Media Stream Summary work area.
Media Stream	Edit	/WEB-INF/oracle/communications/inventory/ui/mediaresource/flow/MediaStreamEditFlow.xml#MediaStreamEditFlow	Edit a Media Stream entity from search results or a Summary work area.
Network	View	/WEB-INF/oracle/communications/inventory/ui/networknode/flow/NetworkNodeSearchResultsFlow.xml#NetworkNodeSearchResultsFlow	Open a Search work area for network nodes. The work area is opened from the topology visualization.

Table 3–1 (Cont.) Taskflow Permissions

Component	Access Type	Permission String	Controls the Ability to:
Network	View	/WEB-INF/oracle/communications/inventory/ui/network/flow/NetworkSearchResultsFlow.xml#NetworkSearchResults	Open a Search work area for Network entities by clicking the **Network** link in the **Tasks** panel.
Network	View	/WEB-INF/oracle/communications/inventory/ui/network/flow/NetworkSummaryFlow.xml#NetworkSummaryFlow	View a Network Summary page.
Network	View	/WEB-INF/oracle/communications/inventory/ui/network/flow/NetworkViewFlow.xml#NetworkViewFlow	View a Network Visualization work area.
Network	View	/WEB-INF/oracle/communications/inventory/ui/nonmaptopology/flow/NonMapTopologyViewFlow.xml#NonMapTopologyViewFlow	Open the Topological View work area.
Network	Edit	/WEB-INF/oracle/communications/inventory/ui/networkedge/flow/NetworkEdgeEditFlow.xml#NetworkEdgeEditFlow	Edit a network edge from Network canvas.
Network	Edit	/WEB-INF/oracle/communications/inventory/ui/network/flow/NetworkEditFlow.xml#NetworkEditFlow	Edit a Network entity from search results or a Summary work area.
Network	Edit	/WEB-INF/oracle/communications/inventory/ui/networknode/flow/NetworkNodeEditFlow.xml#NetworkNodeEditFlow	Edit a network node from Network canvas.
Party	View	/WEB-INF/oracle/communications/inventory/ui/party/flow/PartySearchResultsFlow.xml#PartySearchResultsFlow	Open a Search work area for parties by clicking the **Party** link in the **Tasks** panel.
Party	View	/WEB-INF/oracle/communications/inventory/ui/party/flow/PartySummaryFlow.xml#PartySummaryFlow	Open a Party Summary work area.
Party	Edit	/WEB-INF/oracle/communications/inventory/ui/party/flow/PartyEditFlow.xml#PartyEditFlow	Edit a party from search results or a Summary work area.
Path Analysis	Edit	/WEB-INF/oracle/communications/inventory/ui/connectivity/flow/PathAnalysisFlow.xml#PathAnalysisFlow	Open a Path Analysis work area from a Pipe or Pipe Configuration work area.
Physical Connector	View	/WEB-INF/oracle/communications/inventory/ui/physicalconnector/flow/PhysicalConnectorSearchResultsFlow.xml#PhysicalConnectorSearchResultsFlow	Open a Search work area for physical connectors from a Physiscal Device or Equipment Summary work area.
Physical Connector	View	/WEB-INF/oracle/communications/inventory/ui/physicalconnector/flow/PhysicalConnectorSummaryFlow.xml#PhysicalConnectorSummaryFlow	Open a Physical Connector Summary work area from a Physical Device or Equipment Summary work area..
Physical Connector	Edit	/WEB-INF/oracle/communications/inventory/ui/physicalconnector/flow/PhysicalConnectorEditFlow.xml#PhysicalConnectorEditFlow	Edit a physical connector from a Physiscal Device or Equipment Summary work area.

Table 3–1 (Cont.) Taskflow Permissions

Component	Access Type	Permission String	Controls the Ability to:
Physical Device	View	/WEB-INF/oracle/communications/inventory/ui/physicaldevice/flow/PhysicalDeviceSearchResultsFlow.xml#PhysicalDeviceSearchResultsFlow	Open a Search work area for physical devices by clicking the **Physical Device** link in the **Tasks** panel.
Physical Device	View	/WEB-INF/oracle/communications/inventory/ui/physicaldevice/flow/PhysicalDeviceSummaryFlow.xml#PhysicalDeviceSummaryFlow	Open a Physical Device Summary work area.
Physical Device	Edit	/WEB-INF/oracle/communications/inventory/ui/physicaldevice/flow/PhysicalDeviceEditFlow.xml#PhysicalDeviceEditFlow	Edit a physical device from search results or a Summary work area.
Physical Port	View	/WEB-INF/oracle/communications/inventory/ui/physicalport/flow/PhysicalPortSearchResultsFlow.xml#PhysicalPortSearchResultsFlow	Open a Search work area for physical ports from a Physiscal Device or Equipment Summary work area.
Physical Port	View	/WEB-INF/oracle/communications/inventory/ui/physicalport/flow/PhysicalPortSummaryFlow.xml#PhysicalPortSummaryFlow	Open a Physical Port Summary page from a Physiscal Device or Equipment Summary work area.
Physical Port	Edit	/WEB-INF/oracle/communications/inventory/ui/physicalport/flow/PhysicalPortEditFlow.xml#PhysicalPortEditFlow	Edit a physical port from a Physical Device or Equipment Summary work area.
Pipe	View	/WEB-INF/oracle/communications/inventory/ui/connectivity/flow/EnabledbyViewFlow.xml#EnabledbyViewFlow	Open an Enabled by Visualization work area from a Pipe Summary work area.
Pipe	View	/WEB-INF/oracle/communications/inventory/ui/configuration/flow/PipeConfigurationTrailListFlow.xml#PipeConfigurationTrailListFlow	Open an Enabled By Visualization work area in a Pipe Configuration Summary work area.
Pipe	View	/WEB-INF/oracle/communications/inventory/ui/connectivity/flow/PipeSearchResultsFlow.xml#PipeSearchResultsFlow	Open a Search work area for pipes by clicking the **Pipe** link in the **Tasks** panel.
Pipe	View	/WEB-INF/oracle/communications/inventory/ui/connectivity/flow/PipeSummaryFlow.xml#PipeSummaryFlow	Open a Pipe Summary work area.
Pipe	View	/WEB-INF/oracle/communications/inventory/ui/connectivity/flow/PipeTerminationPointSearchResultsFlow.xml#PipeTerminationPointSearchResultsFlow	Open a Search work area for pipe termination points.
Pipe	View	/WEB-INF/oracle/communications/inventory/ui/connectivity/flow/PipeTerminationPointSummaryFlow.xml#PipeTerminationPointSummaryFlow	Open a Pipe Termination Point Summary work area from a Pipe Summary work area.
Pipe	View	/WEB-INF/oracle/communications/inventory/ui/configuration/flow/PipeConfigurationSummaryFlow.xml#PipeConfigurationSummaryFlow	Open a Pipe Configuration Summary work area.

Table 3–1 (Cont.) Taskflow Permissions

Component	Access Type	Permission String	Controls the Ability to:
Pipe	Edit	/WEB-INF/oracle/communications/inventory/ui/connectivity/flow/PipeEditFlow.xml#PipeEditFlow	Edit a pipe from search results or a Summary work area.
Pipe	Edit	/WEB-INF/oracle/communications/inventory/ui/connectivity/flow/PipeTPDirectionEditPopupFlow.xml#PipeTPDirectionEditPopupFlow	Edit pipe directionality from a Pipe Summary work area.
Pipe	Edit	/WEB-INF/oracle/communications/inventory/ui/connectivity/flow/PipeTerminationPointEditFlow.xml#PipeTerminationPointEditFlow	Edit a pipe termination point from a Pipe Summary work area.
Place	View	/WEB-INF/oracle/communications/inventory/ui/place/flow/PlaceSearchResultsFlow.xml#PlaceSearchResultsFlow	Open a Search work area for places by clicking the **Place** link in the **Tasks** panel.
Place	View	/WEB-INF/oracle/communications/inventory/ui/place/flow/PlaceSummaryFlow.xml#PlaceSummaryFlow	Open a Place Summary work area.
Place	Edit	/WEB-INF/oracle/communications/inventory/ui/place/flow/PlaceEditFlow.xml#PlaceEditFlow	Edit a place from search results or a Summary page.
Product	View	/WEB-INF/oracle/communications/inventory/ui/product/flow/ProductSearchResultsFlow.xml#ProductSearchResultsFlow	Open a Search work area for products by clicking the **Product** link in the **Tasks** panel.
Product	View	/WEB-INF/oracle/communications/inventory/ui/product/flow/ProductSummaryFlow.xml#ProductSummaryFlow	Open a Product Summary work area.
Product	Edit	/WEB-INF/oracle/communications/inventory/ui/product/flow/ProductEditFlow.xml#ProductEditFlow	Edit a product from search results or a Summary work area.
PopertyLocation	View	/WEB-INF/oracle/communications/inventory/ui/location/flow/LocationSearchResultsFlow.xml	View Property Location Search Page.
PropertyLocation	Edit	/WEB-INF/oracle/communications/inventory/ui/location/flow/LocationDetailsFlow.xml	View Property Location Create/Edit Page.
Reservation	View	/WEB-INF/oracle/communications/inventory/ui/consumer/flow/ReservationListFlow.xml#ReservationListFlow	View the reservation list for an entity by selecting from the **Related Pages** menu in an entity Summary page.
Reservation	View	/WEB-INF/oracle/communications/inventory/ui/consumer/flow/ReservationSearchResultsFlow.xml#ReservationSearchResultsFlow	Open a Search work area for reservations by clicking the **Reservation** link in the **Tasks** panel.
Reservation	Edit	/WEB-INF/oracle/communications/inventory/ui/consumer/flow/RedeemReservationFlow.xml#RedeemReservationFlow	Open the Redeem Reservation work area.
Reservation	Edit	/WEB-INF/oracle/communications/inventory/ui/consumer/flow/ReservationEditFlow.xml#ReservationEditFlow	Edit a reservation.
Role	Edit	/WEB-INF/oracle/communications/inventory/ui/role/flow/InventoryRoleEditFlow.xml#InventoryRoleEditFlow	Edit a role from an entity Summary work area.

