**Oracle® Retail Advanced Inventory Planning**
Administration Guide
Release 13.1.1

August 2009

ORACLE®

Oracle® Advanced Inventory Planning Administration Guide, Release 13.1.1

## Value-Added Reseller (VAR) Language

(i) the software component known as **ACUMATE** developed and licensed by Lucent Technologies Inc. of Murray Hill, New Jersey, to Oracle and imbedded in the Oracle Retail Predictive Application Server – Enterprise Engine, Oracle Retail Category Management, Oracle Retail Item Planning, Oracle Retail Merchandise Financial Planning, Oracle Retail Advanced Inventory Planning and Oracle Retail Demand Forecasting applications.

(ii) the **MicroStrategy** Components developed and licensed by MicroStrategy Services Corporation (MicroStrategy) of McLean, Virginia to Oracle and imbedded in the MicroStrategy for Oracle Retail Data Warehouse and MicroStrategy for Oracle Retail Planning & Optimization applications.

(iii) the **SeeBeyond** component developed and licensed by Sun MicroSystems, Inc. (Sun) of Santa Clara, California, to Oracle and imbedded in the Oracle Retail Integration Bus application.

(iv) the **Wavelink** component developed and licensed by Wavelink Corporation (Wavelink) of Kirkland, Washington, to Oracle and imbedded in Oracle Retail Store Inventory Management.

(v) the software component known as **Crystal Enterprise Professional and/or Crystal Reports Professional** licensed by Business Objects Software Limited ("Business Objects") and imbedded in Oracle Retail Store Inventory Management.

(vi) the software component known as **Access Via™** licensed by Access Via of Seattle, Washington, and imbedded in Oracle Retail Signs and Oracle Retail Labels and Tags.

(vii) the software component known as **Adobe Flex™** licensed by Adobe Systems Incorporated of San Jose, California, and imbedded in Oracle Retail Promotion Planning & Optimization application.

(viii) the software component known as **Style Report™** developed and licensed by InetSoft Technology Corp. of Piscataway, New Jersey, to Oracle and imbedded in the Oracle Retail Value Chain Collaboration application.

(ix) the software component known as **WebLogic™** developed and licensed by BEA Systems, Inc. of San Jose, California, to Oracle and imbedded in the Oracle Retail Value Chain Collaboration application.

(x) the software component known as **DataBeacon™** developed and licensed by Cognos Incorporated of Ottawa, Ontario, Canada, to Oracle and imbedded in the Oracle Retail Value Chain Collaboration application.

# Contents

# Preface

This document describes the design and implementation of the Oracle Retail Advanced Inventory Planning (AIP) Online product. This document is intended for the retail client and system administrator of the online application.

## Audience

Oracle Retail Operations Guides are designed so that you can view and understand the applications behind-the-scenes processing, including such information as the following:

- Key system administration configuration settings
- Technical architecture
- Functional integration dataflow across the enterprise
- Batch processing

## Related Documents

For more information, see the following documents in the Oracle Retail Advanced Inventory Planning Release 13.0.1 documentation set:

- *Oracle Retail Advanced Inventory Planning Release Notes*
- *Oracle Retail Advanced Inventory Planning Data Management Online - Online Help*
- *Oracle Retail Advanced Inventory Planning Data Management Online User Guide*
- *Oracle Retail Advanced Inventory Planning Order Management - Online Help*
- *Oracle Retail Advanced Inventory Planning Order Management User Guide*
- *Oracle Retail Advanced Inventory Planning Data Model Volume 1 Oracle Database Data Model*
- *Oracle Retail Advanced Inventory Planning Data Model Volume 2 Measure Reference Guide*
- *Oracle Retail Advanced Inventory Planning Installation Guide*
- *Oracle Retail Advanced Inventory Planning Operations Guide*
- *Oracle Retail Advanced Inventory Planning Implementation Guide*
- *Oracle Retail Advanced Inventory Planning Warehouse Replenishment Planning User Guide*
- *Oracle Retail Advanced Inventory Planning Store Replenishment Planning User Guide*

## Customer Support

https://metalink.oracle.com

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received
- Screen shots of each step you take

## Review Patch Documentation

For a base release (".0" release, such as 13.0), Oracle Retail strongly recommends that you read all patch documentation before you begin installation procedures. Patch documentation can contain critical information related to the base release, based on new information and code changes that have been made since the base release.

## Oracle Retail Documentation on the Oracle Technology Network

In addition to being packaged with each product release (on the base or patch level), all Oracle Retail documentation is available on the following Web site:

http://www.oracle.com/technology/documentation/oracle_retail.html

Documentation should be available on this Web site within a month after a product release. Note that documentation is always available with the packaged code on the release date.

## Conventions

**Navigate:** This is a navigate statement. It tells you how to get to the start of the procedure and ends with a screen shot of the starting point and the statement "the Window Name window opens."

> **Note:** This is a note. It is used to call out information that is important, but not necessarily part of the procedure.

```
This is a code sample
    It is used to display examples of code
```

A hyperlink appears like this.

# 1

## Application Overview

## Introduction

AIP is a suite of products that are designed to manage the supply chain needs of large retailers, from interaction with their suppliers through various layers of warehouses down to individual stores and e-commerce sites. It couples time-phased replenishment and allocation algorithms to produce an actionable receipt plan over time. This is based on demand forecasts, replenishment parameters, and inventory availability at the numerous supply points within the supply chain.

## Data Management Online

Data Management online has some main functions that are related to the physical movement of SKUs through the supply chain:

- Maintain supply points with appropriate order cycles for store orders from warehouses and suppliers
- Maintain multi tier supply points with appropriate order cycles for warehouses from suppliers and warehouses.
- Maintain shared data elements throughout the supply chain, such as pack sizes by warehouse

## Order Management

Order Management allows you to create and edit purchase orders and view purchase orders or transfers from suppliers and warehouses.

Purchase orders are orders that are sourced directly from suppliers.

Transfers are orders that are sourced directly from a warehouse.

Orders exist in Order Management as a result of the following processes.

You can manually create a purchase order in order management.

Orders are automatically generated by AIP.

Purchase orders and transfers are available for review until a specified number of days after their release or delivery date.

# Data Flow

Merchandise data is imported from a merchandise system. Imported data includes stores, suppliers, commodities, and warehouses.



