Oracle® E-Business Suite

System Administrator's Guide - Maintenance

Release 12.1

Part No. E12894-04

June 2010

Oracle E-Business Suite System Administrator's Guide - Maintenance, Release 12.1

Part No. E12894-04

Primary Author: Mildred Wang, Robert Farrington, Clara Jaeckel, Melody Yang

Contributing Author: George Buzsaki, Anne Carlson, Steve Carter, Steven Chan, Siu Chang, Jennifer Collins, Ada Constanzo-Muller, Ivo Dujmovic, Mark Fisher, Paul Ferguson, Rajesh Ghosh, Kunal Kapur, Ravi Mohan, Muhannad Obeidat, Gursat Olgun, Richard Ou, Pranab Pradhan, Traci Short, Jan Smith, Vikas Soolapani, Seth Stafford, Susan Stratton, Leslie Studdard, Vani Subramanian, Suchithra Upadhyayula, Venkat Vengala, Mark Warren, Aaron Weisberg, Sara Woodhull, Yali Wu, Maxine Zasowski

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

This software and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third party content, products and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third party content, products or services.

Contents

3 Oracle Workflow Manager

4 Monitoring Oracle E-Business Suite

5 Administering Oracle E-Business Suite Secure Enterprise Search

6 Technology Inventory Utility

7 Diagnostics and Repair in Oracle Applications Manager

8 Patching and Maintenance with Oracle Applications Manager

9 License Manager

10 User Profiles

A Profile Options in Oracle Application Object Library

B Using Predefined Alerts

Index

Send Us Your Comments

Oracle E-Business Suite System Administrator's Guide - Maintenance, Release 12.1

Part No. E12894-04

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 12.1 of the *Oracle E-Business Suite System Administrator's Guide - Maintenance.*

This guide assumes you have a working knowledge of the following:

- The principles and customary practices of your business area.
- Computer desktop application usage and terminology.

If you have never used Oracle E-Business Suite, we suggest you attend one or more of the Oracle E-Business Suite training classes available through Oracle University.

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

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at http://www.fcc.gov/cgb/consumerfacts/trs.html, and a list of phone numbers is available at http://www.fcc.gov/cgb/dro/trsphonebk.html.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at http://www.oracle.com/accessibility/.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

Structure

Related Information Sources

This book is included on the Oracle E-Business Suite Documentation Library, which is supplied in the Release 12.1 Media Pack. You can download soft-copy documentation as PDF files from the Oracle Technology Network at http://www.oracle.com/technology/documentation/. The Oracle E-Business Suite Release 12.1 Documentation Library contains the latest information, including any documents that have changed significantly between releases. If substantial changes to this book are necessary, a revised version will be made available on the "virtual" documentation library on My Oracle Support (formerly Oracle*MetaLink*).

If this guide refers you to other Oracle E-Business Suite documentation, use only the latest Release 12.1 versions of those guides.

Online Documentation

All Oracle E-Business Suite documentation is available online (HTML or PDF).

- **Online Help** - Online help patches (HTML) are available on My Oracle Support.
- **PDF Documentation** - See the Oracle E-Business Suite Documentation Library for current PDF documentation for your product with each release. The Oracle E-Business Suite Documentation Library is also available on My Oracle Support and is updated frequently.
- **Release Notes** - For information about changes in this release, including new features, known issues, and other details, see the release notes for the relevant product, available on My Oracle Support.
- **Oracle Electronic Technical Reference Manual -** The Oracle Electronic Technical Reference Manual (eTRM) contains database diagrams and a detailed description of database tables, forms, reports, and programs for each Oracle E-Business Suite product. This information helps you convert data from your existing applications and integrate Oracle E-Business Suite data with non-Oracle applications, and write custom reports for Oracle E-Business Suite products. The Oracle eTRM is available on My Oracle Support.

Related Guides

You should have the following related books on hand. Depending on the requirements of your particular installation, you may also need additional manuals or guides.

Maintaining Oracle E-Business Suite Documentation Set

This documentation set provides maintenance and patching information for the Oracle E-Business Suite DBA. *Oracle E-Business Suite Maintenance Procedures* provides a description of the strategies, related tasks, and troubleshooting activities that will help ensure the continued smooth running of an Oracle E-Business Suite system. *Oracle E-Business Suite Maintenance Utilities* describes the Oracle E-Business Suite utilities that are supplied with Oracle E-Business Suite and used to maintain the application file system and database. It also provides a detailed description of the numerous options available to meet specific operational requirements. *Oracle E-Business Suite Patching Procedures* explains how to patch an Oracle E-Business Suite system, covering the key concepts and strategies. Also included are recommendations for optimizing typical patching operations and reducing downtime.

Oracle E-Business Suite Concepts

This book is intended for all those planning to deploy Oracle E-Business Suite Release 12, or contemplating significant changes to a configuration. After describing the Oracle E-Business Suite architecture and technology stack, it focuses on strategic topics, giving a broad outline of the actions needed to achieve a particular goal, plus the installation and configuration choices that may be available.

Oracle Alert User's Guide

This guide explains how to define periodic and event alerts to monitor the status of your Oracle E-Business Suite data.

Oracle Application Framework Personalization Guide

This guide covers the design-time and run-time aspects of personalizing applications built with Oracle Application Framework.

Oracle Diagnostics Framework User's Guide

This manual contains information on implementing and administering diagnostics tests for Oracle E-Business Suite using the Oracle Diagnostics Framework.

Oracle E-Business Suite CRM System Administrator's Guide

This manual describes how to implement the CRM Technology Foundation (JTT) and use its System Administrator Console.

Oracle E-Business Suite Developer's Guide

This guide contains the coding standards followed by the Oracle E-Business Suite development staff. It describes the Oracle Application Object Library components needed to implement the Oracle E-Business Suite user interface described in the *Oracle E-Business Suite User Interface Standards for Forms-Based Products*. It provides information to help you build your custom Oracle Forms Developer forms so that they integrate with Oracle E-Business Suite. In addition, this guide has information for customizations in features such as concurrent programs, flexfields, messages, and logging.

Oracle E-Business Suite Flexfields Guide

This guide provides flexfields planning, setup, and reference information for the Oracle E-Business Suite implementation team, as well as for users responsible for the ongoing maintenance of Oracle E-Business Suite product data. This guide also provides information on creating custom reports on flexfields data.

Oracle E-Business Suite Installation Guide: Using Rapid Install

This book is intended for use by anyone who is responsible for installing or upgrading Oracle E-Business Suite. It provides instructions for running Rapid Install either to carry out a fresh installation of Oracle E-Business Suite Release 12, or as part of an upgrade from Release 11*i* to Release 12. The book also describes the steps needed to install the technology stack components only, for the special situations where this is applicable.

Oracle E-Business Suite Integrated SOA Gateway User's Guide

This guide describes the high level service enablement process, explaining how users can browse and view the integration interface definitions and services residing in Oracle Integration Repository.

Oracle E-Business Suite Integrated SOA Gateway Implementation Guide

This guide explains how integration repository administrators can manage and administer the service enablement process (based on the service-oriented architecture) for both native packaged integration interfaces and composite services (BPEL type). It also describes how to invoke Web services from Oracle E-Business Suite by employing the Oracle Workflow Business Event System, how to manage Web service security, and how to monitor SOAP messages.

Oracle E-Business Suite Integrated SOA Gateway Developer's Guide

This guide describes how system integration developers can perform end-to-end service integration activities. These include orchestrating discrete Web services into meaningful end-to-end business processes using business process execution language (BPEL), and deploying BPEL processes at run time.

This guide also explains how to invoke Web services using the Service Invocation Framework. This includes defining Web service invocation metadata, invoking Web services, and testing the Web service invocation.

Oracle E-Business Suite System Administrator's Guide Documentation Set

This documentation set provides planning and reference information for the Oracle E-Business Suite System Administrator. *Oracle E-Business Suite System Administrator's Guide - Configuration* contains information on system configuration steps, including defining concurrent programs and managers, enabling Oracle Applications Manager features, and setting up printers and online help. *Oracle E-Business Suite System Administrator's Guide - Maintenance* provides information for frequent tasks such as monitoring your system with Oracle Applications Manager, administering Oracle E-Business Suite Secure Enterprise Search, managing concurrent managers and reports, using diagnostic utilities including logging, managing profile options, and using alerts. *Oracle E-Business Suite System Administrator's Guide - Security* describes User Management, data security, function security, auditing, and security configurations.

Oracle E-Business Suite User's Guide

This guide explains how to navigate, enter data, query, and run reports using the user interface (UI) of Oracle E-Business Suite. This guide also includes information on setting user profiles, as well as running and reviewing concurrent requests.

Oracle E-Business Suite User Interface Standards for Forms-Based Products

This guide contains the user interface (UI) standards followed by the Oracle E-Business Suite development staff. It describes the UI for the Oracle E-Business Suite products and how to apply this UI to the design of an application built by using Oracle Forms.

Oracle Workflow Administrator's Guide

This guide explains how to complete the setup steps necessary for any product that includes workflow-enabled processes. It also describes how to manage workflow processes and business events using Oracle Applications Manager, how to monitor the progress of runtime workflow processes, and how to administer notifications sent to workflow users.

Oracle Workflow Developer's Guide

This guide explains how to define new workflow business processes and customize existing Oracle E-Business Suite-embedded workflow processes. It also describes how to define and customize business events and event subscriptions.

Oracle Workflow User's Guide

This guide describes how users can view and respond to workflow notifications and monitor the progress of their workflow processes.

Oracle Workflow API Reference

This guide describes the APIs provided for developers and administrators to access Oracle Workflow.

Oracle Workflow Client Installation Guide

This guide describes how to install the Oracle Workflow Builder and Oracle XML Gateway Message Designer client components for Oracle E-Business Suite.

Oracle XML Gateway User's Guide

This guide describes Oracle XML Gateway functionality and each component of the Oracle XML Gateway architecture, including Message Designer, Oracle XML Gateway Setup, Execution Engine, Message Queues, and Oracle Transport Agent. It also explains how to use Collaboration History that records all business transactions and messages exchanged with trading partners.

The integrations with Oracle Workflow Business Event System, and the Business-to-Business transactions are also addressed in this 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 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

Introduction

Introduction to This Manual

A system administrator is involved in setting up an Oracle E-Business Suite installation, controlling access, and ensuring smooth ongoing operation. The tasks involved in these functions are described in the *Oracle E-Business Suite System Administrator's Documentation Set,* in these three volumes:

- Security
- Configuration
- Maintenance

This Maintenance volume describes maintenance tasks for an Oracle E-Business Suite installation, as well as tasks you might perform on a frequent basis.

Managing Concurrent Processing and Concurrent Programs

This chapter explains how to manage concurrent processing, including managing concurrent managers, reviewing concurrent requests, and managing parallel concurrent processing.

Oracle Workflow Manager

Oracle Workflow Manager is a component of Oracle Applications Manager that allows system administrators to manage Oracle Workflow for multiple Oracle E-Business Suite instances.

Using Oracle Workflow Manager, administrators can control Workflow system services, such as notification mailers, agent listeners, and other service components, background engines, purging obsolete Workflow data, and cleanup of the Workflow control queue. Administrators can also monitor work item processing by viewing the distribution of all work items by status and drilling down to additional information. Additionally, they can monitor event message processing for local Business Event System agents by viewing the distribution of event messages by status as well as queue propagation schedules. With this ability to monitor work items and event messages, a system administrator can identify possible bottlenecks easily.

Monitoring an Oracle E-Business Suite System Using Oracle Applications Manager

Oracle Applications Manager allows you to monitor many components of your applications system, such as database status, system activity, forms sessions and processes, and applications usage.

In addition, the OAM console can provide information on system alerts, metrics, and logs that can help you diagnose potential problems. For example, configuration issues, overdue routine maintenance tasks, and invalid data can cause serious problems requiring either an automated response or manual intervention.

Oracle E-Business Suite Secure Enterprise Search

Oracle E-Business Suite Secure Enterprise Search is a centralized, secure search vehicle with consistent user interfaces throughout the Oracle E-Business Suite. By leveraging Oracle Secure Enterprise Search (SES), Oracle E-Business Suite Secure Enterprise Search enables a powerful keyword search on applications content in a faster, user-friendly way without compromising on the security and context sensitive information.

Technology Inventory Utility

This command-line utility generates reports that list the installed technology stack components and versions on the various nodes of a Release 12 Applications system. The reports can be generated in either HTML (the default) or text format. Separate reports are generated for the Database and application tiers.

Diagnostics and Repair

Oracle Applications Manager provides diagnostics utilities and troubleshooting wizards for your Oracle E-Business Suite system.

Patching and Maintenance

This chapter provides information on several features that help you in patching and maintenance of your applications system:

- Patch Impact Analysis
- Restricted Mode
- Running purge programs through OAM

Additional features are described in the *Maintaining Oracle E-Business Suite Documentation Set.*

User Profiles

A profile is a set of changeable options that affect the way an application looks and behaves. You can control how Oracle E-Business Suite operates by setting profile options to the values you want. This chapter provides an overview to profiles and how to set profile values.

Profile Options in Oracle Application Object Library

This appendix lists profile options in Oracle Application Object Library that the system administrator can set.

Using Predefined Alerts

Oracle Alert provides an immediate view of the critical activity in your database, and gives you flexibility to monitor your business information the way you want. This appendix provides an overview of Oracle Alert and how to use predefined alerts. For more information on Oracle Alert, see the *Oracle Alert User's Guide.*

Other Volumes for System Administrators

Listed below are other volumes in the *Oracle E-Business Suite System Administrator's Documentation Set.* In addition, refer to the Preface for additional related guides.

Oracle E-Business Suite System Administrator's Guide - Configuration

Oracle E-Business Suite System Administrator's Guide - Configuration describes the tasks involved in setting up and configuring Oracle E-Business Suite. These tasks may be done once upon installation, or may also be done as needed, such as setting up a printer or customizing online help files. Areas covered include:

- Basic Configuration Tasks after Running Rapid Install
- Oracle E-Business Suite Tablespace Model and the Tablespace Migration Utility
- System Administrator Setup Tasks
- Introduction to Oracle Applications Manager
- Setting Up Concurrent Processing and Concurrent Managers
- Defining Concurrent Programs and Reports

- Setting Up Printers
- Oracle E-Business Suite Online Help
- Oracle E-Business Suite DBA Duties
- Query Optimization in Oracle E-Business Suite
- Oracle E-Business Suite and Real Application Clusters
- Document Sequences
- Logging
- Administering Process Navigation
- Administering Globalization
- Developer Tools
- Loaders
- Oracle Application Server with Oracle E-Business Suite
- Timezone Support

Oracle E-Business Suite System Administrator's Guide - Security

Oracle E-Business Suite System Administrator's Guide - Security describes security concepts, setup tasks, and maintenance tasks done in the following areas:

- Oracle User Management
- Function Security in Oracle Application Object Library
- Data Security in Oracle Application Object Library
- User and Data Auditing
- Oracle Single Sign-On Integration (optional)

2

Managing Concurrent Processing and Concurrent Programs

Overview of Concurrent Processing

This section explains how a request to run a concurrent program is handled by Oracle E-Business Suite, and what the life cycle of a concurrent request is.

In Oracle E-Business Suite, concurrent processing simultaneously executes programs running in the background with online operations. As System Administrator, you can manage when programs are run and how many operating system processes Oracle E-Business Suite devotes to running programs in the background.

Concurrent Requests, Programs, and Processes

When a user runs a report, a request to run the report is generated. The command to run the report is a *concurrent request*. The program that generates the report is a *concurrent program*. Concurrent programs are started by a *concurrent manager*.

Concurrent Managers start concurrent programs

Every time your users request a concurrent program to be run, their request is inserted into a database table, and is uniquely identified by a request ID. Concurrent managers read requests from this table.

Part of a manager's definition is how many operating system processes it can devote to running requests. This number is referred to as the manager's number of *target processes*.

Running concurrent programs

A concurrent program actually starts running based on:

- When it is scheduled to start

- Whether it is placed on hold
- Whether it is incompatible (cannot run) with other programs
- Its request priority

Concurrent Request Priorities

The priority of a concurrent request is determined by application username, and is set by the System Administrator using the Concurrent:Priority user profile option.

The first available concurrent manager compares the request's priority to other requests it is eligible to process, and runs the request with the highest priority.

When choosing between requests of equal priority, the concurrent manager runs the oldest request first.

Parent requests and Child requests

Often, several programs may be grouped together, as in a request set. Submitting the request set as a whole generates a request ID, and as each member of the set is submitted it receives its own request ID. The set's request ID identifies the *Parent* request, and each of the individual programs' request ID identifies a *Child* request.

Life cycle of a concurrent request

A concurrent request proceeds through three, possibly four, life cycle stages or *phases:*

Pending	Request is waiting to be run
Running	Request is running
Completed	Request has finished
Inactive	Request cannot be run

Within each phase, a request's condition or *status* may change. The following table shows a listing of each phase and the various states that a concurrent request can go through.

Phase	Status	Description
PENDING	Normal	Request is waiting for the next available manager.

Phase	Status	Description
PENDING	Standby	Program to run request is incompatible with other program(s) currently running.
PENDING	Scheduled	Request is scheduled to start at a future time or date.
PENDING	Waiting	A child request is waiting for its Parent request to mark it ready to run. For example, a report in a report set that runs sequentially must wait for a prior report to complete.
RUNNING	Normal	Request is running normally.
RUNNING	Paused	Parent request pauses for all its child requests to complete. For example, a report set pauses for all reports in the set to complete.
RUNNING	Resuming	All requests submitted by the same parent request have completed running. The Parent request is waiting to be restarted.
RUNNING	Terminating	Running request is terminated, by selecting *Terminate* in the Status field of the Request Details zone.
COMPLETED	Normal	Request completes normally.
COMPLETED	Error	Request failed to complete successfully.
COMPLETED	Warning	Request completes with warnings. For example, a report is generated successfully but fails to print.

Phase	Status	Description
COMPLETED	Cancelled	Pending or Inactive request is cancelled, by selecting *Cancel* in the Status field of the Request Details zone.
COMPLETED	Terminated	Running request is terminated, by selecting *Terminate* in the Status field of the Request Details zone.
INACTIVE	Disabled	Program to run request is not enabled. Contact your system administrator.
INACTIVE	On Hold	Pending request is placed on hold, by selecting *Hold* in the Status field of the Request Details zone.
INACTIVE	No Manager	No manager is defined to run the request. Check with your system administrator.

Related Topics

Reviewing Requests, Request Log Files, and Report Output Files, page 2-36

How to View Request Status and Output, page 2-37

Setting End User Report and Log File Access Privileges, page 2-38

Managing Concurrent Processing Files and Tables, page 2-51

Service Management

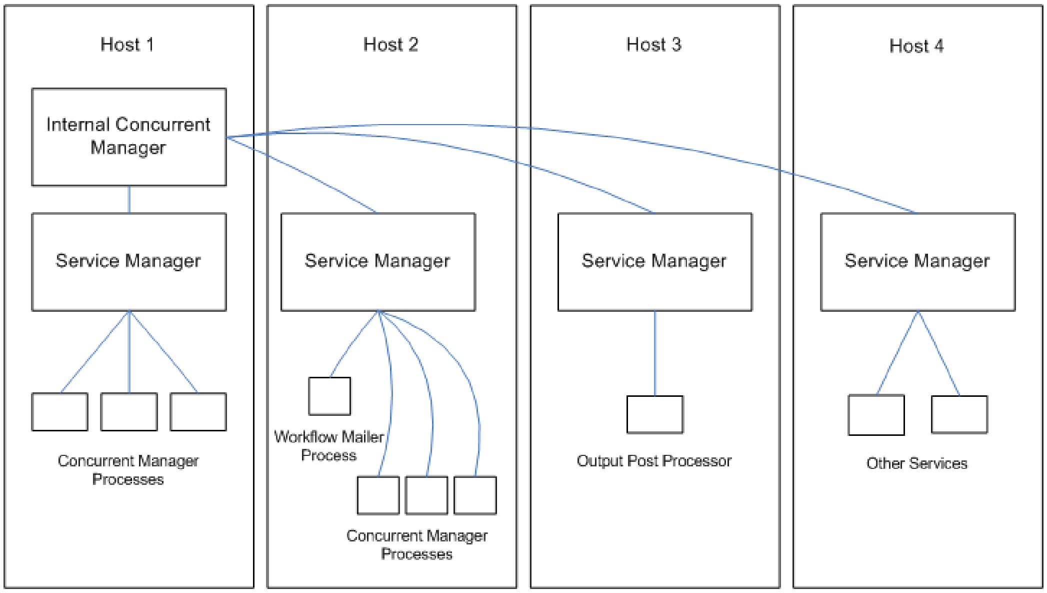
An Oracle E-Business Suite system depends on a variety of services such as Concurrent Managers and Workflow Mailers. Such services are composed of one or more processes that must be kept running for the proper functioning of the applications. Previously many of these processes had to be individually started and monitored by system administrators. Management of these processes was complicated by the fact that these services could be distributed across multiple host machines. Service Management helps to greatly simplify the management of these processes by providing a fault tolerant service framework and a central management console built into Oracle Applications

Manager.