Table 3–1 (Cont.) Taskflow Permissions

Component	Access Type	Permission String	Controls the Ability to:
RuleSet	View	/WEB-INF/oracle/communications/inventory/ui/rule/flow/RuleSearchResultsFlow.xml#RuleSearchResultsFlow	Open a Search work area for rulesets by clicking the **Rule Set** link in the **Tasks** panel.
RuleSet	View	/WEB-INF/oracle/communications/inventory/ui/rule/flow/RuleSummaryFlow.xml#RuleSummaryFlow	Open a RuleSet Summary work area.
Service	View	/WEB-INF/oracle/communications/inventory/ui/service/flow/ServiceSearchResultsFlow.xml#ServiceSearchResultsFlow	Open a Search work area for services by clicking the **Service** link in the **Tasks** panel.
Service	View	/WEB-INF/oracle/communications/inventory/ui/service/flow/ServiceSummaryFlow.xml#ServiceSummaryFlow	Open a Service Summary work area.
Service	View	/WEB-INF/oracle/communications/inventory/ui/service/flow/ServiceTopologyViewFlow.xml#ServiceTopologyViewFlow	Open the topology view for a service.
Service	Edit	/WEB-INF/oracle/communications/inventory/ui/service/flow/ServiceEditFlow.xml#ServiceEditFlow	Edit a service from search results or a Summary page.
Signal Structure	View	/WEB-INF/oracle/communications/inventory/ui/connectivity/flow/SignalStructureSummaryFlow.xml#SignalStructureSummaryFlow	Open the Signal Structure work area from the **Related Pages** menu of a Pipe Summary work area.
Signal Structure	View	/WEB-INF/oracle/communications/inventory/ui/connectivity/flow/SignalTPSpecificationSearchResultsFlow.xml#SignalTPSpecificationSearchResultsFlow	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
Specification	View	/WEB-INF/oracle/communications/inventory/ui/sequencespecification/flow/SequenceSpecificationSearchResultsFlow.xml#SequenceSpecificationSearchResultsFlow	Open a Search work area for sequence specifications by clicking the **Sequence Specification** link in the **Tasks** panel.
Specification	View	/WEB-INF/oracle/communications/inventory/ui/sequencespecification/flow/SequenceSpecificationSummaryFlow.xml#SequenceSpecificationSummaryFlow	Open a Sequence Specification Summary work area.
Specification	View	/WEB-INF/oracle/communications/inventory/ui/specification/flow/SpecificationSearchResultsFlow.xml#SpecificationSearchResultsFlow	Open a Search work area to search for specifications by clicking the **Specification** link in the **Tasks** panel.
Specification	View	/WEB-INF/oracle/communications/inventory/ui/specification/flow/SpecificationSummaryFlow.xml#SpecificationSummaryFlow	Open a Specification Summary work area.
Specification	Edit	/WEB-INF/oracle/communications/inventory/ui/specification/flow/SpecificationRelationshipMaintFlow.xml#SpecificationRelationshipMaintFlow	Edit specification relationships.

Table 3–1 (Cont.) Taskflow Permissions

Component	Access Type	Permission String	Controls the Ability to:
Telephone Number	View	/WEB-INF/oracle/communications/inventory/ui/number/flow/TelephoneNumberSearchResultsFlow.xml#TelephoneNumberSearchResultsFlow	Open a Search work area for telephone numbers by clicking the **Telephone Number** link in the **Tasks** panel.
Telephone Number	View	/WEB-INF/oracle/communications/inventory/ui/number/flow/TelephoneNumberSummaryFlow.xml#TelephoneNumberSummaryFlow	Open the Telephone Number Summary work area.
Telephone Number	Edit	/WEB-INF/oracle/communications/inventory/ui/number/flow/TelephoneNumberEditFlow.xml#TelephoneNumberEditFlow	Edit a telephone number.
Topology	View	/WEB-INF/oracle/communications/inventory/ui/admin/flow/RebuildTopologyFlow.xml#RebuildTopologyFlow	Open the Rebuild Topology work area.

Resource Permissions

Table 3–2 lists all the UIM resource permissions, sorted by component.

Table 3–2 Resource Permissions

Component	Type	Permission Name	Purpose
Business Interaction	Button Action	BusinessInteraction.DELETE	Delete a business interaction from the search results.
Business Interaction	Button Action	BusinessInteractionItem.DELETE	Delete a business interaction item from the Business Interaction Summary work area.
Business Interaction	Button Action	BusinessInteractionItem.TRANSFER	Transfer a business interaction item from the Business Interaction Summary work area.
Business Interaction	Menu	BusinessInteraction.ASSOCIATE	Associate a business interaction item from the Business Interaction Summary work area.
Business Interaction	Menu Action	BusinessInteraction.ACTIVATE	Activate a business interaction from the Business Interaction Summary work area.
Business Interaction	Menu Action	BusinessInteraction.APPROVE_ CONFIGURATIONS	Approve a business interaction from the Business Interaction Summary work area.
Business Interaction	Menu Action	BusinessInteraction.CANCEL	Cancel a business interaction from the Business Interaction Summary work area.
Business Interaction	Menu Action	BusinessInteraction.CANCEL_HIERARCHY	Cancel a business interaction hierarchy from the Business Interaction Summary work area.
Business Interaction	Menu Action	BusinessInteraction.COMPLETE	Complete a business interaction from the Business Interaction Summary work area.

Table 3–2 (Cont.) Resource Permissions

Component	Type	Permission Name	Purpose
Business Interaction	Menu Action	BusinessInteraction.COMPLETE_ HIERARCHY	Complete a business interaction hierarchy from the Business Interaction Summary work area.
Business Interaction	Menu Action	BusinessInteraction.DEACTIVATE	Deactivate a business interaction from the Business Interaction Summary work area.
Business Interaction	Menu Action	BusinessInteraction.ISSUE_ CONFIGURATIONS	Issue a service configuration from from the Business Interaction Summary work area.
Business Interaction	Menu Action	BusinessInteraction.SEND_REQUEST	Send a request from the Business Interaction Summary work area.
Business Interaction	Menu Action	BusinessInteraction.VALIDATE	Validate a business interaction from the Business Interaction Summary work area.
Business Interaction	Menu Action	BusinessInteraction.ASSOCIATE_CHILD_BI	Add a child business interaction to the hierarchy in the Business Iinteraction Summary work area.
Business Interaction	Menu Action	BusinessInteraction.DISASSOCIATE_CHILD_ BI	Remove a child business interaction from the hierarchy in the Business Interaction Summary work area.
Characteristics	Button Action	CharacteristicSpecification.DELETE	Delete a Characteristic specification from the **Characteristic Specification** list.
Common Configuration	Menu Action	Configuration.MAINTAIN_CONFIG_ITEMS	Maintain configuration items from the hierarchy in the Configuration Summary work area.
Condition	Button Action	Condition.DELETE	Delete a condition from the Condition List work area.
Connectivity	Button Action	TDMConnectivity.DELETE	Delete a connectivity from the search results.
Connectivity	Button Action	TDMConnectivityDetails.SAVE	Save the TDM Connectivity details.
Connectivity	Button Action	TDMConnectivityDetails.SAVE_AND_CLOSE	Save the TDM Connectivity details and navigate back to the view mode.
Connectivity	Button Action	TDMConnectivityDetails.EDIT	Edit the TDM Connectivity details.
Connectivity	Button Action	TDMConnectivityCreate.SAVE	Create the TDM Connectivity.
Connectivity	Button Action	TDMConnectivityCreate.SAVE_AND_CLOSE	Create the TDM Connectivity and navigate back to the Search page.