**Data Flow**

# 2
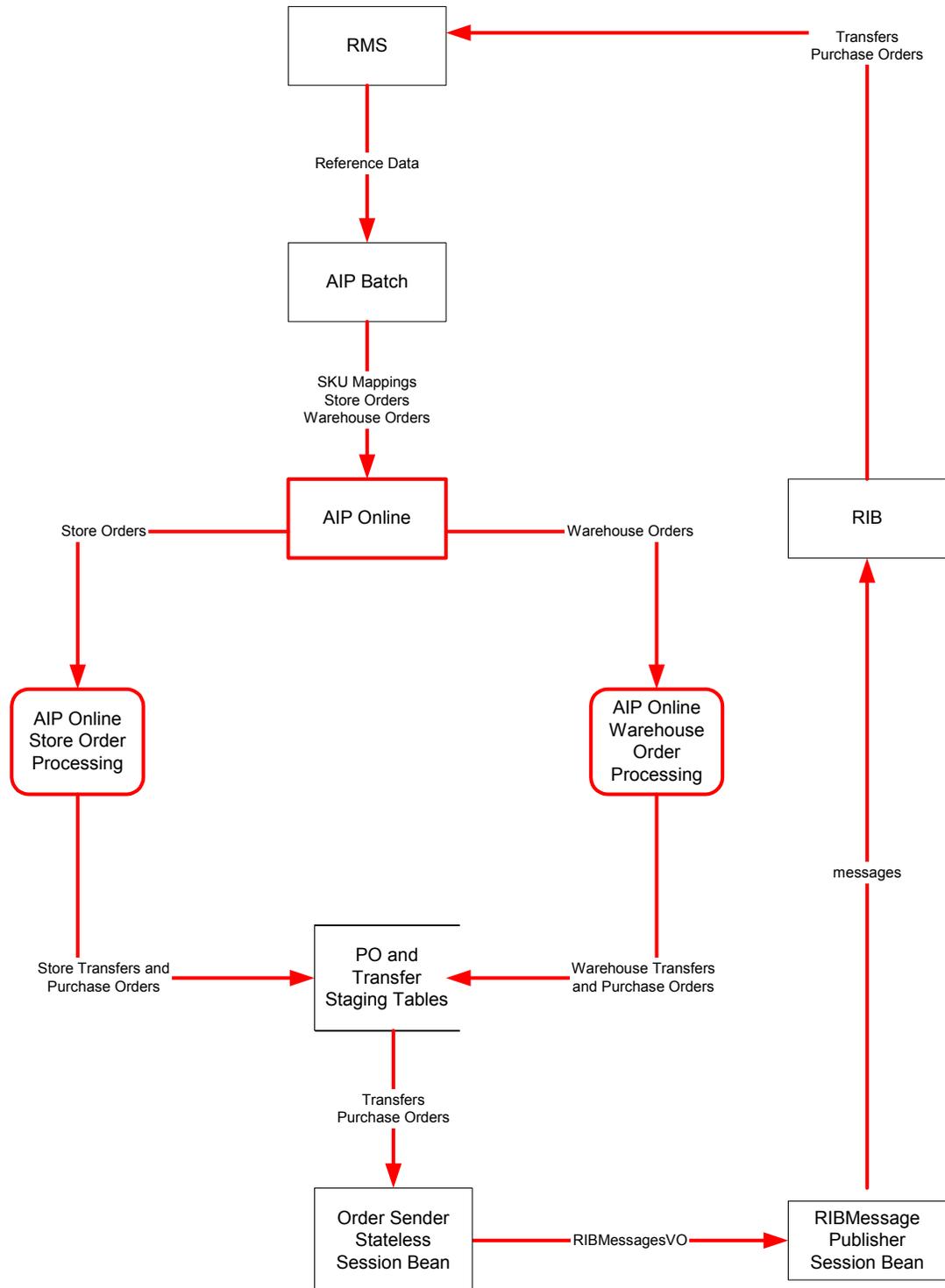
# Set Up the Enterprise

## Overview

System administration and AIP administration allows you to set up and maintain AIP for your enterprise. Through the Administration Consoles you can set up features and default values for your enterprise and the AIP application. You can maintain information at the enterprise and application level.

- **Enterprise:** The enterprise maintenance area allows you to incorporate corporate information into the AIP interface. You can also view services enabled for your enterprise.
- **Application:** The application maintenance area allows you to maintain the information that users can view in the system.

## Security

Security rights for each user is defined at a user level and administrated in the Administration Console. For DMo and OM there is user name and password-controlled access to the applications, data access restrictions that are based on assigned rights to classes, and screen-level access restrictions that are based on assigned privileges.

> **Note:** Details for assigning the security parameters are in the following chapters.

## Log on to the AIP Administration Console

AIP administration is secured by an administrator password. Only individuals with an administrator profile and password can log on to the system administration area of AIP.

1.  Access the AIP Login Window.

### Welcome to Oracle Retail Advanced Inventory Planning Online

**The place to deploy Oracle Retail's supply chain solutions.**

Oracle Retail Advanced Inventory Planning (**AIP**) Online allows retailers to manage capacity planning and scheduling.

Please type in your User name and Password.

Then, click Log In.

| User name: | Password: | |
|---|---|---|
| | | LOG IN |

Visit Oracle's Corporate Web Site at **www.oracle.com**
Copyright © 2004, 2007, Oracle. All rights reserved.