Generic Service Management (GSM, or simply Service Management) is an extension of concurrent processing, which provides a powerful framework for managing processes on multiple host machines. With Service Management, virtually any application tier service can be integrated into this framework. Services such as the Oracle Workflow Mailer or Java services can be managed under Generic Service Management.

With Service Management, the Internal Concurrent Manager (ICM) manages the various service processes across multiple hosts. On each host, a Service Manager acts on behalf of the ICM, allowing the ICM to monitor and control service processes on that host. System administrators can then configure, monitor, and control services though a management console which communicates with the ICM.

Generic Service Management



Service Management provides a fault tolerant system. If a service process exits unexpectedly, the ICM will automatically attempt to restart the process. If a host fails, the ICM may start the affected service processes on a secondary host. The ICM itself is monitored and kept alive by Internal Monitor processes located on various hosts.

Service Management provides significant improvements in the manageability of Oracle E-Business Suite. System administrators can now use the central console in Oracle Applications Manager (OAM) to manage a variety of services that formerly had to be managed independently on separate hosts. The entire set of system services may be started or stopped with a single action. Service Management also provides a great benefit by automatically compensating for certain system failures.

Service processes are very much like concurrent manager and transaction manager processes. They must be kept running on a middle tier for the proper functioning of their respective products. The concurrent processing management feature has been built for concurrent managers and transaction managers, to provide fault tolerance, process distribution, and simplified configuration and control.

Benefits of Service Management

- The service processes will no longer need to be manually and individually started and monitored by Oracle E-Business Suite system administrators.
- Services can take advantage of the process distribution and fault tolerance capabilities that have been developed for concurrent processing.
- As with concurrent manager processes, system administrators can use work shifts to determine the number of processes that will be active for a service on a given node for a given time period.

To extend process management support to the various Applications services, the Internal Concurrent Manager must be able to start, monitor, and control processes on all Applications tiers. Every node of every tier will have an Oracle RPC-based Service Manager installed. The ICM will use the Service Manager to manage processes.

Concepts

Service

A service is a process or collection of processes that perform actions at the request of client processes. A concurrent manager is a type of service where the client submits a request for actions to be processed while the client continues to do other work.

While active, a service must have one or more listener processes that wait to process requests from clients. An example of a listener is a concurrent manager process which periodically polls a queue for requests to process.

Service Instance

Each service controlled by service management may have multiple service instances. Each instance may consist of one or more processes.

Concurrent:GSM Enabled Profile Option

The Concurrent:GSM Enabled profile option should be set to Y to enable Service Management. It is set automatically to Y by AutoConfig. Disabling Service Management is not recommended as that may prevent necessary services from starting.

Network Failure Recovery

As part of its shutdown process, the ICM determines if it's being forced to shutdown due to losing its database connection. This is done by looking for specific error messages ORA-3113, ORA-3114, or ORA-1041. If one of these error messages is detected, the ICM spawns the reviver process, which attempts to make a database connection. If unsuccessful, it sleeps for a period before trying again. This continues until either a successful connection is made or it receives a signal to shut itself down.

When a successful connection is made, the process kills the old ICM database session, and then starts a new ICM using the normal start manager script. Once the ICM is restarted, it starts up any other managers that had also shut down, and normal processing resumes.

Failover Sensitive Workshifts

Nodes can become overloaded when a middle-tier node fails and service instances on that node failover to their secondary nodes. The *Load Distribution* feature allows the System Administrator to control the allocation of resources during normal processing. The *Failover Sensitivity* feature allows Work Shifts to failover with fewer processes than on the original node. This lessens the impact on the existing resources allocated on the secondary node.

The number of failover processes is entered as part of the standard Work Shift settings in the *Service Instance Definition*. When failover occurs, the ICM uses the **Failover Processes** value in place of the normal running processes value as it iterates through service instances to perform queue sizing.

Managing Concurrent Processing with Oracle Applications Manager

The Oracle Applications Manager allows administrators to manage E-Business Suite systems from an HTML console. Oracle Applications Manager can be used for a wide variety of tasks such as administering services including concurrent managers, examining system configuration, managing Oracle Workflow, examining applied patches, and measuring system usage.

Oracle Applications Manager provides diagnostic features for Applications systems. The console displays errors recently reported by system components such as transaction managers or concurrent requests. For running processes such as forms or concurrent requests, system administrators can examine the database session details, including any currently executing SQL.

Oracle Applications Manager allows administrators to configure, monitor, and control concurrent processing. Combined with the Service Management feature, Oracle Applications Manager can be used to monitor and control concurrent managers, as well as other application tier services.

Using the Oracle Applications Manager, you can:

- view a summary of concurrent managers
- view details of a concurrent manager

- create or edit a concurrent manager
- view a summary of concurrent requests
- view details of a concurrent request
- submit a concurrent request
- search for a concurrent request based on its attributes, date submitted or completed, or its duration or wait time.

Service Instances

The Service Instances pages contain detailed information on the service instances for a particular service type, and display functions you can perform on the services.

Service types include, but are not limited to, the following:

- Internal Concurrent Manager
- Conflict Resolution Manager
- Scheduler/Prerelease Manager
- Request Processing Manager
- Internal Monitor
- Transaction Manager

The information and functionality available depends on the service type. Information may include the following:

- Status - Click on the Status icon for a service to see more information.
- State - The current state of a service. If you perform an action on that service, the state column value is updated.
- Node - In a parallel concurrent processing environment, a service's processes are targeted to run on the node displayed here. If a service is defined to use a platform-specific system queue, this column displays the name of the queue to which the service submits its processes.
- Number of Running Requests
- Number of Pending Requests
- Actual Processes - The number of operating system processes. Typically, the number of actual processes equals the number of target processes (the maximum

number of requests a service can run). However, the number of actual processes may be less than the number of target processes service deactivation or service migration.

- Target Processes - This column displays the maximum number of service processes that can be active for this service.

Controlling Service Instances

You can select a service instance and use the drop down menu above the table to perform the actions listed below. Or you can use the drop down menu at the top right to perform a single action on all service instances.

Service Instances of a Request Processing Manager

This page shows you information on service instances for a request processing manager. This type of manager runs concurrent requests.

Navigation: Applications Systems > System Activity > (Services region) Request Processing Manager

The following information is displayed:

- Status
- State
- Node
- Number of Running Requests
- Number of Pending Requests
- Actual Processes
- Target Processes
- Details (Show/Hide) - If you choose Show, the sleep interval will be displayed.

You can use the buttons at the top to perform the following on a selected service instance:

- Delete
- Edit
- View Status
- View Processes

- View Concurrent Requests

To create a new service instance, use the **Create New** button.

Start

You can start (activate) a service instance.

Stop

You can deactivate individual services. Once deactivated, a service does not restart until you select the service and choose the Start button.

When you deactivate a manager, all requests (concurrent programs) currently running are allowed to complete before the manager shuts down.

Restart

When you restart a manager, the processes are shut down and then brought back up.

Abort

You can abort or terminate individual services.

Concurrent Manager Service Status

For concurrent managers, the following information is shown:

General

- Node - the node on which the concurrent manager is running
- Debug - this setting indicates whether debugging information is recorded in the concurrent manager log file. Set this option to "On" using the **Set Debug On** button to record debugging information.
- Sleep Interval - the number of seconds your manager waits between checking the list of pending concurrent requests (concurrent requests waiting to be started).

Processes

- Target
- Active

Concurrent Requests

- Pending
- Stand by
- Running

Processes

The Processes page shows information on the concurrent processes of a service instance. You navigate to this page from the Service Instances page for a service.

Navigation: Site Map - Administration > Service Status (under Application Services) > (Services region) [Service] > (B) View Processes

You navigate to this page from the Service Instances page for a service.

The following information is given for each process:

- Status - The status of the process. The following are valid statuses:
  - Active - Currently running service processes display as "Active".
  - Deactivated - Manager processes that were explicitly deactivated by a system administrator, either by deactivating the service or by shutting down the Internal Concurrent Manager.
  - Migrating - Services that are migrating between primary and secondary nodes display as "Migrating". In a parallel concurrent processing environment, services run on either the primary or secondary node assigned to them. Services migrate to the secondary node if the primary node or the database instance on the primary node is unavailable. Services migrate back to the primary node once it becomes available.
  - Terminating - service processes that are being terminated display as "Terminating". These processes were terminated by you choosing the Terminate button in the Administer Concurrent Managers form, by you choosing Abort in the Service Instances page, or by a user selecting "Terminate" in the Concurrent Requests form.
  - Terminated - service processes that have been terminated display as "Terminated". These processes were terminated by you choosing the Terminate button in the Administer Concurrent Managers form, by you choosing Abort in the Service Instances page, or by a user selecting "Terminate" in the Concurrent Requests form.
- SPID - The operating system process ID associated with the service process.
- AUDSID - The database session ID for the service process. If the AUDSID value appears as a link, you can click on the value to bring up the Database Session Information page.
- Oracle SPID - The ORACLE system process ID associated with the service process.
- Start Date - The start date for the process.

You can use the buttons to view the following:

- Environment - The environment variable values for this service instance.
- Manager Log - The manager log.
- ICM Log - The Internal Concurrent Manager log.

This page can be added to the Support Cart.

Service Instances for a Service Manager

This page shows you information on service instances for a service manager. Service managers perform actions on behalf of the Internal Concurrent Manager (ICM). They are controlled automatically by the ICM as needed and cannot be manually controlled.

Navigation: Applications Systems > System Activity > (Services region) Service Manager

The following information is displayed:

- Status
- State
- Node

You can use the buttons at the top to perform the following on a selected service instance:

- View Status
- View Processes

Service Instances for the Internal Concurrent Manager

This page shows you information on the service instance for the Internal Concurrent Manager (ICM).

Navigation: Applications Systems > System Activity > (Services region) Internal Concurrent Manager

The following information is displayed:

- Status
- State
- Node
- Number of Pending Requests - for the ICM, these are either service control requests (activate, deactivate, etc.) or requests marked for termination.

- Details (Show/Hide) - If you choose **Show,** the sleep interval will be displayed.

You can use the buttons at the top to perform the following on the service instance:

- View Status
- View Processes
- View Actions
- Edit

Controlling Service Instances

You can select the service instance and use the drop down menu above the table to perform the actions below.

Stop

You can stop (deactivate) an individual service.

When you stop the Internal Concurrent Manager, all other managers are deactivated as well. Managers previously deactivated on an individual basis are not affected.

Any service that was active when the ICM was stopped will be restarted when the ICM is brought back up. Managers that were deactivated on an individual basis will not be brought back up with the ICM.

Stop All

Use this function to stop all services.

Stop Selective

Use this function to select which services you want to stop, and then stop only those services.

Abort

You can abort or terminate individual services.

When you abort (terminate) requests and terminate the Internal Concurrent Manager, all running requests (running concurrent programs) are terminated, and all managers are terminated. Managers previously deactivated on an individual basis are not affected.

Any service that was active when the ICM was aborted will be restarted when the ICM is brought back up. Managers that were deactivated on an individual basis will not be brought back up with the ICM.

Verify

The Internal Concurrent Manager periodically monitors the processes of each concurrent manager. You can force this process monitoring, or PMON activity, to occur by choosing the Verify action.

Status Overview

System Activity - Status Overview

This page displays a list of the system's application tier services and their statuses. It also lists the number of actual processes and target processes.

Navigation: Applications Dashboard > System Activity (drop-down menu)

You can select a service and use the **View Details** button to view more information on that service, as well as perform certain actions on them.

- Service Instances
- Internal Concurrent Manager
- Conflict Resolution Manager
- Scheduler/Prerelease Manager
- Request Processing Manager
- Internal Monitor
- Transaction Manager

Click the **View All** button to see all services listed. Click the **View Set** button to view the listing in sets of ten.

Click on the **Activity Monitors** tab to see information on Database Sessions and Concurrent Requests.

Service Instances for the Conflict Resolution Manager

This page shows you information on service instances for the Conflict Resolution Manager (CRM).

Navigation: Applications Systems > System Activity > (Services region) Conflict Resolution Manager

The following information is displayed:

- Status
- State
- Node
- Number of Pending Requests - the number of Pending/Standby requests. For each Pending/Standby request, the CRM will evaluate the constraints (such as

incompatibilities, single thread, user limit, etc.) and change the request to Pending/Normal when appropriate.

You can use the buttons at the top to perform the following on a selected service instance:

- View Status
- View Processes
- View Concurrent Requests
- Edit

Controlling Service Instances

You can select a service instance and use the drop down menu above the table to perform the actions below. Or you can use the drop down menu at the top right to perform a single action on all service instances.

Verify

You can use the Verify option for the Conflict Resolution Manager to force it to "re-cache" its information on incompatibilities among concurrent programs. Concurrent programs may be defined to be incompatible with other programs; that is, they should not run simultaneously with each other because they might interfere with each other's execution.

The Conflict Resolution Manager will also re-cache its information on users. A user may be assigned a maximum number of requests that may be run simultaneously using the "Concurrent: Active Requests Limit" profile option. The Conflict Resolution Manager rebuilds its list of users when you choose Verify.

Service Instances for a Scheduler/Prerelease Manager

This page shows you information on service instances for a Scheduler/Prerelease Manager. The Scheduler checks for and manages requests with advanced schedules.

Navigation: Applications Systems > System Activity > (Services region) Scheduler/Prerelease Manager

The following information is displayed:

- Status
- State
- Node
- Actual Processes
- Target Processes

You can use the buttons at the top to perform the following on a selected service instance:

- View Status
- View Processes
- Edit

Controlling Service Instances

You can use the dropdown list to **Verify** a Scheduler/Prereleaser Manager.

Service Instances of an Internal Monitor

This page shows you information on service instances for an Internal Monitor. The purpose of an Internal Monitor is to monitor the Internal Concurrent Manager and restart it when it exits unexpectedly.

Navigation: Applications Systems > System Activity > (Services region) Internal Monitor

The following information is displayed:

- Status
- State
- Node
- Actual Processes
- Target Processes
- Details (Show/Hide) - If you choose **Show,** the sleep interval will be displayed.

You can use the buttons at the top to perform the following on a selected service instance:

- Delete
- Edit
- View Status
- View Processes

To create a new service instance, use the **Create New** button.

Controlling Service Instances

You can select a service instance and use the drop down menu above the table to perform the actions below. Or you can use the drop down menu at the top right to perform a single action on all service instances.

Start

You can start (activate) a service instance.

Stop

You can deactivate individual services. Once deactivated, a service does not restart until you select the service and choose the Start button.

Abort

You can abort or terminate individual services.

Service Instances of a Transaction Manager

This page shows you information on the transaction manager. service instances.

Navigation: Site Map > Transaction Managers (under Application Services)

The following information is displayed:

- Details (Show/Hide) - Click **Show** to display the Sleep Interval setup for the selected Transaction Manager and the percent Estimated Availability. The sleep interval can be edited by clicking the **Edit** button.

- Name - Drills down to the **Service Instances Processes** page.

- Status - Drills down to the **Status** page for the selected transaction manager.

- State - The current state of a service. If you perform an action on that service, the state column value is updated.

- Node- In a parallel concurrent processing environment, a service's processes are targeted to run on the node displayed here. If a service is defined to use a platform-specific system queue, this column displays the name of the queue to which the service submits its processes.

- Actual Processes - The number of operating system processes. Typically, the number of actual processes equals the number of target processes (the maximum number of requests a service can run). However, the number of actual processes may be less than the number of target processes due to service deactivation or service migration.

- Target Processes - This column displays the maximum number of service processes that can be active for this service.

- Timeouts - the number of timeouts that have occurred for this manager since its last activation.

You can use the buttons at the top to perform the following on a selected service instance:

- Delete
- Edit - Launches the **Edit Manager** page.
- View Status - Launches the **Status** page.
- View Processes - Launches the Service Instances Processes page.

To create a new service instance, use the **Create New** button.

Transaction Manager Diagnostics

The following features can help you diagnose transaction manager issues:

Set Debug Level

Use the drop-down list to set the debug level for the transaction manager. Choose one of the following options and click the **Set Debug Level** button. This will set the debug level for all Transaction Managers and will be enabled for future sessions.

- Client side debugging
- Both Client and Server side debugging
- Server side debugging
- Off

> **Note:** Because debugging can adversely affect performance, it is important to turn it off when you are finished.

Time Transaction Manager

If a transaction manager is performing poorly, use the Time Transaction Manager feature to help diagnose the source of the problem. The Time Transaction Manager test reports the time consumed by each activity involved in a single transaction.

To run the test, select a transaction manager and click the Time Transaction button. This will invoke the Time Transaction Manager launch page. Click the **Run Test** button. The test results page will display the following information:

- Elapsed Time - the total time required to complete the test.
- Program - the test program name.
- User - the user ID of the initiator of the test. Drills down to the User Details page.
- Session ID
- Transaction ID

- Time - the time the activity began.

- Source Type - the type of activity and whether it was initiated by the client or the server. If you activated client-side only or server-side only the test will show only those activities of the selected source. To see both, select Both Client and Server side debugging.

- Action - description of the activity

- Message - any message returned by the activity

- Function - the PL/SQL function

- Elapsed Time (in hundredths of seconds)

From this screen, click **Finish Test** to return to the **Service Instances** page, or click **Purge** to purge the debug information for the session.

Controlling Service Instances

You can select a service instance and use the drop down menu above the table to perform the actions listed below. Or you can use the drop down menu at the top right to perform a single action on all service instances.

Start

Starts (activates) a service instance.

Stop

Deactivates individual services. Once deactivated, a service does not restart until you select the service and choose the **Start** button.

When you deactivate a manager, all transaction requests currently running are allowed to complete before the manager shuts down.

Restart

When you restart a transaction manager, its processes are shut down and then brought back up.

Abort

You can abort or terminate individual services.

OAM Generic Collection Service

The OAM Generic Collection Service is a generic service managed by Generic Service Management. It provides file uploading, signaling, purging, and other management for other service runtime processes such as the Forms Listener runtime process.

A running instance of the OAM Generic Collection service includes a main process which uses the java service cartridge API to consume the messages in the Generic Service Management Advanced Queue (AQ). After the service instance is started, it spawns four subprocesses:

- Forms runtime instance upload process, which uploads the Forms runtime instance files from the node to the Oracle E-Business Suite database periodically based on the load interval.

- On-demand runtime instance upload process, which uploads the Forms runtime instance files based on the custom message received from the AQ.

- On-demand Forms Runtime Diagnostics (FRD) and termination signaling process, which signals the Forms runtime process to generate an FRD log for FRD messages, or terminates the runtime process, producing a termination message. The message is the custom message received from the AQ.

- Forms runtime instance purge process, which purges the runtime instance tables and FRD log files. The numbers of days to keep these data are set as service parameters.

There is only one OAM Generic Collection Instance running per application system per node.

The OAM Generic Collection Service takes these parameters:

- NODE: the name of the node on which the service runs.

- LOADINTERVAL: the load interval for periodic runtime instance information uploading.

- ORACLE_HOME: the ORACLE_HOME in which the Forms Listener runs.

- RTI_KEEP_DAYS: the number of days to keep the runtime instance data in the database.

- FRD_KEEP_DAYS: the number of days to keep Forms Runtime Log files.

Concurrent Processing Charts and Reports

Concurrent Processing Charts

Main Navigation Path: Site Map > Monitoring (subtab) > Performance (heading) > Concurrent Processing Charts (link)

Overview

Oracle Applications Manager offers a number of configurable charts for monitoring the performance of concurrent processing.

There are the following groups of charts:

- Concurrent Requests

- Concurrent Managers
- Utilization

In the Concurrent Requests group, there are several charts, such as "Current Requests by Status," "Running Requests per Application," and "Pending Requests per Responsibility". In the Concurrent Managers group, there are charts such as "Pending Requests per Manager". In the Utilization group, there is a chart that depicts how many running requests and available processes exist per manager.

To view a chart, click its name in the table. In some cases, the charts are interactive and you can drill down on a particular bar or segment to see more details.

To set up a chart, click the **Chart Setting** icon. On the Change Chart Settings page, you can modify the chart type, refresh interval, and data items of a chart.

Concurrent Processing Activity Reports

Navigation: Site Map - Monitoring > Concurrent Processing Reports (under Usage)

Launch the Concurrent Processing Activity Reports from this page. The concurrent processing statistics reports enable you to analyze historical trends relating to request runtimes, success rates, and individual user requests.

- Concurrent Request Statistics by Program
- Concurrent Request Statistics by Username
- Concurrent Program Statistics by Name

Concurrent Request Statistics by Program

Navigation: Site Map - Monitoring > Concurrent Processing Reports (under Usage) > Concurrent Request Statistics by Program

This report summarizes concurrent request statistics by program. These statistics can be useful when scheduling requests or balancing load across nodes (using specialization rules). This report is based on data in the fnd_concurrent_requests table, and is limited to the data in that table since the last time the table was purged using the "Purge Concurrent Request and/or Manager Data" concurrent program.

By default, the report displays data for the past week. Use the Search Criteria region to filter the results based on Application, Minimum Duration, and the reporting time period. The default sort order is by Total duration in descending order. All duration values are in minutes.