Table 3–2 (Cont.) Resource Permissions

Component	Type	Permission Name	Purpose
Connectivity	Button Action	TDMConnectivityCreate.EDIT	Open the TDM Connectivity details in the Edit mode in the Create Page.
Connectivity	Button Action	TDMConnectivityCreate.DELETE	Delete the TDM Connectivity from the New Channelized Connectivity table.
Cross Connect	Button Action	CrossConnectsView.DELETE	Delete the cross connect from the Cross Connect Visual page.
Cross Connect	Button Action	CrossConnectsView.CREATE_CROSS_CONNECTS	Create a cross connect in the Cross Connect Visual page.
Custom Network Address	Button Action	CustomNetworkAddress.DELETE	Delete a custom network address from search results.
Custom Network Address	Menu Action	CustomNetworkAddress.ACTIVATE	Activate a custom network address from the Custom Network Address Summary work area.
Custom Network Address	Menu Action	CustomNetworkAddress.DEACTIVATE	Deactivate a custom network address from the Custom Network Address Summary work area.
Custom Network Address	Menu Action	CustomNetworkAddress.VALIDATE	Validate a custom network address from the Custom Network Address Summary work area.
Custom Network Address	Menu Action	CustomNetworkAddress.ASSOCIATE_CNA	Add a child custom network address to the hierarchy in the Custom Network Address Summary work area.
Custom Network Address	Menu Action	CustomNetworkAddress.DISASSOCIATE_CNA	Remove a child custom network address from the hierarchy in the Custom Network Address Summary work area.
Custom Object	Button Action	CustomObject.DELETE	Delete a custom object from search results.
Custom Object	Menu Action	CustomObject.ACTIVATE	Activate a custom object from the Custom Object Summary work area.
Custom Object	Menu Action	CustomObject.DEACTIVATE	Deactivate a custom object from the Custom Object Summary work area.
Custom Object	Menu Action	CustomObject.VALIDATE	Validate a custom object from the Custom Object Summary work area.
Custom Object	Menu Action	CustomObject.ASSOCIATE_CO	Add a child custom object to the hierarchy in the Custom Object Summary work area.
Custom Object	Menu Action	CustomObject.DISASSOCIATE_CO	Remove a child custom object from the hierarchy in the Custom Object Summary work area.

Table 3–2 (Cont.) Resource Permissions

Component	Type	Permission Name	Purpose
Equipment	Button Action	EquipmentHolder.DELETE	Delete an equipment holder from search results.
Equipment	Button Action	Equipment.DELETE	Delete an Equipment entity from search results.
Equipment	Button Action	Equipment.DUPLICATE	Duplicate an Equipment entity from search results.
Equipment	Menu Action	Equipment.ACTIVATE	Activate an Equipment entity from the Equipment Summary work area.
Equipment	Menu Action	Equipment.DEACTIVATE	Deactivate an Equipment entity from the Equipment Summary work area.
Equipment	Menu Action	Equipment.VALIDATE	Validate an Equipment entity from the Equipment Summary work area.
Equipment	Button Action	Equipment.ASSOCIATE	Associate an entity with Equipment from the Equipment portlet on the Entity Summary Page and/or from the hierarchy in the Physical Device Summary work area.
Equipment	Menu Action	Equipment.DISASSOCIATE	Disaasociate Equipment from the hierarchy in the Physical Device Summary work area.
Inventory Group	Button Action	InventoryGroup.DELETE	Delete an inventory group from search results.
Inventory Group	Button Action	InventoryGroupItem.DELETE	Delete an inventory group from search results.
Inventory Group	Menu Action	InventoryGroup.ACTIVATE	Activate an inventory group from the Inventory Group Summary work area.
Inventory Group	Menu Action	InventoryGroup.DEACTIVATE	Deactivate an inventory group from the Inventory Group Summary work area.
Inventory Group	Menu Action	InventoryGroup.VALIDATE	Validate an inventory group from the Inventory Group Summary work area.
Inventory Group	Button Action	InventoryGroup.ASSOCIATE	Associate an entity with an inventory group from the Inventory Group portlet on the Entity Summary work area.
Inventory Group	Menu Action	InventoryGroup.ASSOCIATE_IG	Add a child inventory group to the hierarchy in the Inventory Group Summary work area and/or add a parent inventorygroup to the Parent Inventory Group section in the Inventory Group Summary work area.

Table 3–2 (Cont.) Resource Permissions

Component	Type	Permission Name	Purpose
Inventory Group	Menu Action	InventoryGroup.DISASSOCIATE_IG	Remove a child inventory group from the hierarchy in the Inventory Group Summary work area and/or remove a parent inventorygroup from the Parent Inventory Group section in the Inventory Group Summary work area.
Inventory Group	Button Action	InventoryGroupItem.ASSOCIATE	Associate inventory group items from the Inventory Group Summary work area.
Involvement	Button Action	Involvement.DELETE	Delete an involvement from an entity Summary work area.
Location	Button Action	LocationSearch.CREATE	Create a location from the Location search page.
Location	Button Action	LocationSearch.DELETE	Delete la ocation from the search results.
Location	Button Action	LocationDetails.EDIT	Edit the location details.
Location	Button Action	LocationDetails.CREATE_NEC	Add a network entity code to the Location details.
Location	Button Action	LocationDetails.DELETE_NEC	Delete a network entity code from the Location details.
Location	Button Action	LocationDetails.VALIDATE_ADDRESS	Validate the location.
Logical Device	Button Action	LogicalDevice.DELETE	Delete a logical device from search results.
Logical Device	Button Action	DeviceMapping.DELETE	Map a physical port or connector to a device interface from the Device Interface Summary work area.
Logical Device	Menu Action	LogicalDevice.ACTIVATE	Activate a logical device from the Logical Device Summary work area.
Logical Device	Menu Action	LogicalDevice.DEACTIVATE	Deactivate a logical device from the Logical Device Summary work area.
Logical Device	Menu Action	LogicalDevice.VALIDATE	Validate a logical device from the Logical Device Summary work area.
Logical Device	Button Action	LogicalDevice.DUPLICATE	Duplicate a logical device from the search results page.
Logical Device	Menu Action	LogicalDevice.ASSOCIATE_LD	Add a logical device to the hierarchy in the Logical Device Summary work area and/or from the hierarchy in the Physical Device Summary work area.

Table 3–2 (Cont.) Resource Permissions

Component	Type	Permission Name	Purpose
Logical Device	Menu Action	LogicalDevice.DISASSOCIATE_LD	Remove a logical device from the hierarchy in the Logical Device Summary work area and/or from the hierarchy in the Physical Device Summary work area.
Logical Device	Menu Action	DeviceInterface.ASSOCIATE_DI	Add a device interface to the hierarchy in the L ogical Device Summary work area and/or to the hierarchy in the Device Interface Summary work area.
Logical Device	Menu Action	LogicalDevice.MAINTAIN_MAPPINGS	Maintain mappings from the hierarchy in the Logical Device Summary work area.
Logical Device	Menu Action	DeviceInterface.DISASSOCIATE_DI	Remove a device interface from the hierarchy in the L ogical Device Summary work area and/or from the hierarchy in the Device Interface Summary work area.
Logical Device Account	Button Action	LogicalDeviceAccount.DELETE	Delete a logical device account from search results.
Logical Device Account	Menu Action	LogicalDeviceAccount.ACTIVATE	Activate a logical device account from the Logical Device Account Summary work area.
Logical Device Account	Menu Action	LogicalDeviceAccount.DEACTIVATE	Deactivate a logical device account from the Logical Device Account Summary work area.
Logical Device Account	Menu Action	LogicalDeviceAccount.VALIDATE	Validate the logical device account from the Logical Device Account Summary work area.
Logical Device Account	Button Action	LogicalDeviceAccount.ASSOCIATE	Associate an entity with a logical device account from the Logical Device Account portlet on the Entity Summary work area.
Logical Device Configuration	Menu Action	LogicalDeviceConfigurationVersion.APPROVE	Approve a configuration from the Logical Device Configuration Summary work area.
Logical Device Configuration	Menu Action	LogicalDeviceConfigurationVersion.AUTO_CONFIGURE	Auto-configure a configuration from the Logical Device Configuration Summary work area.
Logical Device Configuration	Menu Action	LogicalDeviceConfigurationVersion.CANCEL	Cancel a configuration from the Logical Device Configuration Summary work area.
Logical Device Configuration	Menu Action	LogicalDeviceConfigurationVersion.COMPLETE	Complete a configuration from the Logical Device Configuration Summary work area.