**Login Window**

**2.** On the Login window, enter your user ID in the **User Name** field, enter your password in the **Password** field, and click **LOG IN**. The User Console appears.
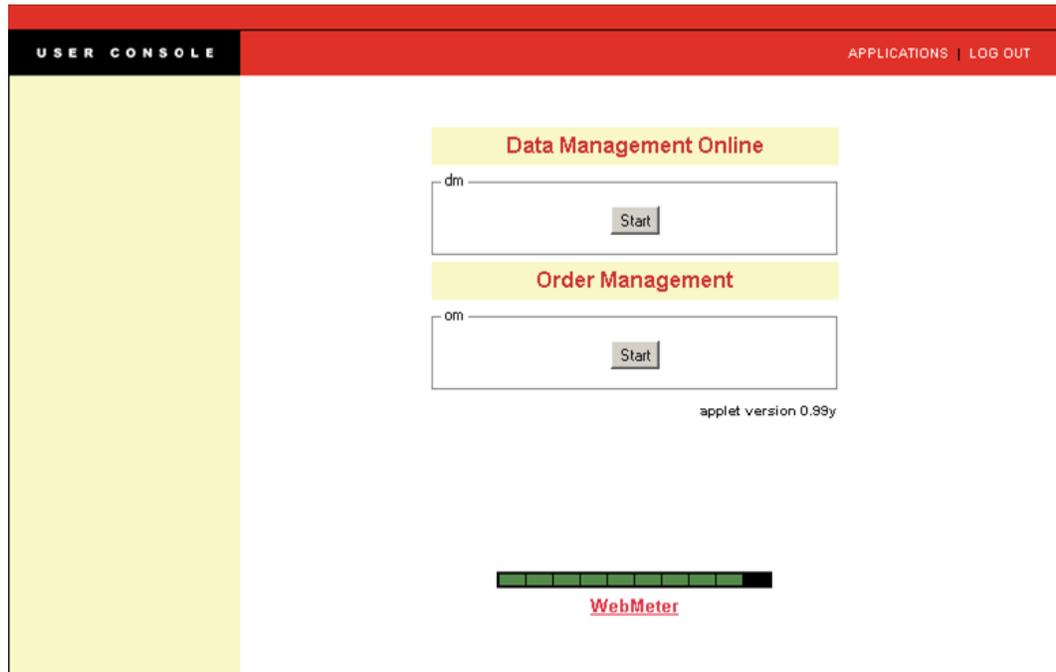


**AIP User Console**

**3.** In the Applications area, click **Core Administration**. The Administration Console opens.
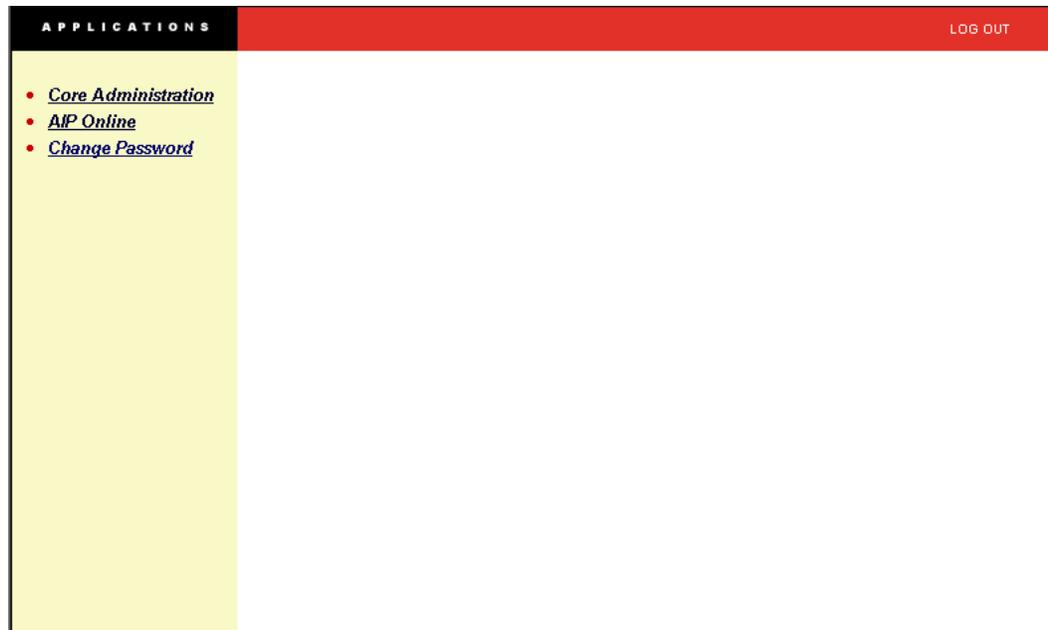


**AIP Applications Area**
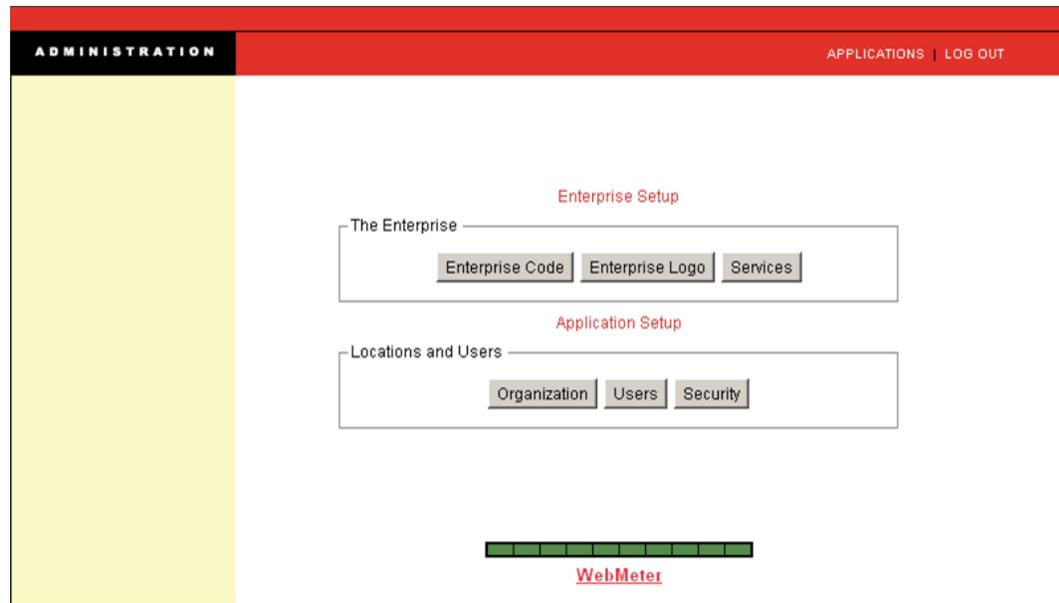
**AIP Administration Console**

# AIP Administration

## Set Up Enterprise Code

When your enterprise is established, an enterprise code or enterprise ID is set up to differentiate your organization from other enterprises set up on the exchange. You can update your enterprise code as necessary.