- Application
- Program
- Total - the total of all individual runtimes for the program.

- Average - the average runtime for this program.

- Minimum - the shortest individual runtime for this program.

- Maximum - the longest individual runtime for this program.

- Times Run - the number of times this program has been run. This field drills down to the Search Results page showing the list of requests.

You can select a row for a concurrent program and click the Requests button to drill down to the Search Results page showing the list of requests.

Concurrent Request Statistics by Username

Navigation: Site Map > Concurrent Processing (under Activity) > Concurrent Request Statistics by Username

This report summarizes the concurrent request statistics by username. These statistics can be useful to determine the usage pattern of different users. The columns displayed in the report are:

- Username - click on the username to drill down to the User Details page.

- Requests Completed (number) - drills down to the Search Results page showing the list of requests.

- Total Runtime - the total runtime for all the requests submitted by the user (in hours).

By default, the report displays data for the past week grouped by username. Use the Search Criteria region to filter the results based on Username, Minimum Total Runtime, and the reporting time period.

You can select a row for a username and click the **Requests** button to drill down to the Search Results page showing the user's list of requests.

User Details

This page is accessed by drilling down on the Username field from those pages which display it.

The following contact information is displayed for the username (if available). Data is retrieved from the FND_USER table

- User Name

- Full Name

- Phone

- Phone

- E-mail
- Fax

Concurrent Request Statistics by Name

Navigation: Site Map > Monitoring > Concurrent Processing Reports (under Usage) > Concurrent Program Statistics by Name

This report provides a summary of statistics on concurrent programs. Summary information is collected when a request is completed, and stored in the table fnd_conc_prog_onsite_info.

Filter the display on this page by Application or Program name.

> **Note:** Statistics recorded here are as of the Reset Date. The reset date can be viewed on the Program Runtime Statistics page.

The report includes the following fields:

- Application - the application to which the concurrent request belongs
- Program - the program name drills down to the Program Runtime Statistics page.
- Average - the average runtime for this program in seconds.
- Minimum - the shortest individual runtime for this program in seconds.
- Maximum - the longest individual runtime for this program in seconds.
- Times Run - the total number of times the report has been run.
- Success Rate - the percent of the total requests that completed with a Normal status.
- Total Time - the total runtime in seconds for all completed submissions of this program.

By default, the report is ordered by Times Run in descending order. Click the View Details button to display the Program Runtime Statistics page for the selected program.

Program Runtime Statistics

The following fields are shown for the concurrent program selected from the Concurrent Program Statistics by Name page:

- Last Run Date - the date and time this program was last run.
- Last Run Request ID
- Reset Date - the date and time from which these statistics have been gathered.

- Times Successful - the number of times this program has completed with a status of Normal.

- Times Warning - the number of times this program has completed with a status of Warning.

- Times Error - the number of times this program has completed with a status of Error.

Viewing Concurrent Requests in Oracle Applications Manager

Oracle Applications Manager enables you to view details of concurrent requests. You can view concurrent requests by category or search for requests by specified criteria.

The Concurrent Requests pages can be accessed at:

Site Map > Monitoring > Concurrent Requests (under Current Activity)

Completed (Last Hour) Concurrent Requests

Choose either Table View or Chart View. The Chart View displays a graph of the completed requests by Status.

The Table View displays the following fields:

- Request ID

- Short Name

- Program Name

- Completion Status - the status in which the request completed. Valid statuses are Normal, Error, Warning, Cancelled, and Terminated.

- Requestor - drills down to the User Details page.

- Duration - the amount of time required for the request to run in hours, minutes, and seconds (HH:MM:SS).

- Started At - the time the request actually started running.

Also, you can click on "Show" under the Details column to see additional details for a request, such as

- Printing information

- Notification recipients

- Parameters

- Language
- Submission time and Completion time
- Schedule
- Parent Request - if the request had a parent click this button to view details information about this request

Use the buttons to perform the following:

- View Diagnostics for the request.
- Launch the Request Log in a separate browser window.
- Launch the Manager Log in a separate browser window.
- View the Request Output.

Inactive Requests

The list of inactive requests is shown with the following information:

- Request ID
- Short Name
- Program Name
- Status - possible values are Disabled, On Hold, or No Manager.
- Requestor - drills down to the User Details page.
- Priority - The priority of the concurrent program to be run. A concurrent program may be given a priority when it is initially defined. However, you can assign a new priority to a request here by typing in the new value and clicking the Apply button.
- Requested Start

Also, you can click on "Show" under the Details column to see additional details for a request, such as

- Printing information
- Notification recipients
- Parameters
- Language

- Submission time
- Schedule

Use the Remove Hold button to remove a hold on the inactive request.

Use the buttons to perform the following:

- View Diagnostics for the request.
- View Managers for the request.
- Cancel the request.

Pending Requests

Choose either Table View or Chart View. The Chart View displays a graph of the completed requests by Status.

The Table View displays the following fields:

- Request ID
- Short Name
- Program Name
- Status - possible values are Normal, Standby, Scheduled, and Waiting.
- Requestor - drills down to the User Details page.
- Priority - The priority of the concurrent program to be run. A concurrent program may be given a priority when it is initially defined. However, you can assign a new priority to a request here by typing in the new value and clicking the Apply button.
- Wait Time - the amount of time after the Requested Start time that the program has been waiting to run.
- Requested Start

Also, you can click on "Show" under the Details column to see additional details for a request, such as

- Printing information
- Notification recipients
- Parameters
- Language

- Submission time
- Schedule

Use the buttons to perform the following:

- View Diagnostics for the request.
- View Managers for the request.
- Place the request on Hold.
- Cancel the request.

Running Requests

Choose either Table View or Chart View. The Chart View displays a graph of the completed requests by Status.

The Table View displays the following fields:

- Request ID
- AUDSID - The database session ID for the request. Drills down to the Database Session Information page.
- Short Name
- Program Name
- Requestor - drills down to the User Details page.
- Responsibility
- Duration

Also, you can click on "Show" under the Details column to see additional details for a request, such as

- Printing information
- Notification recipients
- Parameters
- Language
- Submission time
- Schedule

Use the buttons to perform the following:

- View Diagnostics for the request.
- View the Internal Manager Environment for the request.
- View the Request Log.
- View the Manager Log.
- Cancel the request.

Concurrent Request Diagnostics

For completed, inactive, pending, and running requests, the following information is shown:

Request Status

- Phase - the phase may be Pending, Running, Completed, or Inactive
- Status
  - If the phase is Pending, the status may be: Normal, Standby, Scheduled, or Waiting.
  - If the phase is Running, the status may be: Normal, Paused, Resuming, or Terminating.
  - If the phase is Completed, the status may be: Normal, Error, Warning, Cancelled, or Terminated.
  - If the phase is Inactive, the status may be: Disabled, On Hold, or No Manager.
- Request ID
- Diagnostics
  - For completed requests - provides a completion message and reports the begin and end times for the request.
  - For inactive requests - reports the date and time that the request became inactive and the reason for this status. Provides options based on the status.
  - For pending requests - reports the reason for the status of the request and options available to the system administrator.

Run Times

This portion of the screen shows run time statistics for running, completed, and pending requests. All times are displayed in seconds.

- Average - the average time required to run this request.
- Minimum - the minimum time reported for the completion of this request.
- Maximum - the maximum time reported for the completion of this request.
- Estimated Completion - (displayed for running requests only) based on the statistics recorded for this request, the estimated time that the request will finish. If you need to shut down the system, use this indicator as a guide.
- Actual - (displayed for completed requests only) the actual time required for this request to run.

Waiting on Following Requests

This region of the page displays requests that are incompatible with the selected pending, running, or inactive request. Shown for each request are the following fields:

- Show Details - click this link to drill down to request details.
- Request ID
- Program
- Phase
- Status
- Requestor - click this link to drill down to the User Details page.
- Reason - the reason the selected request is waiting on this request.

You can perform the following actions on the requests listed:

- Hold - place the request on hold to allow the selected request to run.
- Cancel - cancel the request to allow the selected request to run.
- View - view the request details.

Internal Manager Environment

This page shows the environment variables and their values for the ICM environment. You can search for a particular variable using the filter.

Multilingual Support for Concurrent Requests

Users can submit a single concurrent request for a single concurrent program to be run multiple times, each time in a different language. Any output that is produced can be routed to different printers based on language. Users can also route completion notifications based on the language of the output.

For example, a user could submit a request for a Print Invoices program that would cause that program to run several times, each time in a different language, with each set of invoices printed on a different printer.

When submitting requests with multilingual support (MLS), separate requests are actually submitted; one request for each language. To distinguish these requests in the UI, such as the Monitor Requests page, the request names are prefixed with "<ISO language code>-<territory>".

Request Submission

A concurrent program can have a Multilingual Support (MLS) function associated with it. This function determines the set of languages over which the concurrent program will run. For example, the developer might associate a function with a Print Invoices program that would cause any request for that program to run in the preferred languages of the customers who have pending invoices.

If the concurrent program does not have an MLS function associated with it, then a user can choose when submitting the request the list of languages in which the program should run. The language of the current session is the default language.

If a concurrent program does have an MLS function associated with it, users will not be able to select languages for their requests. The associated MLS function determines the languages in which the request will run.

> **Note:** A concurrent program with an associated MLS function should have the "Use in SRS" box checked. If the "Use in SRS" box is not checked then the MLS function will be ignored. See: Concurrent Programs Window, *Oracle E-Business Suite System Administrator's Guide - Configuration*.

Runtime Behavior

Multilingual requests behave similarly to request sets. A user submits a single request. When that request runs, it submits a child request for each language in its list of languages. The parent request remains in the Running/Waiting state until its child requests are completed. If any child request completes with error status, then the parent request completes with error status. If no children complete with error status, but one or more completes with warning status, then the parent completes with warning status. Finally, if all children complete with normal status, then the parent completes with normal status.

MLS Functions

Developers can create an MLS function for concurrent programs. The MLS function determines in which of the installed languages a request should run. For example, an MLS function for a Print Invoices program could require that any request for that program to run only in the preferred languages of the customers who have pending invoices. This restriction saves system resources by assuring that the request does not run in languages for which no output will be produced. This restriction also prevents user error by automatically selecting the appropriate languages for a request.

MLS functions are PL/SQL stored procedures, written to a specific API. When the concurrent manager processes a multilingual request for a concurrent program with an associated MLS function, it calls the MLS function to retrieve a list of languages and submits the appropriate child requests for each language. The concurrent program application short name, the concurrent program short name, and the concurrent request parameters are all available to the MLS function to determine the list of languages that the request should be run in.

Beginning with Release 12.1, MLS functions can also support multiple territories and numeric character settings (",." for example).

MLS functions are registered in the Concurrent Program Executable form. A registered MLS function can be assigned to one or more concurrent programs in the Concurrent Programs form.

Related Topics

Oracle E-Business Suite User's Guide

Oracle E-Business Suite Concepts Guide

Oracle E-Business Suite Developer's Guide

Multiple Organizations Reporting

The Oracle E-Business Suite organization model dictates how transactions flow through different organizations and how those organizations interact with each other. You can define multiple organizations and the relationships among them in a single installation of Oracle E-Business Suite. These organizations can be sets of books, business groups, legal entities, operating units, or inventory organizations.

Multiple organizations reporting improve reporting capabilities of Oracle E-Business Suite products by allowing reporting across operating units.

Understanding Operating Units

An operating unit is an organization that uses *Oracle Cash Management*, *Order Management and Shipping Execution*, *Oracle Payables*, *Oracle Purchasing*, and *Oracle Receivables*. An operating unit is associated with a legal entity and may be a sales office, a division, or a department. Information is secured by operating unit for these applications and each user sees information only for their operating unit. To run any of these applications, you choose a responsibility associated with an organization classified as an operating unit.

> **Note:** The profile option *MO:Operating Unit* links an operating unit to a responsibility. You must set this profile option for each responsibility.

Running Reports

To run reports using multiple organizations reporting:

1. Navigate to the **Submit Requests** page.
2. Choose the report that you want to run.

   A list of available operating units displays.
3. Choose the operating unit for this report.
4. Continue scheduling and submitting the request as usual.

Related Topics

Multiple Organizations in Oracle E-Business Suite

The Output Post Processor

Concurrent processing uses the Output Post Processor (OPP) to enforce post-processing actions for concurrent requests. Post-processing actions are actions taken on concurrent request output. An example of a post-processing action is that used in publishing concurrent requests with XML Publisher. For example, say a request is submitted with an XML Publisher template specified as a layout for the concurrent request output. After the concurrent manager finishes running the concurrent program, it will contact the OPP to apply the XML Publisher template and create the final output.

The OPP runs as a service that can be managed through Oracle Applications Manager. One service instance of the OPP service is seeded by default. This seeded OPP service instance has one work shift with one process.

A concurrent manager contacts an available OPP process when a running concurrent request needs an OPP processing action. A concurrent manager uses a local OPP process (that, is, on the same node) by default, but will choose a remote OPP if no local OPP process is available.

There should always be at least one OPP process active in the system. If no OPP service is available, completed requests that require OPP processing will complete with a status of Warning.

An OPP service is multi-threaded and will start a new thread for each concurrent request it processes. You can control the number of simultaneous threads for an OPP service instance by adjusting the Threads per Process parameter for the instance. If all the OPP services have reached their respective maximum number of threads, the requests waiting to be processed remain in a queue to be processed as soon as threads become available. If request throughput has become slow, you may want to increase the number of threads per process for the OPP. It is recommended that you keep the number of threads per process between 1 and 20.

Delivery Options for Concurrent Request Output

Oracle XML Publisher offers a feature called Delivery Manager which delivers documents through e-mail, fax, and other delivery channels. Users can direct the output of their concurrent requests to any of the channels that Delivery Manager supports. This capability is present for single requests and request sets using the Forms-based request submission UI, and for single requests in the HTML-based request submission UI.

For more information on Delivery Manager and related setup in Oracle XML Publisher, see the Oracle E-Business Suite online help.

> **Note:** Delivery options using the HTML-based request submission UI is not supported currently for request sets.

In the Forms-based Standard Request Submission (SRS) window, users can enter their delivery options in a Delivery Options window available from a button in the "Upon Completion ... region in the SRS window. In the HTML-based request submission UI, delivery options in the Delivery step.

The following delivery channels are possible:

- Internet Printing Protocol (IPP) Printer
- E-mail
- Fax
- FTP

Request Submission

At the time of request submission, a user can enter details for the chosen delivery option(s) as described below.

IPP Printer

- Username/Password - A user can enter a username and password for the selected IPP printer, if required. These will override any default values entered by the system administrator when the IPP printer was registered.
- Copies - The number of copies. This must be greater than 0.
- Orientation - Portrait or Landscape.
- Language - Users can select a specific language or "All languages".

E-mail

The email delivery option requires that an Simple Mail Transfer Protocol (SMTP) host and port be defined in the profiles FND: SMTP Host (FND_SMTP_HOST) and FND: SMTP Port (FND_SMTP_PORT), respectively. The profile values for these can be viewed and updated on the site and user level by a System Administrator, and can be viewed and updated by users themselves.

- From - The user's default e-mail ID.
- Subject - Populated with a default value composed of the Oracle E-Business Suite instance, program name, and name of the user submitting the request.

To add a recipient for the e-mail, the user must click the **Add Another Row** button and add recipients.

- "To" Recipients - Required. Comma-separated e-mail IDs are supported.
- "Cc" Recipients - Optional. Comma-separated e-mail IDs are supported.
- For Language - The language for the report. If different languages are desired, additional rows can be used.

Fax

Printers that support faxing must be registered. See: Managing Delivery Options, page 2-35.

The Fax option here will list only those IPP printers that support faxing.

- IPP Printer/Fax Server - Required.
- Username/Password - A user can enter a username and password for the selected IPP printer, if required. These will override any default values entered by the system administrator when the IPP printer was registered.

- Fax Number
- For Language - The language for the report.

If different fax servers or languages are desired, additional rows can be used.

FTP

Both FTP and SFTP are supported. Secure FTP is indicated by checking the box "Secure FTP". Only password-authenticated SFTP is supported.

- Host Name - Required.
- Port - The default port value is 22.
- User Name - Required.
- Password - Required.
- Remote Directory - Required. If this is left blank, the file is transferred to the remote home directory.
- For Language - The language for the report.
- Secure FTP

Additional rows can be used for sending output to additional servers.

Managing Delivery Options

Use the Manage Delivery Options page available under the System Administration responsibility to search for, register, update, or delete these options. Currently, only the IPP printer delivery type is available.

To search for a delivery option:

You can search by delivery type.

> **Note:** Currently, the only delivery type available is IPP Printer type.

You can search by the delivery name given by the user at the time of the delivery option creation.

To create (register) a delivery option:

1. Enter a delivery name.
2. Enter a delivery type.

Note: Currently, only IPP Printer registration is supported.

3. Enter a host name an port. (Required)
4. Enter a username and password.

   A system administrator can enter a default username and password which can be overridden by a user during request submission.
5. Enter a printer name. (Required)
6. Enter the number for sided printing.

   The lookup codes in the following table are used:

Lookup Code	Meaning
1	One-sided printing
2	Two-sided printing

7. For the options Authentication, Encryption, Use Full URL, and Use Chunked Body, check the boxes as needed. These features are documented in the Delivery Manager documentation in the Oracle XML Publisher online help.
8. If the IPP Printer supports faxing, then the Support Fax box should be checked. This option will be used to enable the LOV for the fax server in the SRS Fax tab.

To update a delivery option:

You can update a delivery option definition except for the delivery name and delivery type. These fields are read-only.

You can select a delivery option to update from the search results table in the Search page.

To delete a delivery option:

You can delete a delivery option by selecting the Delete icon for it in the Search page. A confirmation message will be shown before deletion.

Reviewing Requests, Request Log Files, and Report Output Files

This essay explains how you, as System Administrator, can view and change the status of concurrent requests, and how to view request log and report output files.

How To View Request Status and Output

Use any of the following methods to view the status and output of concurrent requests.

Use the Requests Window

Use the Requests window to view the status of concurrent requests, and to view request log and report output files.

The System Administrator and Oracle Alert Manager have a privileged version of the Requests window that provides you with more capabilities than your end users. For example, using the Requests window, you can view the status of and log files for *all* concurrent requests (not just your own), including requests that completed unsuccessfully. On some platforms, you can even view the log files of running requests.

Using the same window, you can view your own report output online. You cannot, however, view report output from other users' requests.

From the Requests window, you can also:

- place and remove holds from any pending or inactive request
- cancel a pending request, or terminate a running request
- restart a request set.
- change the priority of any pending request
- view the manager log file
- determine where *any* pending request stands in the queue for each manager defined to accept the request
- determine when the concurrent manager is inactive and needs to be restarted.

Run the Completed Concurrent Requests Report

You can run a report that lists parameters and any error messages associated with concurrent requests that have completed running. See: Completed Concurrent Requests Report, *Oracle E-Business Suite System Administrator's Guide - Configuration*.

How to Modify Request Diagnostic Output

The Request Diagnostics window provides the user with request status information. This information consists of messages that explain the request's current status.

Collect Runtime Data

Set the profile option Concurrent:Collect Request Statistics to "Yes" to collect runtime statistics.

A concurrent request may be comprised of one or two processes: a Net8*i* shadow which consumes database server resources, and a front-end process such as a C executable. The time used by the CPU is collected for both of these types of processes.

Summarize and View Runtime Statistics

To review the statistics you must run the Purge Concurrent Request and/or Manager Data program to process the raw data and have it write the computed statistics to the FND_CONC_STAT_SUMMARY table. You can review the statistics on a request by request basis using the Diagnostics window from the Requests window.

Setting End User Report and Log File Access Privileges

The user profile option *Concurrent:Report Access Level* determines report output file and log file access privileges for your end users. As System Administrator, you can set this profile option to either "User" or "Responsibility."

All users can can review the log and report output files from requests that they submitted.

If you set the *Concurrent:Report Access Level* option to "Responsibility" at the User level, that user can also review the log and report output files from all requests submitted from the current responsibility.

If you set the *Concurrent:Report Access Level* option to "Responsibility" at the Responsibility level, any user of that responsibility can also view the log and report output files from all requests submitted by any other user of that responsibility.

Defining the Reports Viewer

The Oracle E-Business Suite Report File Viewer is used by default for viewing your text report files. You can also display text files in a browser or use another application such as Microsoft Word. You define your default viewer by setting a profile option.

Set the Viewer:Text Profile Option

If the Viewer:Text profile option is set to "Browser" then reports are sent to a web browser. If this profile option is left blank, the Report File Viewer is used instead.

If this profile option is left blank, a report or log file can still be viewed in a browser by first viewing it using the Report File Viewer, and then choosing "Copy File..." from the Tools menu.

Viewing HTML Report Output

You can view your reports with HTML output in a browser. Once an HTML report has been sent to a browser, it can be saved to the desktop by using the Save As functionality of the browser.

> **Note:** HTML reports are displayed by the browser in the character set of the server. This character set may or may not match the character set on the client. Therefore, it may be necessary to convert the output to the client character set when saving the report. If the browser supports character set conversion with Save As, there will be a poplist in the Save As dialog box. The user can then choose an encoding which matches the client character set.