Table 3–2 (Cont.) Resource Permissions

Component	Type	Permission Name	Purpose
Logical Device Configuration	Menu Action	LogicalDeviceConfigurationVersion.CREATE_NEW_VERSION	Create a new configuration from the Logical Device Configuration Summary work area.
Logical Device Configuration	Menu Action	LogicalDeviceConfigurationVersion.ISSUE	Issue a configuration from the Logical Device Configuration Summary work area.
Logical Device Configuration	Menu Action	LogicalDeviceConfigurationVersion.RESUME	Resume a configuration from the Logical Device Configuration Summary work area.
Logical Device Configuration	Menu Action	LogicalDeviceConfigurationVersion.SUSPEND	Suspend a configuration from the Logical Device Configuration Summary work area.
Logical Device Configuration	Menu Action	LogicalDeviceConfigurationVersion.VALIDATE	Validate a configuration from the Logical Device Configuration Summary work area.
Media	Button Action	Media.DELETE	Delete a media file from search results.
Media Stream	Button Action	MediaStream.DELETE	Delete a media stream from search results.
Media Stream	Button Action	MediaStream.DUPLICATE	Duplicate a media stream from search results.
Media Stream	Menu Action	MediaStream.ACTIVATE	Activate a media stream from the Media Stream Summary work area.
Media Stream	Menu Action	MediaStream.DEACTIVATE	Deactivate a media stream from the Media Stream Summary work area.
Media Stream	Menu Action	MediaStream.VALIDATE	Validate a media stream from the Media Stream Summary work area.
Media Resource	Button Action	MediaResource.ASSOCIATE	Add a media resource to the Media Resource portlet on the Entity Summary work area.
Media Resource	Button Action	MediaResource.DELETE	Delete a media resource from the Media Resource portlet on the Entity Summary work area.
Media Resource	Button Action	MediaResource.DUPLICATE	Duplicate a media resource from the Media Resource portlet on the Entity Summary work area.
Media Resource	Button Action	MediaResource.EDIT	Edit a media resource from the Media Resource portlet on the Entity Summary work area.
Network	Button Action	Network.DELETE	Delete a network from search results.
Network	Menu Action	Network.ACTIVATE	Activate a network from the Network Summary work area.

Table 3–2 (Cont.) Resource Permissions

Component	Type	Permission Name	Purpose
Network	Menu Action	Network.DEACTIVATE	Deactivate a network from the Network Summary work area.
Network	Menu Action	Network.VALIDATE	Validate a network from the Network Summary work area.
Network	Menu Action	NetworkNodeEdge.DISASSOCIATE	Disassociate a network node/node edge from the Network Map View and Network View.
Network	Menu Action	NetworkNodeEdge.UPDATE_ASSOCIATION	Update a network node/node edge association from the Network Map View & Network View.
Network Configuration	Menu Action	NetworkConfigurationVersion.APPROVE	Approve a configuration from the Network Configuration Summary work area.
Network Configuration	Menu Action	NetworkConfigurationVersion.AUTO_CONFIGURE	Auto-configure a configuration from the Network Configuration Summary work area.
Network Configuration	Menu Action	NetworkConfigurationVersion.CANCEL	Cancel a configuration from the Network Configuration Summary work area.
Network Configuration	Menu Action	NetworkConfigurationVersion.COMPLETE	Complete a configuration from the Network Configuration Summary work area.
Network Configuration	Menu Action	NetworkConfigurationVersion.CREATE_NEW_VERSION	Create a new configuration from the Network Configuration Summary work area.
Network Configuration	Menu Action	NetworkConfigurationVersion.ISSUE	Issue a configuration from the Network Configuration Summary work area.
Network Configuration	Menu Action	NetworkConfigurationVersion.RESUME	Resume a configuration from the Network Configuration Summary work area.
Network Configuration	Menu Action	NetworkConfigurationVersion.SUSPEND	Suspend a configuration from the Network Configuration Summary work area.
Network Configuration	Menu Action	NetworkConfigurationVersion.VALIDATE	Validate a configuration from the Network Configuration Summary work area.
Party	Button Action	Party.DELETE	Delete a party from search results.
Party	Button Action	Party.EDIT	Edit a party from Party search results or the Service Summary work area.
Party	Menu Action	Party.ACTIVATE	Activate a party from the Party Summary work area.
Party	Menu Action	Party.DEACTIVATE	Deactivate a party from the Party Summary work area.

Table 3–2 (Cont.) Resource Permissions

Component	Type	Permission Name	Purpose
Party	Menu Action	Party.VALIDATE	Validate a party from the Party Summary work area.
Party	Button Action	Party.ASSOCIATE	Associate an entity with a party from the Party portlet on the Entity Summary work area.
Physical Device	Button Action	PhysicalDevice.DELETE	Delete a physical device from search results.
Physical Device	Button Action	PhysicalDevice.DUPLICATE	Duplicate a physical device from search results.
Physical Device	Menu Action	PhysicalDevice.ACTIVATE	Activate physical device from the Physical Device Summary work area.
Physical Device	Menu Action	PhysicalDevice.DEACTIVATE	Deactivate a physical device from the Physical Device Summary work area.
Physical Device	Menu Action	PhysicalDevice.VALIDATE	Validate a physical device from the Physical Device Summary work area.
Physical Device	Menu Action	PhysicalDevice.ASSOCIATE	Add a physical device to the Equipment Summary page and/or to the hierarchy in the Logical Devie Summary work area and/or to the Physical Device portlet.
Physical Device	Button Action	PhysicalDevice.ASSOCIATE_PD	Add a physical device to the hierarchy in the Physical Device Summary work area.
Physical Device	Menu Action	PhysicalDevice.DISASSOCIATE	Remove a physical device from the Equipment Summary page and/or from the hierarchy in the Logical Devie Summary work area and/or from the Physical Device portlet.
Physical Device	Button Action	PhysicalDevice.DISASSOCIATE_PD	Remove a physical device from the hierarchy in the Physical Device Summary work area.
Physical Device	Menu Action	PhysicalDevice.MAINTAIN_MAPPINGS	Maintain mappings from the hierarchy in the Physical Device Summary work area.
Pipe	Button Action	Pipe.DELETE	Delete a pipe from search results.
Pipe	Button Action	Pipe.DUPLICATE	Duplicate a pipe from search results.
Pipe	Menu Action	Pipe.ACTIVATE	Activate a pipe from the Pipe Summary work area.
Pipe	Menu Action	Pipe.DEACTIVATE	Deactivate a pipe from the Pipe Summary work area.
Pipe	Menu Action	Pipe.MAP_SIGNAL_STRUCTURE	Associate a signal structure to a pipe from the Pipe Summary work area.

Table 3–2 (Cont.) Resource Permissions

Component	Type	Permission Name	Purpose
Pipe	Menu Action	Pipe.REMOVE_SIGNAL_STRUCTURE	Disassociate a signal structure from a pipe from the Pipe Summary work area.
Pipe	Menu Action	Pipe.VALIDATE	Validate a pipe from the Pipe Summary work area.
Pipe	Button Action	Pipe.MAINTAIN_CAPACITY	Update Capacity from Pipe Summary work area.
Pipe	Button Action	Pipe.MAINTAIN_DIRECTIONALITY	Create Directionality from Pipe Summary work area.
Pipe	Button Action	Pipe.MAINTAIN_TERMINATION_ RESOURCES	Delete TPs from Pipe TP Summary work area.
Pipe	Button Action	PipeProvides.DELETE	Delete on Pipe Provides page.
Pipe	Button Action	PipeTrail.ASSOCIATE	Associate a pipe trail from the Manual Configure page.
Pipe	Button Action	PipeTrail.DELETE	Delete a pipe trail from the Manual Configure page.
Pipe	Button Action	PipeTrail.UPDATE	Update a pipe trail from the Manual Configure page.
Pipe Configuration	Menu Action	PipeConfigurationVersion.APPROVE	Approve a configuration from the Pipe Configuration Summary work area.
Pipe Configuration	Menu Action	PipeConfigurationVersion.AUTO_ CONFIGURE	Auto-configure a configuration from the Pipe Configuration Summary work area.
Pipe Configuration	Menu Action	PipeConfigurationVersion.CANCEL	Cancel a configuration from the Pipe Configuration Summary work area.
Pipe Configuration	Menu Action	PipeConfigurationVersion.COMPLETE	Complete a configuration from the Pipe Configuration Summary work area.
Pipe Configuration	Menu Action	PipeConfigurationVersion.CREATE_NEW_ VERSION	Create a new configuration from the Pipe Configuration Summary work area.
Pipe Configuration	Menu Action	PipeConfigurationVersion.ISSUE	Issue a configuration from the Pipe Configuration Summary work area.
Pipe Configuration	Menu Action	PipeConfigurationVersion.RESUME	Resume a configuration from the Pipe Configuration Summary work area.
Pipe Configuration	Menu Action	PipeConfigurationVersion.SUSPEND	Suspend a configuration from the Pipe Configuration Summary work area.
Pipe Configuration	Menu Action	PipeConfigurationVersion.VALIDATE	Validate a configuration from the Pipe Configuration Summary work area.
Pipe Configuration	Menu	PipeConfigurationVersion.ACTIONS	Actions on the Pipe Config Trail List from the Pipe Configuration Summary work area.