## Set Up Enterprise Logo

You can maintain the company logo displayed in the AIP application. When you change the logo in the Set Logo window, the logo will be changed on the Administration Console and on the User Console.

## View Services

Your enterprise's e-service license agreement with Oracle Retail defines the number of users you are able to set up in your enterprise. You can view this information in the Services window.

## Change the Enterprise Code

1. On the AIP Administration Console, click **Enterprise Code**. The Set Code window is displayed.
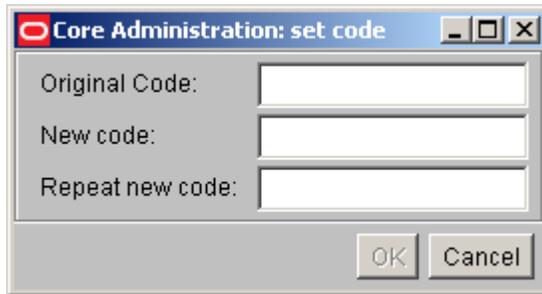


**Set Code Window**

2. In the **Original Code** field, enter the code assigned to your organization by Oracle Retail.

3. In the **New Code** field, enter the new code.

4. In the **Repeat New Code** field, reenter the new code.

5. Click **OK** to save the new Enterprise code.

## Add the Company Logo

1. On the AIP Administration Console, click **Enterprise Logo**. The Set Logo window dialog box is displayed.

2. Click **Choose Logo**.

3. Navigate to and select the file containing the image of your logo.

> **Note:** The logo image file must be a .gif, .jpeg, or .jpg.

4. Click **Open**.

5. Click **Update Logo**.

> **Note:** After you click **Update Logo**, you cannot cancel your changes.

### View e-services Subscription Information

**Navigate:** On the AIP Administration Console, click **Services**. The read-only Services window is displayed.
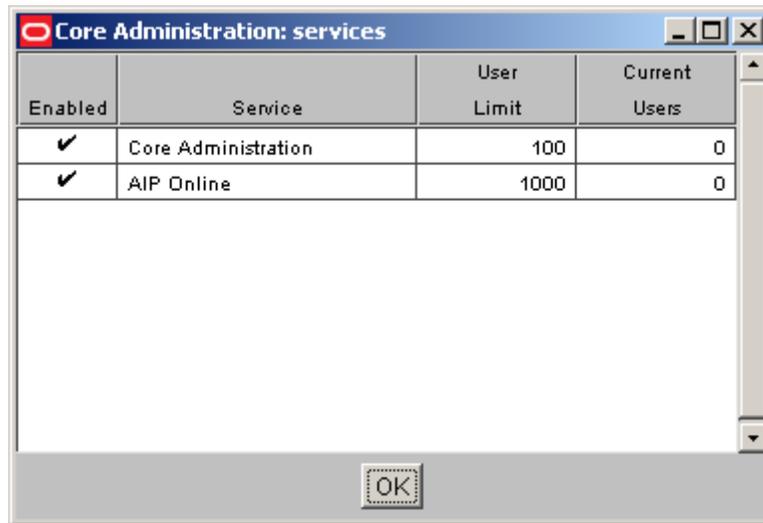


**Services Window**

1. On the Services window, you can:

   a. View the subscription information for your enterprise. A check mark in the Enabled column indicates that you can access that e-service in your current subscription agreement.

   b. View the number of users at your Enterprise that can use each e-service.

   c. View the current number of users at your Enterprise configured for each e-service.

   > **Note:** The software license counts each user once. If an administrator also configures a user account for him or herself, both accounts are counted.

2. To change your service user limit, contact Oracle Retail Customer Support.

3. After viewing the information, click **OK** to close the window.

**3**

# Set Up the Application

## Introduction

You can set up information pertaining to security privileges.

## Log on to the System Administration Console

System administration is secured by an administrator password. Only individuals with an administrator profile and password can log on to the system administration area of AIP.

1. At the standard application login the "address" or URL should be modified to include "phantasm" after the AIP online location: http://servername:port/aiponline/phantasm

2. On the Oracle Retail Login window, enter your user ID in the User Name field.
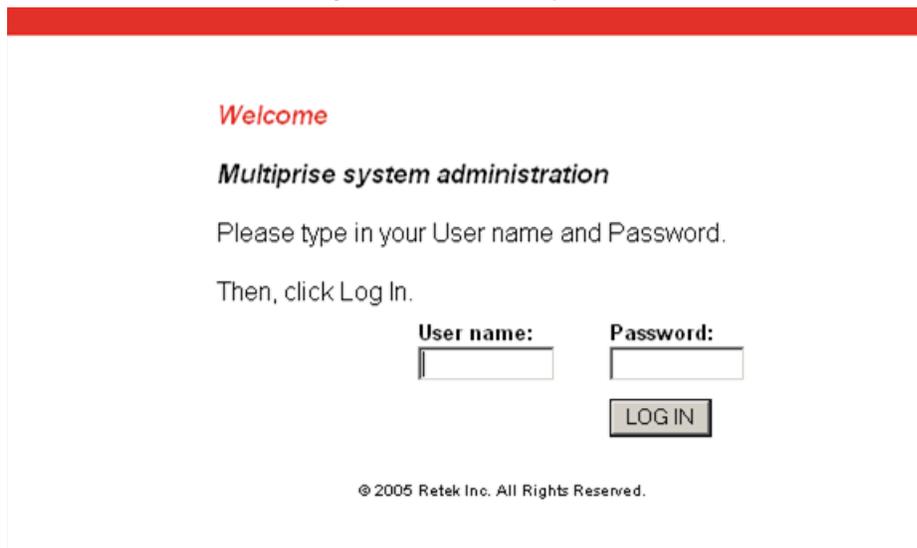