Online Report Review using Other Applications

You can set up your Online Report Review implementation to enable viewing output files in other applications, such as Microsoft Word or Excel. To do this you associate MIME types with file output formats.

Users can then set their preferred MIME types for particular output formats using profile options, or the users may be prompted to choose the appropriate MIME type for a file at runtime.

You can register more than one MIME type file format with each output format. In the Viewer Options window, you enter in the file format, the MIME type, whether you want to utilize the value of the FND: Native Client Encoding profile option, and a description. The description is displayed to the user in the Profile Values window and the Submit Request form.

If the Allow Native Client Encoding box for the associated MIME type has been checked in the Viewer Options window, the Report Viewer will convert the output file into the character set specified by the profile option FND: Native Client Encoding.

When the report is viewed, it is first sent to a browser. The browser then uses the associated MIME type to display the report.

> **Important:** For printing, if users choose either HTML or PDF as the output type with Oracle Report programs, they must use appropriate printer drivers to handle the PDF and HTML file for printing their output. See: Overview of Printers and Printing, *Oracle E-Business Suite System Administrator's Guide - Configuration*.

> **Note:** For PDF files, the Adobe Acrobat Reader application must have options set as described below:

- For Acrobat 4, under File > Preferences > General: uncheck Web browser integration.
- For Acrobat 5 and 5.1, under Edit > Preferences: under options, unselect "Display PDF in Browser".
- For Acrobat 6 and higher, under Edit > Preferences > Internet: under Web browser options, unselect "Display PDF in browser".

See: Viewer Options Window, *Oracle E-Business Suite System Administrator's Guide - Configuration*

Changing the Status of Concurrent Requests and Request Sets

This essay explains how to change a request's phase and status, and how to change the priority of a Pending or Inactive request. It also discusses how to restart request sets and how to prioritize requests by placing request sets on hold.

Changing a Request's Phase and Status

A request is in one of four phases: Pending (waiting to be run), Running, Completed, or Inactive (unable to run). Within each phase, a request's condition is referred to as its status.

You can change the phase of a Pending, Running, or Inactive request by changing its status.

Pending and Inactive Requests

You may cancel Pending and Inactive requests. The request's phase and status becomes *Completed - Cancelled*.

You may place on hold Pending and Inactive requests. The request's phase and status becomes *Inactive - On Hold*. You can reverse this action by later selecting the request removing the hold.

Running Requests

You can terminate Running requests. The request's phase and status becomes *Completed - Terminated*.

Changing a Request's Status

You can change the status of a request, and its resulting phase, using the Requests window.

Changing the Priority of a Pending or Inactive request

Requests normally run according to start time, on "first-submitted, first-run" basis. However, a higher priority request starts before an earlier request.

As System Administrator, you can change the priority of any Pending or Inactive request using the Requests window.

Request Priority is associated with an application User

The priority of a user's requests defaults to the value you, as System Administrator, set for their *Concurrent:Priority* user profile option. Users cannot change the priority of their requests.

If a concurrent program has a defined priority, that priority overrides the user's profile option.

- Priorities range from 1 (highest) to 99 (lowest).
- The standard default is 50.
- Concurrent programs submitted by the Internal Concurrent Manager have a priority of zero (0), and override all other requests.

> **Tip:** If you need to change the priority of a request frequently, you should consider assigning that concurrent program its own priority.

Related Topics

Overview of Concurrent Processing, page 2-1

Life cycle of a concurrent request, page 2-2

Concurrent Processing User Profile Settings, page 2-55

Managing Request Sets

This section discusses how to restart request sets and how to yield a request set to higher priority requests.

Restarting Request Sets

If a request set completes with a status of *Error*, the **Restart** button, on the Oracle Applications Manager - View Completed Requests page is enabled. The system also automatically captures, records, and saves the information of the first stage that fails so that when the user clicks on the **Restart** button the request set can restart from that point.

Once the stage has been identified, the request set program submits the stage program in resubmit mode. In this mode, the program looks at the same stage from the previous run and determines which programs need to be rerun, (only those that ended in error), and runs those programs. If this stage completes successfully or has a *Warning* status, the system proceeds to the next stage using the normal mechanism of restarting the request set program.

> **Note:** Users may restart a request set multiple times. The logs for each stage and individual programs are maintained independent of the number of runs as each stage and program submission generates a new request. However, the logs and associated files for a request set are rewritten each time the set is restarted.

Holding Request Sets

In some circumstances, such as when a request set has a large number of stages and takes a long time to execute, administrators may want to yield a request set to higher priority requests. By utilizing the *Hold Request Set* feature, users can place a running request set on hold and effectively control the execution of request set stages.

The **Hold** and **Remove Hold** buttons are available on the OAM View Running Requests page. To hold a request set, simply select the request set and click the **Hold** button. Click **Remove Hold** when you want the request set to continue executing.

Controlling Concurrent Managers

This essay explains how to control your concurrent managers.

Manager States

Individual managers read requests to start concurrent programs and actually start programs running when certain conditions are satisfied, such as the manager's work shift definition, number of target processes, and specialization rules.

You can start, shut down, or reset the concurrent managers at any time. Oracle E-Business Suite provides an Internal Concurrent Manager that processes these commands. You can issue commands either to individual managers, or, by altering the state of the Internal Concurrent Manager, you can control every manager at once.

> **Note:** Start your concurrent managers on machines with hostnames of 30 or fewer characters. Managers may fail to start on machines with longer hostnames.

Starting Individual Managers

You can restart or activate managers on an individual basis. Restarting a concurrent manager forces the Internal Concurrent Manager to reread the definition for that concurrent manager. Activating a manager cancels a previous command to deactivate it, and allows the Internal Concurrent Manager to submit a request to start that manager when its work shift starts.

You should restart an individual manager when you:

- modify its work shift assignments
- modify a work shift's target number of processes
- modify its specialization rules
- change a concurrent program's incompatibility rules

Deactivating Individual Managers

When you shut down an individual manager, you can choose whether to abort all requests and deactivate the manager immediately, or to allow it to finish processing its current requests before deactivating.

If you choose to Deactivate the manager, requests that are currently running are allowed to complete.

When you terminate requests and deactivate an individual manager, requests that are currently running are immediately stopped and marked for resubmission (when the manager is activated).

Oracle E-Business Suite concurrent programs are designed so that no data is lost or duplicated when a terminated request is resumed after a shut down. This applies for shutdowns that are normal (e.g., using the "Deactivate concurrent manager" request) or abnormal (e.g., after a hardware failure).

> **Important:** When a manager is selected and explicitly deactivated, it remains that way until you select and explicitly activate that manager. As a prerequisite, the Internal manager must be activated beforehand.

Controlling the Internal Concurrent Manager

When you activate the Internal Concurrent Manager, you activate all other managers as well, except those managers that were deactivated on an individual basis.

When you deactivate the Internal Concurrent Manager, it issues commands to deactivate all active managers. Managers that were deactivated on an individual basis are not affected.

If you terminate requests and deactivate the Internal Concurrent Manager, it issues commands to all other managers to terminate their requests and deactivate. Requests that are currently running are immediately stopped and marked for resubmission when the managers are activated.

Verify Concurrent Manager Status

The Internal Concurrent Manager continuously monitors each concurrent manager's operating system process. This process monitoring is referred to as the Internal Concurrent Manager's PMON cycle. The length of the PMON cycle is one of the arguments passed by the STARTMGR command, which starts up the Internal Concurrent Manager.

You can instruct the Internal Concurrent Manager to immediately verify the operating status of your individual concurrent managers, or to perform a PMON check.

Startup Threshold for Concurrent Managers

Concurrent Managers are started from a Service Manager, which in turn is started by the Internal Concurrent Manager. You can set a threshold for the number of requests the Internal Concurrent Manager will make to start a concurrent manager after it fails to start.

During each ICM PMON cycle, the managers are verified and the system attempts to place a lock on each specific manager. If a manager is not up as expected, then the ICM submits a request to start it. However, a manager may have an underlying issue, such as a configuration issue or corrupted executable, that prevents it from starting. By setting a maximum number of attempts the ICM will make to start a manager over a set time, you can prevent the ICM from continuously making futile attempts to start these managers.

After the underlying problem is fixed, you can restart the manager from the Administer Managers window.

The startup threshold is defined by two profile options:

- CONC: Manager Startup Threshold Limit - This value determines the number of attempts to restart a manager before the system will stop and alert the system administrator. The default value of this profile is 10 (attempts).

- CONC: Manager Startup Threshold Time (minutes) - This value determines the length of time the attempts will be made to restart a manager. If the Threshold Limit as defined above is reached within this time limit, the attempts will stop until the underlying issue has been addressed. The default value of this profile is 60 minutes (1 hour).

If a manager has failed to start after the specified number of attempts (cycles), the manager will not be checked. You can fix the underlying problem, and after it is addressed, you can go to the Administer Managers window, select the manager, and click the **Fixed** button.

The concurrent manager startup threshold can be disabled by setting the profile option CONC: Manager Startup Threshold Limit to 0. This setting will cause the Threshold functionality to be ignored when managers are being checked for restarting.

Controlling Managers from the Administer Managers form

Use the Administer Concurrent Managers form to issue commands to your concurrent managers.

You can also have the Internal Concurrent Manager "manually" verify the status of your individual managers, and restart individual managers. See: Administer Concurrent Managers, *Oracle E-Business Suite System Administrator's Guide - Configuration*.

The following table describes control functions for the Internal Manager.

Control Function	Description
Activate concurrent manager	Activates the Internal manager and all other managers, except managers that were deactivated individually using "Deactivate concurrent manager".
Verify concurrent manager status	Manually executes the process monitoring (PMON) cycle.
Deactivate concurrent manager	Deactivates the Internal manager and all other managers.
Terminate requests and deactivate manager	All running requests (running concurrent programs) are terminated, and all managers are deactivated.

The following table describes control functions for any other manager.

Control Function	Description
Activate concurrent manager	If the manager is defined to work in the current work shift, it starts immediately. Cancels "Deactivate concurrent manager" and "Terminate requests and deactivate manager".

Control Function	Description
Restart concurrent manager	Internal manager rereads the manager's definition, and the rules for concurrent program incompatibilities. You should restart a manager when you: - Change work shift assignments - Modify the number of target processes - Modify specialization rules - Change concurrent program incompatibilities
Deactivate concurrent manager	Deactivates the manager. All requests (concurrent programs) currently running are allowed to complete before the manager shuts down. A manager will not restart until you select the manager and choose "Activate concurrent manager".
Terminate requests and deactivate manager	All running requests (running concurrent programs) handled by the manager are terminated. Once deactivated, a manager will not restart until you select the manager and choose "Activate concurrent manager".

Controlling the Internal Concurrent Manager from the Operating System

To start the Internal Concurrent Manager, use the shell script adcmctl.sh.

Alternatively, use one of two other commands you may use from the operating system to control the Internal Concurrent Manager: STARTMGR, which starts the Internal Concurrent Manager; and CONCSUB, which can be used to deactivate or abort the Internal Concurrent Manager, or to instruct the Internal Concurrent Manager to verify the operating system process for each individual manager.

The following table compares the Internal manager control states displayed by the Administer Concurrent Managers form with their corresponding operating system command. Not all arguments are shown.

From the Administer Concurrent Managers Form	From the Operating System (not all arguments shown)
Activate concurrent manager	STARTMGR (syntax may vary with platform)
Verify concurrent manager status	CONCSUB FND VERIFY

From the Administer Concurrent Managers Form	From the Operating System (not all arguments shown)
Deactivate concurrent manager	CONCSUB FND DEACTIVATE
Terminate requests and deactivate manager	CONCSUB FND ABORT

Starting the Internal Concurrent Manager from the Operating System

To start the Internal Concurrent Manager, use the shell script adcmctl.sh.

This command starts the Internal Concurrent Manager, which in turn starts any concurrent managers you have defined.

Alternatively, to start the concurrent managers, you can invoke the STARTMGR command from your operating system prompt.

You must have write privileges to the "out" and "log" directories of every application so that the concurrent managers can write to these directories. You can start the concurrent managers with many different options. An option on some operating systems is to send an electronic mail note to a given user when the concurrent managers shut down. See your installation guide for a discussion of this command.

Use the STARTMGR command:

- during installation of Oracle E-Business Suite
- after you shut down the concurrent managers
- after MIS restarts the operating system
- after the database administrator restarts the database

The STARTMGR command takes up to ten optional parameters.

- Each parameter except PRINTER has a default.
- You can modify the STARTMGR command and your environment to set your own defaults.

Enter the following command at your system prompt to start the Internal Concurrent Manager:

```
$ startmgr  <optional parameters>
```

You can pass the parameters in any order. For example:

```
$ startmgr sysmgr="<username>/<password>"  mgrname="std"
 printer="hqseq1"  mailto="jsmith"  restart="N"
 logfile="mgrlog"  sleep="90"  pmon="5"  quesiz="10"
```

The startmgr script accepts an Oracle username/password as the sysmgr parameter. Alternatively, you could pass an Oracle E-Business Suite username/password as an appmgr parameter. If no sysmgr or appmgr parameter is provided on the command line, startmgr will prompt you for the Oracle password.

See: Setting Up Concurrent Managers, *Oracle E-Business Suite System Administrator's Guide - Configuration*

Viewing the Internal Concurrent Manager startup parameters

The Internal Concurrent Manager's log file displays startup parameter values executed by the STARTMGR command. An example is shown below. You cannot change the parameter values.

```
logfile=/fnddev/fnd/6.0/log/FND60.mgr  (path is port-specific)
 PRINTER=hqunx138
 mailto=appldev
 restart=N
 diag=N
  sleep=60 (default)
 pmon=20 (default)
 quesiz=1  (default)
```

Shutting down the Internal Concurrent Manager from the Operating System

From the operating system prompt, you can use the CONCSUB utility to submit a concurrent request, under the SYSADMIN username and the System Administrator responsibility.

The CONCSUB utility submits a concurrent request and returns you to the operating system prompt. You must wait until the concurrent request completes.

To check on the status of your concurrent request, use the Concurrent Requests form.

```
CONCSUB username/password 'Responsibility application shortname'
 'Responsibility name' 'Username' [WAIT={Y|N|n}] CONCURRENT
 'Program application shortname' PROGRAM
```

Parameters

username/password

The ORACLE username and password that connects to Oracle Application Object Library data. Alternatively, an Oracle E-Business Suite username and password for a user with the System Administrator responsibility.

Responsibility application shortname

The application shortname of the responsibility. For the System Administrator responsibility, the application shortname is SYSADMIN.

Responsibility name

The name of the responsibility. For the System Administrator responsibility, the responsibility name is

System Administrator.

Username

The application username of the person who submits the request. For example, SYSADMIN is the username of the System Administrator.

WAIT={Y|N|*n*}

Set WAIT to Y if you want CONCSUB to wait until the request you submitted completes before CONCSUB returns you to the operating system prompt.

Set WAIT to N (the default value) if you do not want CONCSUB to wait.

You can also enter an integer value of *n* seconds for CONCSUB to wait before it exits.

When used, WAIT must be entered before CONCURRENT.

Program application shortname

The application shortname of the program. For the DEACTIVATE, ABORT, and VERIFY programs, the application shortname is FND.

PROGRAM

To submit the Shutdown All Managers concurrent request, use the program DEACTIVATE.

To submit the Shutdown Abort Managers concurrent request, use the program ABORT.

To submit the Verify All Managers Status concurrent request, use the program VERIFY.

Example Syntax using CONCSUB

```
CONCSUB <Username/Password> SYSADMIN 'System Administrator'
 SYSADMIN  CONCURRENT FND DEACTIVATE

CONCSUB <Username/Password> SYSADMIN 'System Administrator'
 SYSADMIN  CONCURRENT FND ABORT

CONCSUB <Username/Password> SYSADMIN 'System Administrator'
 SYSADMIN  CONCURRENT FND VERIFY
```

Using CONCSUB to shut down your managers

Use CONCSUB to shut down the concurrent managers:

- before MIS shuts down the operating system

- before the database administrator shuts down the database

- when you want concurrent manager and concurrent program definitions to take effect

Then, use the STARTMGR command to restart the Internal Concurrent Manager, which starts the concurrent managers.

Example - nightly shutdown using CONCSUB

You can use the token WAIT with value Y (WAIT=Y) if you want to use CONCSUB to issue a concurrent request from within a shell script containing a sequence of steps. Using the token WAIT insures the managers deactivate, abort, or verify status before the shell script proceeds to the next step.

See: Controlling the Internal Concurrent Manager from the Operating System, page 2-46

1. Shell script customized for specific operating system starts.

2. CONCSUB *username/password* SYSADMIN'System Administrator' SYSADMIN WAIT=Y CONCURRENTFND DEACTIVATE

   When the shell script passes control to CONCSUB, CONCSUB waits until the program DEACTIVATE is complete before it returns control to the shell script.

3. Script issues the command to shut down the database.

4. Script issues the command to backup the database.

5. Script issues the command to startup the database.

6. $ startmgr sysmgr="apps/fnd" mgrname="std" printer="hqseq1" mailto="jsmith" restart="N" logfile="mgrlog" sleep="90" pmon="5" quesiz="10"

   The shell script passes control to STARTMGR, which starts up the Internal manager (and all the other managers).

7. Shell script completes.

Hiding the password using CONCSUB

If the username/password are still supplied, the CONCSUB utility will work as usual.

If username only is supplied (no '/password' in the first argument), it will prompt you for an Oracle E-Business Suite username and password.

In the following example, CONCSUB would connect using the .dbc file, and then only run if the Oracle E-Business Suite user "sysadmin" with password "sysadmin" is successfully authenticated.

```
CONCSUB Apps:User SYSADMIN 'System Administrator' SYSADMIN/sysadmin
 CONCURRENT FND VERIFY
```

The user can put the password in a file, and then redirect it to standard input (stdin). In

UNIX the command would be executed as follows:

```
CONCSUB Apps:User SYSADMIN 'System Administrator' SYSADMIN
 CONCURRENT FND
FNDMNRMT Y 0 20221 < password.file
```

where password.file is an ASCII file that contains the password. This method is recommended for use in shell scripts or batch processes.

Managing Concurrent Processing Files and Tables

This section explains how to maintain the number of log and output files the operating system retains, and how to manage Application Object Library database tables that store information about concurrent requests and concurrent manager processes.

The database tables that are affected by running the Purge Concurrent Request and/or Manager Data program are:

FND_CONCURRENT_REQUESTS

This table contains a complete history of all concurrent requests.

FND_RUN_REQUESTS

When a user submits a report set, this table stores information about the reports in the report set and the parameter values for each report.

FND_CONC_REQUEST_ARGUMENTS

This table records arguments passed by the concurrent manager to each program it starts running.

FND_DUAL

This table records when requests do not update database tables.

FND_CONCURRENT_PROCESSES

This table records information about Oracle E-Business Suite and operating system processes.

FND_CONC_STAT_LIST

This table collects runtime performance statistics for concurrent requests.

FND_CONC_STAT_SUMMARY

This table contains the concurrent program performance statistics generated by the

Purge Concurrent Request and/or Manager Data program. The Purge Concurrent Request and/or Manager Data program uses the data in FND_CONC_STAT_LIST to compute these statistics.

Maintenance Suggestions

Your MIS department and application users should agree on an archiving and file retention policy that is appropriate for your organization. To avoid running out of space on your disk drives, you should periodically delete Oracle E-Business Suite log files and output files.

> **Tip:** You can run the program "Purge Concurrent Request and/or Manager Data" once and automatically resubmit the program for you at specific time intervals.

There are some sample guidelines for when to run the Purge Concurrent Requests and/or Manager Data program. Adopt these guidelines according to your user community's usage of Oracle E-Business Suite.

- every 30 days for normal usage
- every two weeks (14 days) for heavy usage
- if using the AGE mode, set the Mode Value to 5 to retain the five most recent days of concurrent request data, log files, and report output files.

Purging removes Audit data

When you purge concurrent request information, you lose audit details. The Signon Audit Concurrent Requests report uses this audit information.

Managing Parallel Concurrent Processing

This section describes how to manage parallel concurrent processing.

Parallel concurrent processing is always active when Generic Service Management (GSM) is active. Parallel concurrent processing can no longer be activated independently of Generic Service Management.

However, automatic activation of PCP does not additionally require that primary nodes be assigned for all concurrent managers and other GSM-managed services. If no primary node is assigned for a service instance, the Internal Concurrent Manager (ICM) assigns a valid concurrent processing server node as the target node. In general, this node will be the same node where the Internal Concurrent Manager is running. In the case where the ICM is not on a concurrent processing server node, the ICM chooses an active concurrent processing server node in the system. If no concurrent processing server node is available, no target node will be assigned.

Note that if a concurrent manager does have an assigned primary node, it will only try to start up on that node; if the primary node is down, it will look for its assigned secondary node, if one exists. If both the primary and secondary nodes are unavailable, the concurrent manager will not start (the ICM will not look for another node on which to start the concurrent manager). This strategy prevents overloading any node in the case of failover.