Table 3–2 (Cont.) Resource Permissions

Component	Type	Permission Name	Purpose
Pipe Configuration	Button Action	PipeConfigurationVersion.ASSOCIATE	Associate a Pipe Config Trail List from the Pipe Configuration Summary work area.
Place	Button Action	Place.DELETE	Delete a place from search results.
Place	Button Action	Place.EDIT	Edit a place from search results or an entity Summary work area.
Place	Menu Action	Place.ASSOCIATE	Associate a place from the hierarcy in the Place Summary work area and/or Place portlet.
Place	Menu Action	Place.ASSOCIATE_PLACE	Add a child place to the hierarchy in the Place Summary work area.
Place	Menu Action	Place.DISASSOCIATE_PLACE	Remove a child place from the hierarchy in the Place Summary work area.
Place Configuration	Menu Action	PlaceConfigurationVersion.APPROVE	Approve a configuration from the Place Configuration Summary work area.
Place Configuration	Menu Action	PlaceConfigurationVersion.AUTO_CONFIGURE	Auto-configure a configuration from the Place Configuration Summary work area.
Place Configuration	Menu Action	PlaceConfigurationVersion.CANCEL	Cancel a configuration from the Place Configuration Summary work area.
Place Configuration	Menu Action	PlaceConfigurationVersion.COMPLETE	Complete a configuration from the Place Configuration Summary work area.
Place Configuration	Menu Action	PlaceConfigurationVersion.CREATE_NEW_VERSION	Create a new configuration from the Place Configuration Summary work area.
Place Configuration	Menu Action	PlaceConfigurationVersion.ISSUE	Issue a configuration from the Place Configuration Summary work area.
Place Configuration	Menu Action	PlaceConfigurationVersion.RESUME	Resume a configuration from the Place Configuration Summary work area.
Place Configuration	Menu Action	PlaceConfigurationVersion.SUSPEND	Suspend a configuration from the Place Configuration Summary work area.
Place Configuration	Menu Action	PlaceConfigurationVersion.VALIDATE	Validate a configuration from the Place Configuration Summary work area.
Product	Button Action	Product.DELETE	Delete a product from search results.
Product	Menu Action	Product.ACTIVATE	Activate a product from the Product Summary work area.
Product	Menu Action	Product.DEACTIVATE	Deactivate a product from the Product Summary work area.

Table 3–2 (Cont.) Resource Permissions

Component	Type	Permission Name	Purpose
Product	Menu Action	Product.VALIDATE_PRODUCT	Validate a product from the Product Summary work area.
Product	Menu Action	Product.ASSOCIATE_PRODUCT	Associate a product to the hierarchy in the Product Summary work area.
Product	Menu Action	Product.DISASSOCIATE_PRODUCT	Disassociate a product from the hierarchy in the Product Summary work area.
Reservation	Button Action	Reservation.DELETE	Delete a reservation from the **Reservations** list.
Role	Button Action	Role.DELETE	Delete a role from the **Roles** list in an entity Summary work area.
Role	Button Action	Role.EDIT	Edit a role from the **Roles** list in an entity Summary work area.
Ruleset	Button Action	Rule.DELETE	Delete a ruleset.
Service	Button Action	Service.DELETE	Delete a service from search results.
Service	Menu Action	Service.ACTIVATE	Activate a service from the Service Summary work area.
Service	Menu Action	Service.CANCEL	Cancel a service from the Service Summary work area.
Service	Menu Action	Service.COMPLETE	Complete a service from the Service Summary work area.
Service	Menu Action	Service.DEACTIVATE	Deactivate a service from the Service Summary work area.
Service	Menu Action	Service.DISCONNECT	Disconnect a service from the Service Summary work area.
Service	Menu Action	Service.RESUME	Resume a service from the Service Summary work area.
Service	Menu Action	Service.SUSPEND	Suspend a service from the Service Summary work area.
Service	Menu Action	Service.VALIDATE	Validate a service from the Service Summary work area.
Service	Menu Action	Service.ASSOCIATE	Add a service to the hierarchy in the Service Summary work area.
Service Configuration	Menu Action	ServiceConfigurationVersion.APPROVE	Approve a configuration from the Service Configuration Summary work area.
Service Configuration	Menu Action	ServiceConfigurationVersion.AUTO_ CONFIGURE	Auto-configure a configuration from the Service Configuration Summary work area.
Service Configuration	Menu Action	ServiceConfigurationVersion.CANCEL	Cancel a configuration from the Service Configuration Summary work area.

Table 3–2 (Cont.) Resource Permissions

Component	Type	Permission Name	Purpose
Service Configuration	Menu Action	ServiceConfigurationVersion.COMPLETE	Complete a configuration from the Service Configuration Summary work area.
Service Configuration	Menu Action	ServiceConfigurationVersion.CREATE_NEW_VERSION	Create a new configuration from the Service Configuration Summary work area.
Service Configuration	Menu Action	ServiceConfigurationVersion.ISSUE	Issue a configuration from the Service Configuration Summary work area.
Service Configuration	Menu Action	ServiceConfigurationVersion.RESUME	Resume a configuration from the Service Configuration Summary work area.
Service Configuration	Menu Action	ServiceConfigurationVersion.SUSPEND	Suspend a configuration from the Service Configuration Summary work area.
Service Configuration	Menu Action	ServiceConfigurationVersion.VALIDATE	Validate a configuration from the Service Configuration Summary work area.
Specification	Button Action	Specification.DELETE	Delete a specification from the **Specifications** list.
Specification	Button Action	SequenceSpecification.DELETE	Delete a Sequence specification.
Telephone Number	Button Action	TelephoneNumber.DELETE	Delete a telephone number from search results.
Telephone Number	Menu Action	TelephoneNumber.ACTIVATE	Activate a telephone number from the Telephone Number Summary work area.
Telephone Number	Menu Action	TelephoneNumber.DEACTIVATE	Deactivate a telephone number from the Telephone Number Summary work area.
Telephone Number	Menu Action	TelephoneNumber.SNAPBACK	Configure the Snapback action on a telephone number from the Telephone Number Summary work area.
Telephone Number	Menu Action	TelephoneNumber.VALIDATE	Validate a telephone number from the Telephone Number Summary work area.

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

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

   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 **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
3. Navigate to the **Security Policies** page. Right-click **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 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. Click on the deployed web service.
3. Select the **Configuration** tab and **WS-Policy** sub-tab. Click on the **+** sign next to the Service Endpoint 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 **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**.
3. In the **Domain Structure** tree, select **Security Realms**.

   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
   ```

4 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
- Configuring a Geocode Service
- Performing a UIM Service Purge

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

ora_uim_us_tn

> **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.

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.

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:

```
import java.util.*;

public class TimeZoneList {

public static void main(String[] args) {

String[] sZoneIds = TimeZone.getAvailableIDs();

List 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.

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 4–1 lists each property's file name, error ID range, and the error messages or items it localizes.

Table 4–1 Properties Files for Localizing UIM Error Messages and Items.

Property File Name	Error ID Range	Error Message or Item It Localizes
addressrange.properties	N/A	Property names for the address range cartridge

Table 4–1 (Cont.) Properties Files for Localizing UIM Error Messages and Items.

Property File Name	Error ID Range	Error Message or Item It Localizes
businessInteraction.properties	270000-279999	Error messages generated by the business interaction module
capacity.properties	320000-329999	Error messages generated by the capacity module
configaction.properties	240000-249999	Error messages generated by the configuration actions
configuration.properties	240000-249999	Tree node label names
connectivity.properties	260000-269999	Error messages generated by the connectivity module
consumer.properties	220000-229999	Error messages generated by the consumer module
countries.properties	N/A	Error messages generated by the countries module
custom.properties	280000-289999	Error messages generated by the custom module
enum.properties	N/A	Error messages generated by enumeration
equipment.properties	210000-219999	Error messages generated by the equipment module
extensibility.properties	180000-189999	Error messages generated by the extensibility module
inventoryGroup.properties	190000-199999	Error messages generated by the inventory group module
location.properties	420000-420999	Error messages generated by the location module
logicaldevice.properties	290000-299999	Error messages generated by the logical device module
media.properties	350000-359999	Error messages generated by the media module
mediaResource.properties	360000-369999	Error messages generated by the mediaResource module
network.properties	300000-309999	Error messages generated by the network module
number.properties	120000-129999	Error messages generated by the number module
party.properties	230000-239999	Error messages generated by the party role module
place.properties	250000-259999	Error messages generated by the place module
product.properties	390000-399999	Error messages generated by the product module
project.properties	140000-149999	Error messages generated by the project module
resource.properties	330000-339999	Resource entity names and resource-related error messages

Table 4–1 (Cont.) Properties Files for Localizing UIM Error Messages and Items.