**Oracle Retail Login Window**

3. In the **Password** field, enter your password.

4. Click **Log In**. The System Administration Console opens.
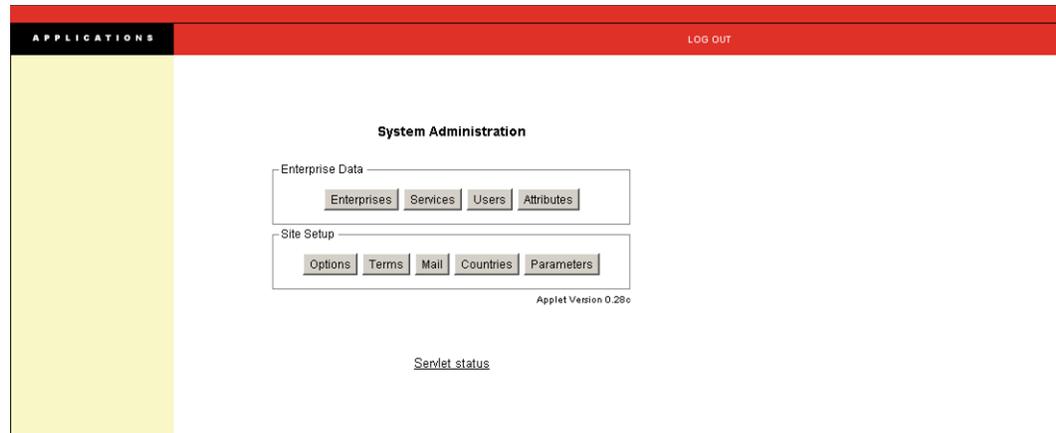
**System Administration Console**

# Set Up System Security

Each user must have their application permissions granted by the administrator. The administrator can choose to set up default selections, remove options, or create new security roles. The security setup will be used during the set-up and maintenance of each user's security permissions.

The creation of screen privileges will be provided in the installation. Application upgrades may also provide new screen privileges when necessary. The table for the permission list is WT_SRVUSERTYPES. Permission groups will be defined only by the client, either during implementation or later.

Setting a privilege as a default will cause the privilege to be defaulted as a "selected" security option when the security privileges are displayed for a new user.

Adding a new permission group will allow you to set up groups of screen privileges which can be assigned to users. Assigning a permission group to a user grants them permission to all privileges assigned to the permission group. This provides a way to mass assign privileges. The permission group must first be created in the System Administration console before screen privileges can be assigned to the group.

Removing a privilege or permission group will prevent the privilege from being displayed as a user security privilege. This will prevent you or other administrators from assigning the privilege to any users.

## Create a Default Privilege

**Navigate:** On the System Administration Console, click **Services**. The Services Administration window opens.
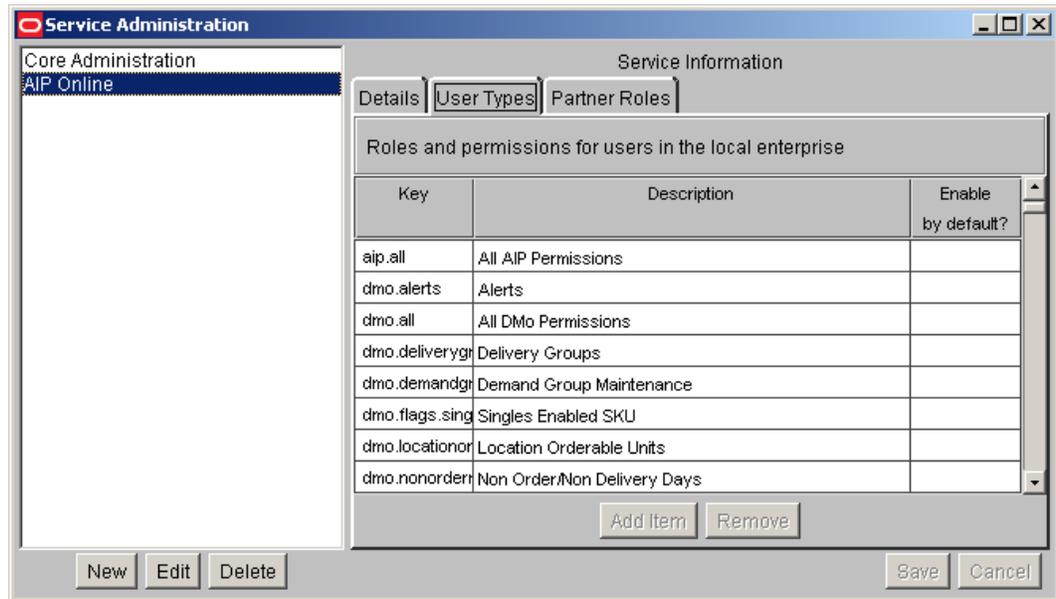


**Services Administration Window –User Types Tab**

1. Select **AIP Online** in the services list.
2. Click the **User Types** tab.
3. Click **Edit**.
4. Click the **Enable by default** column next to the appropriate permission.
5. Click **Save**.

## Delete a Default Privilege

**Navigate:** On the System Administration Console, click **Services**. The Services Administration window opens.

1. Select **AIP Online** in the services list.
2. Click the **User Types** tab.
3. Click **Edit**.
4. Click the check mark in the **Enable by default** column next to the appropriate permission. The check mark is removed.
5. Click **Save**.

## Create a Permission Group

**Navigate:** On the System Administration Console, click **Services.** The Services Administration window opens.

1. Select **AIP Online** in the services list.
2. Click the **User Types** tab.
3. Click **Edit**.
4. Click **Add Item**.
5. Enter a key in the field.

> **Note:** The key must start with **sec:** to be recognized as a permission group.

6. Enter a description.
7. Determine the desired default option.
8. Click **Save**.

## Delete a Permission Group

**Navigate:** On the System Administration Console, click **Services.** The Services Administration window opens.

1. Select **AIP Online** in the services list.
2. Click the **User Types** tab.
3. Click **Edit.**
4. Select the permission group to be deleted.
5. Click **Remove.**
6. Click **Save**.

# Set Up Permission Groups

Permission groups are created in the System Administration console. Once created, you can assign privileges to them. By assigning privileges you are creating groupings of privileges that can be assigned to a user en masse rather than individually picking each privilege and assigning it to the user. This also provides a type of mass maintenance capability. By adding a privilege to a permission group you are automatically assigning the privilege to every user which is assigned the permission group. Similarly, removing a privilege from the permission group denies that privilege to all users which are assigned the permission group.

