Oracle® Demantra

Security Guide

Release 12.2

Part No. E49182-04

August 2016

ORACLE

Oracle Demantra Security Guide, Release 12.2

Part No. E49182-04

Primary Author: Jason Lansdowne

Contents

Send Us Your Comments

Preface

1 General Security Principles

Keeping Software Up-to-date 1-1
Restricting Access to Critical Services 1-1
Data Security 1-2
Changing Worksheet Access 1-5
Redirecting Demantra to a Different Database 1-6
Following the Principle of Least Privilege 1-6
Monitoring System Activity 1-7
Keeping Security Information Up-to-date 1-7

2 Configuring Security During Installation

Setting Component Security 2-1
Creating or Modifying a Component 2-1
Deleting a Component 2-10
Configuring the Security Provider 2-10
Running SYS_GRANTS.SQL Script 2-13
Configuring Web Applications for SSL and Firewalls 2-14

3 Configuring Security Post-installation

Overview 3-1
Security 3-2
How the User Interfaces Can Be Configured 3-2

Other Security Features....3-3
Logging onto the Collaborator Workbench Administrator....3-3
Providing Access to the Workflow Editor....3-4
Dropdown Security....3-5
Controlling Access to Series....3-7
Feature Security....3-8
Program Groups....3-12
Defining a Program Group....3-13
Redefining a Program Group....3-16
Deleting a Program Group....3-17
Configuration Notes....3-17
Specifying Permissions for Menu Items....3-18

4 Other Security Features

The SysAdmin User....4-1
Creating or Modifying a User....4-2
Copying a User....4-8
Deleting a User....4-9
Creating or Modifying a User Group....4-9
Deleting a Group....4-12
Logging Out Users....4-13
Changing Your Password....4-14
Password Policy....4-15
Mutual Authentication....4-16
Logging Messages of the Application Server....4-17
Viewing the Workflow Process Log....4-17
Specifying Content Pane Security....4-18
Checking the Log Files and Tables....4-19

A Security Checklist

Checklist....A-1

Index

Send Us Your Comments

Oracle Demantra Security Guide, Release 12.2

Part No. E49182-04

Oracle welcomes customers' comments and suggestions on the quality and usefulness of this document. Your feedback is important, and helps us to best meet your needs as a user of our products. For example:

- Are the implementation steps correct and complete?
- Did you understand the context of the procedures?
- Did you find any errors in the information?
- Does the structure of the information help you with your tasks?
- Do you need different information or graphics? If so, where, and in what format?
- Are the examples correct? Do you need more examples?

If you find any errors or have any other suggestions for improvement, then please tell us your name, the name of the company who has licensed our products, the title and part number of the documentation and the chapter, section, and page number (if available).

Note: Before sending us your comments, you might like to check that you have the latest version of the document and if any concerns are already addressed. To do this, access the new Oracle E-Business Suite Release Online Documentation CD available on My Oracle Support and www.oracle.com. It contains the most current Documentation Library plus all documents revised or released recently.

Send your comments to us using the electronic mail address: appsdoc_us@oracle.com

Please give your name, address, electronic mail address, and telephone number (optional).

If you need assistance with Oracle software, then please contact your support representative or Oracle Support Services.

If you require training or instruction in using Oracle software, then please contact your Oracle local office and inquire about our Oracle University offerings. A list of Oracle offices is available on our Web site at www.oracle.com.

Preface

Intended Audience

Welcome to Release 12.2 of the *Oracle Demantra Security Guide.*

See Related Information Sources on page viii for more Oracle E-Business Suite product information.

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 that have purchased support 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=trsif you are hearing impaired.

Structure

1 General Security Principles

Important: The Demantra Local Application replaces Collaborator Workbench. You may see both names in this text.

2 Configuring Security During Installation

Important: The Demantra Local Application replaces Collaborator Workbench. You may see both names in this text.

3 Configuring Security Post-installation

Important: The Demantra Local Application replaces Collaborator Workbench. You may see both names in this text.

4 Other Security Features

Important: The Demantra Local Application replaces Collaborator Workbench. You may see both names in this text.

A Security Checklist

Important: The Demantra Local Application replaces Collaborator Workbench. You may see both names in this text.

Related Information Sources

Oracle Demantra Implementation Guide

Oracle Demantra Installation Guide

Oracle Demantra User's Guide

Oracle Demantra Demand Management User's Guide

Oracle Demantra Deduction and Settlement Management User's Guide

Oracle Demantra Predictive Trade Planning User's Guide

Oracle Demantra Real-Time Sales and Operations Planning User's Guide

Integration Repository

The Oracle Integration Repository is a compilation of information about the service endpoints exposed by the Oracle E-Business Suite of applications. It provides a complete catalog of Oracle E-Business Suite's business service interfaces. The tool lets users easily discover and deploy the appropriate business service interface for integration with any system, application, or business partner.

The Oracle Integration Repository is shipped as part of the Oracle E-Business Suite. As your instance is patched, the repository is automatically updated with content appropriate for the precise revisions of interfaces in your environment.

Do Not Use Database Tools to Modify Oracle E-Business Suite Data

Oracle STRONGLY RECOMMENDS that you never use SQL*Plus, Oracle Data Browser, database triggers, or any other tool to modify Oracle E-Business Suite data unless otherwise instructed.

Oracle provides powerful tools you can use to create, store, change, retrieve, and maintain information in an Oracle database. But if you use Oracle tools such as SQL*Plus to modify Oracle E-Business Suite data, you risk destroying the integrity of your data and you lose the ability to audit changes to your data.

Because Oracle E-Business Suite tables are interrelated, any change you make using an Oracle E-Business Suite form can update many tables at once. But when you modify Oracle E-Business Suite data using anything other than Oracle E-Business Suite, you may change a row in one table without making corresponding changes in related tables. If your tables get out of synchronization with each other, you risk retrieving erroneous information and you risk unpredictable results throughout Oracle E-Business Suite.

When you use Oracle E-Business Suite to modify your data, Oracle E-Business Suite automatically checks that your changes are valid. Oracle E-Business Suite also keeps track of who changes information. If you enter information into database tables using database tools, you may store invalid information. You also lose the ability to track who has changed your information because SQL*Plus and other database tools do not keep a record of changes.

1

General Security Principles

Important: The Demantra Local Application replaces Collaborator Workbench. You may see both names in this text.

This chapter covers the following topics:

- Keeping Software Up-to-date
- Restricting Access to Critical Services
- Data Security
- Changing Worksheet Access
- Redirecting Demantra to a Different Database
- Following the Principle of Least Privilege
- Monitoring System Activity
- Keeping Security Information Up-to-date

Keeping Software Up-to-date

One of the principles of good security practice is to keep all software versions and patches up-to-date. This document is based on a release level of 12.2 on all software and documentation.

Restricting Access to Critical Services

Keep both the E-Business application middle-tier and the database behind a firewall. In addition, place a firewall between the middle-tier and the database. The firewalls provide assurance that access to these systems is restricted to a known network route, which can be monitored and restricted, if necessary. As an alternative, a firewall router substitutes for multiple, independent firewalls.

If firewalls cannot be used, be certain to configure the TNS Listener Valid Node Checking feature which restricts access based upon IP address. Restricting database access by IP address often causes application client/server programs to fail for DHCP clients. To resolve this, consider using static IP addresses, a software/hardware VPN or Windows Terminal Services or its equivalent.

Data Security

Demantra data is secured as follows:

- The data is partitioned into components, which generally correspond to organizational roles, which can overlap. Each component has an owner, who acts as the administrator and who can create additional users. (See "Creating or Modifying a Component" in this document.)

- Each user is authorized for one component. In addition, you can further restrict a specific user's access to data by applying filters so that the user can see only specific level members as well as only certain series.

- Users can belong to groups, and group members can collaborate, inside or outside of workflows. When a user creates a note, he or she can control access to that note by user or by group.

The following table summarizes how Demantra controls access to data elements.

Data Element	Options	Controlled by Component	Controlled by User Group	Controlled by User ID
Series	Visible or not visible	Yes	No	Yes
Series indicators (which indicate the presence of a note or promotion within the worksheet table.)	Visible or not visible	Yes	No	No
Levels	Visible or not visible	Yes	No	No

Level members	Full control, including ability to delete members Read/write existing members Read existing members No access	Yes	No	Yes
Units of measure	Visible or not visible	Yes	No	No
Indexes and exchange rates	Visible or not visible	Yes	No	No
Notes	Similar to level member options	No	As specified by creator of note	

It is useful to remember that each user of a component sees a subset of the data associated with that component. You cannot give user access to data that is not contained in the component.

Components

Each component has the following properties:

- Series, levels, units of measure, indexes, and exchange rates. For each level, you define permissions that the users have for the members of that level. The choices are as follows:
  - Full control, including ability to delete members
  - Read/write existing members
  - Read existing members
  - No access
- An owner. This owner acts as the administrator of the component.
- Possible additional users, created by the owner. The owner can also further restrict data access for particular users.

Users

User details are defined using the Business Modeler (Security > Create/Modify User). For more information about users, see **Creating or Modifying a User**.

For users, you can specify the following details:

- Overall permission level, which can enable the user to log onto Demantra administrative tools and modify the component.
- Series that the user can access, generally a subset of the series included in the component.
- Optional permissions to control which level members the user can see and edit. The choices are as follows:
  - Full control, including ability to delete members
  - Read/write existing members
  - Read existing members
  - No access (the members are filtered out entirely for this user)
- Group or groups to which the user belongs.

User Groups

For user groups, you can specify the following details:

- Which users are in the group.
- Whether this user group is also a collaboration group (for use by the Workflow Engine).
- Whether users of this group can log into the Workflow Editor.

Security for Deleting Members

Most level members are created by integration and it would generally be undesirable to delete them. Most users, therefore, do not have delete access to these members. The exception is a user with System Manager permission; see "Permission Levels" in this document.

Level members can be created directly within Demantra (through Member Management). For any these members, the user who created the member has permission to delete it.

Data Security at Higher Levels

When a user views data at an aggregation level that is higher than where the

permissions are set, it is necessary to resolve how to aggregate editable members and uneditable members. Demantra uses the following rules:

- If all lower-level members are editable (either as read/write or full control), the member is editable.
- If some of the lower-level members are visible but read-only, the member is not editable.
- If some of the lower-level members are not visible, those members are filtered out and do not affect the aggregation. The upper-level member may or may not be editable, depending on the preceding rules.

Custom Methods

As the implementer, you can define custom methods to perform operations on a selected member, for users to access as an option on the right-click menu. You can apply security to your methods, just as you do with the core right-click actions.

You can define a user security threshold for visibility of that method. For example, you can state the method should only be visible to users who have 'Full Control' of the member from which you launch the method. To control this, you log into the Business Modeler, select 'Configure > Configure Methods'. For 'Method Type'= Custom, you can select from the Security Threshold of Full Control, Read & Write or Read Only.

For information on methods, see "Methods and Workflow" in this document.

Changing Worksheet Access

If a worksheet is private, it can be seen only by its owner. If it is public, it is visible to all users.

To change who can access a worksheet:

1. Log onto the Business Modeler as described in "Logging onto the Business Modeler. "
2. Click Tools > Worksheet Management.

   The Worksheet Manager is displayed.
3. In the row corresponding to the worksheet, click the Permission Type field.
4. Click Private or Public and click OK.

Redirecting Demantra to a Different Database

Oracle does not support Microsoft SQL Server in this release. Please monitor My Oracle Support for versions supporting SQL Server. Items marked with ** are not valid unless support for Microsoft SQL Server is available.

In Demantra, the database connection (and data source configuration) is controlled by the Java Naming Directory Interface (JNDI).

To point Demantra to a different database without rerunning the installer, complete the following steps:

1. Make a backup copy of server.xml. This file is located in …\Oracle Demantra\Collaborator\Tomcat\conf\.

2. Open server.xml for editing.

3. Locate the following sections:

```
Context path="/demantra"
 docBase="E:\Program Files\Oracle Demantra
73b37\Collaborator\demantra"
 crossContext="false"
 debug="0"
 reloadable="false"

Resource
 name="jdbc/DemantraDS"
 auth="Container"
 type="javax.sql.DataSource"
 driverClassName="oracle.jdbc.driver.OracleDriver"
 url="jdbc:oracle:thin:@dempm2db.us.oracle.com:1521:ORCL"

 username="demo73b37"
 password="manager"
```

4. Modify the "username" and "password" sections to point to the new schema and to use the new password.

5. To point to a different DB, modify the DB host and SID within the URL, which in this example are "dempm2db.us.oracle.com" and "ORCL", respectively.

6. Restart the web server. (If you are not using Apache Jakarta Tomcat, refer to your application server's version-specific documentation to learn how to modify the database hostname, username, password, and SID (system identifier) specified by the JNDI.)

Following the Principle of Least Privilege

The principle of least privilege states that users should be given the least amount of privilege to perform their jobs. Over-ambitious granting of responsibilities, roles,

grants, etc., especially early on in an organization's life cycle when people are few and work needs to be done quickly, often leaves a system wide open for abuse. User privileges should be reviewed periodically to determine relevance to current job responsibilities.

Monitoring System Activity

System security stands on three legs: good security protocols, proper system configuration and system monitoring. Auditing and reviewing audit records address this third requirement. Each component within a system has some degree of monitoring capability. Follow audit advice in this document and regularly monitor audit records.

Keeping Security Information Up-to-date

Oracle continually improves its software and documentation. Check the notes on My Oracle Support regularly for the latest information.