Property File Name	Error ID Range	Error Message or Item It Localizes
role.properties	90000-99999	Error messages generated by the role module
service.properties	110000-119999	Error messages generated by the service module
signal.properties	310000-319999	Error messages generated by the connectivity signal module
specification.properties	130000-139999	Error messages generated by the specification module
status.properties	N/A	Error messages generated by the status module
subscriber.properties	150000-159999	Error messages generated by the subscriber module
system.properties	100000-109999	Error messages generated by the framework module
topology.properties	340000-349999	Error messages generated by the topology module
wsservice.properties	400000-409999	Error messages generated by the wsservice module

For more information on how to localize UIM, see *UIM Developer's Guide*.

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**.

> **Note:** If you want to change the database connection, perform steps 9 and 10

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

Refer to the *Deployment Guide: Deploying F5 with Oracle's WebLogic Server 10* found at:

http://www.f5.com/pdf/deployment-guides/f5-weblogic10-dg.pdf

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.

```
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.

> **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.

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 UIM.
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*`\uim\logs\****Server_uim_rebuild.log`

Configuring a Geocode Service

To configure a geocode service, see the following topics:

- About Oracle eLocation
- Using a Geocode Service other than Oracle eLocation

About Oracle eLocation

UIM uses Oracle eLocation as the default geocode service, but you may opt to use a different geocode service. This section describes Oracle eLocation, and provides information about configuring UIM to use a different geocode service.

UIM interfaces with Oracle eLocation through an XML API request that is sent when you click **Validate Address** from within UIM when creating a location. Oracle eLocation returns an XML API response to UIM, indicating whether or not the address sent in the request was a valid address. For valid addresses, the response includes a geocode, which is a specific latitude and longitude that represents the location.

Using a Geocode Service other than Oracle eLocation

Upon installation, UIM is configured to use the Oracle eLocation geocode service. However, you can configure UIM to use a geocode service other than the default Oracle eLocation. For example, you may opt to use a thrid-party geocode service, or create a custom geocode service to use.

UIM is tightly coupled with Oracle eLocation. As a result, when you click **Validate Address** from within UIM when creating a location, UIM creates an XML request based on what the Oracle eLocation geocode service is expecting. Similarly, UIM expects an XML response based on what the Oracle eLocation geocode service returns. You can find detailed information about the eLocation XML request and response structures at the following Web site:

http://elocation.oracle.com/geocoder/concept.html

Using a Third-Party Geocode Service

To use a third-party geocode service, you can host your own eLocation service that:

- Handles the input XML request from UIM
- Creates a new XML request based on what the third-party geocode service is expecting
- Maps the data from the input XML request to the new XML request
- Sends the new XML request to the third-party geocode service
- Handles the response from the third-party geocode service
- Creates a new XML response based on what UIM is expecting
- Maps the data from the XML response to the new XML response
- Sends the new XML response to UIM

In this scenario, the eLocation service is just a middle tier that performs XML mapping, allowing UIM and the third-party geocode service to communicate.

For information on how to host your own eLocation service, see *Oracle Spatial eLocation Quick Start Guide*:

http://download.oracle.com/otndocs/products/spatial/pdf/elocation_quickstart.pdf

Using a Custom Geocode Service

To use a custom geocode service, you can host your own eLocation service that:

- Handles the input XML request from UIM

- Performs custom address analysis based on input XML request data to determine the geocode
- Creates an XML response based on what UIM is expecting
- Sends the new XML response to UIM

In this scenario, the eLocation service hosts the custom geocode service.

For information on how to host your own eLocation service, including how to develop the custom geocode service that runs on your eLocation service, see *Oracle Spatial eLocation Quick Start Guide*:

`http://download.oracle.com/otndocs/products/spatial/pdf/elocation_quickstart.pdf`

Configuring UIM

After your eLocation service is up and running, you must configure the *UIM_Home*/**config**/**system-config.properties** file to point to your eLocation service. This file defines several properties related to the geocode service that UIM is using, such as host name, user ID, password, and so forth. See "Updating the system-config.properties File" for more information.

Performing a UIM Service Purge

This section describes how to perform a service purge for UIM. The tool is available as part of the **ora_uim_dbtools.jar** file, located in the *UIM_Home***/util/** folder.

WARNING: Performing a service purge will delete database records permanently. Ensure that the database has been backed up before proceeding with any service purge operations.

Prerequisites

The prerequisites to perform a UIM service purge include the following:

- Gather the statistics of the schema before and after running purge scripts, use the following command:

  EXEC DBMS_STATS.gather_schema_stats(*uim_db_schema_username***);**
- Provide admin privileges to the database user.
- Back up the database before executing purge scripts, as scripts will delete the records matching specified criteria permanently.
- Must have Java version 1.6 or higher installed.
- Must run **ServicePurgeScripts.sql** on the database, which is part of **ora_uim_dbtools.jar**. **ServicePurgeScripts.sql** is located at **ora_uim_dbtools.jar/sqlscripts**. To install this script, use sqlplus to run the sql script, following are the steps to install the scripts:

  1. Login to sqlplus
  2. Execute following command:

     @<dbtools_extracted_dir>/sqlscripts/ServicePurgeScripts.sql

Configuring the UIM Service Purge Environment

Extract the **ora_uim_dbtools.jar** from the UIM Installer. Use the following command to extract the file:

jar -xvf ora_uim_dbtools.jar

After the file is extracted, edit the **servicePurge.sh** file and set the following variables:

1. Set JAVA_HOME.
2. Modify these parameters to point to the database:
   - DB_HOSTNAME - hostname of the database.
   - DB_PORT - database port
   - DB_SERVICE_NAME - database service name
3. Add extracted folder path to <add-extracted-path> for the 'sqlFileLocation' variable.

Database Tables

The following tables will be created to capture the Service Purge execution audit and error details:

- Purge_Error_Log
- Purge_Audit

Purge_Error_Log

This table is used to record errors/failures. The Service Purge can fail due to any invalid data created using tools which are not part of UIM. Such failures are recorded in this table. Table 4–2 contains the following information about the failure:

Table 4–2 Purge_Error_Log

Name	Description
ID	Refers to purge helper’s ID
Error Code	SQL error code
Error Message	SQL error message
Reported Date	Time when error is recorded

Purge_Audit

This table records the Service Purge execution information. Table 4–3 contains the following detailed information for each attribute:

Table 4–3 Purge_Audit

Attribute Name	Description
JOBID	For every execute or resume purge operation, a new record will be created in this table.
PURGETYPE	Defaulted to SERVICE.

Table 4–3 (Cont.) Purge_Audit

Attribute Name	Description
START_DATE	The date when the purge process is initiated. **Note:** In the case of a scheduled execution, the value will be set to the scheduled time and once the process starts the process will update this value with the time when the process is initiated.
END_DATE	The date when the purge process is completed or cancelled.
USERNAME	The database schema user name through which the user will perform the operation.
CRITERIA	This field contains the criteria string which will be generated by API, using criteria specified by the user. The field will also contain information about parallel processes and batch size specified by the user. For example: (ADMINSTATE LIKE 'CANCELLED') AND LASTMODIFIEDDATE <= to_date('07/30/2012:23:59:59','mm/dd/yyyy:hh24:mi:ss'):10 : 1000 Where the first part of the value is the criteria *('(ADMINSTATE LIKE 'CANCELLED') AND LASTMODIFIEDDATE <= to_date('07/30/2012:23:59:59','mm/dd/yyyy:hh24:mi:ss')')* followed by the parallel processes *('10')* and batch size *('1000')*.
STATUS	This is the status of the service purge, with one of the following values: INPROGRESS, SCHEDULED, CANCELLED, or FAILED. Following is a description for each of the status. INPROGRESS: the purge execution has started. SCHEDULED: a purge execution is scheduled. **Note:** When a scheduled purge execution starts, the STATUS and START_DATE will be updated to INPROGRESS and with the scheduled time respectively. CANCELLED: the purge execution has been cancelled. FAILED: the purge execution has failed, due to errors when one or more services were not processed, one of the reasons can be inconsistent data.
PARENTJOB	New child record, created when a job is suspended and resumed, which will refer to the parent record through this attribute. For example, if a purge is executed and later suspended, there will be a record for this job with a status of **SUSPENDED**. When the purge is resumed, the older record which was suspended will be updated with a status of **COMPLETED** and a new record will be created which will refer to the completed record through **JOBID**. This will enable us to maintain a history of the operations that were performed.
REPORTNAME	Report name generated when service purge execution is performed.

Operations

The Service Purge can be executed with the following options:

- Report
- Execute
- Status
- Suspend

- Resume
- Cancel

Report

The report option allows the user to specify criteria, determine the total number of records to be deleted, and estimate the amount of disc space to be freed up. Please note that this option will provide the report, but will not actually purge the records.

The following arguments can be used during report generation:

-ed: This argument is mandatory. The **ed** argument stands for End Date, which means that services with a "last modified date" on or before this date will be considered for puge. The user must specify this date in the following format: [MM/DD/YYYY]. Following is an example:

```
./servicePurge.sh report -ed 02/21/2005
```

-status: This argument is optional. The **status** argument indicates the admin state of the service. As a value for this argument only "disconnected" can be mentioned. All services with a "disconnected" admin state will be considered for purge and by default services in a "cancelled" state will be considered for purge. For example:

```
./servicePurge.sh report -status disconnected
```

In the above example, all services with an admin state of disconnected or cancelled will be considered for report generation.

-sd: This argument is optional. The **sd** argument stands for Start Date, which means that services with a "last modified date" on or before this date will be considered for purge. The date must be specified in the following format: [MM/DD/YYYY]. Following is an example:

```
./servicePurge.sh report -sd 02/21/1990
```

-icsc: This argument is optional. The **icsc** argument stands for ignore cancelled service configuration, which means that all the cancelled service configuration versions, that were part of any "in-service" services, will not be purged and will be retained. Following is an example:

```
./servicePurge.sh report -icsc
```

Execute

> **WARNING: Performing a service purge will delete database records permanently. Ensure that the database has been backed up before proceeding with any service purge operations.**

The execute option enables the user to purge cancelled and (or) disconnected services, which includes rows from several tables listed below, using the specified criteria. The execute option always creates a report for the specified criteria and prompts the user for confirmation, if the purge end date specified is within one year range from now. The user cannot run more than one execute operation at a time. If the user wishes to start a new execute operation, then the old execute operation must be cancelled. In case of a suspended purge operation, no new execute operations can be initiated unless the suspended operation is cancelled.

The following is the list of tables which will be impacted:

- Service
- Service_Char
- Party_ServiceRel
- Place_ServiceRel
- ServiceAssignment
- ServiceConsumer
- ServiceReservation
- ServiceCondition
- ServiceConfigurationVersion
- BusinessInteraction
- ConfigurationInput
- TopologyProfile
- TopologyProfileEdge
- TopologyProfileNode
- ServiceConfigurationItem
- ServiceConfigurationItem_Char
- BusinessInteractionItem
- <Entity>Consumer
- <Entity>Assignment
- <Entity>ConfigRef

In the above list of tables, th **<Entity>Consumer**, **<Entity>Assignment** and **<Entity>ConfigRef** tables are applicable to the following entity resources, which can be consumed by Service:

- Custom Network Address
- Custom Object
- Device Interface
- Equipment
- Equipment Holder
- Geographic Location
- Geographic Site
- Logical Device Account
- Logical Device
- Network
- Physical Connector
- Physical Device
- Physical Port
- Pipe

- Service
- Telephone Number

When an execute operation is performed, a new record is created in the Purge Audit table, with a status of INPROGRESS and after the execute operation completes successfully, it updates the record with a status of COMPLETED.

The following arguments can be used during the execute operation:

-ped: This argument is mandatory. The **ped** argument stands for Purge End Date which indicates that services with a "last modified date" on or before this date will be considered for purge. The date must be specified in the following format: [MM/DD/YYYY]. For example:

```
./servicePurge.sh report -ped 02/21/2005
```

-status: This argument is optional. The **status** argument indicates the admin state of the service. As a value for this argument only 'disconnected' can be mentioned, so all services with a disconnected admin state will be considered and by default services in a cancelled admin state will also be considered. For example:

```
./servicePurge.sh report -status disconnected
```

In this case all services with an admin state of disconnected or cancelled will be considered for report generation.

-psd: This argument is optional. The **psd** argument stands for Purge Start Date which means that services with a "last modified date" on or after this date will be considered for purge. The date must be specified in the following format: [MM/DD/YYYY]. For example:

```
./servicePurge.sh report -psd 02/21/1990
```

-s: This argument is optional. This argument will schedule the execution of the purge. The date must be specified in the following format: [MM/DD/YYYY:HH:mm:ss]. For example:

```
./servicePurge.sh execute -s 07/26/2012:19:30:00
```

-force: This argument is optional. Service Purge will not ask for confirmation when this option is specified by the user. For example:

```
./servicePurge.sh execute -force
```

-icsc: This argument is optional. The **icsc** argument stands for ignore cancelled service configuration, which means that all the cancelled service configuration versions, that were part of any "in-service" services, will not be purged and will be retained. Following is an example:

```
./servicePurge.sh execute -icsc
```

-c: Sets the commit size to the given value. By default, it is set to 1000 Services. The Max value for this argument is 10000. If the user prompts more than this value, the tool will take consider it as 10000. For example:

```
./servicePurge.sh execute -c 1000
```

-t: This argument is optional. Sets the Number of Parallel Processes to the given value. The Max value that user can specify is 100, if the user specifies more than this, only 100 parallel processes will be created. This is optional argument and by default it is set to 10. For example

./servicePurge.sh execute -t 15

> **Note:** The service purge execute operation will exclude disconnected services, which have any of its Telephone Number resources Aging.
>
> The service purge execute operation will only delete Entity Assignment information. It does not delete resources which were consumed/referred by the service.

Status

The status option shows information for in-progress/suspended purge operations. It also provides the following information, related to the purge process before seeking confirmation on cancellation:

- Active service purge operation.
- Number of services purged.
- All the jobs related to service purge.
- Report file name which is generated while services are purged.
- Number of services purged.

Suspend

The suspend option will suspend the service purge operation and allow active parallel processes to continue to run and complete, but no new processes will be created. Before suspending the active service purge operation, the service purge will provide the following information:

- Active service purge operation.
- Number of services purged.
- All the jobs related to service purge.
- Report file name which is generated while services are purged.
- Number of services purged.

A suspended operation can be cancelled or resumed, but once the operation is in a suspended state, no new purge operations can be initiated. After an execute operation is suspended, the Purge Audit table Status record will be updated to a COMPLETED state and a new record will be created with a status of SUSPENDED.

Please note that there are processes which are still in RUNNING status when a purge operation is suspended. After these processes complete execution, the processes will change to a DISABLED state. When all the processes have changed to aDISABLED status, no new processes will be created.

Resume

The resume option restarts the service purge operation ,using arguments specified by the user. In this case, the Purge Audit table Status record is updated with a status of INPROGRESS for the record which was in a 'suspended' state. The following arguments can be specified while resuming purge operations:

-s: This is an optional argument. This argument will schedule the execution of the purge. The user must specify the date in the following format [MM/DD/YYYY:HH:mm:ss]. For example:

./servicePurge.sh execute -s 06/26/2012:19:30:00

-c: Sets the commit size to the given value. By default it is set to 1000 Services. Max value this argument will take it 10000. If the user prompts more than this value tool will take it as 10000. For example:

./servicePurge.sh execute -c 1000

-t: Sets the Number of Parallel Processes to the given value. Max value that user can specify is 100, if the user specifies more than this only 100 parallel processes will get created. This is optional argument and by default it is set to 10. For example

./servicePurge.sh resume -t 15

Cancel

The cancel option terminates all service purge related processes with a status of INPROGRESS or SUSPENDED. It also provides the following information related to purge process, before seeking confirmation on cancellation:

- Active service purge operation.
- Number of services purged.
- All the jobs related to service purge.
- Report file name which is generated while services are purged.
- Number of services purged.

After this information is provided, the user will be asked for a confirmation to go ahead with cancellation of In-progress/Suspended operations. When the Service Purge is cancelled, the Purge Audit table Status record will be updated with a status of CANCELLED for records with anINPROGRESS/SUSPENDED status.

5 Improving Unified Inventory Management Performance

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
- Updating the System Configuration Files
- Setting Timeout Values for UIM

Configuring a Shared Index Directory

For muiltiserver deployment environments (including configurations for multiple single servers, administration/managed servers, and administration/clustered servers), you must deploy a common shared storage, such as a storage area network, for all UIM WebLogic application servers. Without a storage area network, 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`

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 *UIM_Home*/**logs/***WebLogic_Name*_**uim.log**

- **rebuildRollingFile**

  Rolling File Appender - used to log the rebuild topology messages to the rolling file *UIM_Home*/**logs/***WebLogic_Name*_**uim_rebuild.log**

The following is an example of the layout of the **appender** log message:

%d{yyyy-MM-dd HH:mm:ss,SSS} %-5p [%X{userName}] ["%X{requestSession}] [%c{1}] %m%n

where:

- *%d{yyyy-MM-dd HH:mm:ss,SSS}*

  is the Date in the format yyyy-MM-dd HH:mm:ss,SSS)

- *%-5p*

  is the priority of the logging event>

- *%X{userName}*

  is the user name associated with the thread that generated the logging event

- *%X{requestSession}*

  is the session ID associated with the thread that generated the logging event. Note that the *requestSession* is not included by default. The layout value needs to be modified to add the *requestSession*.

- *%c{1}*

  is the category of the logging event with the **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 *oracle.communications.inventory.techpack.video.impl.VideoManagerImpl* the pattern %c{1} will output **VideoManagerImpl**.

- *%m*

  is the application supplied message associated with the logging event. For example: *[INV-801005] No subscriber is associated to the service.*

- *%n*

  is the platform dependent line separator character or characters

For all parameters, see:

`http://logging.apache.org/log4j/1.2/apidocs/org/apache/log4j/PatternLayout.html`

This is a localized logging output message example:

2012-01-03 15:20:22,087 ERROR [uimuser1] [VideoManagerImpl] [INV-801005] No subscriber is associated to the service.

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 **appender**:

<filter class="oracle.communications.inventory.api.logging.util.FilterUtil">

<param name="userName" value=""/>

```
</filter>
```

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:

```
<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:

```
<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:

```
<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:

```
<logger name=" oracle.communications.inventory.techpack" additivity="false">
```

<level value="debug" />

<appender-ref ref="stdout"/>

<appender-ref ref="rollingFile"/>

</logger>

Note: Appender Additivity

The output of a log statement of logger C will go to all the appenders in C and its ancestors. This is the meaning of the term **appender additivity**.