## Assign Privileges to a Permission Group

**Navigate:** On the AIP Administration Console, click **Security**. The Security Administration window opens.
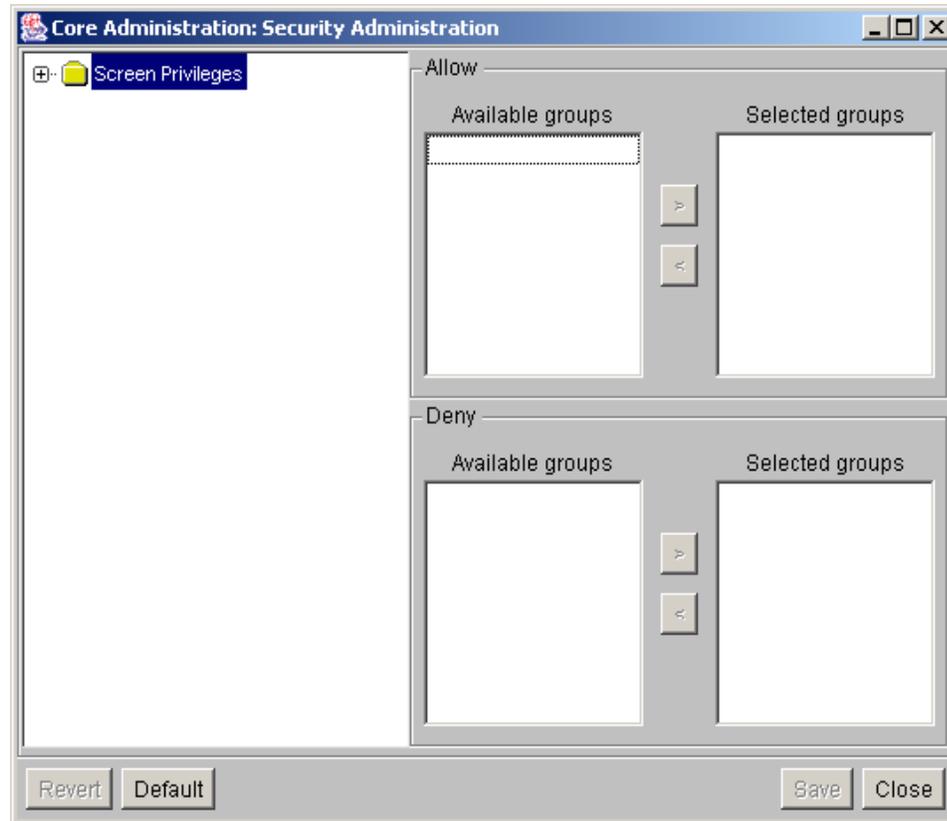


**Core Administration Window**

1. Click **+** to display the screen privileges
2. Select a screen privilege
3. In the **Allow Available** groups select a permission group to be assigned to the screen privilege.
4. Click **>** to move the permission group to the Allow Selected groups list.
5. Click **Save**.

## Delete Privilege from Permission Group

**Navigate:** On the AIP Administration Console, click **Security**. The Security Administration window opens.

1. Click **+** to display the screen privileges
2. Select a screen privilege
3. In the **Allow Selected Groups**, select a permission group to be removed from the screen privilege.
4. Click **<** to move the permission group to the Allow Available groups list.
5. Click **Save**.

# Set Up Users

Each user must be set up by an administrator. There are two types of users, administrators and users. Administrators have access to and can maintain the administration console. There must be at least one system administration user. This user is created during implementation and has the access to create new privilege types as described below.

Users have access to the User Console of AIP. They cannot maintain any of the system level settings. A user's permissions may be further limited by scope set by the administrator. Scope defines which departments a user has access to maintain tracks for.

> **Note:** When you set up the users, you assign local user types.

## User Definition

### User Name Restrictions
- Must be a minimum of 1 and a maximum of 16 characters in length
- May contain any characters, which means that symbols, including spaces, are allowed
- Must be unique

### Password Restrictions
- Must be a minimum of 6 and a maximum of 128 characters in length
- Must have at least five different characters
- Must not be simple; The following are not allowed:
  - Sequences (ABCDE or ABCXYZ)
  - Four consecutive characters as this results in "pairing" (ABCDEF results in give pairs AB, BC, CD, DE, EF)
- Must not be easily derivable from the user name or full name
- Must not be easily derivable from the previous password
- Must not be derivable from a dictionary entry (the dictionary is configurable)

The rules are defined via the opt/rfp/properties/security.properties file. The format of this is:
- Password:
- trackeradmin.prop.pwrules.code=uk.co.webtrak.security.passwords.rules.simple.Checker
- trackeradmin.prop.simplepw.dictionary=pw_dictionary

### Failed Login Lockout

Three invalid entries of a password for a given user ID within twenty-four hours turns off that user ID for five days. The password must be reset using the enterprise administrator screen shown above.

The properties for setting the parameters, the number of failed login tries, and the number of days locked out can be set in the opt/rfp/properties/security.properties file:

**Lockout Parameters**

```
trackeradmin.prop.password.lockout.count=3
trackeradmin.prop.password.lockout.interval=20m
trackeradmin.prop.password.lockout.wait=3d
```

### Auditing

Security changes and session activity are recorded in an audit table (ENT_AUDIT).

> **Note:** Password cycling, failed logins, and so on are driven from this table. It is important to recognize the impact of clearing this table too frequently.

opt/rfp/properties/security.properties file setting:

**Auditing (On or Off)**

```
trackeradmin.prop.audit=1
```

### Password Cycling

A password may be set to NOT be reused within 'N' changes or 'M' days. For example:

- If an "N" change is set to 5, the first password cannot be used on turns 2, 3, 4, or 5; however, the first password can be used again in turn 6.
- If an "M" change is set to 3, the same password cannot be used again in the space of days.

These parameters are specified via the opt/rfp/properties/security.properties file.

> **Note:** The history used to validate these parameters is the audit table (ENT_AUDIT). See the Auditing section above.

```
Uniqueness parameters:
trackeradmin.prop.password.uniqueness=1
trackeradmin.prop.password.uniqueness.interval=120d
```

Here the password can be reused every time or after 120 days.

### Password Aging

The aging of passwords can be set to be seconds, minutes, hours, or days. The settings are specified via the opt/rfp/properties/security.properties file. See the following format:

**Password Expiry**

```
trackeradmin.prop.passwordexpiry=300s
```

In this example the password expires in five minutes.