2

Configuring Security During Installation

Important: The Demantra Local Application replaces Collaborator Workbench. You may see both names in this text.

This chapter covers the following topics:

- Setting Component Security
- Creating or Modifying a Component
- Deleting a Component
- Configuring the Security Provider
- Running SYS_GRANTS.SQL Script
- Configuring Web Applications for SSL and Firewalls

Setting Component Security

The following section explains how to create and modify components. Since this process determines what is available to a user, it is an important way for controlling access to series, and levels, engine profiles, and other data.

Creating or Modifying a Component

To create or modify a component:

1. Click Components > Create/Open Component. Or click the Create/Open Component button.

   Note: This option may not be available, depending on the user name with which you logged onto Business Modeler.

The Create/Open Component dialog box appears.

2. Now do one of the following:

   - To create a new component, click the New Component button and then click OK. Or double-click the New Component icon.

     Note: This option is available only if you log into Business Modeler as the user with the highest permission.

   - To open an existing component, double-click the icon corresponding to the component. Or click the icon and then click OK.

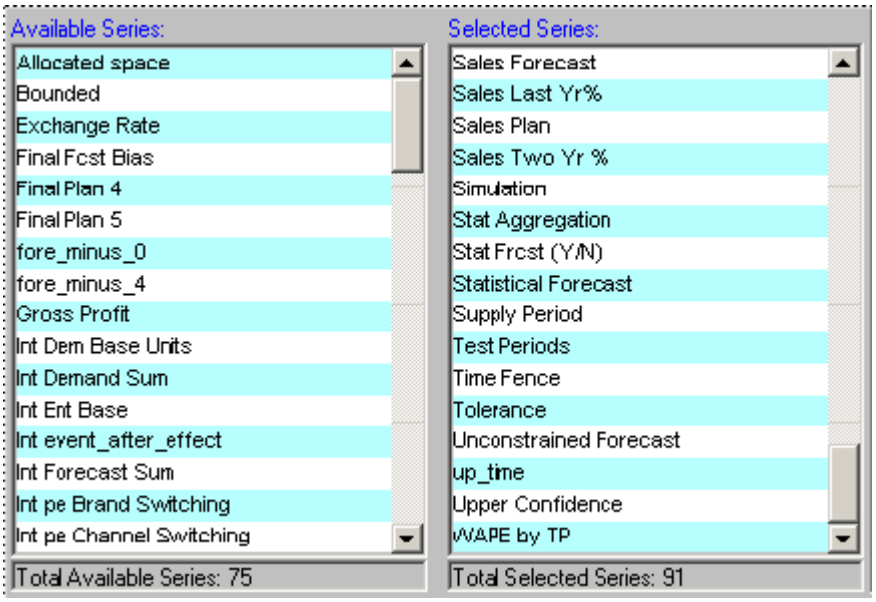
   The Component Configuration Wizard displays its first dialog box.

3. Enter or edit general information for the user interface, as follows:

Component Name	Unique name for this component.
Component Description	Description
About Window Description	Optional description to include in the About page of this component.

4. Click Next.

   The Business Modeler displays the Available Series and Selected Series lists.



5. Select the series that should be available in the component.

    1. Move all series that you want into the Selected Series list, using any of the techniques in "Working with Lists".

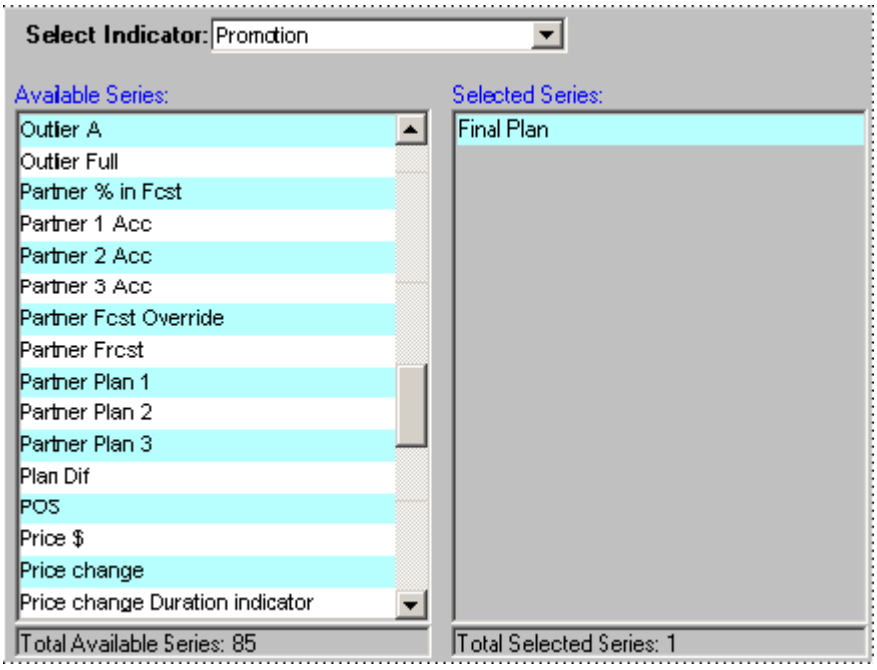
    2. Remove any unwanted series from the Selected Series list.

    3. When you are done specifying series, click Next.

        Note: By default, this configuration affects all users of this component. To hide additional series for a given user, see " Creating or Modifying a User" in this document..

6. Click Next.

    The Business Modeler displays the Select Component Indicators for Series window. Here you specify which series should have indicators to indicate associated promotions or notes.



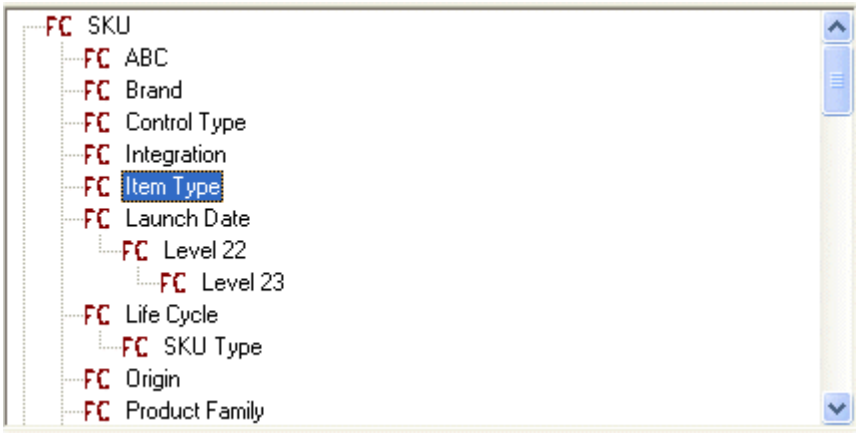
Within a worksheet, a user can attach a promotion (in the case of Promotion Effectiveness) or a note to a given item-location combination, at a given date. If a series has been configured as using an indicator for that particular promotion or note, the series will be displayed with an indicator in all worksheet cells that correspond to that item-location combination and date.

- You can associate an indicator for any general level at the lowest level (that is, any general level that do not have child levels).
- The default associations are different for different kinds of series. Sales series have notes indicators by default. Promotion series have both notes and promotion indicators by default.
- This configuration affects all users of this component. No further fine tuning is possible.

7. To associate indicators with different series, do the following for each general level:
   1. In Select Indicator, select the general level, either Note or Promotion.
   2. Move all series that should use the associated indicator into the Selected Series list, using any of the techniques in "Working with Lists".
   3. Remove any unwanted series from the Selected Series list.

8. Click Next.

   The system displays all the levels and indicates the current permission settings in this component.

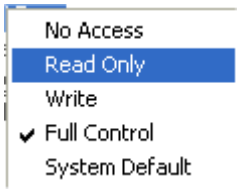


   The following icons indicate the permissions:

FC	Full control (including permission to delete members)
W	Read/write access
R	Read access
X	No access

9. For each level that you want to change, right-click the level and select the appropriate permission:

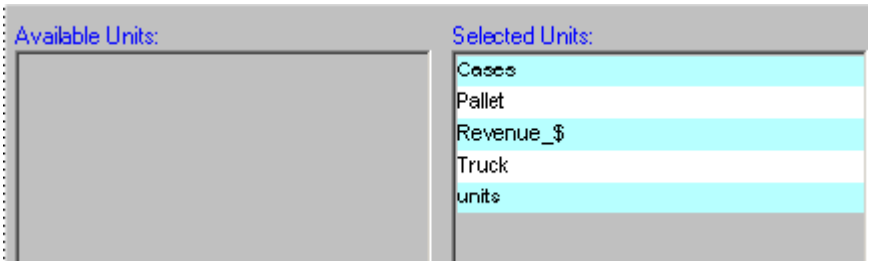
   - No Access (the user does not have access to this member; this option is equivalent to not including this member in the filter)
   - Read Only (the user can view this member but cannot make any changes)
   - Write (the user can view or edit this member)
   - Full Control (user can view, edit, create, and delete within this member)
   - System Default (use the default permission controlled by the DefaultLevelSecurityAccess parameter.



Note: By default, this configuration affects all users of this component. To fine tune permissions for a given user, see " Creating or Modifying a User" in this document..

10. Click Next.

    The system displays the Available Units and Selected Units lists.



11. Select the units of measure that should be available in the component.

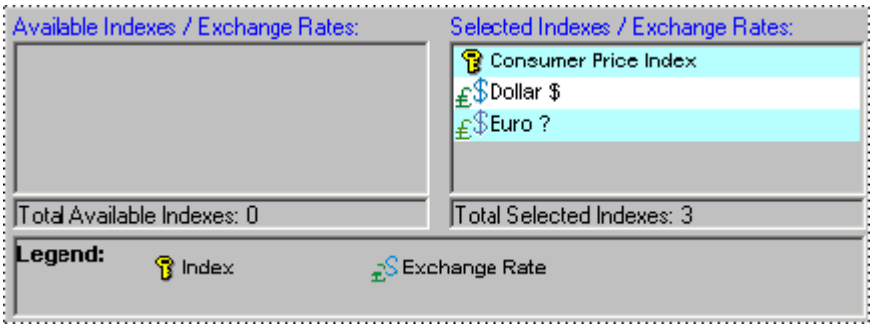
    1. Move all units that you want into the Selected Units list, using any of the techniques in "Working with Lists".

    2. Remove any unwanted units from the Selected Units list.

       Note: This configuration affects all users of this component. No further fine tuning is possible.

12. Click Next.

    - The system displays the Available Indexes and Exchange Rates and Selected Indexes and Exchange Rates lists.



13. Select the indexes and exchange rates that should be available in the component.

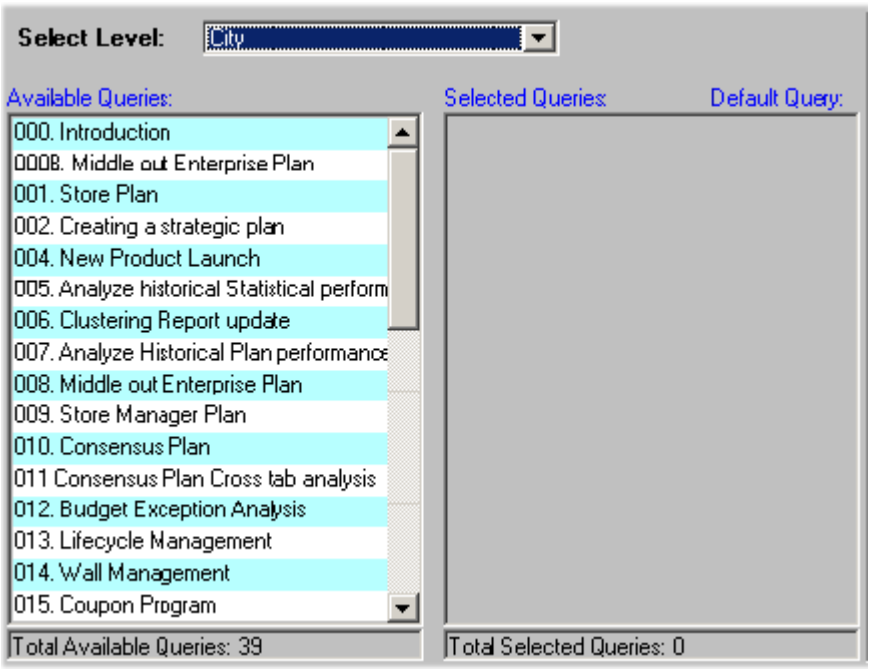
    1. Move all indexes and exchange rates that you want into the Selected Indexes and Exchange Rates list, using any of the techniques in "Working with Lists".

    2. Remove any unwanted indexes and exchange rates from the Selected Indexes and Exchange Rates list.

    Note: This configuration affects all users of this component. No further fine tuning is possible.

14. Click Next.

    The next dialog box allows you to associate public worksheets with levels.



This association is used in two ways:

- Within the Members Browser, a user can use the right-click menu to open any of these associated worksheets directly from a member of the level (via the Open With menu option). In this case, Demantra opens the associated worksheet. The worksheet is filtered to show only data relevant to the member.

- A worksheet can include an embedded worksheet that shows details for the member that is currently selected in the worksheet. Specifically, within the worksheet designer, users can add a subtab to a worksheet. The subtab consists of any of the worksheets that are associated with a level included in the main worksheet. The embedded worksheet is filtered to show only data relevant to the member.

  Note: This configuration affects all users of this component. No further fine tuning is possible.

15. At this point, do one of the following:

    - To continue without associating any worksheets and levels, click Next.