The concurrent managers are aware of many aspects of the system state when they start up. When an ICM successfully starts up it checks the TNS listeners and database instances on all remote nodes and if an instance is down, the affected managers and services switch to their secondary nodes. Processes managed under GSM will only start on nodes that are in Online mode. If a node is changed from Online to Offline, the processes on that node will be shut down and switch to a secondary node if possible.

Concurrent processing provides database instance-sensitive failover capabilities. When an instance is down, all managers connecting to it switch to a secondary middle-tier node.

However, if you prefer to handle instance failover separately from such middle-tier failover (for example, using TNS connection-time failover mechanism instead), use the profile option Concurrent:PCP Instance Check. When this profile option is set to OFF, Parallel Concurrent Processing will not provide database instance failover support; however, it will continue to provide middle-tier node failover support when a node goes down.

Defining Concurrent Managers

You define concurrent managers either in the Create New Request Processing Manager page in Oracle Applications Manager or in the Concurrent Managers form. When you define a manager, you specify the manager type, which may be either Concurrent Manager, Internal Monitor, or Transaction Manager.

There are three other types of managers that Oracle E-Business Suite predefines for you: the Internal Concurrent Manager, which describes the Internal Concurrent Manager process, the Conflict Resolution Manager, and the Scheduler. For the Conflict Resolution Manager and Scheduler you can assign the primary and secondary nodes. For the Internal Concurrent Manager you assign the primary node only.

To each concurrent manager and each Internal Monitor Process, you may assign a primary and a secondary node. You may also assign primary and secondary system queue names, if a platform-specific queue management system is available on your platform. See: Concurrent Managers, *Oracle E-Business Suite System Administrator's Guide - Configuration*.

Administering Concurrent Managers

Target Nodes

Using the Services Instances page in Oracle Applications Manager (OAM) or the

Administer Concurrent Managers form, you can view the target node for each concurrent manager in a parallel concurrent processing environment. The target node is the node on which the processes associated with a concurrent manager should run. It can be the node that is explicitly defined as the concurrent manager's primary node in the Concurrent Managers window or the node assigned by the Internal Concurrent Manager.

If you have defined primary and secondary nodes for a manager, then when its primary node and ORACLE instance are available, the target node is set to the primary node. Otherwise, the target node is set to the manager's secondary node (if that node and its ORACLE instance are available). During process migration, processes migrate from their current node to the target node.

Control Across Nodes

Using the Services Instances page in Oracle Applications Manager or the Administer Concurrent Managers form, you can start, stop, abort, restart, and monitor concurrent managers and Internal Monitor Processes running on multiple nodes from any node in your parallel concurrent processing environment. You do not need to log onto a node to control concurrent processing on it. You can also terminate the Internal Concurrent Manager or any other concurrent manager from any node in your parallel concurrent processing environment.

In an environment enabled with parallel concurrent processing, primary node assignment is optional for the Internal Concurrent Manager. The Internal Concurrent Manager can be started from any of the nodes (host machines) identified as concurrent processing server enabled. In the absence of a primary node assignment for the Internal Concurrent Manager, the Internal Concurrent Manager will stay on the node (host machine) where it was started. If a primary node is assigned, the Internal Concurrent Manager will migrate to that node if it was started on a different node.

If the node on which the Internal Concurrent Manager is currently running becomes unavailable or the database instance to which it is connected to becomes unavailable, the Internal Concurrent Manager will be restarted on a alternate concurrent processing node. If no primary node is assigned, the Internal Concurrent Manager will continue to operate on the node on which it was restarted. If a primary node has been assigned to the Internal Concurrent Manager, then it will be migrated back to that node whenever both the node and the instance to which the Internal Concurrent Manager connects to from that node becomes available

Starting Up Managers

You start up parallel concurrent processing as you would ordinary concurrent processing, by running the adcmctl.sh script from the operating system prompt.

The Internal Concurrent Manager starts up on the node on which you run the adcmctl.sh script. If it has a different assigned node, it will migrate to that node if available.

After the Internal Concurrent Manager starts up, it starts all the Internal Monitor

Processes and all the concurrent managers. It attempts to start Internal Monitor Processes and concurrent managers on their primary nodes, and resorts to a secondary node only if a primary node is unavailable.

Shutting Down Managers

You shut down parallel concurrent processing by issuing a "Stop" command in the OAM Service Instances page or a "Deactivate" command in the Administer Concurrent Managers form. All concurrent managers and Internal Monitor processes are shut down before the Internal Concurrent Manager shuts down.

Terminating Concurrent Processes

You can terminate running concurrent processes for a concurrent manager on the local node or on remote nodes by issuing an "Abort" command from the OAM Service Instances page or a "Terminate" command from the Administer Concurrent Managers form.

Migrating Managers

Most process migration occurs automatically in response to the failure or subsequent availability of a primary node. However, you may migrate processes manually by changing the node assignments for a concurrent manager or Internal Monitor Process using the Concurrent Managers form. To put your changes into effect, issue a "Verify" command against the Internal Concurrent Manager from the Administer Concurrent Managers form.

Related Topics

Concurrent Managers, *Oracle E-Business Suite System Administrator's Guide - Configuration*

Concurrent Processing User Profile Settings

This essay explains the user profile option settings relevant to submitting concurrent requests.

Setting Concurrent Processing Options

End users can control certain runtime options for their concurrent requests. For example, you can choose a specific date on which to start a request.

If a user does not explicitly enter these options at the time of the request, concurrent processing options default to their user profile values.

As System Administrator, you set user profile values for your end users with the System Profile Values window. Both you and your end users can set some of your own profile values using the Personal Profile Values form.

Changing Concurrent Processing Options for submitted requests

You or your users can use the Requests window to change the concurrent processing options for a submitted request up until the time it starts running.

- As System Administrator you can change all concurrent options for any request.

- Your users can change most of their request's concurrent options.

  End users cannot change (nor set) the priority of their request, or the report access level for viewing request log files and report output files online.

The following table lists the concurrent processing user profile options and an explanation of each:

User Profile Option	Explanation
Concurrent: Hold Requests	"Yes" places concurrent requests on hold. "No" starts programs according to the request's priority and start time.
Concurrent: Multiple Time Zones	"Yes" ensures that requests are scheduled immediately regardless of the time zone your client is running in.
Concurrent: Report Access Level	Viewing a request's output/log files online and reprinting reports can be accessed according to: "Responsibility" - by anyone using the responsibility that submitted the request "User ″ - by only the user who submitted the request.
Concurrent: Report Copies	The number of output copies that print for each report.
Concurrent: Request Priority	Requests normally run according to start time, on a "first-submitted, first-run" basis. Priority overrides request start time. A higher priority request starts before an earlier request. Priorities range from 1 (highest) to 99 (lowest). The standard default is 50.
Concurrent: Request Start Time	The date and time requests are available to start running. If the start date and time is at or before the current date and time, requests may be run immediately.

User Profile Option	Explanation
Concurrent: Save Output	"Yes" saves concurrent program outputs in a standard file format. Some concurrent programs do not generate an output file.
Concurrent: Sequential Requests	"Yes" forces requests to run one at a time (sequentially) according to the requests' start dates and times. "No" means requests canrun concurrently when their concurrent programs are compatible.
Concurrent: Wait for Available TM	You can specify the maximum number of seconds that the client will wait for a given transaction manager (TM) to become available before moving on to try a different TM.
Concurrent: URL Lifetime	This profile option determines the length of time in minutes a URL for a request ouput is retained before it is deleted from the system.
Printer	The printer which prints your reports.

Updating Concurrent Request Profile Options

Most concurrentuser profile options may be set by the System Administrator at all four levels: site, application, responsibility, and user. The user profile *Concurrent:Report Access Level* may not be set at the application level.

Your users can change the default values for most of the concurrent processing profile options. However, they cannot set Concurrent: Request Priority, or Concurrent: Report Access Level.

Related Topics

Overview of Concurrent Processing, page 2-1

Managing Concurrent Programs and Requests

This section describes reports used in managing concurrent programs and reports. The following topics are covered in this chapter:

- Request Sets Report

- Report Group Responsibilities Report

- Concurrent Program Details Report

- Concurrent Programs Report

Request Sets Report

This report documents request set definitions, including the set's owner, program incompatibilities, as well as printer and print style information. Use this report when defining or editing request set definitions.

Report Parameters

None.

Report Headings

The report headings provide you with general information about the contents of the report.

Related Topics

Overview of Concurrent Programs and Requests, *Oracle E-Business Suite System Administrator's Guide - Configuration*

Organizing Programs into Request Sets, *Oracle E-Business Suite System Administrator's Guide - Configuration*

Concurrent Programs Report, page 2-60

Report Group Responsibilities Report

This report lists those responsibilities which have access to a report or a request set. Use this report when granting access privileges to reports and request sets, either by assigning reports and request sets to request security groups, or when assigning owners to a request set.

Report Parameters

Application Name

Choose the application name associated with the report or request set.

Report Name/Request Set Name

Either choose the name of a report or request set.

Related Topics

Overview of Concurrent Programs and Requests, *Oracle E-Business Suite System Administrator's Guide - Configuration*

Organizing Programs into Request Groups, *Oracle E-Business Suite System Administrator's Guide - Configuration*

Request Groups, *Oracle E-Business Suite System Administrator's Guide - Configuration*

Concurrent Program Details Report

This report documents concurrent program definitions, including executable file information, execution method, incompatible program listings, and program parameters. If a concurrent program generates a report, column and row information, as well as print output and print style, are also documented.

Use this report when considering concurrent program modifications, such as modifying program incompatibility rules.

Report Parameters

> **Caution:** If you do not enter any parameters, the report returns values for *all* concurrent programs, and may be very lengthy.

Application Name

Choose the application name associated with the concurrent program whose program definition details you wish to report on.

Choose only an application name, without a program name, if you wish to run a program definition details report on all concurrent programs associated with an application.

Program

Choose the name of a concurrent program whose program definition details you wish to report on. You must enter a value for Application Name before entering a value for Program.

Report Headings

The report headings display the specified report parameters and provide you with general information about the contents of the report.

Concurrent Programs Report, page 2-60

Concurrent Programs Report

This report shows which concurrent programs are currently enabled nand which programs are disabled.

Use this report to record the execution method, argument method, run alone status, standard submission status, request type, and print style information associated with your concurrent programs.

Report Parameters

Application Name

Choose the application name associated with the concurrent programs whose program information you wish to report on.

If you do not enter an application name, the report will return values for *all* concurrent programs.

Report Headings

The report headings display the specified report parameters and provide you with general information about the contents of the report.

Related Topics

Overview of Concurrent Programs and Requests, *Oracle E-Business Suite System Administrator's Guide - Configuration*

Concurrent Program Details Report, page 2-59

Concurrent Programs, *Oracle E-Business Suite System Administrator's Guide - Configuration*

Purge Concurrent Request and/or Manager Data Program

Use this program to delete:

- request log files, concurrent manager log files, and report output files from your product directories maintained by the operating system
- records (rows) from Application Object Library database tables that contain history information about concurrent requests and concurrent manager processes.

Use this program to compute performance statistics for each of the concurrent programs, if the Concurrent: Collect Request Statistics profile option is set to "Yes".

Report Options

Entity

All

Purges records from database tables that record history information for concurrent requests, history information for concurrent managers, and purges request log files, manager log files, and report output files from the operating system.

Manager

Purges records from database tables that record history information for concurrent managers, and purges manager log files from the operating system.

Request

Purges records from database tables that record history information for concurrent requests, and purges request log files and report output files from the operating system.

Mode

Age

Enter the number of days for which you want to save concurrent request history, log files, and report output files. The purge program deletes all records older (in days) than the number you enter.

For example, if you enter "5", then all concurrent request history, log files, and report output files older than five days is purged.

Count

Enter the number of (most recent) records for which you want to save concurrent request history, log file, and report output files. The purge program starts from the most recent records, retains the number you enter, and purges all remaining records.

For example, if you enter "5", then the five most recent concurrent request history records, request log files, manager log files, report output files are saved, and all remaining records are purged.

Mode Value

Enter a value to define the number of days for Mode=Age or the number of records for Mode=Count. The valid values are 1 - 9999999.

Oracle ID

Enter the Oracle ID that concurrent programs connect to for which you want to purge concurrent request records, and associated log files and report output files. Oracle ID has relevance when the Entity is either "Request" or "All".

For example, if you enter AP1, then the program purges all request records, log files, and report output files associated with requests to run programs that connect to the AP1 Oracle ID.

User Name

Enter the application username whose concurrent request records and associated log files and report output files you wish to purge. Username has relevance when the Entity is either "Request" or "All".

For example, if you enter JSMITH, then the program purges all request records, log files, and report output files associated with requests submitted by user JSMITH.

Select the application associated with the responsibility for which you want to purge concurrent request records, and associated log files and report output files. Responsibility Application is used with the *Responsibility* option, and has relevance when the Entity is either "Request" or "All".

Responsibility

Select the responsibility for which you want to purge concurrent request records, and associated log files and report output files. Responsibility has relevance when the Entity is either "Request" or "All".

For example, if you select the System Administrator responsibility, then the program purges all request records, log files, and report output files associated with requests submitted by users operating under the System Administrator responsibility.

Program Application

Select the application for which you want to purge concurrent request records, and associated log files and report output files. Program Application has relevance when the Entity is either "Request" or "All".

For example, if you select Oracle Payables, then the program purges all request records, log files, and report output files associated with requests to run Oracle Payables programs.

Program

Select the program for which you want to purge concurrent request records, and associated log files and report output files. Program has relevance when the Entity is either "Request" or "All".

For example, if you select Program X, then the purge program purges all request records, log files, and report output files associated with requests to run Program X.

Manager Application

Select the application associated with the concurrent manager for which you want to purge concurrent request records, and associated log files and report output files.

Manager Application is used with the *Manager* option, and has different effects when Entity is set to "Request, and when Entity is set to "Manager" or "All".

- When Entity is set to "Request", the program purges all request records, log files, and report output files associated with requests run by the concurrent manager named in the *Manager* option.
- When Entity is set to either "Manager" or "All", in addition to the above, the program also purges all manager log files associated with the concurrent manager named in the *Manager* option.

Manager

Select the concurrent manager for which you want to purge concurrent request records, and associated log files and report output files.

Manager is used with the *Manager Application* option, and has different effects when Entity is set to "Request," and when Entity is set to "Manager" or "All".

- When Entity is set to "Request", the program purges all request records, log files, and report output files associated with requests run by the concurrent manager named in the *Manager* option.
- When Entity is set to either "Manager" or "All", in addition to the above, the program also purges all manager log files associated with the concurrent manager named in the *Manager* option.

Report

Select whether you want a report listing the number of records purged by the Purge Concurrent Request and/or Manager Data program.

No	Run the program but do not generate a report.
Yes	Run the program and generate a report.

Purge Other

Select whether you want to delete records from the FND_DUAL table.

No	.Do not delete records from FND_DUAL.

Yes	Delete records from FND_DUAL.

Related Topics

Overview of Concurrent Processing, page 2-1

Life cycle of a concurrent request, page 2-2

Reviewing Requests, Request Log Files, and Report Output Files, page 2-36

3

Oracle Workflow Manager

Oracle Workflow Manager Overview

Oracle Workflow Manager is a component of Oracle Applications Manager that allows system administrators to manage Oracle Workflow for multiple Oracle E-Business Suite instances from a single console.

Using Oracle Workflow Manager, administrators can control Workflow system services, such as notification mailers, agent listeners, and other service components, background engines, purging obsolete Workflow data, and cleanup of the Workflow control queue. Administrators can also monitor work item processing by viewing the distribution of all work items by status and drilling down to additional information. Additionally, they can monitor event message processing for local Business Event System agents by viewing the distribution of event messages by status as well as queue propagation schedules. With this ability to monitor work items and event messages, a system administrator can identify possible bottlenecks easily.

To access Oracle Workflow Manager, log into Oracle Applications Manager and select an applications system. Then, you can follow one of the following navigation paths:

- Choose Workflow Manager from the pull-down menu in the Applications Dashboard page and click the Go button.

- Choose Site Map, choose the Administration tab, and then choose the Home link in the Workflow region of the Site Map page. You can also choose one of the other links in the Workflow region to navigate directly to the corresponding page within Oracle Workflow Manager.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go

You can also use other features to help manage Oracle Workflow.

- Use Oracle Diagnostics Framework to run diagnostic tests that check the setup of your Oracle Workflow installation and review debugging information.

- Use Oracle E-Business Suite Logging to review Oracle Workflow logs. Oracle Workflow uses the Oracle E-Business Suite Logging framework to standardize and centralize in the database logging activities related to the Oracle Workflow Business Event System and Oracle XML Gateway.

  > **Note:** The Java middle tier components of Oracle Workflow, including notification mailers and agent listeners, also use Oracle E-Business Suite Logging; however, due to the high volume of messages that pass through these components, their information is logged to the file system by default.

Gathering Oracle Workflow Statistics

Some Oracle Workflow Manager graphs and lists may summarize large volumes of data, depending on the level of activity in your Oracle E-Business Suite instance. To enhance performance in displaying these statistics, Oracle Workflow Manager periodically runs concurrent programs to gather the statistics and displays the graphs and lists based on the latest data from the concurrent programs.

- Workflow Agent Activity Statistics Concurrent Program (FNDWFAASTATCC) - Gathers statistics for the Agent Activity graph in the Workflow System status page and for the agent activity list in the Agent Activity page.

- Workflow Mailer Statistics Concurrent Program (FNDWFMLRSTATCC) - Gathers statistics for the throughput graph in the Notification Mailer Throughput page.

- Workflow Work Items Statistics Concurrent Program (FNDWFWITSTATCC) - Gathers statistics for the Work Items graph in the Workflow System status page, for the Completed Work Items list in the Workflow Purge page, and for the work item lists in the Active Work Items, Deferred Work Items, Suspended Work Items, and Errored Work Items pages.

These concurrent programs are scheduled to run every 24 hours by default. They do not require any parameters. You can optionally cancel the default scheduled requests and run the programs with a different schedule if you want to gather statistics at a different frequency.

Each of these graphs and lists displays the date and time when its statistics were last updated, as well as a refresh icon that you can select to refresh the statistics immediately if necessary. However, note that if your Oracle E-Business Suite instance contains very large volumes of workflow data, you may encounter delays or page timeouts when refreshing the data.

> **Note:** Oracle Workflow Manager statistics that typically represent smaller volumes of data, such as work item details and work item

activity details, are queried directly rather than through the concurrent programs.

Oracle Workflow System Status

The Workflow System status page provides a high-level view of the status of your Oracle Workflow instance. The page displays the date and time when the system status information was last updated. To refresh this information, click the refresh icon. To add the information from this page to your support cart, click the Add to Support Cart button.

> **Note:** The system status information is queried directly, separately from the concurrent programs that gather other Oracle Workflow statistics.

The Workflow System status page shows the up, down, or unavailable summary status of the following Workflow features:

- Notification Mailers - To manage notification mailer service components, click the Notification Mailers status icon.
- Agent Listeners- To manage agent listener service components, click the Agent Listeners status icon.
- Service Components - To manage all types of service components, click the Service Components status icon.
- Background Engines - To view Workflow Background Process concurrent requests, click the Background Engines status icon.
- Purge - To view summary information about Purge Obsolete Workflow Runtime Data concurrent requests and completed work items, click the Purge status icon.
- Control Queue Cleanup - To view Workflow Control Queue Cleanup concurrent requests, click the Control Queue Cleanup status icon.

For service component features, including notification mailer service components, agent listener service components, and all types of service components grouped together, the summary status icons represent the following statuses:

- Down - At least one service component of this type has a status of Stopped with Error or System Deactivated. You should investigate the error.
- Up - At least one service component of this type has a status of Running or Suspended, and no service components of this type have a status of Stopped with Error or System Deactivated.

- Unavailable - No service components of this type have a status of Running, Suspended, Stopped with Error, or System Deactivated. For example, if all service components of this type either have not yet been completely configured, or have stopped without errors, then the Unavailable summary status is displayed.

To submit a concurrent request for a feature that runs as a concurrent program, choose the program you want from the Submit Request For pull-down menu and click the Go button. You can submit requests for the following programs:

- Background Engines
- Purge
- Control Queue Cleanup

Related Database Parameters

This region displays information about database initialization parameters required for Oracle Workflow. For each parameter, the list shows the parameter name, actual parameter value, recommended value, and description. If the actual value does not match the recommended value, the recommended value is marked with a warning indicator icon.

The JOB_QUEUE_PROCESSES parameter defines the number of job queue processes for your instance. Oracle Workflow requires job queue processes to handle propagation of Business Event System event messages by AQ queues and for notification mailers. The recommended number of processes for Oracle Workflow is ten or more.

> **Note:** In Oracle Database 10*g* and higher, you do not need to set the AQ_TM_PROCESSES parameter.

Workflow Metrics

This region displays summary information about work items and Business Event System agent activity.

Work Items

This graph displays the distribution of all work items with the following statuses: Active, Deferred, Suspended, and Error.