**Tables Referenced**

ENT_ATTRS

ENT_AUDIT

ENT_LOCATIONS

ENT_LOCKS

ENT_MCLDATA

ENT_MCLHEADINGS

ENT_PARAMETERS

ENT_PARAMVALUES

ENT_PARTNERDEPTS

ENT_PARTNERS

ENT_PHASES

ENT_RESOURCES

ENT_SEASONS

ENT_SRVUSERTYPES

ENT_STAMPS

ENT_USERS

**Properties Files**

opt/rfp/properties/security.properties

## Add an Administrator

**Navigate:** On the AIP Administration Console, click **Users**. The User Administration window opens.
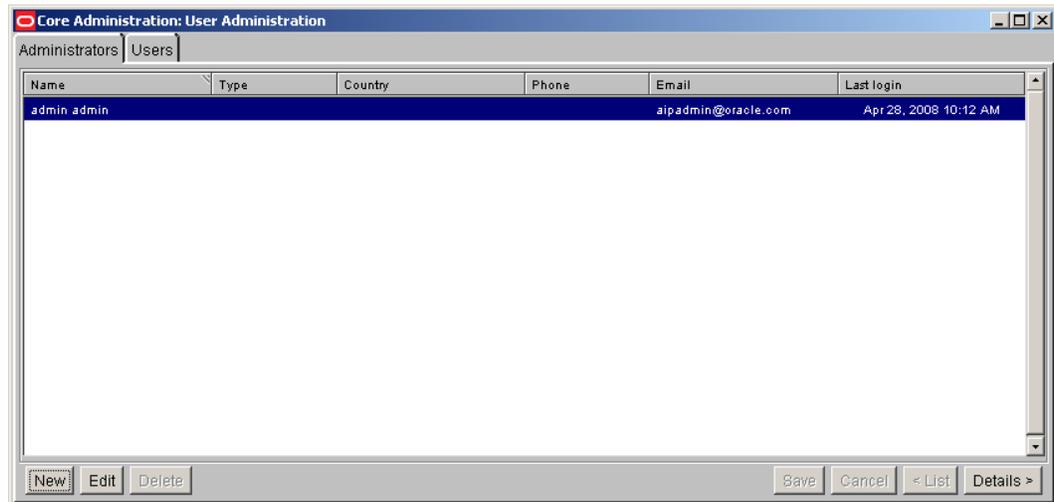


**User Administration Window – Administrators Tab List View**

1. Click **New**. The details view of the Administrators tab is displayed.



**User Administration Window – Administrators Tab Detail View**

2. Enter necessary information in the fields. Required fields are:
   - First and last Name
   - E-mail
   - Username
   - New Password
   - Retype New Password

   > **Note:** Save is not enabled until all required entries are made.

3. Click **Save** to save the changes.
4. Click the close window ☒ button to return to the Administration Console window.

## Edit an Administrator

**Navigate:** On the AIP Administration Console, click **Users**. The User Administration window opens.

1. Select the name of an administrator.
2. Click **Edit**. The details list is displayed.
3. Update the information as necessary.
4. Click **Save** to commit the changes.
5. Click the close window ☒ button to return to the Administration Console window.

## Delete an Administrator

**Navigate:** On the AIP Administration Console, click **Users**. The User Administration window opens.

1. Select the name of an administrator. All contact information is highlighted.
2. Click **Delete**. A dialog box is displayed to confirm your decision.
3. To proceed, click **OK**. The administrator's name is deleted from the list.
4. Click the close window ☒ button to return to the Administration Console window.

## Add a User

**Navigate:** On the AIP Administration Console, click **Users**. The User Administration window opens.

1. Click on the **Users tab**. The Users list is displayed.
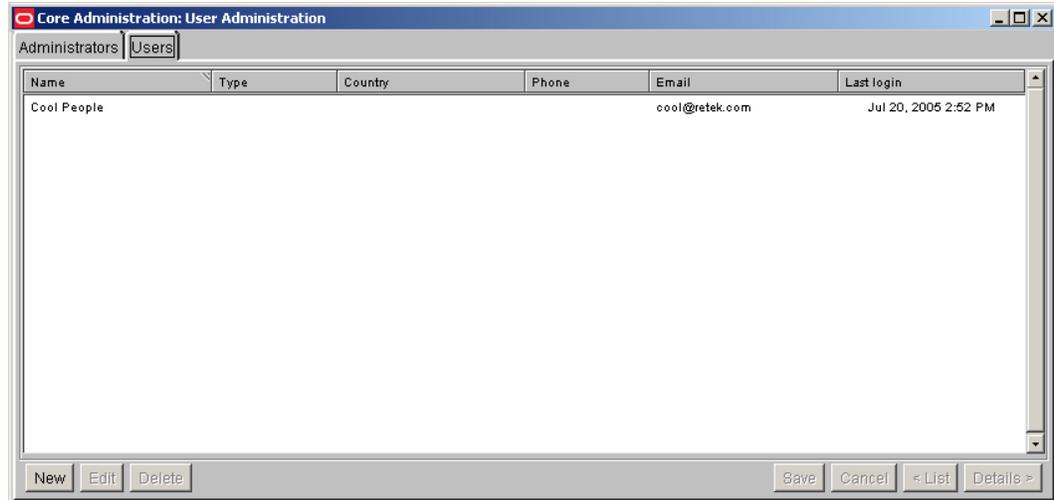


**User Administration Window – Users Tab List View**

2. Click **New**. The details view of the Users tab is displayed.



**User Administration Window – Users Tab Details View**

3. Add user details.

On the Details tab, enter necessary information about the new user. Entries are required in these fields:

- **First Name**
- **Last Name**
- **E-mail**
- **Username**
- **New Password**
- **Retype New Password**

4. Define a user's scope

a. Select the **Scope** tab. The Scope tab is displayed.

b. In the **Available Classes** list, click on a class name to be assigned to the user. At least one Class is required to create a user.

c. Click **>** to move the class to the Selected Class list.

d. To remove a class from the Selected Classes list, select the class name. The Left Arrow at the center of the window is enabled. Click **<** to return the class to the Available Classes list.

> **Note:** Save is not enabled until there are entries in all required fields.

5. Define a user's system permissions

a. Select the **Permissions** tab. The Permissions tab is displayed.

b. In the **Enabled** column, select **AIP** from the list of Services. The Available Types column lists the user roles for your enterprise.

c. In the **Available Types** list, select the role that applies to this user.