    - To associate a worksheet with a level, do the following:

      1. Click the level in the Select Level dropdown menu.

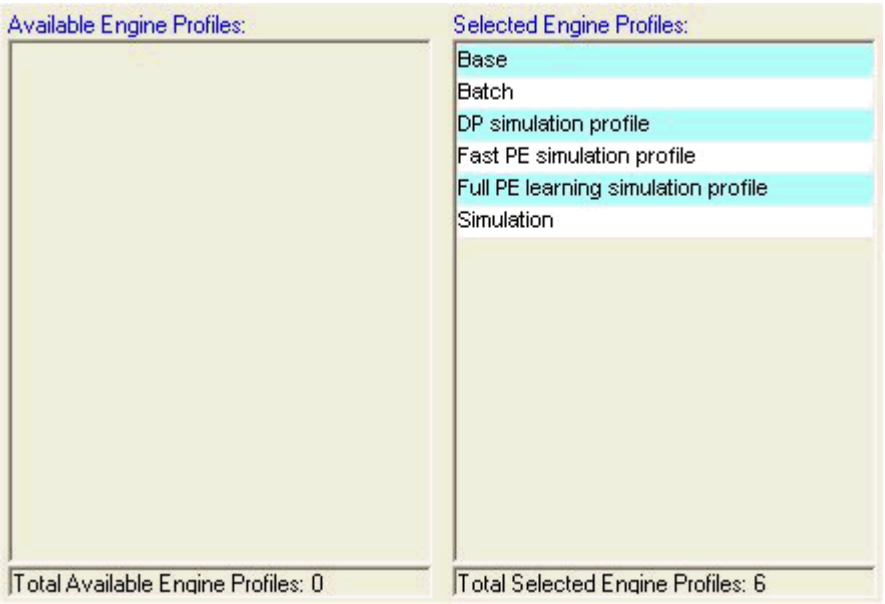
      2. Double-click the worksheet in Available Queries list, which moves it to the Selected Queries list.

      3. Move other worksheets from the Available Queries list to the Selected Queries list, as needed.

      4. Decide which worksheet in the Selected Queries list should be the default worksheet for this level. For that worksheet, click the Default check box. When the user right-clicks and selects Open, this is the worksheet that will be used.

      5. When you are done on this screen, click Next.

      If you are using the PE Analytical Engine, the system displays engine profiles that could potentially be used within this component. The Business Modeler displays the Available Engine Profiles and Selected Engine Profiles lists.



16. Select the engine profiles that should be available in the component. Profiles can be used only with the Promotion Effectiveness engine.

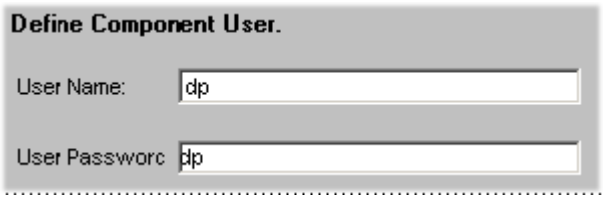
    1. Move all profiles that you want into the Selected Engine Profiles list, using any of the techniques in "Working with Lists".

    2. Remove any unwanted profiles from the Selected Engine Profiles list.

    1. When you are done specifying profiles, click Next.

       Note: This configuration affects all users of this component. No further fine tuning is possible.

In the next step, you specify the user name and password of the user who owns the component. This user will be able to log into the Business Modeler and create additional users for this component.



17. To specify the owner of the component:

    - In the User Name box, type the user name.

- In the User Password box, type the user password.

18. To exit and save the configuration, click OK.

19. Modify the newly created user so that it has access to the appropriate Demantra modules. To do so, use the Security menu; see "Creating or Modifying a User" in this document.

Deleting a Component

To delete a component:

1. Click Components > Create/Open Component. Or click the Create/Open Component button.

   Note: This option may not be available, depending on the user name with which you logged onto Business Modeler.

   The Create/Open Component dialog box appears.

2. Click the icon corresponding to the component.

3. Click Delete.

4. Click Yes to confirm the deletion.

Configuring the Security Provider

Integration with JAAS

OracleAS Web Services provides an implementation of Java Authentication and Authorization Service (JAAS) for J2EE applications that is fully integrated with J2EE declarative security. This allows Demantra to take advantage of the JAAS constructs such as principal-based security and pluggable login modules. OracleAS Web Services Security provides out-of-the-box JASS authentication login modules that allow J2EE applications running on OracleAS Web Services to leverage the central security services of Oracle Identity Management.

The JAAS Provider ensures secure access to and execution of Java applications, and integration of Java-based applications with Oracle Application Server Single Sign-On.

Demantra has implemented a custom login module that is deployed in the OracleAS.

Configuring the Security Provider of the Application Server

Demantra has implemented a custom login module that is deployed in the OracleAS. The following procedure configures the application server to use this login module:

1. Connect to Oracle Enterprise Manager.
2. Deploy Demantra
3. Define Security Provider as follows:
   - Select – 'Administration' -> 'Security Providers' (by Go to Task) -> 'demantra' application -> edit (demantra) -> 'Change Security Provider'.
   - In the Drop Down of 'Security Provider Type', select 'Custom Security Provider'.
   - In the 'JAAS Login Module Class' field, set 'com.demantra.common.authentication.DemantraLoginModule'.
   - Click OK.

     Note: This step can be done only through a deployment of the Demantra application
4. Return to the Home Page and select 'Web Service'.
   - If no web services are found, open the link of the WF Web Service: http://(ROOT)/demantra/MSC_WS_DEMANTRA_WORKFLOWSoapHttpPort
   - Then refresh the Enterprise Manager page.
   - Click on the link: MSC_WS_DEMANTRA_WORKFLOWSoapHttpPort.
   - Select 'Administration' -> 'Enable/Disable Features'
   - Move 'Security' to the 'Enabled Features' box and then click OK.
   - Make sure that the 'Security' Feature is marked as Enabled.
5. On the same page, select the 'Edit Configuration' icon of the 'Security' Feature, Press the 'Inbound Policies' button, and in the 'Authentication' tab, mark the checkbox 'Use Username/Password Authentication' and select 'Password Type' = 'Plain Text'. Click OK.
6. Test the Workflow Web Service by providing User Name & Password in the WS-Security section.

Details of the Demantra custom login module

Location: **package** com.demantra.common.authentication;

DemantraLoginModule.java

Methods

- public void initialize(Subject subject, CallbackHandler callbackHandler, Map sharedState, Map options)

  Initialize this LoginModule.

  Parameters:

  subject the Subject to be authenticated.

  callbackHandler a CallbackHandler for communicating with the end

  user (prompting for usernames and passwords, for example).

  sharedState shared LoginModule state.

  options options specified in the login Configuration for this particular LoginModule.

- public boolean login() throws LoginException

  Authenticate the user by prompting for a username and password.

  Returns: true if the authentication succeeded, or false if this LoginModule should be ignored. **Throws**:

  FailedLoginException if the authentication fails.

  LoginException if this LoginModule is unable to perform the authentication.

- public boolean commit() throws LoginException

  This method is called if the LoginContext's overall authentication succeeded (the relevant REQUIRED, REQUISITE, SUFFICIENT and OPTIONAL LoginModules succeeded).

  If this LoginModule's own authentication attempt succeeded (checked by retrieving the private state saved by the login method), then this method associates a Principal with the Subject located in the LoginModule. If this LoginModule's own authentication attempted failed, then this method removes any state that was originally saved.

  Returns: true if this LoginModule's own login and commit attempts succeeded, or false otherwise.

  Throws: LoginException if the commit fails.

- public boolean abort() throws LoginException

This method is called if the LoginContext's overall authentication failed. (the relevant REQUIRED, REQUISITE, SUFFICIENT and OPTIONAL LoginModules did not succeed).

If this LoginModule's own authentication attempt succeeded (checked by retrieving the private state saved by the login and commit methods), then this method cleans up any state that was originally saved.

Returns: false if this LoginModule's own login and/or commit attempts failed, and true otherwise.

Throws: LoginException if the abort fails.

- public boolean logout() throws LoginException

  Logout the user.

  This method removes the Principal that was added by the commit method.

  Returns: true in all cases since this LoginModule should not be ignored.

  Throws: LoginException if the logout fails.

Running SYS_GRANTS.SQL Script

You need to run this script manually after installing or upgrading Demantra only if you did not specify a database user with full SYSDBA privileges when running the Installer. In this scenario, the Installer displays a message at the end of the installation/upgrade prompting you to run this script.

SYS_GRANTS.sql performs the following:

- Adds 'EXECUTE' privileges to access DBMS_CRYPTO (UPGRADE_PASSWORDS): Provides the highest level of user password encryption.
- Adds 'EXECUTE' privileges to access DBMS_LOCK: Provides as SLEEP operation for improved concurrency.
- Adds 'EXECUTE' privileges to access V_$PARAMETER so that Oracle Demantra can better adapt to your database's configuration.
- (10g only) Adds 'GRANT' privileges to access the package UTL_HTTP, which enables Oracle Demantra to send notification messages to the application server and engine.
- (11g only) Adds an ACL to enable HTTP communications for Oracle Demantra to send notification messages to the application server and engine.

Syntax:

```
C:\DEMANTRA_INSTALL_DIRECTORY\Demand Planner\Database
Objects\Oracle Server\admin> sqlplus SYS@SERVER as sysdba
```

```
@sys_grants.sql DB_USER ACL_for_WebServerURL
ACL_for_EngineServerURL
```

Where:

- DEMANTRA_INSTALL_DIRECTORY is the location of the unzipped Demantra installation file
- SYS is the DB user with SYSDBA privileges · SERVER is the DB server TNS name
- DB_USER is the Demantra database user name (must be entered in upper case)
- ACL_for_WebServerURL is the full path to the access control list (ACL) for the Web Server URL. If you pass the name ACL_DEFAULT it will use the ACL named /sys/acls/demantra.xml. The ACL will be created if it does not exist.
- ACL_for_EngineServerURL is the full path to the access control list for the Engine Server URL. If you pass the name ACL_DEFAULT it will use the ACL named /sys/acls/demantra.xml. The ACL will be created if it does not exist.

Configuring Web Applications for SSL and Firewalls

To use SSL security or if users need to work through a firewall, perform the following procedure:

1. When you install Oracle Demantra, be sure to configure all URLs with https instead of http.
2. Switch off the HTTP server on port 80. The procedure to perform this is dependent on the Web server.
3. Configure the Web server for SSL support. You will need to obtain a VeriSign certificate or equivalent certificate authority.
4. Configure the firewalls to allow connections to port 443.
5. Optional: Configure the firewall to disallow all communication to port 80 instead of disabling it on the Web server.
6. If you have a firewall between the Web Platform Server and the database, you will also need to open the port that is defined for the connection between the Application Server and the database. For Oracle, this port is 1521 by default.
7. If you change any of the default port numbers, make sure to also change them in the Oracle Demantra URLs, the Web server, and the firewall. See Other Configuration Files in this document.
8. If you want to enable mutual (client) SSL Authentication, set the

client.ssl.authentication parameter in to "1" (true). You define this parameter in Business Modeler > Parameters > System Parameters > Application Server > DP Web. By default, this parameter is false, which means only standard (server) SSL authentication is supported.

After client SSL authentication is enabled, a pop-up dialog box appears prompting you to insert keystore, truststore locations and passwords. Once validated, Demantra will save these parameters in an encrypted file under the user.home/demantra directory for future logins.

> **Note:** Demantra supports both standard and mutual (client) SSL Authentication. In IE 7.x, the Java plugin cannot obtain user credentials from the browser and users will be prompted to enter this information for every applet within the current Demantra page (in Collaborator Workbench, there may be between 2-4 applets).
>
> To avoid this issue, it is recommended that the web server administrator exclude the Demantra .jar files from the Web Server Basic Authentication rules. To do this, add the following filter to the <files> directive in httpd-sll.conf:
>
> ```
> <Files ~ "^(\.jar"> </Files>
> ```

3

Configuring Security Post-installation

Important: The Demantra Local Application replaces Collaborator Workbench. You may see both names in this text.

This chapter covers the following topics:

- Overview
- Logging onto the Collaborator Workbench Administrator
- Providing Access to the Workflow Editor
- Dropdown Security
- Controlling Access to Series
- Feature Security
- Program Groups
- Defining a Program Group
- Redefining a Program Group
- Deleting a Program Group
- Configuration Notes
- Specifying Permissions for Menu Items

Overview

For an overview of post-installation security configuration, see the following "Security" section.

For an overview of post-installation security configuration of the user interface, see the section "How the User Interfaces Can Be Configured."

For additional information regarding user login access, see the sections "Other Security Features" and "Logging onto the Collaborator Workbench Administrator."

Security

The Demantra data and menus are secured, so that not all users have access to the same data and options. The security model includes the following features:

- The Oracle *license* controls which menus are secured, so that not all users have access to the same data and options. The security model includes the following features:

- The data is partitioned into components, which generally correspond to organizational roles. In the definition of a component, you can control the following:

  - The levels that can be seen

  - The degree of access for members of each level: no access, read-only access, read/write access, or full control (including the ability to delete members)

  - The series that can be seen

  Each component has an owner, who acts as the administrator and who can create additional users:

- Within a component, you can restrict each user to a subset of the data associated with that component. You can control the same data elements as previously described.

- You can control access to menu items at the component level, the group level, or the user level. This includes both the menu bar and the right-click menu.

- You can define program groups, or sets of menu items, and apply security at that level, for greater convenience.

For details, see "Security".