- To show this graph if it is hidden, click the Show link.
- To hide this graph if it is shown, click the Hide link.
- The graph header displays the date and time when the work item statistics were last updated. To refresh this information, click the refresh icon. See: Gathering Oracle Workflow Statistics, page 3-2.

- To view the distribution of item types within a status, either click the bar for that status in the graph, or click the status name link.

- To view the number of work items with a particular status, position the mouse pointer over the bar for that status in the graph.

  Note: A work item can be counted in more than one status. For example, all work items that do not have an end date are counted as Active work items, including deferred, suspended, and errored work items as well as running work items. Also, if an activity within an item is deferred, and the work item as a whole is suspended, the work item is included in the count for both the Deferred and Suspended statuses. Consequently, the total of the counts for all the statuses is greater than the actual number of work items.

Agent Activity

This graph displays the distribution of all event messages on Business Event System agents with the following statuses: Ready, Waiting, Expired, Undeliverable, and Error.

> **Note:** Messages are not explicitly assigned a status of Error. The Error bar in the graph represents messages of any status on the WF_ERROR agent.

- To show this graph if it is hidden, click the Show link.

- To hide this graph if it is shown, click the Hide link.

- The graph header displays the date and time when the agent activity statistics were last updated. To refresh this information, click the refresh icon. See: Gathering Oracle Workflow Statistics, page 3-2.

- To view the distribution of event messages with different statuses on different agents, either click the bar for a status in the graph, or click an event message status name link.

- To view the number of event messages with a particular status, position the mouse pointer over the bar for that status in the graph.

Related Links

This region provides links to other Oracle Workflow management features.

Configuration

Click the Service Components link to configure service components, including notification mailers and agent listeners.

Click the Queue Propagation link to view database initialization parameters required for queue propagation and a list of propagation schedules for Business Event System agents.

Throughput

- Click the Work Items link to view the distribution of completed work items across different item types.
- Click the Notification Mailers link to view the notification mailer throughput. This graph shows the throughput of the notification mailers by displaying the distribution of notifications in the WF_NOTIFICATIONS table with the following statuses:
  - Processed - Outbound notifications for which an e-mail message has been sent by a notification mailer service component.
  - Waiting - Outbound notifications for which an e-mail message has not yet been sent.

  The graph header displays the date and time when the notification mailer throughput statistics were last updated. To refresh this information, click the refresh icon. See: Gathering Oracle Workflow Statistics, page 3-2.

  To view the number of notifications with a particular status, position the mouse pointer over the bar for that status in the graph.

  Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Related Links > Throughput > Notification Mailers
- Click the Agent Activity link to view the distribution of event messages with different statuses on different agents.

Service Components

The Generic Service Component Framework helps to simplify and automate the management of background Java services. Service component containers and their service components are run through Generic Service Management (GSM), which you can control through Oracle Applications Manager (OAM).

A service component container is an instance of a service that manages the running of the individual service components that belong to it. The container monitors the status of its components and handles control events for itself and for its components. These actions are recorded in a log for the container.

A service component is an instance of a Java program which has been defined according to the Generic Service Component Framework standards so that it can be managed through this framework. Currently, Oracle Workflow provides four service component types: Workflow Mailer, Workflow Agent Listener, Workflow Java Agent Listener, and Workflow Web Services Outbound.

Oracle Workflow provides several seeded service components of these types, within seeded containers, to perform standard processing. You can optionally create additional service components to perform custom processing. If you create custom service components, you can either assign them to the seeded containers, or, based on the volume to be handled by the seeded containers, you can also choose to create your own custom containers.

All service components have certain attributes required by the Generic Service Component Framework. General definition attributes for a component include the component name, startup mode, container type, inbound agent, outbound agent, and correlation ID. Detail attributes include the container that owns the component, the maximum idle time for an on-demand component, maximum error count, number of inbound and outbound processing threads, component log level, read timeout period, minimum sleep time, maximum sleep time, error sleep time, and whether to close connections when the read timeout period expires.

A service component can have one of three startup modes.

- Automatic - When a component container is started, it will automatically start its automatic service components. It will also monitor these components and restart them automatically when necessary.

- On-Demand - A component container will start its on-demand service components if those components have messages waiting to be processed. For example, an on-demand notification mailer service component will be started if there are messages waiting on the WF_NOTIFICATION_OUT queue. The container will stop an on-demand service component when that component's maximum idle time has been exceeded.

- Manual - You must manually start and stop the service component through Workflow Manager. The component container does not start or stop its manual service components.

All service components use the Oracle Applications GSM container type. A component can have either an inbound agent to process inbound messages, an outbound agent to process outbound messages, or both. An Oracle Advanced Queuing (AQ) correlation ID can be assigned to a component to limit its processing to only messages marked with that correlation ID.

Oracle Workflow provides three predefined containers in which you can create components, the Workflow Mailer Service, the Workflow Agent Listener Service, and the Workflow Document Web Services Service. For an on-demand service component, you can specify the maximum amount of time that the service component can remain idle before it is stopped by its container. A service component can have either one inbound processing thread, to enable inbound processing, or none, to disable inbound processing. A service component can have one or more outbound processing threads, to enable outbound processing depending on the volume of outbound messages, or none, to disable outbound processing. Some types of service components perform only inbound processing or only outbound processing. For example, agent listeners only process inbound event messages and consequently should always have an outbound thread count of zero.

A diagnostic log is recorded for each component container, from the time the container starts to the time it stops. When a container is restarted, a new log is begun. You can view the log through Workflow Manager. Each log entry is marked with the container ID, and, if applicable, with the ID of the service component that generated it. You can specify the level of detail of the information you want to record for each component container. You can also specify a separate log level for an individual service component within the container. The log levels you can select, in order from most detailed to least detailed, are as follows:

- 1 - Statement
- 2 - Procedure
- 3 - Event
- 4 - Exception
- 5 - Error
- 6 - Unexpected

The default log level for both containers and service components is Error. This level is the recommended setting for normal usage.

A processing thread for a service component runs in a loop in which it reads messages from the queue associated with its assigned agent and then waits during a specified amount of sleep time before checking the queue for messages again. The read timeout period defines the amount of time the service component continues attempting to read messages from the queue, after the last message has been dequeued, before timing out. If another message is received before this time expires, that message is processed and the timeout period begins again. If the timeout period expires and no more messages have been received, the service component stops reading and its sleep time begins.

The minimum sleep time for a service component defines the minimum amount of time during which the service component waits, after its read timeout period expires, before it checks the queue for messages again. If a queue receives messages infrequently, you can choose to increase the sleep time between read attempts when no messages are received by setting a maximum sleep time greater than the minimum sleep time. In this case, the service component initially waits for the minimum sleep time after it finishes reading messages from its queue. If no messages are read in subsequent attempts, then the sleep time between read attempts gradually increases until the maximum sleep time is reached. Increasing the sleep time can help enhance performance if messages are received infrequently. You can also set the maximum sleep time parameter to 0 (zero) to indicate that the sleep time should not be increased. In this case, the service component always waits for the minimum sleep time between read attempts.

The error sleep time for a service component defines the amount of time during which the service component waits, after an error occurs, before it attempts to begin processing again. Additionally, a service component processing thread can either close its connections after its read timeout period expires, when its sleep time begins, or the connections can remain open until the processing thread stops.

A service component may also have additional configuration parameters that are specific to the type of processing it performs. For example, a notification mailer service component has configuration parameters to specify the inbound and outbound e-mail servers it uses.

Among both the common and the type-specific configuration parameters, some parameters can be refreshed dynamically while a service component is running. These parameters are identified by a refresh icon in the configuration pages for the component. For example, the component log level, inbound thread count, and outbound thread count are refreshable parameters.

The control events you can perform for a service component include:

- Starting a service component
- Suspending a running service component, so that the threads stop processing but connections are not closed
- Resuming a suspended service component
- Refreshing a running service component with changed parameters
- Stopping a running or suspended service component

A service component may also have additional control commands that are specific to the type of processing it performs. For example, Workflow Mailer components include a command to launch summary notifications.

You can perform these control events manually at runtime by choosing the relevant command for the component in the Service Components page. You can also schedule single or repeating control events when you are configuring a service component.

A service component can have one of the following statuses.

- Not Configured - Some required configuration parameters for the component have not been completed. The component cannot be started until its configuration is complete.
- Starting - The component is preparing to run.
- Running - The component is running normally. You can choose to suspend processing for a component in this state, refresh the configuration parameters for

the component that are dynamically refreshable, or stop the component.

- Suspending - The component is preparing to suspend its processing.

- Suspended - The component's thread has stopped processing, but its connections remain open. When a component is suspended, you can either resume its processing or stop it altogether.

- Resuming - The component is preparing to resume processing and return to a Running status.

- Stopping - The component is preparing to stop running.

- Stopped - The component was stopped normally, without errors.

- Stopped with Error - The component reached the maximum number of errors specified in its Max Error Count parameter and has stopped. The component container will restart an automatic component in this status, or an on-demand component in this status that has messages waiting to be processed.

- System Deactivated - An automatic or on-demand component was deactivated automatically by its container because the component was stopped with an error the maximum number of times specified in the container's SVC_COMP_MAX_ERROR_COUNT service parameter. A component in this status will not be restarted automatically until the container is restarted.

- User Deactivated - An automatic or on-demand component was manually stopped by a user. It will not be restarted automatically. If you want to restart it, you must do so manually.

A component with a status of Starting, Running, Suspending, Suspended, Resuming, or Stopping is considered to be active. While a component is active, you cannot edit the component name, startup mode, container type, inbound agent, outbound agent, correlation ID, container, or, for an on-demand component, the maximum idle time. You must stop the component before you can change these attributes. However, you can edit the component's other configuration parameters while it is active. If you edit any refreshable parameters, the component will be dynamically refreshed with the new parameter values.

You can manually stop a component from any status. Also, if a container stops for any reason, all of its components are stopped as well.

If the status of a service component changes to Stopped with Error or System Deactivated, Oracle Workflow posts a system alert to the System Alerts and Metrics page in Oracle Applications Manager.

Viewing Service Components

The Service Components page shows the service components that are defined in your Oracle Workflow installation.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Service Components status icon

To add the information from this page to your support cart, click the Add to Support Cart button.

For each service component, the list displays the service component name, status, type, startup mode, container type, and container. Click any column heading to sort the list by that column.

- To filter the service components displayed in the list, select a service component property from the Filter pull-down menu, enter a filter value in the text field, and click the Go button. You can filter by the following properties:
  - Service component name
  - Service component status
  - Service component type display name
  - Service component type internal name
- To verify that the statuses displayed for the service components in the list are current, click the Verify All button.
- To create a new service component, click the Create button.
- To edit a service component's configuration, select the service component and click the Edit button. The steps to edit the configuration depend on the service component type.
- To view the diagnostic log of the service component container in which this service component is running, select the service component and click the View Log button. The log includes log messages for this component and any other component belonging to that container.
- To view details about a service component, either click the service component link in the Name column, or select the service component and click the View Details button. The information that is displayed depends on the service component type.
- To review the events that have been scheduled to control the running of the service component, click the View Event History button. For each event, the Event History page displays the event name, status, user who requested the event, component

status before the event was processed, date the event processing was completed, container for the service component, container type, and any event parameters for a refresh event. You can use this event history as an audit trail to review who scheduled control events for the service component. The status of an event may be Pending, Skipped, In Progress, Completed, or Error. In some cases, an event may be skipped if the component is not in an appropriate status at the time for which the event is scheduled. For example, a refresh event cannot be executed if the component is stopped at the scheduled time.

- To delete a service component, select the service component and click the Delete button. If the service component is currently active, you must stop it before you can delete it.

  > **Note:** Several of the seeded service components are required by Oracle Workflow and Oracle XML Gateway and cannot be deleted. If you want to disable them, you can stop them manually using the Stop command from the command pull-down menu. However, note that stopping these components disables the features they support. For example, stopping the Workflow Error Agent Listener and Workflow Java Error Agent Listener disables error handling for the Business Event System.

- To manually control the running of a service component, select the service component, choose the command you want from the command pull-down menu, and click the Go button. You can choose the following commands:
  - Refresh
  - Resume
  - Start
  - Stop
  - Suspend
  - Launch Summary Notifications (Workflow Mailer service components only)

- To manage the service instances for the container of a service component through GSM, click the container link in the Container column.

Creating Service Components

The Pick Component Type page lets you choose the type of service component you want to create. This page lists the name and description of each available type. Select the type that you want and click the Continue button. The steps to complete the service component configuration depend on the type you select.

Oracle Workflow provides the following service component types.

- Workflow Mailer - Service components that perform send and respond e-mail processing for the Notification System.
- Workflow Agent Listener - Service components that process inbound messages on Business Event System agents in the database.
- Workflow Java Agent Listener - Service components that process inbound messages on Business Event System agents in the middle tier.
- Workflow Web Services Outbound - Service components that process outbound Web service messages.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Service Components status icon > Create

Reviewing Service Component Details

The Component Details page lets you review the configuration of a service component.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Service Components status icon > (B) View Details

The Component Details page displays the configuration parameters defined for the service component and any special status information, as well as the control events that are currently scheduled for the service component. For each event, the list shows the event name, initial start time, whether the event is currently running, the next scheduled execution time for a repeating event, the last previous execution time for a repeating event, the interval in minutes between executions of a repeating event, the number of times the event has failed, the job ID of the DBMS job used to schedule the event, and the PL/SQL API that DBMS job runs.

- To add the information from this page to your support cart, click the Add to Support Cart button.
- For Workflow Mailer service components only, to send test messages, click the Test Mailer button. In the Test Notification Mailer page, select the recipient role to which the messages should be sent, and click the Send Test Message button.

  > **Note:** To send a test message successfully, you must select a recipient role that either has a valid e-mail address defined, or that has members with valid e-mail addresses defined. The recipient role must also have a notification preference that includes individual e-mail notifications.
  >
  > If you set an override e-mail address for the notification mailer, the

> Test Notification Mailer page displays that address. In this case the test message is sent to the override address rather than the e-mail address of the recipient role. However, you must still select a recipient role to enable the notification mailer to send the test messages.

Oracle Workflow sends two test messages to the recipient role: one message with content built using PL/SQL and one message with Oracle Application Framework content. Check the e-mail account for the recipient role to view the test messages and reply to them with the Acknowledge response. If you did not implement inbound e-mail processing for this mailer, use the Worklist pages to respond to the test messages after viewing the outbound messages in e-mail. After you acknowledge both test messages, Oracle Workflow sends a confirmation message to the same recipient role to show that the notification mailer successfully processed the inbound response e-mails.

If you do not receive the test messages or the response confirmation message, or if the message content does not appear correctly, check the notification mailer setup, including the mail servers and the mailer configuration parameters. In particular, if the Oracle Application Framework content does not appear correctly, check the Application Framework Agent and WF: Workflow Mailer Framework Web Agent profile options, as well as the Framework User, Framework Responsibility, Framework Application ID, and Framework URL Timeout parameters in the advanced configuration wizard. See: Setting Up a Notification Mailer, page 3-22 and Message Generation, page 3-47.

> **Note:** Oracle Workflow sends the test messages by launching the PLSQL/OAFwk Response Test Process in the System: Tests (WFTESTS) item type. This item type is stored in a file called wftstmlr.wft in the `$FND_TOP/import/<lang>` subdirectory. You can optionally use the Status Monitor to check the status of the test process.

- For Workflow Mailer service components only, to set an override address where you want to send all outgoing e-mail notifications, click the Set Override Address button. Use an override address when you are testing workflow definitions or mailer processing so that you can automatically receive all the test notifications at one e-mail address, instead of having to check or change each individual recipient's e-mail address. To ensure that the override address is accessible and that its use is authorized, you must verify the request before the notification mailer can use the address.

  In the Set Override Address page, review the current override address, if any. Enter the e-mail address you want to set as the new override address, and choose Submit. Then check the e-mail account you specified for the verification e-mail message.

In the Verify Override Address page, enter the verification code shown in the e-mail message, and choose Apply. If necessary, you can use the link provided in the verification e-mail message to navigate back to the Verify Override Address page. You must log in to Oracle Applications Manager before you can access this page.

To remove the override address, navigate to the Set Override Address page and choose the Clear Override Address button. The notification mailer then resumes sending e-mail notifications to the individual recipients' e-mail addresses.

- To review the events that have been scheduled to control the running of the service component, click the View Event History button. For each event, the Event History page displays the event name, status, user who requested the event, component status before the event was processed, date the event processing was completed, container for the service component, container type, and any event parameters for a refresh event. You can use this event history as an audit trail to review who scheduled control events for the service component. The status of an event may be Pending, Skipped, In Progress, Completed, or Error. In some cases, an event may be skipped if the component is not in an appropriate status at the time for which the event is scheduled. For example, a refresh event cannot be executed if the component is stopped at the scheduled time.

- To view the diagnostic log of the Generic Service Management (GSM) service component container in which this component is running, click the View Log button. The log includes log messages for this component and any other component belonging to that container.

- To change the values of the configuration parameters or the scheduled events, click the Edit button and navigate to the appropriate page within the service component configuration wizard.

- To return to the Service Components page, click the OK button.

Service Instances for Service Component Containers

You can use Oracle Applications Manager to control service component containers as service instances of type Generic Service Component Container in GSM.

Editing Service Parameters for a Container

Among other properties, a GSM service instance can have work shifts assigned to it. A work shift in turn can have service parameters associated with it. For a service instance that is a service component container, these service parameters apply to the container as a whole to determine how the container manages the components that belong to it.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Service Components status icon > container link > (B) Edit > (B) Edit Service Parameters

The Edit Service Parameters page initially displays the service parameters that can be specified for a container in the Edit Service Parameters field, together with their seeded default values. In most cases, you do not need to change these values. However, you can optionally edit these values in the Edit Service Parameters field if you choose.

You can also optionally delete any of the service parameters from the Edit Service Parameters field. In this case, for all parameters except the proxy setting parameters, the parameter values are obtained from the global settings stored in the WF_RESOURCES table. The default values in the WF_RESOURCES table are the same as the initial default values in the Edit Service Parameters page.

In the Edit Service Parameters field, the service parameter names and values should be specified separated by colons, in the following format:

```
<name1>=<value1>:<name2>=<value2>: . . . <nameN>=<valueN>
```

The following service parameters can be specified for a container:

- SVC_WRITE_DIAG_TO_GSM_LOG - Specify `Y` if you want to write diagnostic information to the GSM log file in all cases. The default value is `Y`. Specify `N` if you want to let the FND: Debug Log Filename (AFLOG_FILENAME) profile option determine where to write the log, either to a specified file or to the database if no file is specified. For more information about FND: Debug Log profile options, please refer to the *Oracle E-Business Suite System Administrator's Guide - Maintenance*.

- SVC_CONTAINER_LOOP_SLEEP - Specify the sleep time in seconds during which the container waits, after it finishes reading control messages from its GSM queue, before it checks that queue for messages again. The default sleep time is 10 seconds.

- SVC_CONTAINER_READ_TIMEOUT - Specify the maximum amount of time in seconds that the container continues to block on the GSM queue after processing the last message. If another message is received before this time expires, that message is processed and the timeout period begins again. If the timeout period expires and no more messages have been received, the container stops blocking on the queue and its sleep time begins. The default timeout period is 10 seconds.

- SVC_CONTAINER_LOG_LEVEL - Specify the level of detail to record for the container in its log. The default value is `5` (Error). The valid levels, in order from most detailed to least detailed, are:

  - 1 - Statement

  - 2 - Procedure

  - 3 - Event

  - 4 - Exception

  - 5 - Error

  - 6 - Unexpected

- SVC_COMP_MONITOR_LOOP_SLEEP - Specify the sleep time in seconds during which the container waits, after it starts any automatic components that need to be started, before it checks its automatic components again. The default value is 60 seconds.

- SVC_COMP_MONITOR_ONDEMAND_FREQ - Specify the interval in seconds to determine how often the container checks whether its on-demand components need to be started or stopped. This activity is more costly than monitoring the automatic components and should usually be performed less frequently. The default value is 300 seconds.

- SVC_COMP_MAX_ERROR_COUNT - The container-level maximum error count. If any automatic or on-demand component in the container is stopped with an error the specified number of times, the component status will be set to System Deactivated, and the container will no longer automatically restart the component. The default value is `5`.

You can also optionally specify the following service parameters for proxy settings. You should set these parameters if components in this container need to use a proxy server to access web content that is outside a firewall. For example, a mailer component may need to access outside web content that is to be included in an e-mail notification. The Generic Service Component Framework uses the values you set in these service parameters to set the relevant Java System Properties.

- SVC_PROXY_SET - Specify `true` to indicate that you want to use a proxy for your connections. The default value is `NONE`.

- SVC_PROXY_HOST - Specify the host machine for the proxy. The default value is `NONE`.

- SVC_PROXY_PORT - Specify the port on which the proxy is listening. The default value is `NONE`.

Selecting the Log Level for a Container

You can use the Service Status page to control the running of a service component container, including changing the log level for the container. The log level controls how much information is recorded in the log. Note that the log level you select here applies only to the log messages for the container. You can assign separate log levels to the individual components within the container.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Service Components status icon > container link > (B) View Status

The log level with which the container starts is determined by the value of the SVC_CONTAINER_LOG_LEVEL service parameter. If no value is defined for that parameter, the log level is obtained from the default setting stored in the WF_RESOURCES table. The default container log level, which is also the recommended setting, is Error.