> **Note:** The permission groups are listed along with each individual screen privilege. The selected individual screen privileges along with the screen privileges assigned to any selected permissions groups comprise the list of the users security permissions.

d. Click **>** to move the role to the **Selected Types** list.

6. Click **Save** to commit your changes.

7. Click the close window ☒ button to return to the Administration Console window.

## Edit User Information

**Navigate:** On the AIP Administration Console, click **Users**. The User Administration window opens.

1. Select the **Users tab**. The Users list is displayed.

2. Select the user name you wish to edit.

3. Click **Edit**. The Details tab is displayed with the entry fields enabled.

4. Change the information in any or all of the entry fields.

5. Click **Save** to save the changes.

6. Click the close window ☒ button to return to the Administration Console window.

## Delete a User

**Navigate:** On the AIP Administration Console, click **Users**. The User Administration window opens.

1. Select the **Users tab**. The Users list is displayed.

2. Select the name you wish to delete.

3. Click **Delete**. You are prompted to confirm your decision.

4. Click **OK**. The selected user is deleted from the list and the database.

5. Click **List** to return to the Users tab list view. The user's name is deleted from the list.

6. Click the close window ☒ button to return to the Administration Console window.

# Privileges

## Access Control

Rights are assumed to be denied unless explicitly assigned. Permissions exist for granting all rights within a given application or across the AIP suite.

For Data Management and Order Management, all fields within the windows in inaccessible tabs are disabled. An alert message displays when a user attempts to access an unassigned or denied tab. The message indicates that this area is not accessible for the user.

> **Note:** This alert message will not display if the tab is the default selection in a selected area.

Message: The security privileges of the current user do not grant access to this functionality.

Table for permission list is WT_SRVUSERTYPES.

## Privileges

| Key | Description |
| --- | --- |
| aip.all | All AIP Permissions |
| dmo.alerts | Alerts |
| dmo.all | All DMo Permissions |
| dmo.deliverygroups | Delivery Groups |
| dmo.demandgroupmaintenance | Demand Group Maintenance |
| dmo.locationorderableunits | Location Orderable Units |
| dmo.nonordernondelivery | Non Order/Non Delivery Days |
| dmo.nonrelease | Non Release/Non Receipt Days |
| dmo.onsupplyoffsupply | On Supply/Off Supply |
| dmo.ordercyclecreation | Order Cycle Creation/Maintenance |
| dmo.ordercycle | Order Cycle |
| dmo.ordergroups | Order Groups |
| dmo.pallet.order.multiples | Pallet Order Multiples |
| dmo.planninghorizon | Planning Horizon |
| dmo.profilecopyexceptions | Copy Profile Exceptions |
| dmo.profilereleaseplacement | Profile Release and Placement Schedule Exceptions |
| dmo.profiles.department | Class to Profile Assignment |
| dmo.profiles.planninggroup | Planning Group Maintenance |

| Key | Description |
| --- | --- |
| dmo.profiles.supplyprofiles | Supply Profiles |
| dmo.promstartenddates | Promotional Start and End Dates |
| dmo.rangingwarehouse | Ranging |
| dmo.receipt.avail.leadtimes | Receipt to Availability Lead Time |
| dmo.receivingwindows | Receiving Windows |
| dmo.release.placement.schedule | Release And Placement Schedule Exceptions |
| dmo.release.profile.store | Profile - Store Schedule Exceptions |
| dmo.siteandchamber | Scheduling Location Maintenance |
| dmo.skukeeptogether | SKU Keep Together |
| dmo.skureleaseschedule | SKU Release Schedule Exceptions |
| dmo.slotsandshifts | Slots and Shifts |
| dmo.sourcesplits.timebalanced | Time Balanced Supply Source Splits |
| dmo.stockless.ind.exceptions | Stockless Indicator Exceptions |
| dmo.storeformatpacksize | Store Format Packsize Defaults |
| dmo.storepriority | Store Priority |
| dmo.storereceivingcalendar | Store Receiving Calendar |
| dmo.storereconflag | RDC Demand Reconciliation Flag Exceptions |
| dmo.storesource | Store Source |
| dmo.storesource.massmaintenance | Store Source Mass Maintenance |
| dmo.supplierlocks | Supplier Locks |
| dmo.supplierreleaseplacement | Supplier Release and Placement Schedule Exceptions |
| dmo.warehouse.coupled | Warehouse Coupled Flag |
| dmo.warehousecalendar | Warehouse Calendar |
| dmo.whstoreorderingschedules | WH and Store Ordering Schedules |
| dmo.secondary.sources | Secondary Sources |
| dmo.scalinggroups | Supplier and Container Scaling Groups |
| dmo.skuattributes | SKU attributes |
| om..all | All Order Management Permissions |
| om.ordercreation | Order Creation |
| om.ordermaintenance | Order Maintenance |
| om.orderreview | Order Review |
| om.scalinggrouppreview | Scaling Group Order Reivew |

# Caching

Data objects that are used in more than one screen are usually cached. Those that are used in a single screen are not usually cached. The data cache resides on the client layer, so the contents are specific to the data that is requested by a given user. When cached data is updated, all attributes are updated, such as name, flags, and so on.

## Cached Data

The following is a list of cached data:

- Commodity
- CommodityPackSize
- DeliveryGroup
- DemandGroup
- Class
- NetworkGroup
- OrderCycle
- OrderGroup
- PlanningGroup
- ProductType
- Profile
- ReceivingWindow
- Shift
- Slot
- StockingPoint
- StockingPointStatus
- Store
- StoreFormat
- StoreOrderCycle
- Supplier
- SupplierCommodityPackSize
- SupplierLocation

## Cached Data Update

In the following table:

- The first column defines cached data status.
- The first row defines how data are retrieved.
- The second row defines retrieved data status.
- Each cell defines whether the cached data is updated.

| | Data Retrieved by Querying | | Data Retrieved by Refreshing | |
|---|---|---|---|---|
| | **No Timestamp Change** | **Timestamp Changed** | **No Timestamp Change** | **Timestamp Changed** |
| Cached data unmodified | Do not update cached data | Update cached data | Do not update cached data | Update cached data |
| Cached data modified | Update cached data | Update cached data | Update cached data | Update cached data |