How the User Interfaces Can Be Configured

Whether you start from a Demantra application as-is or from the Application Platform, you can configure the user interfaces in the following complementary ways:

- You typically create worksheets to meet the needs of specific users. A worksheet is a working environment that shows specific data, aggregated and filtered as needed. Users can view, sort, edit, print, and so on. The next chapter, "Core Concepts", describes the elements of worksheets.

- You can create methods that the users can execute from within worksheets. The methods appear in the worksheets as options on the right-click menu. Demantra also provides default methods that you can redefine or disable. These allow users to

create, edit, and delete level members.

- You create components that subdivide the data as needed for different organizational roles. Each component has an owner, who acts as the administrator of the component. In turn, the owner can log onto the Business Modeler and further restrict data access for particular users.

- You apply security so that different users have access to different menu options. See "Managing Security".

- You can configure the default layout of Collaborator Workbench, access to different elements of Collaborator Workbench, and the links and menus in Collaborator Workbench. You can also substitute custom graphics throughout the Web products. See "Customizing Demantra Web Pages" in this document..

Other Security Features

Note the following additional security features:

- To access the Workflow Manager, a User Group must be assigned to the workflow.group parameter (in the Business Modeler). For details, refer to Providing Access to the Workflow Editor.

- After adding a user to a Collaboration Group, the Web server must be restarted before that user can access the Workflow Manager. For more information about User Groups see: **Creating or Modifying a User Group**.

- A user with the System Manager permission level can see all public worksheets and all private worksheets. Users with lower permission levels can see all public worksheets and all private worksheets created by themselves.

- A user with the System Manager permission level can see the System menu in the desktop Demand Planner, in addition to the other menus.

- Any user can log onto the Business Modeler. If the user's permission level is lower than System Manager, the user can only change his or her own password, as documented in the user guides.

Logging onto the Collaborator Workbench Administrator

You use the Collaborator Workbench Administrator to control access to menu items.

To log onto the Collaborator Workbench Administrator:

1. Open the administration login page:

   http://server name/virtual directory/portal/adminLogin.jsp

For example:

http://frodo/demantra/portal/adminLogin.jsp

2. Enter the user name and password and click Log on.

   Demantra displays the Administration page, which includes the following choices:

   See also

   "Customizing Demantra Web Pages"

Providing Access to the Workflow Editor

> **Caution:** Access to the Workflow Manager, including the ability to add and edit a workflow, should only be provided to key users. Workflows are used to drive many administrative flows and critical behind-the-scene processes, including data loading, purging, and execution of the analytical engine.

For a given user to log into the Workflow Editor, that user must be configured a specific way.

To provide access to the Workflow Editor:

1. Log on to the Business Modeler as described in "Logging onto the Business Modeler."

2. Create a group that includes all users who need to log into the Workflow Editor. See "Creating or Modifying a User Group".

3. Using a database tool, query the user_security_group table (i.e. select * from user_security_group). The results will list the group_name and corresponding application_id for each group. For example, for the workflow group_name 'Collaborator', the application_id is 'USER_GROUP:5'.

4. Obtain the application_id of the newly-created group.

5. Set the workflow.group parameter in the APS_PARAMS table using the Business Modeler. Go to Parameters > System Parameters > Application Server > Workflow (tab). Add the application ID from the query above to the existing values for this parameter (separate values with a comma), save the changes, and then restart the application server.

   See also

   "Managing Workflows" in the *Oracle Demantra Implementation Guide*

Dropdown Security

The fields "Security" and "Minimum Privilege Displayed" are enabled when Lookup Type is set to Level, or when Lookup Type is set to Table and the specified Table Name is a level table. Examples of level tables include Location, Items, Promotion, and Settlement. These control which level members a worksheet will be able to access.

If the lookup type is set as 'Table' but the table name is a level table, as listed in GTABLE column of GROUP_TABLES, security will be applied as though the lookup was on a Level.

Security

This dropdown has the following four options:

None (default)	Dropdown security is turned off.
Direct	Security will be respected on the level being looked up and its direct parent level. If security has been defined explicitly on the level (for example, Site) a user will see those Sites to which they have access. If security has been defined on the immediate parent (for example, Account), the user will see only those Sites they have access to, as inherited through Account restrictions.

Uni-Dimensional	Security will be respected within the complete dimensional hierarchy of the level being looked up—both the direct parent hierarchy and indirect sibling hierarchies within the single dimension (item, location or GL). For example, if security has been defined on the 'Customer' level and a Lookup is created on the 'Site' level, a user would be restricted to seeing only those Sites for which they have access, as inferred from 'Customer' security.
Cross-dimensional	Security will be inherited across hierarchies via matrix relationships. For example, if security has been defined on the 'Region' level and a dropdown is created to lookup on 'Item' level in the Item hierarchy, the user will be restricted to only those products selling into the Regions they have access to, as determined through mdp_matrix.

Minimum Privilege Displayed

When security is enabled (all but 'None' option), only those level members for which the user has Full Control or Read & Write access will be visible in the dropdown by default. If a user has no visibility or read-only visibility to a member, they will not be able to select that member as part of their planning process, particularly for hierarchical objects such as Accounts or Product Category.

However, in some instances a member may be secured as Read Only but accessible. For example, Promotion Type. The user will be unable to change the value, but should be able to select it when planning a promotion.

This access is controlled by the Minimum Privilege Displayed parameter, which has the following three options:

Read Only	User can view all members of this level but cannot select or modify them.
Read & Write (default)	User can view, select, and edit members of this level but cannot delete members.
Full Control	User can view, select, edit, and delete members of this level.

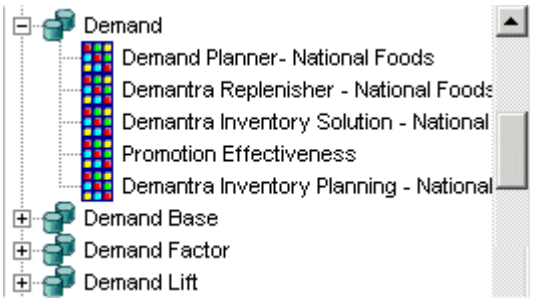
Controlling Access to Series

When you create a series in the Business Modeler, Demantra automatically adds that series to your component. You can give access to this series to other users of your component.

To control access to a series:

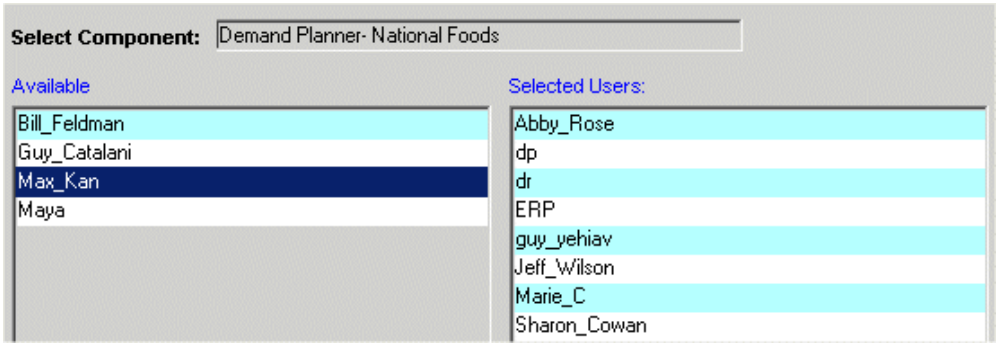
1. Click Configuration > Configure Series or click the Configure Series button.

2. To see which components include a specific series, click the plus sign (+) to the left of the series name. The display expands to list all the components that include this series:



3. To make changes, right-click the series and then select Open > Expression Properties.

4. Click Next to access the Security page.



5. If you logged into Business Modeler with one of the internal Demantra passwords, you can select any component. Otherwise, you can make changes only within the component with which your ID is associated.

6. For each user of this component who needs access to this series, double-click the user name to move the user name from the Available list to the Selected Users list.

Feature Security

Demantra features are secured as follows:

- Permission levels control access to administrative tools and to menu items. Demantra provides four predefined permission levels that you can customize. You can control access to all of the Demantra menus:
  - Menus on the Collaborator Workbench menu bar
  - Menus on the DSM menu bar
  - Menus on the Promotion Effectiveness menu bar
  - Menus on the Demand Management menu bar
  - Right-click menus associated with each level in your system
- You can also control access to all the same menu items at the group and user ID level.

For convenience, you control access to individual menu items, to predefined collections of menu items, or to your own collections of menu items (your own program groups).

Permission Levels

Demantra defines four permission levels, as follows:

- System Manager
- Supervisor
- Power user
- Casual user

> **Note:** Each Demantra software component (such as Demand Management or Sales & Operations Planning) has a component manager who has the highest permission level, and can assign all levels of permissions including system managers.

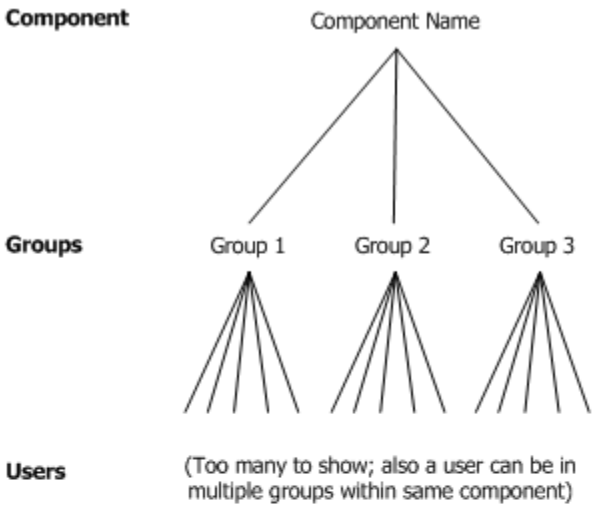
The table below shows the default rights for these four permission levels. Note that only the System Manager has a different set of permissions from the other three. However, users with the System Manager permission level can utilize the Collaborator Workbench Administration tool to modify the access restrictions for specific menu items, or sets of menu items, thereby changing these defaults. See the section **Specifying Permissions for Menu Items**.

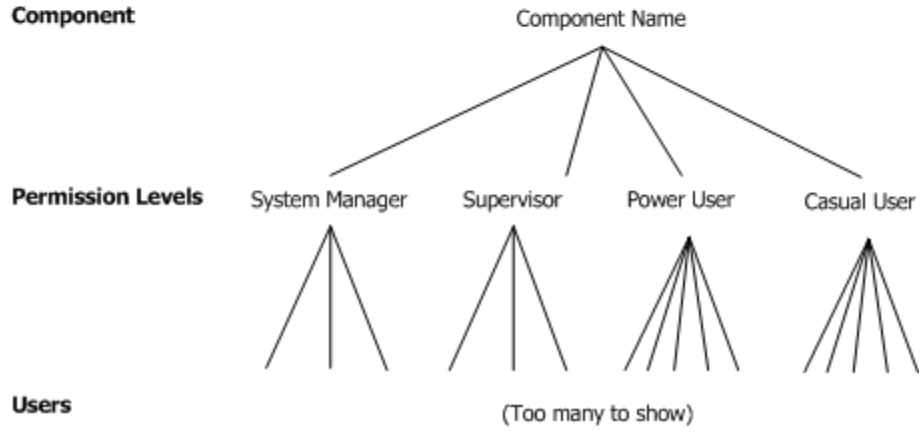
Permission Level	Business Modeler – login / change pwd	Business Modeler – All Menus	Collaborator Workbench Administration tool	Collaborator Workbench - view public and own worksheets	Collaborator Workbench - view all worksheets	Demand Planner - System menu
System Manager	X	X	X	X	X	X
Supervisor	X	-	-	X	-	-
Power User	X	-	-	X	-	-
Casual Supervisor	X	-	-	X	-	-

Permission Hierarchies

In order to understand how Demantra determines a given user's access to a given menu item, it is necessary to understand the permission hierarchies and how Demantra combines them.

Demantra has two independent permission hierarchies. In the first hierarchy, each component includes groups, and each group includes users. A user can belong to multiple groups, provided that all those groups belong to the same component. In the second hierarchy, each component includes four permission levels, and each user has one permission level.



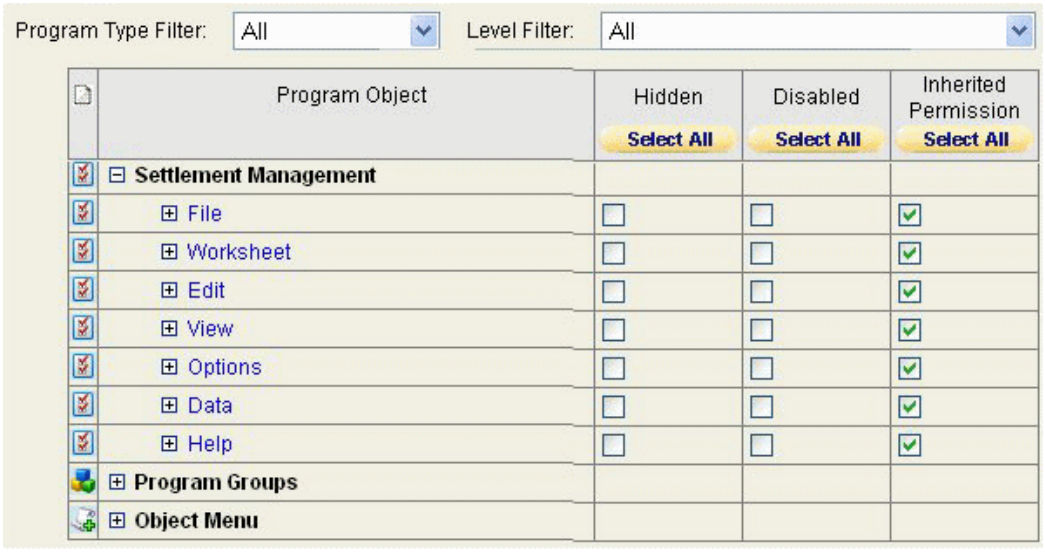


Explicit and Implicit Permissions

In Collaborator Workbench you can display or hide any menu item. You can also display but disable a menu item, which can provide a useful clue about advanced features that are available to other users. Each permission is either explicit or implicit (inherited).