If the container is running, you can optionally specify a different container log level for the current session. To change the log level, select the level you want from the Change Log Level To pull-down menu and click the Go button. The log levels you can select, in order from most detailed to least detailed, are as follows:

- 1 - Statement
- 2 - Procedure
- 3 - Event
- 4 - Exception
- 5 - Error
- 6 - Unexpected

Note that the log level you set dynamically in the Service Status page applies only for the duration of the current container session, and does not change the log level stored for the container in the service parameters. To set the log level permanently, so that the container starts with that log level in each new session, edit the value of the SVC_CONTAINER_LOG_LEVEL service parameter in the Edit Service Parameters page. See: Editing Service Parameters for a Container, page 3-15.

If the log level has been changed dynamically for the current session, the Service Status page may not display the log level that is currently in effect for the container. However, you can always review the current log level in the container log file by choosing View Log in the Service Components page or the Component Details page.

Creating Service Component Containers

If you create custom service components, you can choose to create custom containers to manage those service components. You create a container as a GSM service instance of type Generic Service Component Container in Oracle Applications Manager.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Service Components status icon > container link > (B) Create New

Among other properties, a GSM service instance can have work shifts assigned to it. A work shift in turn can have service parameters associated with it. For a service instance that is a service component container, these service parameters apply to the container as a whole to determine how the container manages the components that belong to it. If you create a custom container, you should specify service parameters for the work shifts for your new service instance in order to specify how to run the new container. To enter service parameters easily, copy the service parameters from one of the seeded Oracle Workflow containers to your new container.

After creating a customer container, you can assign service components to it using the appropriate service component configuration wizard. Ensure that your custom containers are running in order to run the service components belonging to them.

Notification Mailers

A notification mailer is a Java program that performs e-mail send and response processing for the Oracle Workflow Notification System, using the JavaMail API. You need to implement one or more notification mailers only if you want to have your workflow users receive their notifications by e-mail, as well as from the Worklist Web pages.

Managing Notification Mailers

The notification mailer program is defined as a service component type in the Generic Service Component Framework. This framework helps to simplify and automate the management of background Java services.

Oracle Workflow provides one seeded notification mailer service component, called Workflow Notification Mailer. Most of the configuration parameters for this mailer are set to default values. You can enter several of the remaining required parameters using AutoConfig. After installation, you then only need to enter the e-mail inbox password in order to complete the configuration of this mailer. Alternatively, if you only want to send outbound messages and do not need to receive inbound messages, you only need to disable inbound processing in order to complete the configuration of this mailer. If the mail servers and Business Event System components used by the notification mailers are set up, and the Workflow Mailer Service container to which the Workflow Notification Mailer belongs is started, the seeded notification mailer automatically starts running once its configuration is complete.

You cannot delete the seeded Workflow Notification Mailer or edit its name, assigned agents, correlation ID value, or container. However, if necessary you can optionally update other configuration parameters, schedule control events, or manually choose control commands to start, stop, suspend, resume, or refresh this notification mailer.

> **Note:** Oracle Alert also uses the Workflow Notification Mailer to send and receive alert e-mail messages. If you use Oracle Alert, ensure that the configuration of the Workflow Notification Mailer meets your alert requirements. See: Setup Steps, *Oracle Alert User's Guide*.

You can also optionally create additional notification mailer service components. For example, you can create a notification mailer that processes only messages that belong to a particular workflow item type, or instances of a particular message from a particular item type. You can create additional mailers that process the same types of message to increase throughput.

The correlation ID for a notification mailer determines which messages it can process.

- To create a general notification mailer that can process any message from any item type, leave the correlation ID blank. The seeded Workflow Notification Mailer has a blank correlation ID so that it can run as a general mailer.
- To dedicate a notification mailer to processing messages from a particular item type, set the correlation ID to the internal item type name followed by a colon and a percent sign.
- To dedicate a notification mailer to processing instances of a particular message from a particular item type, set the correlation ID to the internal item type name followed by a colon and then the internal message name.

> **Note:** If you run a general notification mailer and a dedicated notification mailer at the same time, a message that matches the dedicated notification mailer's correlation ID may still be processed by the general mailer if that mailer is the first to access the message. If you want only the dedicated notification mailer to process its matching messages, disable any general mailers. In this case, however, ensure that you define dedicated mailers for all item types used in your Oracle E-Business Suite installation.

To ensure consistency in message handling, all notification mailers that can process the same messages must share the same values for certain parameters. Multiple mailers can process the same messages in the following cases:

- A general mailer runs at the same time as any dedicated mailers.
- Multiple general mailers run at the same time.
- Multiple dedicated mailers for the same item type or message definition run at the same time.

In these cases, the notification mailers must share the same values for the following parameters:

- HTML Agent
- Attach Images to Outbound E-mails
- Attach Stylesheet to Outbound E-mail
- Autoclose FYI
- Direct Response
- Reset NLS

- Inline Attachments
- All message template parameters

However, these mailers can have different values for the From and Reply-to Address parameters. The headers of each notification e-mail message will contain the From and Reply-to Address values of the notification mailer that actually sent the message, unless the message itself has the special `#WFM_FROM` and `#WFM_REPLYTO` message attributes defined to override the notification mailer's parameters. See: Notification Mailer Attributes, *Oracle Workflow Developer's Guide*.

You can also configure any notification mailer service component to process only inbound messages, or only outbound messages. You associate inbound and outbound mailers with each other by assigning them the same mailer node name. The mailer node name indicates which inbound mailer can process incoming responses to outbound messages sent by a particular outbound mailer.

You can optionally assign the same node name to multiple mailers for load balancing purposes. However, each mailer that performs inbound processing for a node must have its own inbox.

- If you enable both outbound and inbound processing for the same mailer, that mailer will automatically use the same node name for both types of processing, enabling it to process incoming responses to the outbound messages it sent. You can optionally also create other notification mailers that share the same node name.
- If you create an outbound-only mailer, but you still want to perform response processing for e-mail responses to the outbound messages it sends, you should create at least one other mailer with the same node name that does perform inbound message processing. Otherwise, there will be no inbound mailer that can process incoming responses to outbound messages sent by this outbound mailer.
- If you only want to implement outbound message processing, without inbound e-mail response processing, then you can configure an outbound-only mailer without creating a corresponding inbound mailer. In this case you should configure the mailer to use message templates for response-required notifications that do not request a response by e-mail, but instead direct recipients to respond from the Notification Details Web page. For example, you can configure the mailer to send response-required notifications using the Workflow View From UI message template, which is an alternative template provided by Oracle Workflow in the System: Mailer item type, or create your own custom message templates. The outbound-only mailer can still use the standard message templates to send outbound summary notifications or For Your Information (FYI) notifications that do not require a response.
- Create an inbound-only mailer only if you have also created at least one mailer with the same node name that performs outbound message processing. If no outbound mailer shares the same node name, no incoming response messages will be marked

with that node name, and the inbound-only mailer will have no messages to process.

Dedicated mailers for different item types or message definitions should use different node names.

If you create custom notification mailer service components, you can either assign them to the seeded container for notification mailers, named Workflow Mailer Service, or, based on the volume to be handled by the seeded container, you can also choose to create your own custom containers.

Setting Up a Notification Mailer

Currently, Oracle Workflow supports the Simple Mail Transfer Protocol (SMTP) for outbound messages and the Internet Message Access Protocol (IMAP) for inbound messages. You must have an SMTP server set up in order to send Oracle Workflow notification e-mail messages, and an IMAP server set up if you want to receive e-mail notification responses. Users can receive e-mail notifications using various e-mail clients, although notifications may be displayed differently in different clients, depending on the features each client supports.

> **Note:** Oracle Workflow supports IMAP version 4 (IMAP4) compliant mail servers. Ensure that your mail server uses this IMAP version. For more information, see the JavaMail API Design Specification: http://java.sun.com/products/javamail/JavaMail-1.2.pdf

> **Note:** If you have certain types of software installed, you may already have the necessary mail server functionality available. For example, products such as Oracle Email, Microsoft Exchange, or Lotus Notes include IMAP services. You can use a UNIX server as an SMTP server by configuring the Sendmail program.
>
> Additionally, you can choose to use IMAP server software that is available for download from some sources. For example, the University of Washington offers the UW IMAP Server as a public service, and Carnegie Mellon University offers the Cyrus IMAP Server. You might choose this option if your enterprise uses UNIX Sendmail e-mail accounts, for instance. For more information, see: http://www.washington.edu/imap/, http://cyrusimap.web.cmu.edu/, and http://www.imap.org/.

> **Note:** Third party software products are mentioned as examples only. Oracle makes no recommendation or endorsement of these third party software products.

To set up a notification mailer, you must perform the following steps.

1. Set up an SMTP mail server to send outbound messages.

   You can optionally configure the SMTP server to require authentication for server connections through the Simple Authentication and Security Layer (SASL). The Oracle Workflow notification mailer supports the PLAIN, LOGIN, and DIGEST-MD5 authentication mechanisms. Additionally, if you have applied patch 9452181 for JavaMail version 1.4.x, then the notification mailer can also support the Microsoft NTLM authentication mechanism. If you configure your SMTP server to use one of these authentication mechanisms, set up a user name and password for the notification mailer to use in establishing an authenticated connection to the server.

   If you configure your SMTP server to support more than one authentication mechanism, then the notification mailer uses the mechanism that appears first in the server's list of supported mechanisms. Consequently, if you want the notification mailer to use a particular mechanism, ensure that that mechanism appears first in the server's list. At a minimum, you should ensure that the first authentication mechanism listed for the server is one that the notification mailer supports.

   > **Note:** If you use the PLAIN or LOGIN authentication mechanisms, it is recommended to connect to the SMTP server through Secure Sockets Layer (SSL) to encrypt the user name and password that are sent to the server. See: Connecting to Mail Servers Through SSL, *Oracle Workflow Administrator's Guide*. If you use the DIGEST-MD5 or NTLM authentication mechanisms, the JavaMail API encrypts the user name and password before sending the data to the SMTP sever.

2. Set up an IMAP4 compliant mail server with an e-mail account for the notification mailer if you want to receive inbound messages.

   The notification mailer requires three folders in this e-mail account: the inbox, a folder to store processed messages, and a folder to store discarded messages. If the e-mail account does not already include folders named PROCESS and DISCARD, Oracle Workflow automatically creates these two folders when you complete the basic notification mailer configuration. You can optionally specify other folders for the notification mailer using the advanced configuration wizard.

   > **Note:** If you create the PROCESS and DISCARD folders manually before configuring the notification mailer, use your e-mail client to create these folders. A notification mailer may not be able to access folders that were created using command line tools outside the e-mail client.

However, note that you must not use an e-mail client to access the notification mailer's e-mail account while the notification mailer is running. Use the e-mail client only during setup.

3. You can use AutoConfig to enter the following configuration parameters for the seeded Workflow Notification Mailer service component during installation. For more information about running AutoConfig, see *Using AutoConfig to Manage System Configurations with Oracle Applications Release 12*, My Oracle Support Knowledge Document 387859.1 and AutoConfig, *Oracle E-Business Suite Concepts*.

   - SMTP Server
   - IMAP Server (if you want to receive inbound messages)
   - Inbox Username (if you want to receive inbound messages)
   - Reply To E-mail Address (if you want to receive inbound messages)
   - HTML Agent Name - This parameter defaults to the value you enter for the Applications Servlet Agent parameter in AutoConfig. Use the following format:

     ```
     http://<server_name:port>/OA_HTML/
     ```

   > **Note:** When you enter the SMTP Server and IMAP Server parameters, specify the actual host name for each server. Do not use `localhost` as the setting for these parameters. You can optionally specify the port number to use on each server. If you do not specify a port number, the notification mailer uses port 143 on the IMAP server and port 25 on the SMTP server by default. Specify each server in the following format: `<server_name>[:<port_number>]`

4. Ensure that the Business Event Local System status is set to Enabled in the Workflow Configuration page, and that the JOB_QUEUE_PROCESSES database initialization parameter, which is required for the Business Event System, is set to an appropriate value. The Business Event Local System status is set to Enabled by default, and usually you do not need to change this status. If notification processing is not being completed, however, you should check this preference value.

5. **(Recommended)** You can optionally set the WF: Workflow Mailer Framework Web Agent profile option to the host and port of the Web server that notification mailers should use to generate the content for Oracle Application Framework regions that are embedded in notifications. If this profile option is not set, notification mailers will use the same Web agent specified in the Application Framework Agent profile option. However, if necessary for load balancing purposes, you can optionally

specify a different Web agent for notification mailers to use. The WF: Workflow Mailer Framework Web Agent profile option should be set at site level. See: Overview of Setting User Profiles, *Oracle E-Business Suite System Administrator's Guide - Maintenance*.

6. Before a service component can run, the container which manages it must first be started. The seeded Workflow Notification Mailer service component belongs to a container named Workflow Mailer Service, while the seeded agent listener service components that are also required for notification mailer processing belong to a container named Workflow Agent Listener Service. You should ensure that these two containers are running. If you create your own custom containers for custom service components, ensure that those containers are running as well. Use the Service Instances page to start the containers as service instances in Generic Service Management (GSM).

7. When the Workflow Agent Listener Service container is running, it automatically starts seeded agent listener service components named Workflow Deferred Notification Agent Listener, Workflow Error Agent Listener, and Workflow Inbound Notifications Agent Listener, which are required for notification mailer processing. Ensure that these agent listeners are running.

8. Use the notification mailer configuration wizard to configure your notification mailer service component. The Basic Configuration page lets you configure a notification mailer quickly by entering only the minimum required parameters, while the advanced configuration wizard lets you specify additional parameters to control how the notification mailer processes messages.

   If you entered configuration parameters for the seeded Workflow Notification Mailer through AutoConfig, you only need to enter the password for the e-mail inbox in order to complete the configuration for that mailer and begin running it. If you did not enter parameters for the seeded mailer through AutoConfig, then in order to complete the configuration for that mailer you need to enter only the SMTP server, IMAP server, e-mail inbox username, e-mail inbox password, and reply-to e-mail address. All other configuration parameters for the seeded Workflow Notification Mailer are initially set to default values and do not need to be changed, although you can optionally do so if you choose.

   > **Note:** The IMAP server, e-mail inbox username, e-mail inbox password, and reply-to e-mail address are required only if you want to receive inbound messages. Alternatively, if you only want to send outbound messages and do not need to receive inbound messages, you only need to disable inbound processing in order to complete the configuration of the Workflow Notification Mailer.

9. **(Optional)** By default, the seeded Workflow Notification Mailer has a Launch Summary Notifications event scheduled to send summary notifications once a day.

You can optionally use the notification mailer configuration wizard to modify the start time and interval for this event's schedule, or to schedule the Launch Summary Notifications event at the interval you choose for any notification mailer service component. When this event is processed, a summary notification is sent to each role with a notification preference of SUMMARY or SUMHTML, listing all the notifications that are currently open for that role.

10. **(Optional)** You can configure a notification mailer to connect to the SMTP server and IMAP server through Secure Sockets Layer (SSL) to encrypt the data exchanged. See: Connecting to Mail Servers Through SSL, *Oracle Workflow Administrator's Guide*.

11. **(Optional)** You can optionally set the internal mailer parameter named `HTML_DELIMITER` to specify which characters the notification mailer uses to delimit response values in response templates for HTML-formatted e-mail notifications. Valid values for the `HTML_DELIMITER` parameter are:

    - `DEFAULT` - The notification mailer uses the default delimiters, currently set as the single quote (`'`) for both the opening and the closing delimiter. The notification mailer also uses the default delimiters if the `HTML_DELIMITER` parameter value is left null.

    - `APOS` - The notification mailer uses the single quote, or apostrophe (`'`) , as both the opening and the closing delimiter. This setting is currently the same as the default.

    - `QUOTE` - The notification mailer uses the double quote (`"`) as both the opening and the closing delimiter.

    - `BRACKET` - The notification mailer uses the left bracket (`[`) as the opening delimiter and the right bracket (`]`) as the closing delimiter.

    Using single quotes as the delimiters accommodates e-mail applications that cannot process double quotes in the <A HREF="mailto:"> tag for the response template link, but can accept single quotes. However, if you want users to be able to use apostrophes or single quotes in their response values without entering an escape character, you can use double quotes or brackets as the delimiters, depending on what your e-mail application supports. See: To Respond to an HTML E-mail Notification, *Oracle Workflow User's Guide*.

    > **Note:** If the `HTML_DELIMITER` parameter is set to an invalid value, the notification mailer throws an exception at startup. Any notifications created during this time are rendered with the default delimiters instead.

    By default, the `HTML_DELIMITER` parameter is set to the value `DEFAULT`. Use the `afsvcpup.sql` script to change the parameter value to specify the delimiters you want to use. See: To Set Internal Mailer Parameters, *Oracle Workflow Administrator's Guide*.

If a particular notification message has the special `#WFM_HTML_DELIMITER` message attribute defined, however, the notification mailer will use the `#WFM_HTML_DELIMITER` attribute value to determine which delimiters to use for that notification, instead of using the `HTML_DELIMITER` parameter value.

> **Note:** The `HTML_DELIMITER` parameter only controls the response templates for HTML-formatted notifications. This parameter does not apply to plain text notifications.

12. **(Optional)** The seeded Workflow Notification Mailer uses the Automatic startup mode by default and will be started automatically when you complete its configuration. If you select the Manual startup mode for a notification mailer service component, use the Service Components page to start that notification mailer. You can also use this page to manage any notification mailer service component.

Outbound Notification Mailer Processing

When the Workflow Engine determines that a notification message must be sent, it raises an event in the Business Event System called oracle.apps.wf.notification.send. Oracle Workflow provides a seeded subscription to this event, which is defined to be deferred immediately so that the workflow process that owns the notification can continue. The event is placed on the standard WF_DEFERRED agent. Oracle Workflow provides a seeded agent listener named Workflow Deferred Notification Agent Listener that runs on this agent to continue notification processing. This agent listener is dedicated solely to processing deferred notification events.

When the event is dequeued from WF_DEFERRED and the subscription is processed, the subscription requires the event data for the event, causing the generate function for the event to be executed. The generate function for this event performs the following actions:

- Resolves the notification recipient role to a single e-mail address, which itself can be a mail list.

- Checks the notification preference of the recipient to determine whether an e-mail notification is required, and in what type of format.

- Switches its database session to the recipient role's preferred language and territory as defined in the directory service.

- Generates an XML representation of the notification message and any optional attachments using the appropriate message template.

Finally, the subscription places the event message on the standard WF_NOTIFICATION_OUT agent.

A notification mailer service component polls the WF_NOTIFICATION_OUT agent for messages that must be sent by e-mail. When the notification mailer dequeues a message from this agent, it uses a Java-based notification formatter to convert the XML representation of the notification into a MIME (Multipurpose Internet Mail Extensions) encoded message and sends the message by the Simple Mail Transfer Protocol (SMTP).

The e-mail notifications are based on message templates defined in Oracle Workflow Builder. Oracle Workflow provides a set of standard templates in the System: Mailer item type, which are used by default. It is not recommended to modify the standard templates. However, you can customize the message templates used to send your e-mail notifications by creating your own custom message templates in a custom item type using the Workflow Builder. Then assign these templates to a particular notification in a workflow process by defining special message attributes. In this case the templates assigned to the notification override any other templates.

You can also create your own custom message templates in the System: Mailer item type using the Workflow Builder, and assign these templates to a particular notification mailer service component in the mailer configuration parameters. The templates assigned to a mailer override the default System: Mailer templates. However, if any notifications have templates specifically assigned to them through message attributes, the notification-level templates still override the templates assigned to the mailer.

If the notification mailer cannot deliver an e-mail notification because the recipient's e-mail address is invalid, it performs the following actions:

- Sets the mail status of the notification to `FAILED`. This mail status indicates that an exception prevented this e-mail notification from being delivered but does not prevent the mailer from processing other notifications.

- Adds the e-mail address to its invalid e-mail address list. To avoid unnecessary processing, each notification mailer stores a list of e-mail addresses to which it could not deliver messages, and does not attempt to send any further messages to those addresses. Instead, for any subsequent notifications to the listed addresses, the notification mailer simply sets the mail status directly to `FAILED`.

  > **Note:** Each notification mailer can store up to 100 e-mail addresses in its invalid e-mail address list. If the notification mailer encounters additional invalid addresses when the list is already full, the notification mailer removes the oldest addresses from the list and adds the new addresses in their place. Also, the notification mailer clears the list by removing all addresses whenever you stop and restart the mailer.

- Changes the notification preference of the recipient to `DISABLED`. To further help avoid unnecessary processing, if a recipient has a notification preference of

DISABLED, Oracle Workflow does not generate a complete XML representation of any notifications to that recipient, and a notification mailer does not attempt to send e-mail notifications to that recipient. Instead, the notification mailer simply sets the mail status of the notifications directly to FAILED. The change in notification preference also indicates to the user that e-mail notifications cannot be delivered. The user must correct the invalid e-mail address and then reset the notification preference in order to receive e-mail notifications.