However, if an ancestor of logger C, say P, has the additivity flag set to false, then C's output will be directed to all the appenders in C and its ancestors up to and including P but not the appenders in any of the ancestors of P.

Loggers have their additivity flag set to true by default.

Source: `http://logging.apache.org/log4j/1.2/manual.html`

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:

<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:

   ```
   ./wlst.sh
   ```

4. Connect to the server on which you want to change the logging level, use the following command:

   connect(*userid,password,'t3://hostname:port'*)

5. Go to Custom settings using the following command:

   ```
   custom()
   ```

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

6. Go to TopLink using the following command:

   ```
   cd('TopLink')
   ```

7. List the sessions at this level using the following command:

   ```
   ls()
   ```

   Note: The following is an example of a TopLink session:

   'TopLink:Name=Session(file/share/uimcluster/domains/clusterUim720b1357/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)
   ```

   EclipseLink provides nine logging levels, refer to Table 5–1 for a list of the different logging levels and a brief description of each.

Table 5–1 EclipseLink Logging Levels

Level	Description
OFF	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.
SEVERE	This level enables reporting of failure cases only. Usually, if the failure occurs, the application stops.
WARNING	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.
INFO	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.
CONFIG	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.
FINE	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.
FINER	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.
FINEST	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.
ALL	This level currently logs at the same level as FINEST.

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 in UIM is set, by default, to org.exolab.castor.xml.XercesJDK5XMLSerializerFactory.

   By default, UIM does not ship the external Xerces jar file and uses the Xerces file shipped with the JDK.

   The org.exolab.castor.xml.XercesJDK5XMLSerializerFactory is only valid for Sun JDK for Windows, Linux and Solaris. For IBM AIX JDK, the **org.exolab.castor.xml.serializer.factory** value should be set to 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:

   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:

   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:

   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:

   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:

   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:

   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 **AllowDeactivateReferencedCustomNetworkAdrress** 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 **AllowedDeactivateReferencedLogialDevice** property of the **reference.properties** file is used to deactivate the ReferencedLogicalDevice property.

   The default value is false.

   Example:

   AllowDeactivateReferencedLogicalDevice=false

5. The **AllowDeactivateReferencedLogialDeviceAccount** 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.default.paging.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

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

    Examples:

    uim.entitySpecificCache.enable=false

    eLocation.URL=http://eLocation.oracle.com/eLocation/lbs

    eLocation.matchMode=Default

    eLocation.http.proxyExists=false

    eLocation.http.proxyHost=

    eLocation.http.proxyPort=

    eLocation.http.proxyUser=

    eLocation.http.proxyPassword=

For detailed information on eLocation configuration, refer to the *UIM Developer's Guide*.

18. The following properties of the **system-config.properties** file are used for setting Property Location settings.

    Examples:

    uim.networkentity.code.maxlength=3

    uim.propertylocation.name.maxlength=200

    uim.networklocation.code.minlength=3

    uim.networklocation.code.maxlength=10

    uim.networkentitylocation.code.delimiter.enabled=true

    uim.propertylocation.name.delimiter=

19. The following property of the **system-config.properties** file is used for setting Pipe Capacity settings.

    Examples:

    connectivity.capacityVariant=4

20. The following property of the **system-config.properties** file is used for setting Connectivity Termination settings.

    Examples:

    connectivity.termination.apply.compatibility=false

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:

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

2. The **customTimer** timer of the **timers.properties** file is a customer timer for custom extensions.

   There should be only one instance of this timer in the cluster.

   Examples:

   ```
   customTimer.firstTime=300
   customTimer.period=600
   customTimer.listener=oracle.communications.inventory.api.common.TimeoutEven
   tListener
   ```

3. The **cleanReservation** timer of the **timers.properties** file is a timer to cleanup expired reservations.

   There should be only one instance of this timer in the cluster.

   Examples:

   ```
   cleanReservation.firstTime=600
   cleanReservation.period=600
   cleanReservation.listener=oracle.communications.inventory.api.consumer.impl.Re
   servationManagerImpl
   ```

4. The **telephoneNumberAging** timer of the **timers.properties** file is a timer for recalling disconnected telephone numbers.

   Examples:

   ```
   telephoneNumberAging.firstTime=600
   telephoneNumberAging.period=600
   telephoneNumberAging.listener=oracle.communications.inventory.api.number.Tel
   ephoneNumberHelper
   ```

5. The **rowLockExpiration** timer of the **timers.properties** file is a timer to cleanup the expired entity row locks.

Examples:

rowLockExpiration.firstTime=120
rowLockExpiration.period=600
rowLockExpiration.listener=oracle.communications.inventory.api.common.impl.R
owLockExpiryTimerListener

For more information on telephone number aging and TN life cycles, see *UIM Concepts*.

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 refresh Topology 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 and JTA. In general, the JTA timeout should be less than or equal to the Oracle database timeout:

JTA timeout <= database timeout

Oracle recommends setting the 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.

   > **Note:** Oracle recommends setting the database timeout value higher than the XA transaction timeout value. Otherwise, in-doubt table locks can occur on the database side before the WebLogic server JTA or JDBC XA can close the transaction.

4. Exit sqlplus.

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 5–2 describes the options available for the Query Behavior and Row Limit parameters.

Table 5–2 Query Behavior and Row Limit Parameters

Behavior (option #)	Row Limit	Count	Scrolling
FULL_COUNT_FULL_QUERY (1)	N/A	The exact count is displayed.	User can scroll through the entire result set.
NO_COUNT_FULL_QUERY (2)	N/A	Not displayed	User can scroll through the entire result set.
LIMIT_COUNT_FULL_QUERY (3)	Used for count only	If total count < row limit, then total count is displayed else: Total count: row limit (Limit Reached) is displayed	User can scroll the results up to the row limit.
LIMIT_COUNT_LIMIT_QUERY (4)	Used for count and query	If total count < row limit, then total count is displayed else Total count: row limit (Limit Reached) is displayed	User can scroll the results up to the row limit.

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 5–3 for a description of the pros and cons of the parameter options.
5. Save and close the **system-config.properties** file.

Table 5–3 Parameter Options Pros and Cons

Behavior	Advantages	Disadvantages
FULL_COUNT_FULL_QUERY(1)	You know the exact count of rows satisfying the criteria. You can scroll through the entire result set.	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.
NO_COUNT_FULL_QUERY(2)	The query for finding the total count is not performed. So it will help the performance of the pages.	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.
LIMIT_COUNT_FULL_QUERY(3)	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).	User cannot scroll to the rows past the row limit.
LIMIT_COUNT_LIMIT_QUERY(4)	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.	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.

6

Unified Inventory Management Backup and Restore

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 no_stage 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.

> **Note:** Verify that the file/folder being backed up meets the file size or pathname length requirements for the backup utility being used. For example, the maximum pathname length for the tar application is 256 characters.

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 administrator 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 following link describes the different scenarios and what needs to be restored in each of the scenarios.

`http://www.oracle.com/technetwork/database/features/availability/maa-wp-wls-br-scenarios-128715.pdf`

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 the 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

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://docs.oracle.com/cd/E17904_01/web.1111/e13707/ldap.htm

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://docs.oracle.com/cd/E11882_01/rac.112/e16795/rman.htm

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.

7

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 7–1 and Table 7–2 provide recommended database parameters for tuning your database. These are the minimum requirements for UIM.

Table 7–1 Database Creation Parameters

Parameter	Recommended Value
SGA+PGA	At least 4 GB in total. Oracle recommends that you use as much memory as you have available in the system, and also use Automatic Memory Management.
Processes	2000
Connection mode	Dedicated server
Redo log file size	1024 MB minimum

Table 7–2 Database Initialization Parameters

Parameter	Recommended Value
db_file_multiblock_read_count	16
distributed_lock_timeout	1800
dml_locks	9700
job_queue_processes	10
log_buffer	31457280

Table 7–2 (Cont.) Database Initialization Parameters

Parameter	Recommended Value
open_cursors	5000
parallel_max_servers	640
plsql_code_type	NATIVE