> **Note:** For more information see:**Logging into the Collaborator Workbench Administrator**..

You define permissions in an expandable hierarchy like the following. For now, let's focus on the three check boxes:



The following table describes how to use these check boxes:

Desired outcome	Hidden	Disabled	Inherited Permission
Menu option is explicitly hidden	Checked	Irrelevant	Unchecked
Menu option is explicitly displayed but disabled	Unchecked	Checked	Unchecked
Menu option is explicitly displayed and enabled	Unchecked	Unchecked	Unchecked
Use implicit permissions for this menu item	Unchecked	Unchecked	Checked

How Demantra Combines Multiple Permissions

For a given user and a given menu item, Demantra checks for all the following permission descriptions:

- For the component
- For each group to which the user belongs
- For the permission level that the user has

- For the user ID
- For each program group to which the menu item belongs

To determine whether a user has access to a given menu item, Demantra searches for and combines the permission descriptions as follows.

1. Demantra checks to see if the user has an explicit permission setting (for a given menu item). If so, that setting is used, and all others are disregarded.
2. If the user does not have an explicit permission setting for a given menu item, then Demantra looks at the settings for the groups to which the user belongs, the permission level that the user has, and each program group that the menu item is in. Here, the following rules apply:
   - An explicit permission takes precedence over an implicit permission.
   - Among explicit permissions, the most liberal permission takes precedence.
   - Among implicit permissions, the most liberal permission takes precedence.
3. If no explicit permission setting for the menu item has been found so far, then Demantra uses the permission setting at the component level, if any.
4. If there is no setting at the component level, Demantra displays and enables the menu item.

See Also

"Data Security"

"Specifying Permissions for Menu Items"

Program Groups

For more information about Program Groups see:

Defining a Program Group

Redefining a Program Group

Deleting a Program Group

A program group is a collection of menu items, typically related to each other in some way. You create program groups so that you can easily control access to all the menu items in the group.

Demantra provides several predefined program groups, for convenience. These program groups contain only menu items from the right-click menus.

Program group	Menu items in this group, by default
Add	New *member* right-click menu option for every level in the system.
Edit	Edit *member* right-click menu option for every level in the system.
Delete	Delete *member* right-click menu option for every level in the system.
View	View *member* right-click menu option for every level in the system.
Copy	Copy, Paste, and Paste from Clipboard right-click menu options for every applicable level in the system. (Note that this option is available only for promotional-type levels.)
Open	Open and Open With right-click menu options for every level in the system.

Defining a Program Group

A program group is a collection of menu items, typically related to each other in some way. You create program groups so that you can easily control access to all the menu items in the group; see "Specifying Permissions for Menu Items".

Demantra provides several predefined program groups, for convenience. These program groups contain only menu items from the right-click menus.

Program group	Menu items in this group, by default
Add	New *member* right-click menu option for every level in the system.
Edit	Edit *member* Unmapped Conditional Text: HelpOnly right-click menu option for every level in the system.

Program group	Menu items in this group, by default
Delete	Delete *member* right-click menu option for every level in the system.
View	View *member* right-click menu option for every level in the system.
Copy	Copy, Paste, and Paste from Clipboard right-click menu options for every applicable level in the system. (Note that this option is available only for promotional-type levels.)
Open	Open and Open With right-click menu options for every level in the system.

To define a program group:

1. Log into the Collaborator Workbench Administrator. See "Logging onto the Collaborator Workbench Administrator".

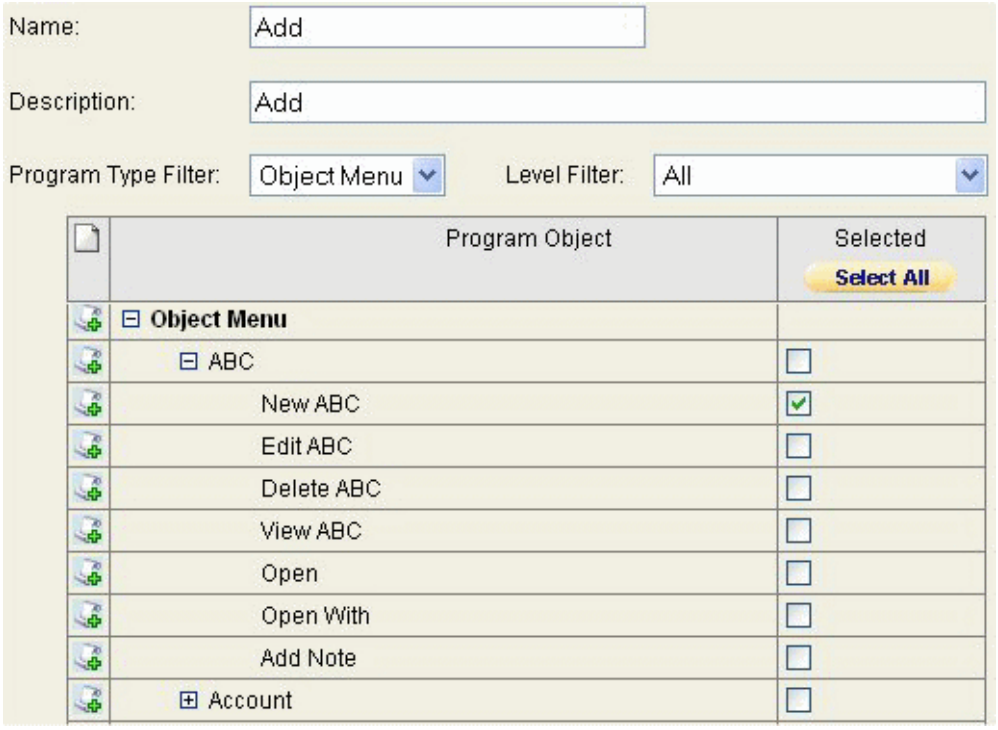
   The Administration page appears.

2. Click Define Program Groups.

   The system displays a page that lists the existing program groups.

3. Click the Add Program Group button.

   Demantra displays a page where you can define a new program group:



4. For Name and Description, specify a name and optional description for this program group.

5. Optionally select an item from the Program Type Filter selection list, to reduce the number of menus and menus items shown on this screen.

   - To display only options on the right-click menus, click Object Menu.
   - To display only options on the menu bars, click Menu.

6. Optionally select a level from the Level Filter selection list, to reduce the number of menus and menus items shown on this screen. (This filtering is available only if you are viewing right-click menus.)

7. In the table, expand the menus as needed.

8. In the Selected column, select the check box for each menu item to include within this program group.

9. Click OK.

   You are now ready to define permissions for this program group; see "Specifying

Permissions for Menu Items".

See also

"Deleting a Program Group"

Redefining a Program Group

To redefine a program group:

1. Log into the Collaborator Workbench Administrator. See "Logging onto the Collaborator Workbench Administrator".

   The Administration page appears.

2. Click Define Program Groups.

   The system displays a page that lists the existing program groups.

3. In the row corresponding to the group you want to redefine, click the Edit Program Group button.

   Demantra displays a page where you can edit this program group.

4. Optionally edit the Name and Description.

5. Optionally select an item from the Program Type Filter selection list, to reduce the number of menus and menus items shown on this screen.

   - To display only options on the right-click menus, click Object Menu.
   - To display only options on the menu bars, click Menu.

6. Optionally select a level from the Level Filter selection list, to reduce the number of menus and menus items shown on this screen. (This filtering is available only if you are viewing right-click menus.)

7. In the table, expand the menus as needed.

8. In the Selected column, select the check box for each menu item to include within this program group.

9. Click OK.

   See also

   "Deleting a Program Group"

Deleting a Program Group

To delete a program group:

1. Log into the Collaborator Workbench Administrator. See "Logging onto the Collaborator Workbench Administrator."

   The Administration page appears.

2. Click Define Program Groups.

   The system displays a page that lists the existing program groups.

3. In the row corresponding to the group you want to delete, click the Delete Program Group button. No confirmation message is displayed; the group is deleted immediately.

   See also

   "Defining a Program Group"

Configuration Notes

The following table summarizes the Demantra security tools.

Tool	Purpose/Notes
Components > Open/Create Component option*	Creates components, which are usually created as part of basic implementation.
Security > Create/Modify User option*	Creates users and configures all information except for access to menu items.
Security > Create/Modify Group option*	Creates user groups and configures all information except for access to menu items.
Collaborator Workbench Administrator	Controls access to menu items; defines program groups.

*These options are in the Business Modeler.

Specifying Permissions for Menu Items

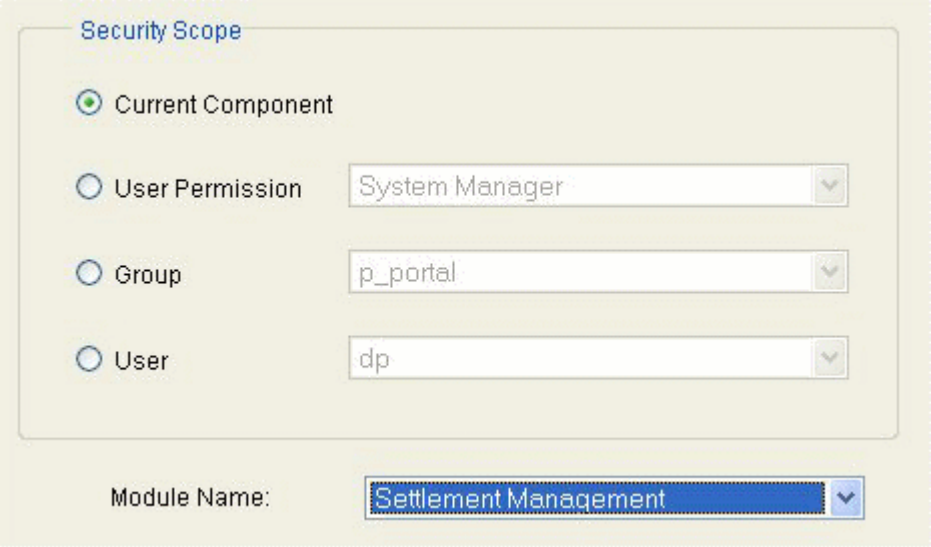
To specify permissions for menu items:

1. Log into the Collaborator Workbench Administrator. See "Logging onto the Collaborator Workbench Administrator".

   The Administration page appears.

2. Click Define Program Permissions.

   The system displays a page where you specify the category upon which to apply the menu availability.



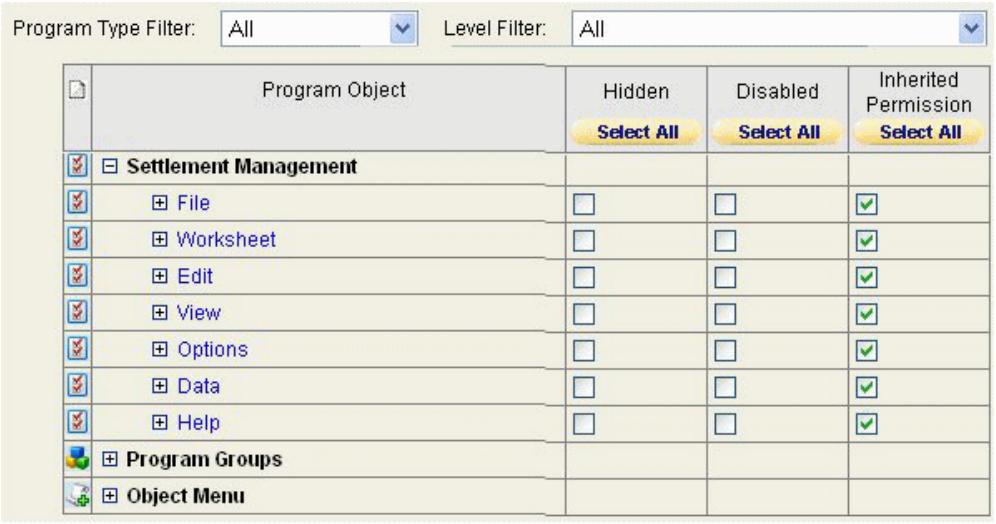
3. To define the scope, check one of the following radio buttons and select an item from the associated drop down list:

Current Component	Use this option to enable or disable menu items for all users of the component that you own.
User Permission	Use this option to enable or disable menu items for a specific permission level. See " Permission Levels".
Group	Use this option to enable or disable menu items for a specific user.

User	Use this option to enable or disable menu items for a specific user group.
Module Name	Use this option to specify if the changes you make should apply to all modules or to specific modules.

4. Click Next.

   Demantra displays an expandable hierarchy that shows all the menu items you chose, like the following example:



   Initially, the Inherited Permission check boxes are all checked, which means that the permissions that will be used are inherited from higher in the security hierarchies. Likewise, the Hidden and Disabled check boxes display the current inherited settings.

5. Optionally select an item from the Program Type Filter selection list, to reduce the number of menus and menus items shown on this screen.

   - To display only options on the right-click menus, click Object Menu.
   - To display only options on the menu bars, click Menu.

6. Optionally select a level from the Level Filter selection list, to reduce the number of menus and menus items shown on this screen. (This filtering is available only if you are viewing right-click menus.)

7. In the table, expand the menus as needed.

8. For each item in this table, specify permissions as follows:

Desired outcome	Hidden	Disabled	Inherited Permission
Menu option is explicitly hidden	Checked	Irrelevant	Unchecked
Menu option is explicitly displayed but disabled	Unchecked	Checked	Unchecked
Menu option is explicitly displayed and enabled	Unchecked	Unchecked	Unchecked
Use implicit permissions for this menu item	Unchecked	Unchecked	Checked

Note: To understand how multiple permissions are combined, see "How Demantra Combines Multiple Permissions".

9. Click Finish. The settings are saved.

See also

"Configuring Menus in Collaborator Workbench"

4

Other Security Features

Important: The Demantra Local Application replaces Collaborator Workbench. You may see both names in this text.

This chapter covers the following topics:

- The SysAdmin User
- Creating or Modifying a User
- Copying a User
- Deleting a User
- Creating or Modifying a User Group
- Deleting a Group
- Logging Out Users
- Changing Your Password
- Password Policy
- Mutual Authentication
- Logging Messages of the Application Server
- Viewing the Workflow Process Log
- Specifying Content Pane Security
- Checking the Log Files and Tables

The SysAdmin User

The SysAdmin user is a predefined, highly secure user account that can be used to define new or additional Demantra components (similar to the seeded components, which include DM, AFDM, S&OP, and PTP). Demantra users only need this account when defining new Demantra components or need to change lost component

passwords.

The Permission Level for the SysAdmin user is 'System Manager'. This is the same permission level for all Demantra component owners, including dm, sop, and ptp.

> **Caution:** The password for the SysAdmin user account should only be assigned to trusted administrators within the organization.

By default, the SysAdmin user only has access to the following modules:

- Demantra Administrative Tools
- Security Management

Oracle does not recommend adding any other modules as this user is meant to only for a specific administrative role. For more information about these modules, refer to "Creating or Modifying a User" in the Oracle Demantra Implementation Guide.

A password for this user must be entered when installing or upgrading to the Demantra version in which this user was added. Please make sure administrator installing Demantra notes the SysAdmin password as it is impossible to reset without help from Oracle support.

Only the SysAdmin user can modify the SysAdmin account. To do this, log into the Business Modeler as SysAdmin and follow the instructions in "Creating or Modifying a User" in the Oracle Demantra Implementation Guide. Alternatively, log into the Business Modeler as the SysAdmin user, choose Components > Create/Open component, select a component, and navigate to the User Name screen.

When the SysAdmin user's password expires, the user is prompted to change it.

Creating or Modifying a User

You can create additional users to work within the component you own.

> **Warning:** When passing sensitive information (uid/password) to new users, be sure to use a secure mechanism (not just email).

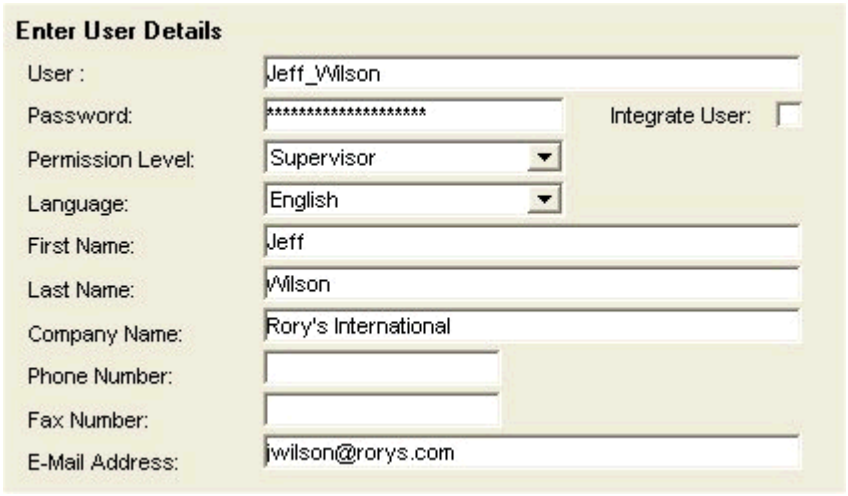
To create or modify a user:

1. Log on to the Business Modeler as described in "Logging onto the Business Modeler ".
2. Click Security > Create/Modify User. Or click the Create/Modify User button.

   The Create/Modify User dialog box appears.
3. Next:

- To create a new user, click the New User button, and then click OK.
- To modify a user, click the button of that user then click OK. Or double-click the icon of the user whose details you want to modify.

The User Details dialog box appears.



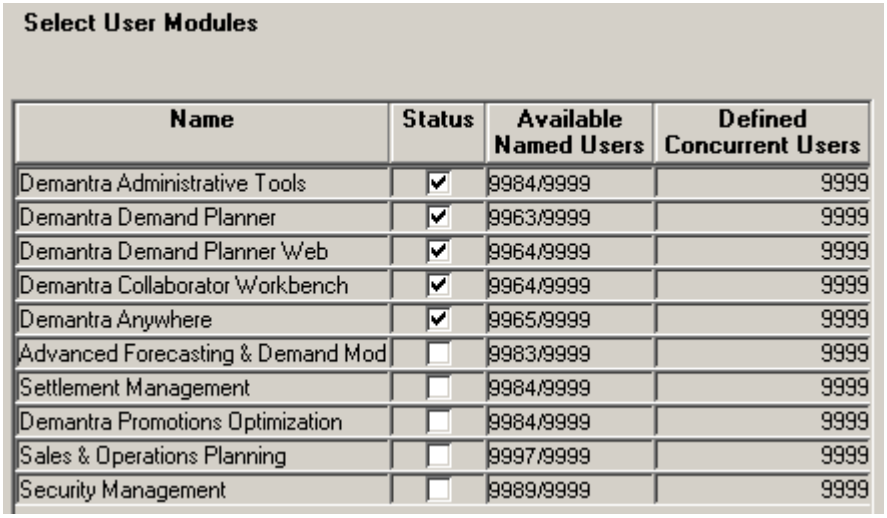
4. Specify basic user details as follows:
   - Under Enter User Details, type the following information in the appropriate boxes (or select from the drop down lists):
   - The user name, password, permission level, and the language in which the system will be operated. Each user name must be unique within your Demantra implementation.
   - The first and last name of the user, the company name, phone and fax number, and the email address. If you set up automated email within workflows, it is important to make sure the email address is correct here.

     Note: The Integration User check box is not currently supported.

5. For Permission Level, see "Permission Levels".

   Click Next.

   The User Modules dialog box appears. Here you specify which Demantra user interfaces this user can access.

6. 

Click the check box next to each module that the user needs. Then click Next.

If you are logged in as the component owner and the user's permission level is 'System Manager', then the following two options will be enabled for selection (otherwise, they will be disabled):

- Demantra Administrative Tools – Select this option if you want the user to be able to access the Engine Administrator, Chaining Management, and Member Management applications as well as all functions in the Business Modeler except the Security function.

- Security Management - Select this option if you want the user to be able to access the Security function within the Business Modeler. The Security function is used to create new, or modify existing, users and user groups.

  Note that only component owners can grant access to the Security Management and Administrative Tools modules and that these modules can only be granted to Users with a Permission Level of System Manager

Users with access to the 'Security Management' module will be able to:

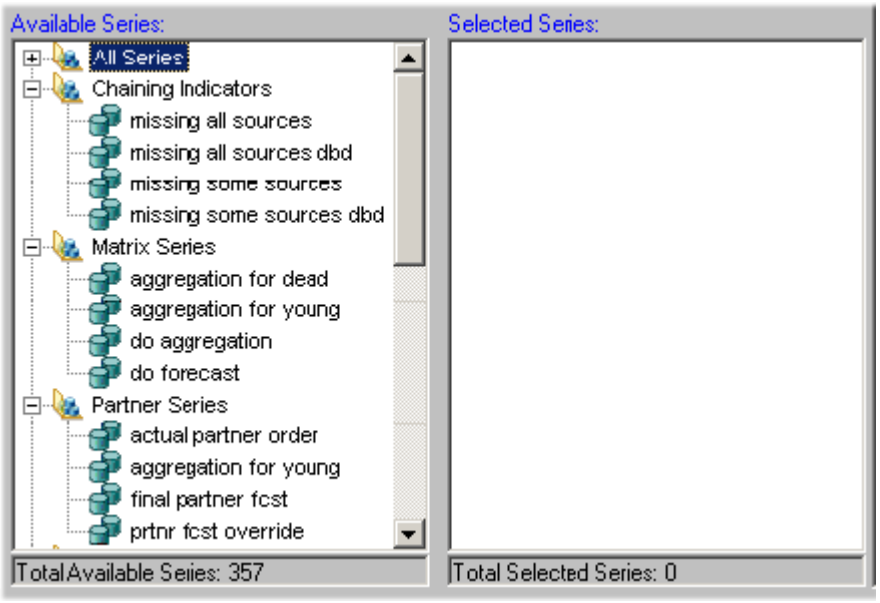
- Maintain (create, copy, modify, and delete) any users with the same or lower module access then they have themselves. For example, if User A does not have access to the Demand Management module, then that user will not be able to maintain other users that do have access to that module.

- Maintain Series, User Filters, and User Groups for the Users that they can maintain. This is true regardless of the Series, User Filters, and User Groups that they have access to. For example, even if User A does not have access to the Series "Mfg Profit," User A can still grant access to that series to other Users.

The New User - Select User Series dialog box appears. This dialog box allows you to determine what data series will be active for the new user, from the entire set of

series in this component. Each list is a collapsible list of series groups and the series in them.

If a User does not have access to either the Demantra Administrative Tools module or the Security Management module, then they can login to Business Modeler, but can only change their password.



If a series is not active for a user, it is not available when the user creates worksheets and is not viewable in existing worksheets to which the user has access.

7. Specify the series that a user can see, as follows:

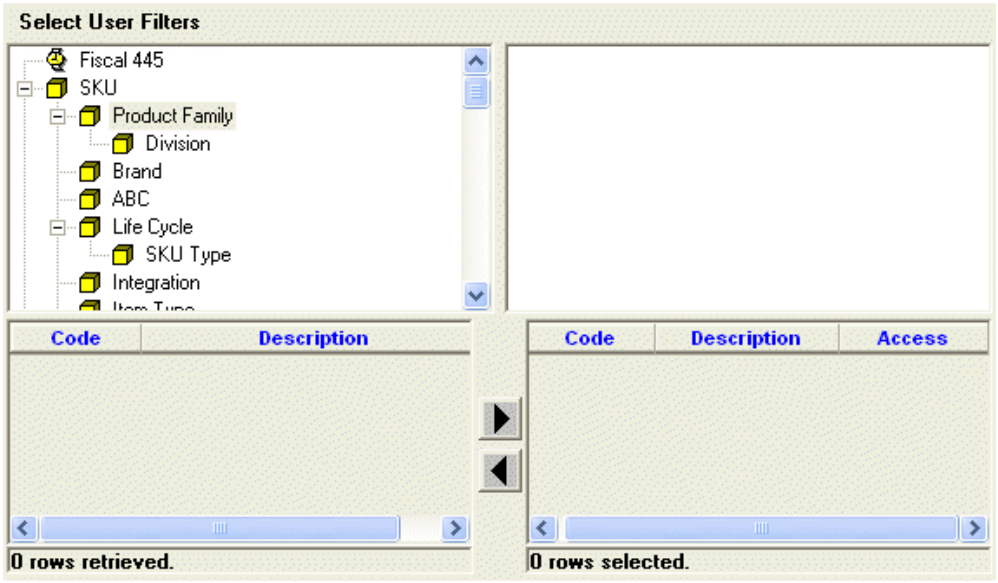
    1. Move all series that you want into the Selected Series list. To do so, either double-click each series or drag and drop it.

    2. Remove any unwanted series from the Selected Series list.

        Note: You can also move an entire series group from one list to the other in the same way.

    3. When you are done specifying series, click Next.

The New User - Select User Filters dialog box appears. This dialog box lets you filter the data that the user can see; specifically, you control which levels and which members of those levels the user can see.

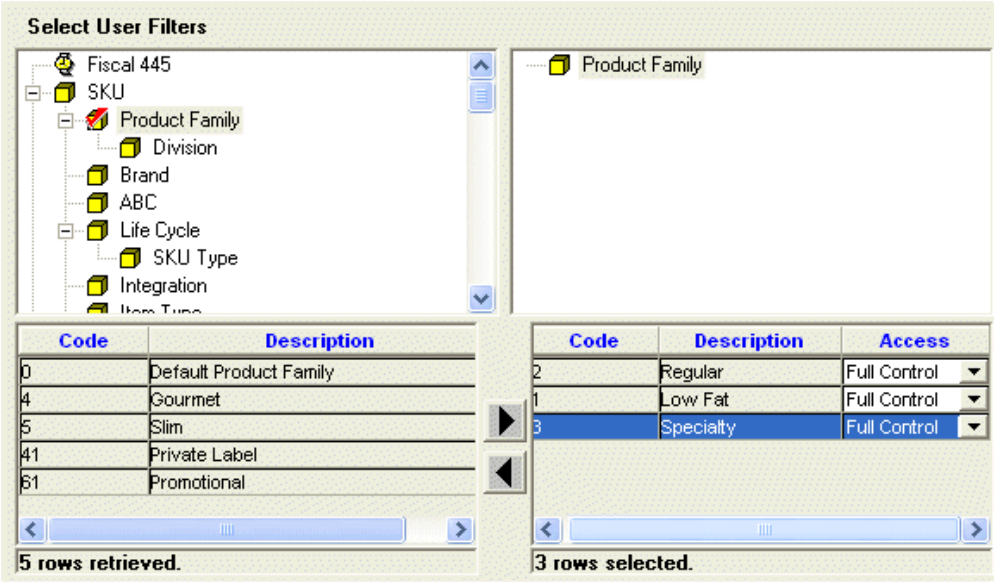


8. Filter the data that the user can see, as follows:

    1. Click a level in the left side of the dialog box and drag it to the box on the right. Or double-click a level in the left side.

    2. Now specify which members of this level the user can see. To do so, click a member in the list, and then click the right arrow button. Or double-click the member you want to filter out.

    The system moves the selected members to the box on the lower right side, as in this example:



9. Now the user can see only the selected members of this level. In the preceding example, the user can see only data that is associated with the Rainbow brand.

   Note: The Selected Members list cannot include more than 200 members.

   In the lower right, refine the security settings that control the access that the user has to each member. To do so, in the Access column, click one of the following:

   1. Full Control (user can view, edit, create, and delete within this member)
   2. Read & Write (the user can view or edit this member)
   3. Read only (the user can view this member but cannot make any changes)
   4. No access (the user does not have access to this member; this option is equivalent to not including this member in the filter)
   5. System Default (use the default permission controlled by the DefaultContentSecurityAccess parameter)

10. Repeat the preceding steps for each filter you want to add. Each filter automatically limits the choices available in subsequent filters.

    When you have appropriately filtered data for the user, click Next.

    The New User - Select User Groups dialog box appears. This dialog box allows you to select the group or groups to which the new user will belong.

11. Specify the collaboration groups to which a user belongs, as follows:

    1. Move all groups to which the user should belong into the Selected Groups list. To do so, either double-click each group or drag and drop it.

       Note: You can also select and move multiple groups with the standard Ctrl+click or Shift+click actions.

    2. Remove any unwanted groups from the Selected Groups list.

    3. Click Next.

12. Click Finish.

    For more information, see **API to Create, Modify or Delete Users**, **Copying a User**, and **Deleting a User**.

Copying a User

If you need to create multiple similar users, it is useful to create one of those users and then copy it to create the other users.

To copy a user:

1. Log on to the Business Modeler as described in "Logging onto the Business Modeler."

2. Click Security > Create/Modify User. Or click the Create/Modify User button.

   The Create/Modify User dialog box appears.

3. Click the button of the user you want to copy, and then click Create Copy.

   The User Details dialog box appears. Some of the information, such as user name, is blank. Other details, such as the company name, are copied from the original user.

4. Specify the user name and password for the new user.

5. Make other changes as needed.

6. Do one of the following:

   - Click Next to continue editing information for the new user. Demantra initially uses all the same values as for the original user.

   - Click Finish.

   Demantra also copies menu permissions of the original user; see "Specifying

Permissions for Menu Items".

See also

"Creating or Modifying a User"

Deleting a User

Warning: When a user is deleted, the current session is not immediately stopped. To stop the user from continuing operation, use the web user management page to log out the user and terminate their session.

To delete a user:

1. Log on to the Business Modeler as described in "Logging onto the Business Modeler."
2. Click Security > Create/Modify User. Or click the Create/Modify User button.

   The Create/Modify User dialog box appears.
3. Click the button of the user you want to delete, and then click Delete.

   A question box appears, inquiring if you are sure you want to delete the selected user.
4. To delete the selected user, click Yes.

   See also

   "Creating or Modifying a User"

Creating or Modifying a User Group

Demantra uses user groups for several purposes:

- Group members can collaborate, within Collaborator Workbench.
- The Workflow Engine can send tasks to groups (as well as to users).
- Groups can be authorized to view and edit notes attached to worksheets.
- Groups can authorized to use menu items.

Groups are visible in all components. Note that the users in a group can belong to different components.

To create or modify a group:

1. Log on to the Business Modeler as described in "Logging onto the Business Modeler."

2. Click Security > Create/Modify Group. Or click the Create/Modify User Group button.

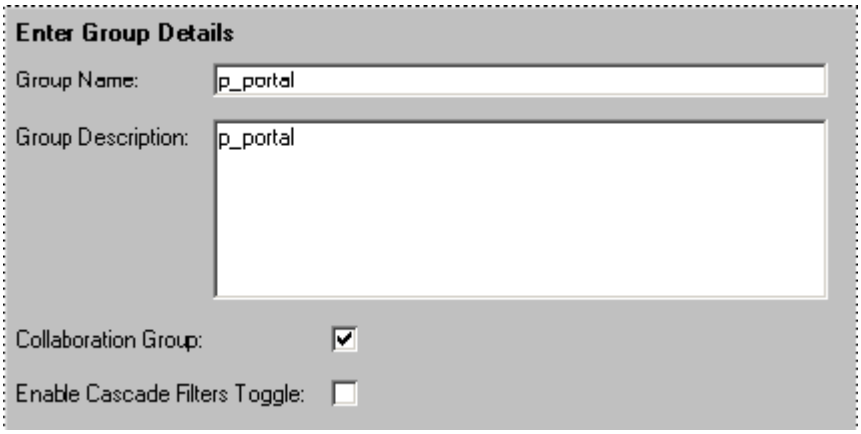
   The Create/Modify Group dialog box appears.

3. Next:

   - To create a new group, double-click the New Group button.

   - To modify a group, click the button of that group then click OK. Or double-click the icon of the group whose details you want to modify.

   The system prompts you for information about the group.



4. Specify group details as follows:

   1. Under Enter Group Details, type a name and optional description in the appropriate boxes. Each group name must be unique within your Demantra implementation.

   2. If users of this group should be able to see either other in the Who's Online pane in Collaborator Workbench, make sure the Collaboration Group check box is checked. To access the Workflow Manager, a User Group must be assigned to the workflow.group parameter (in the Business Modeler). For details, refer to Providing Access to the Workflow Editor.

      The users will also be able to send tasks to each other.

      If you clear this check box, users of the group will not see one another.

3. Check or clear the Enable Cascade Filters Toggle check box.

   Click this option to enable users in the group to toggle between cascade and non-cascade filter modes. If not selected, the user will have cascade filtering only.

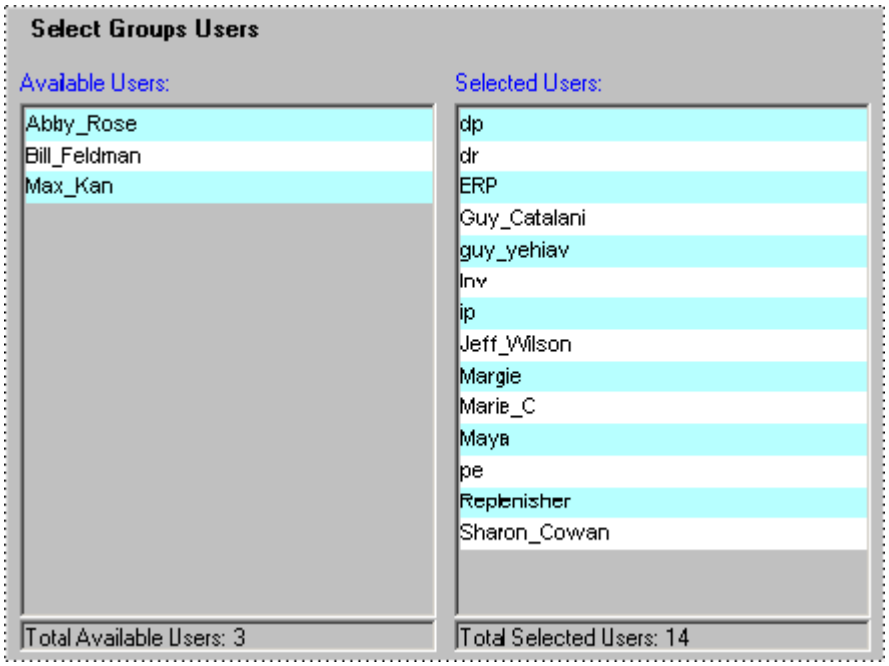
   In cascade mode, users see only members that have combinations with the previously selected members. Members that do not have combinations will not be available in the list. It is generally easier to work with filters in cascade mode.

   In non-cascade mode, users see all the members of the selected level regardless of the previously selected members from other levels.

   > **Note:** If Cascade Filters are enabled, you can define whether they should initially be toggled on or toggled off. To do this you need to set the value for the column CASCADE_FILTERS_DEF_VAL in the table GROUP_ATTRIBUTES_POPULATION. A value of 1 means that Cascade Filters are initially toggled on. A value of 0 or null means they are initially toggled off. The default is 1. You set this value using a database utility such as Oracle SQL Developer. If Cascade Filters are not enabled then this setting has no effect.

4. Click Next.

   The New Group - Select Group Users dialog box appears. This dialog box allows you to select existing users who will belong to the new group.



5. Specify the users in a group, as follows:

    1. Move all users that should be in this group into the Selected Users list. To do so, either double-click each user name or drag and drop it.

        Note: You can also select and move multiple users with the standard Ctrl+click or Shift+click actions.

    2. Remove any unwanted users from the Selected Users list.

    3. Click Next.

6. Click Finish.

    See Also

    "Data Security"

    "Deleting a Group"

Deleting a Group

To delete a group:

1. Log on to the Business Modeler as described in "Logging onto the Business

Modeler."

2. Click Security > Create/Modify Group. Or click the Create/Modify Group button.

   The Create/Modify Group dialog box appears.

3. Click the button of the group that you want to delete.

   A box appears, inquiring if you are sure you want to delete the selected group.

4. Click Delete.

   See also

   "Data Security"

   "Creating or Modifying a User Group"

Logging Out Users

Demantra provides a tool that you can use to log out users whose sessions have hung due to network or other problems. This applies only to the users of the Web-based products.

> **Note:** You must have a permission level of "System Manager" to use this tool.

To log a user out of Demantra:

1. Browse to the following case-sensitive URL:

   http://server name/virtual directory/portal/userManagement.jsp

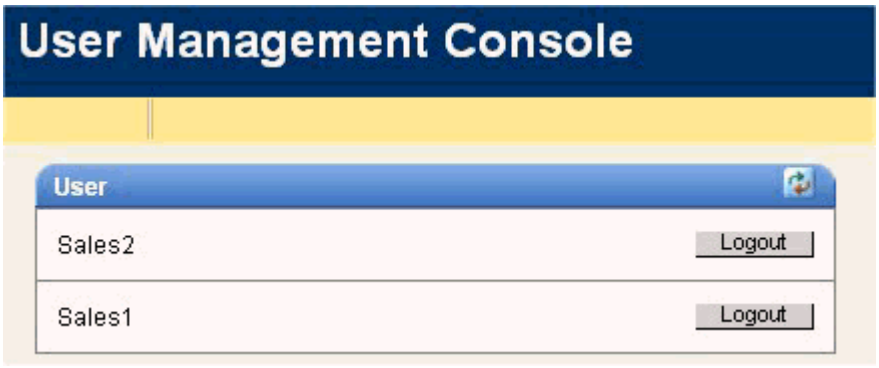
   For example:

   http://frodo/demantra/portal/userManagement.jsp

   A login page appears.

2. Type your username and password and then click Log on.

   Demantra displays the following screen:



3. Click Logout in the row corresponding to the user you want to log out.

Changing Your Password

You can log into the Business Modeler and change your own password. If your permission level is lower than System Manager, your password is the only information you can access.

> **Note:** You can also change your password by using the Administration link in Collaborator Workbench.

To change your password:

1. Log into the Business Modeler. If you do not have access to this tool, contact your Oracle Demantra system administrator.

2. Click Security > Change Password. Or click the Change Password button.

   The Business Modeler displays the Change Password screen:

3. Type your current password in the Old Password field.
4. Type your new password in the New and Confirm New fields.
5. Click OK.

Password Policy

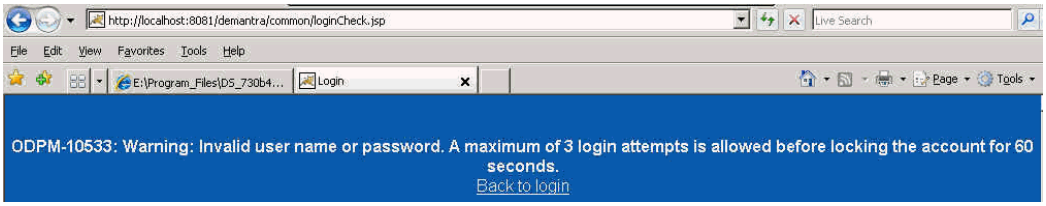
You can set up Demantra to enforce password policies and ensure that passwords are well-formed and are changed frequently. By default, Demantra password policies are enforced. An administrator can change this by modifying the system parameter PasswordRulesEnforcedGlobal. For details about this parameter, see Non-Engine Parameters.

Once enabled, the password polices are:

- Password length must be 8 to 12 characters.
- At least one character must be in UPPER CASE.
- At least one digit or special character must be used in the password.
- At least one digit or special character must be used in the password.
- Password should NOT be a Security Dictionary Word (please contact your administrator for details).
- Password should NOT be the same as User name.
- Password should NOT be the same as current password.

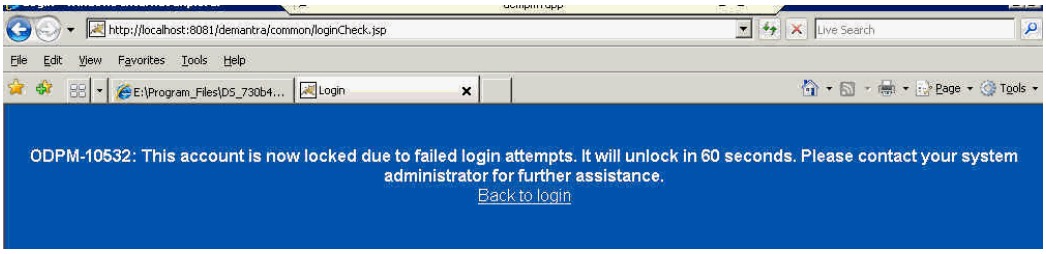
If a user attempts to create a new password that does not follow these policies, a message notifies the user of the password policies.

If the user attempts to login and fails, a message similar to the following appears:



The number of tries allowed by the password policy is determined by the system parameter "AccountLockoutThreshold". (see System Parameters).

If the user is locked out because of too many failed attempts, the following message appears:



An administrator can unlock the user's account by logging into Business Modeler, navigating to Security > Create/Modify User, and then deselect the Locked check box. If the component owner is locked out, they can log into the Business Modeler and unlock themselves.

If an administrator explicitly locks a user's account, a different message appears, saying that the account is locked and to please contact your system administrator.

Note that this locking applies to Collaborator Workbench, Workflow Manager, Administrator Login, Demand Planner Web, Dynamic Open Link (DOL) , Demantra Anywhere.Locking does not apply to the Business Modeler, Member Management, or Chaining Management.

When a user's password expiration date is within 10 days, a message displays prompting the user to change his password.

For more information see these system parameters:

- PasswordHistoryCount
- PasswordRulesEnforcedGlobal
- AccountLockoutThreshold
- AccountLockoutDuration
- PasswordResetTime

Mutual Authentication

The following system parameter can be used for configuring mutual authentication (taken from the System Parameters table in the Demantra Implementation Guide).

Parameter	Location	Default	Details

client.ssl.authenticati on	System Paramete rs > Applicati on Server > DP Web	false	This parameter controls two-way (mutual) SSL authentication.

Logging Messages of the Application Server

By default, the Application Server writes logs into the directory Demantra_root/Collaborator/virtual_directory/portal/logs. These logs record activity of the server and clients.

To change the behavior of this logging, edit the file Demantra_root/Collaborator/virtual_directory/portal/conf/logconf.lcf. In this file, you can specify items such as the following:

- Name and location of the log file
- Maximum size of the log file
- Number of log files to keep
- Information on user login/logout events

For details, see the comments in *Demantra_root*/Collaborator/*virtual_directory* /portal/conf/logconf.lcf.

> **Important:** If the default language uses a **non-ASCII character set** (such as Korean, Japanese, Chinese, Russian) then the text editor for viewing server log files must support the UTF-8 character set. Otherwise the text may not display correctly.

collaborator.login.user

This parameter is set in the logconf.lcf file. Users can turn on this log category and the following information will print out to the collaborator.log file:

- date/time : User "username" logged in, "number" users online."
- date/time : User "username" has been brutally logged out, "number" users online.
- date/time : User "username" logged out, "number" users online.

Viewing the Workflow Process Log

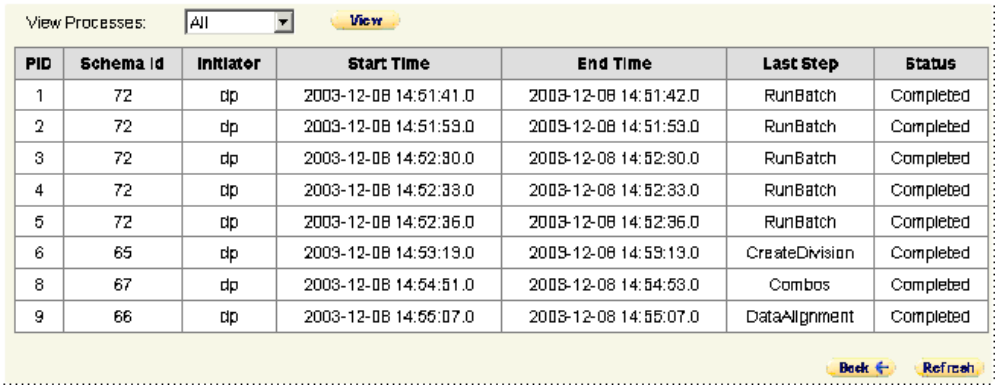
The workflow process log displays information on all the workflow instances that have

run or that are running.

To view the process log:

1. On the bottom of the Workflow Management page, click Process Log.

   The Process Log page appears.


View Processes: All View

PID	Schema Id	Initiator	Start Time	End Time	Last Step	Status
1	72	dp	2003-12-08 14:51:41.0	2003-12-08 14:51:42.0	RunBatch	Completed
2	72	dp	2003-12-08 14:51:53.0	2003-12-08 14:51:53.0	RunBatch	Completed
3	72	dp	2003-12-08 14:52:30.0	2003-12-08 14:52:30.0	RunBatch	Completed
4	72	dp	2003-12-08 14:52:33.0	2003-12-08 14:52:33.0	RunBatch	Completed
5	72	dp	2003-12-08 14:52:36.0	2003-12-08 14:52:36.0	RunBatch	Completed
6	65	dp	2003-12-08 14:53:13.0	2003-12-08 14:53:13.0	CreateDivision	Completed
8	67	dp	2003-12-08 14:54:51.0	2003-12-08 14:54:53.0	Combos	Completed
9	66	dp	2003-12-08 14:55:07.0	2003-12-08 14:55:07.0	DataAlignment	Completed

Back Refresh

To filter process log entries:

1. Select the required filter from the View Processes drop-down menu.

2. Click View.

   The filtered processes are shown.

   See also:

   "Viewing Workflow Status"

Specifying Content Pane Security

You can control access to the different Collaborator Workbench panes (My Tasks, My Worksheets, and Who's Online).

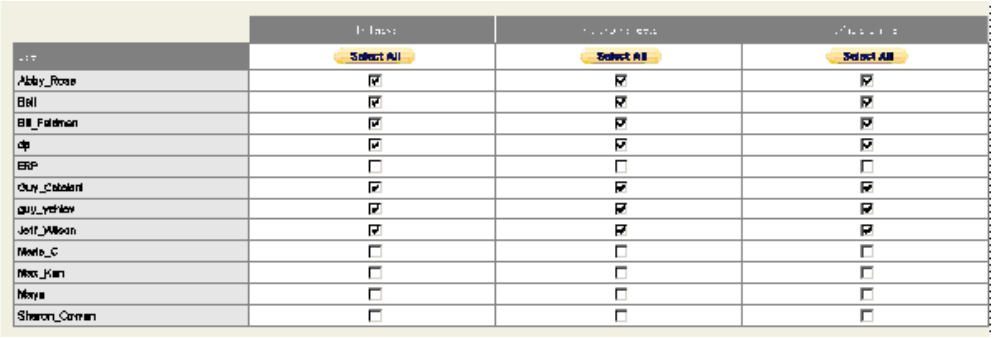
To specify access to Collaborator Workbench panes:

1. Log into the Collaborator Workbench Administrator. See "Logging onto the Collaborator Workbench Administrator".

   The Administration page appears.

2. Click Define Content Security.

   The system displays a table with one row for each user. Here you specify which panes to make available to each user.



3. Do one of the following:
   - Check the check box for a pane to grant user access to the user.
   - Clear the check box for a pane to deny access to the user.
4. Click Finish.

   See also

   "Configuring the Pane Configuration"

Checking the Log Files and Tables

To check the installation logs:

1. Check the basic installer log file: C:\tmp\Demantra-install.log.
2. Check the database log files written by the Installer. Depending on the installation, the Installer writes some or all of the following log files into Demantra_root\Demand Planner\Database Objects\database_type_name:
   - import.log (Information on the import process of the dump file)
   - For Oracle: run_build_procedures.LST (Information on the loading of the procedures into the new user.) and other *.LST files.
3. Check the db_exception_log table.

If you upgraded the database user, also check the following:

- The upgrade.log file provides details on the database upgrade process. This file is in the same directory as the other Installer log files.
- version_detail table is updated to the new version only if the upgrade procedure finishes successfully.

A

Security Checklist

Important: The Demantra Local Application replaces Collaborator Workbench. You may see both names in this text.

This appendix covers the following topics:

- Checklist

Checklist

- Install only what is required.
- Lock and expire default user accounts.
- Enforce password management.
- Enable data dictionary protection.
- Practice the principle of least privilege.
  - Grant necessary privileges only.
  - Revoke unnecessary privileges from the PUBLIC user group.
  - Restrict permissions on run-time facilities.
- Enforce access controls effectively and authenticate clients stringently.
  - Use a firewall.
  - Never poke a hole through a firewall.
  - Protect the Oracle listener.

    - Monitor listener activity.
    - Monitor who accesses your systems.
    - Check network IP addresses.
    - Encrypt network traffic.
    - Harden the operating system.
- Apply all security patches and workarounds.
- Contact Oracle Security Products if you come across vulnerability.

Index

A

associating
- indicators with series, 2-4
- levels and worksheets (for Open With), 2-7
- series and users, 3-7
- users and groups, 4-12

B

Business Modeler
- configuring components, 2-1

C

cascade mode for filter, enabling, 4-11
casual user, 3-8
Collaborator Workbench
- configuring, 3-3
- configuring content security, 4-18
- how configurable, 3-3
- specifying menu permissions, 3-18

Collaborator Workbench Administrator
- configuring menu permissions in Collaborator, 3-14, 3-16, 3-17, 3-18
- configuring pane security in Collaborator, 4-18
- logging on, 3-3

component
- creating or modifying, 2-1
- deleting, 2-10
- engine profiles, specifying, 2-8
- indexes and exchange rates
  - specifying, 2-6
- introduction, 1-2, 1-2
- levels, specifying, 2-5
- owner, 2-9
- series
  - adding, 2-2
  - viewing, 3-7
- series indicators, specifying, 2-3
- units
  - specifying, 2-6
- users, specifying, 4-2
- worksheet-level associations, 2-7

Component Configuration Wizard, 2-2
content
- setting security, 4-18

D

database
- using a different database without reinstalling, 1-6

default
- general level indicators for series, 2-4
- methods, 3-2
- worksheet associated with a level, 2-8

delete access, security for, 1-4
dropdown security, 3-5

E

email
- specifying for users, 4-3

embedded worksheets
- backend configuration, 2-8

engine profile
- including in a component, 2-9

exchange rate
including in a component, 2-7

F

filter
and Open With menu, 2-8
at user level, 1-2, 1-4, 4-5
cascade versus non-cascade mode, per user, 4-11
firewalls, 2-14

G

general level
and series indicators, 1-2
specifying series indicators, 2-4
group
access to Workflow Editor/Manager, 3-4
adding users to, 4-7
creating, 4-9
deleting, 4-12
introduction, 1-2
overview, 1-2
selecting users for, 4-12
users in, 4-12

H

hung session
ending, 4-13

I

index (financial)
including in a component, 2-7
indicators for notes, promotions, or general levels, 2-3

L

level
associating with worksheets (for Open With), 2-7
including in component, 2-5
specifying security at component level, 2-5
logconf.lcf, 4-17
log files, 4-19
logging off
if session hangs, 4-13

M

member security, 4-7
menu
Collaborator Workbench
configuring menu permissions, 3-18
right-click
configuring Open with menu, 2-8
My Tasks
configuring user access, 4-18
My Worksheets
configuring user access, 4-18

N

non-cascade mode for filter, enabling, 4-11
note
access at group level, 4-9
configuring indicators in worksheet table, 2-3

O

Open With menu
associating levels and worksheets, 2-7

P

password
permission needed for changing, 3-3
policy, 4-15
permission level
customizing, 3-9
introduction, 1-2
specifying for user, 4-3
specifying menu items for, 3-18
permission level
specifying for user, 4-3
power user, 3-8
process log, 4-17
profile
for engine parameters
adding to component, 2-8
program group
defining, 3-14, 3-16
deleting, 3-17
promotion
configuring indicators in worksheet table, 2-3

R

right-click menu
configuring Open With menu, 2-8

S

security
dropdown, 3-5
security model, 1-2
series
available to user, 4-5
including in a component, 2-3
indicators for notes or promotions, 2-3
making available for specific user, 4-4
SSL, 2-14
SYS_GRANTS.SQL script, 2-13
System Manager permission
and delete access, 1-4

U

units of measure
including in a component, 2-6
user
access to levels, 2-5
access to series, 2-2, 2-3, 4-5
access to worksheets, 1-5
adding to groups, 4-7, 4-12
copying, 4-8
creating, 4-2
filtering data, 4-5
filter mode (cascade vs non-cascade), 4-11
forcing logout, 4-13
overview, 1-2, 1-2
specifying modules, 4-3

W

Whoxd5 s Online
controlling user access, 4-18
workflow
email addresses used in, 4-3
workflow.group parameter, 3-5
Workflow Editor/Manager
login access, 3-4
viewing process log, 4-17
worksheet
changing access, 1-5
configuration
adding to Open With menu, 2-7
indicators for notes and promotions, 2-3
overview, 3-2