- Sends a notification to the SYSADMIN user with the information that an e-mail notification could not be sent to one or more recipients, that the notification preference for those recipients has been set to DISABLED, and that those recipients' original notification preferences, which are listed, should be reset after the issues that caused the failures are corrected. See: User Notification Preference Update Report Message, *Oracle Workflow Administrator's Guide*.

After correcting invalid e-mail addresses and resetting DISABLED notification preferences, you can run the Resend Failed/Error Workflow Notifications concurrent program to retry open notifications that previously could not be sent. See: Handling Mailer Errors, *Oracle Workflow Administrator's Guide*.

Inbound Notification Mailer Processing

Notification mailers can also process e-mail responses from users, using the Internet Message Access Protocol (IMAP). A notification mailer uses a Java-based e-mail parser to interpret the text of each message and create an XML representation of it.

A notification mailer uses three folders in your response mail account for response processing: one to receive incoming messages, one to store processed messages, and one to store discarded messages.

A notification mailer does the following to process response messages:

- Logs into its IMAP e-mail account.

- Checks the inbox folder for messages. If a message exists, the notification mailer reads the message, checking for the notification ID (NID) and node identifier in the NID line.

- If the message is not a notification response, meaning it does not contain an NID line, the notification mailer moves the message to the discard folder and treats it as an unsolicited message. For the first unsolicited message from a particular e-mail address, the notification mailer also sends a warning message back to the sender of the message. However, to avoid sending unnecessary warnings due to bounced or auto-reply messages, each mailer node stores a list of e-mail addresses from which it has received unsolicited mail, and does not send any further warning messages to those addresses. Instead, if the node receives a second unsolicited message from a particular address, the notification mailer discards the message and raises the oracle.apps.wf.mailer.unsolicited event. You can optionally define a subscription to this event if you want to perform some other action in response to the second unsolicited message. For all subsequent unsolicited messages, the notification mailer simply discards the message.

> **Note:** Each mailer node can store up to 100 e-mail addresses in its warned list. If the node receives unsolicited messages from additional addresses when the list is already full, the notification mailer removes the oldest addresses from the list and adds the new addresses in their place. Also, the notification mailer clears the list by removing all addresses when you start the mailer for the first time, and again whenever you stop and restart its container. In these cases, the mailer may send another warning message if it receives further unsolicited e-mail from an address that is no longer on the warned list.

> **Note:** You can optionally use the Send Warning for Unsolicited E-mail mailer parameter to prevent notification mailers from sending any warning messages at all. See: Notification Mailer Configuration Wizard, page 3-31.

- If the message is a notification response, but for a different node, the notification mailer leaves the message in the inbox and adds the e-mail's Unique Message ID (UID) to its ignore list.

- If the message is a notification response for the current node, meaning it contains an NID line including the node identifier of the current node, the notification mailer processes the message.

The notification mailer performs the following steps for messages that belong to its node.

- Retrieves the notification ID.

- Checks to see if the message bounced by referring to the tags specified in the configuration parameters, if any. If the message bounced, the notification mailer updates the notification's status and stops any further processing, based on the specifications of the tag list.

- Checks the Oracle Workflow database for this notification based on the NID line.

  - If the notification does not exist, meaning the notification ID or the access key in the NID line is invalid, the notification mailer moves the message to the discard folder. If the NID line is incorrectly formatted, the notification mailer moves the message to the discard folder and treats it as an unsolicited message.

- If the notification exists, but is closed or canceled, the notification mailer moves the message to the processed folder and sends a Workflow Closed Mail or Workflow Canceled Mail message to the recipient role, respectively.

  > **Note:** You can optionally use the Send E-mails for Canceled Notifications mailer parameter to prevent notification mailers from sending any notification cancellation messages. See: Notification Mailer Configuration Wizard, page 3-31.

- If the inbound message is a response to a request for more information that has already been answered, or if the message is formatted as a more information response but no information was requested for that notification, then the notification mailer moves the message to the discard folder and sends a Workflow More Info Answered Mail message to the sender of the message.

- If the notification exists and is open, the notification mailer generates an XML representation of the message and places it on the standard WF_NOTIFICATION_IN agent as an event called oracle.apps.wf.notification.receive.message. The notification mailer then moves the message for the completed notification to the processed folder.

  > **Note:** If the character encoding of the response message is not compatible with the database codeset, the notification mailer may not be able to parse the response and recognize the response values. Ensure that the character encoding of messages in your mail client is compatible with the codeset of your database.

Finally, if there are no more unprocessed messages in the inbox, the notification mailer logs out of the e-mail account.

Oracle Workflow provides a seeded agent listener named Workflow Inbound Notifications Agent Listener that runs on the WF_NOTIFICATION_IN agent to continue notification processing for the valid response messages placed on that agent. When an event message is dequeued from WF_NOTIFICATION_IN, Oracle Workflow executes a seeded subscription that calls the appropriate notification response function. This function verifies the response values with the definition of the notification message's response attributes in the database. If a response value is invalid, or if no response value is included, the notification mailer sends a Workflow Invalid Mail message to the recipient role, or, for an invalid response to a request for more information, the notification mailer sends a Workflow Invalid Open Mail (More Information Request) message to the recipient role. If the responses are valid, the notification response function records the response and completes the notification.

Notification Mailer Configuration Wizard

Use the notification mailer configuration wizard to configure a new notification mailer service component, or to edit the configuration of an existing notification mailer service component. The notification mailer configuration wizard begins with the Basic Configuration page, which lets you configure a notification mailer quickly by entering only the minimum required parameters.

From the Basic Configuration page, you can also navigate to the advanced configuration wizard to specify additional parameters that control how the notification mailer processes messages. The advanced configuration wizard lets you define general and detail attributes, define e-mail server and message generation parameters, schedule control events, and define tags to assign statuses to unusual messages.

Some parameters appear in both the Basic Configuration page and the advanced configuration wizard. Both the Basic Configuration page and the advanced configuration wizard also let you send test messages.

> **Note:** If you are configuring the seeded Workflow Notification Mailer and you entered configuration parameters for this mailer through AutoConfig, then you only need to enter the password for the e-mail inbox in order to complete the configuration for that mailer. If you did not enter parameters for the seeded mailer through AutoConfig, then in order to complete the configuration for that mailer you need to enter only the SMTP server, IMAP server, e-mail inbox username, e-mail inbox password, and reply-to e-mail address. All other configuration parameters for the seeded Workflow Notification Mailer are initially set to default values and do not need to be changed, although you can optionally do so if you choose.
>
> Note that the IMAP server, e-mail inbox username, e-mail inbox password, and reply-to e-mail address are required only if you want to receive inbound messages. Alternatively, if you only want to send outbound messages and do not need to receive inbound messages, you only need to disable inbound processing in order to complete the configuration of the Workflow Notification Mailer.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Notification Mailers status icon > (B) Create > (B) Continue

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Notification Mailers status icon > (B) Edit

Basic Configuration

This page lets you configure a notification mailer quickly by entering only the minimum required parameters in a single page. You must set parameters marked with an asterisk (*) to appropriate values for your environment before you can run the notification mailer.

Details

- **Name** - The name of the service component. This name must be unique. The name of the seeded notification mailer service component is `Workflow Notification Mailer`, and you cannot change this value.

Outbound E-mail Account (SMTP)

- **Server Name** - The name of the outbound SMTP mail server. Note that you must specify the actual host name for the server. Do not use `localhost` as the setting for this parameter. You can optionally specify the port number to use on that server. If you do not specify a port number, the notification mailer uses port 25 by default. Specify the server in the following format: `<server_name>[:<port_number>]`

  For example: `mysmtpserver.mycompany.com:25`

- **Username** - If the outbound SMTP server is configured to require authentication, enter the user name of the account that the notification mailer uses to connect to the SMTP server.

- **Password** - If the outbound SMTP server is configured to require authentication, enter the password for the account specified in the Username parameter. The password value is masked as asterisks in the display and is stored in encrypted form.

- **Outbound SSL Enabled** - Select this parameter to enable the notification mailer to use Secure Sockets Layer (SSL) for connections to the SMTP server. Deselect this parameter to use non-SSL connections.

  > **Note:** When you enable SSL, the notification mailer connects to the SMTP server through port 465 by default. You can optionally specify a different port number along with the SMTP server name in the Outbound E-mail Account (SMTP): Server Name parameter.

  Before you can use SSL, you must also complete additional setup steps. See: Connecting to Mail Servers Through SSL, *Oracle Workflow Administrator's Guide*.

Inbound E-mail Account (IMAP)

- **Inbound Processing** - Select this parameter to enable inbound e-mail processing with this notification mailer. Deselect this parameter to disable inbound e-mail processing for this notification mailer and dedicate the notification mailer solely to outbound processing.

  If you disable inbound processing, you can leave the other inbound parameters blank.

- **Server Name** - The name of the inbound IMAP mail server. Note that you must specify the actual host name for the server. Do not use `localhost` as the setting for this parameter. You can optionally specify the port number to use on that server. If you do not specify a port number, the notification mailer uses port 143 by default. Specify the server in the following format: `<server_name>[:<port_number>]`

  For example: `myimapserver.mycompany.com:143`

- **Username** - The user name of the mail account that the notification mailer uses to receive e-mail messages.

- **Password** - The password for the mail account specified in the Username parameter. The password value is masked as asterisks in the display and is stored in encrypted form.

- **Reply-To Address** - The address of the e-mail account that receives incoming messages, to which notification responses should be sent. This value must be a full RFC822-compliant e-mail address.

  If a particular notification message has the special #WFM_REPLYTO message attribute defined, however, the notification mailer will use the #WFM_REPLYTO attribute value as the reply address for that message, instead of the Reply-To Address parameter value.

  > **Note:** If you enable inbound processing, Oracle Workflow by default sets the From parameter, which is displayed in the From field of the message headers, to the name portion of the reply-to address. For example, if the reply-to address is `Workflow@mycompany.com`, the notification mailer sets the From parameter to `Workflow`.
  >
  > If you disable inbound processing, Oracle Workflow by default sets both the Reply-To Address parameter and the From parameter to `nobody@<server_name>`, where *`<server_name>`* is the name of the outbound SMTP mail server.
  >
  > To specify a different From value, navigate to the advanced configuration wizard.

- **Inbound SSL Enabled** - Select this parameter to enable the notification mailer to use SSL for connections to the IMAP server. Deselect this parameter to use non-SSL connections.

  > **Note:** When you enable SSL, the notification mailer connects to the IMAP server through port 993 by default. You can optionally specify a different port number along with the IMAP server name in the Inbound E-mail Account (IMAP): Server Name parameter.

Before you can use SSL, you must also complete additional setup steps. See: Connecting to Mail Servers Through SSL, *Oracle Workflow Administrator's Guide*.

> **Note:** The notification mailer requires three folders in the IMAP mail account: the inbox, a folder to store processed messages, and a folder to store discarded messages. If you enable inbound processing and the mail account you specify in the Username parameter does not already include folders named PROCESS and DISCARD, Oracle Workflow automatically creates these two folders. To specify other folders for the notification mailer, navigate to the advanced configuration wizard.

> **Note:** If you enable inbound processing, the notification mailer uses the Workflow Open Mail (Templated) message, which provides a response template for sending responses by e-mail, as the default message template for e-mail notifications that require a response. If you disable inbound processing, the notification mailer uses the Workflow Open Mail (Outlook Express) message, which provides a link in HTML notifications for entering responses in the Notification Details page, as the default message template for e-mail notifications that require a response. To specify other message templates, navigate to the advanced configuration wizard.
>
> Note that the plain text version of the Workflow Open Mail (Outlook Express) message requests a response by e-mail. If you disable inbound processing, ensure that your users do not have a notification preference of MAILTEXT or MAILATTH. Alternatively, if you disable inbound processing and you want users to receive plain text notifications, use the advanced configuration wizard to specify a message template that directs recipients to respond from the Notification Details Web page, such as the standard Workflow View From UI message template or a custom message template.

To cancel any changes on this page, click the Cancel button.

To save this configuration, click the Apply button.

To send test messages, click the Test Mailer button. In the Test Notification Mailer page, select the recipient role to which the messages should be sent, and click the Send Test Message button.

> **Note:** To send a test message successfully, you must select a recipient role that either has a valid e-mail address defined, or that has members with valid e-mail addresses defined. The recipient role must also have a notification preference that includes individual e-mail notifications.
>
> If you set an override e-mail address for the notification mailer, the Test

> Notification Mailer page displays that address. In this case the test message is sent to the override address rather than the e-mail address of the recipient role. However, you must still select a recipient role to enable the notification mailer to send the test messages. See: Reviewing Service Component Details, page 3-13.

Oracle Workflow sends two test messages to the recipient role: one message with content built using PL/SQL and one message with Oracle Application Framework content. Check the e-mail account for the recipient role to view the test messages and reply to them with the Acknowledge response. If you did not implement inbound e-mail processing for this mailer, use the Worklist pages to respond to the test messages after viewing the outbound messages in e-mail. After you acknowledge both test messages, Oracle Workflow sends a confirmation message to the same recipient role to show that the notification mailer successfully processed the inbound response e-mails.

If you do not receive the test messages or the response confirmation message, or if the message content does not appear correctly, check the notification mailer setup, including the mail servers and the mailer configuration parameters. In particular, if the Oracle Application Framework content does not appear correctly, check the Application Framework Agent and WF: Workflow Mailer Framework Web Agent profile options, as well as the Framework User, Framework Responsibility, Framework Application ID, and Framework URL Timeout parameters in the advanced configuration wizard. See: Setting Up a Notification Mailer, page 3-22 and Message Generation, page 3-47.

> **Note:** Oracle Workflow sends the test messages by launching the PLSQL/OAFwk Response Test Process in the System: Tests (WFTESTS) item type. This item type is stored in a file called wftstmlr.wft in the `$FND_TOP/import/<lang>` subdirectory. You can optionally use the Status Monitor to check the status of the test process.

To set additional parameters for this notification mailer in the advanced configuration wizard, click the Advanced button.

Define

This page lets you define general attributes for the service component. Some attributes are already set to required values and cannot be modified. You must set attributes marked with an asterisk (*) to appropriate values for your environment before you can run the service component.

- **ID** - The configuration wizard displays the identifier for the service component.
- **Status** - The configuration wizard displays the status of the service component.
- **Name** - The name of the service component. This name must be unique. You can only edit the name when the notification mailer is not running. The name of the

seeded notification mailer service component is `Workflow Notification Mailer`, and you cannot change this value.

- **Startup Mode** - Select Automatic, Manual, or On-Demand as the startup mode for the service component. You can only edit the startup mode when the notification mailer is not running. The seeded Workflow Notification Mailer is assigned the Automatic startup mode by default, but you can optionally change this value.

- **Container Type** - The container type to which this service component belongs, which is always Oracle Applications Generic Service Management (Oracle Applications GSM).

- **Inbound Agent** - The Business Event System agent for inbound processing. The inbound agent for a notification mailer service component is always WF_NOTIFICATION_IN.

- **Outbound Agent** - The Business Event System agent for outbound processing. The outbound agent for a notification mailer service component is always WF_NOTIFICATION_OUT.

- **Correlation ID** - Enter a correlation ID value to determine which messages this notification mailer can process.

  - To create a general notification mailer that can process any message from any item type, leave the correlation ID blank. The seeded Workflow Notification Mailer has a blank correlation ID so that it can run as a general mailer to process all messages; you cannot change this setting.

  - To dedicate a notification mailer to processing messages from a particular item type, set the correlation ID to the internal item type name followed by a colon and a percent sign, in the following format:

    ```
    <item_type_name>:%
    ```

    For example:

    ```
    WFDEMO:%
    ```

  - To dedicate a notification mailer to processing instances of a particular message from a particular item type, set the correlation ID to the internal item type name followed by a colon and then the internal message name, in the following format:

    ```
    <item_type_name>:<message_name>
    ```

    For example:

    ```
    WFDEMO:APPROVE_REQUISITION
    ```

  By dedicating a notification mailer to a particular item type or message definition, you can increase throughput for the associated messages.

Both dedicated and general notification mailer components are compatible with each other. You can run several dedicated and general notification mailers at the same time if you choose. In this case, note that even if you have configured a dedicated mailer, a message that matches the dedicated notification mailer's correlation ID may still be processed by a general mailer if that mailer is the first to access the message.

To cancel any changes on this page, click the Cancel button.

To save these settings and proceed to the next step of the configuration wizard, click the Next button.

Details

This page lets you define detail attributes for the service component. You must set attributes marked with an asterisk (*) to appropriate values for your environment before you can run the service component. A refresh icon identifies attributes that can be refreshed dynamically while the service component is running.

- **ID** - The configuration wizard displays the identifier for the service component.
- **Status** - The configuration wizard displays the status of the service component.
- **Name** - The configuration wizard displays the name defined for the service component.
- **Container** - The container to which the service component will belong. Oracle Workflow provides a container called Workflow Mailer Service for notification mailer service components.
- **Maximum Idle Time** - If you selected the On-Demand startup mode for the service component, enter the maximum time in minutes that the service component can remain idle before it is stopped. An on-demand component that is stopped in this way will be restarted by its container when it is needed again to process new messages.
- **Max Error Count** - The number of consecutive errors the service component can encounter before its container stops it and changes its status to Stopped with Error. If an error is resolved and processing can continue, the error count is reset. The default value for the maximum error count is 10.
- **Inbound Thread Count** - Set the inbound processing thread count to 1 (one) to enable inbound message processing with this notification mailer. Select 0 (zero) to disable inbound message processing for this notification mailer and dedicate the notification mailer solely to outbound processing. If you selected the Inbound Processing parameter in the Basic Configuration page, the inbound thread count is set to 1; if you deselected the Inbound Processing parameter, the inbound thread count is set to 0.

The inbound thread count cannot be greater than 1, because only one thread can access the e-mail inbox at a time. If you disable inbound message processing for this notification mailer, but you still want to perform e-mail response processing, you should create at least one other notification mailer with the same node name that does perform inbound message processing. Otherwise, there will be no inbound mailer that can process incoming responses to outbound messages sent by this outbound mailer.

- **Outbound Thread Count** - Specify the number of outbound processing threads you want to execute simultaneously with this notification mailer. You can set the outbound thread count to 1 (one) or more depending on the volume of outbound messages you need to send. Specify 0 (zero) to disable outbound message processing for this notification mailer and dedicate the notification mailer solely to inbound processing. If you disable outbound message processing for this notification mailer, you should create at least one outbound notification mailer with the same node name. Otherwise, no inbound response messages will be marked with that node name and this inbound mailer will have no messages to process. The default value for the outbound thread count is 1.

- **Log Level** - Select the level of detail for the information you want to record in the service component container log. The recommended log level, which is also the default value, is Error. Usually the log level only needs to be changed if you want to record additional detailed information for debugging purposes. You can choose the following levels:

  - 1 - Statement
  - 2 - Procedure
  - 3 - Event
  - 4 - Exception
  - 5 - Error
  - 6 - Unexpected

- **Processor Read Wait Timeout** - Specify the amount of time in seconds that the service component's processing thread continues to wait, after reading the last message from its assigned queue, before timing out. If another message is received before this time expires, that message is processed and the timeout period begins again. If the timeout period expires and no more messages have been received, the service component stops reading and its sleep time begins. The default read timeout period for a notification mailer is 10 seconds.

- **Processor Min Loop Sleep** - Specify the minimum sleep time in seconds during which the service component waits, after its read timeout period expires, before it checks its queue for messages again. The default minimum sleep time for a notification mailer is 5 seconds.

- **Processor Max Loop Sleep** - Specify the maximum sleep time in seconds if you want to increase the sleep time between read attempts when no messages are received. If you specify a maximum sleep time that is greater than the minimum sleep time, then the service component initially waits for the minimum sleep time after it finishes reading messages from its queue. If no messages are read in subsequent attempts, then the sleep time between read attempts gradually increases until the maximum sleep time is reached. Increasing the sleep time can help enhance performance if messages are received infrequently. You can also specify 0 (zero) for this parameter to indicate that the sleep time should not be increased. In this case, the service component always waits for the minimum sleep time between read attempts. The default maximum sleep time for a notification mailer is 60 seconds.

- **Processor Error Loop Sleep** - Specify the sleep time in seconds during which the service component waits, after an error occurs, before it attempts to begin processing again. The default error sleep time for a notification mailer is 60 seconds.

- **Processor Close on Read Timeout** - Select this parameter to specify that the service component should close its connections after its read timeout period expires, when its sleep time begins. Deselect this parameter to specify that the connections should remain open until the processing thread stops.

  Selecting this parameter lets the notification mailer close its session with the IMAP server or SMTP server if it could not read a message from the IMAP inbox or from the database, respectively, before the read timeout period ended. For example, if an external process is accessing the IMAP inbox, the notification mailer may not be able to read or access the inbox for some time. In this case it may be advantageous for the notification mailer to close the existing connection, wait for a while, and then try to re-establish a new connection. Additionally, some IMAP servers may cause an idle session to time out and become invalid. In this case also, it is advantageous for the notification mailer to close the existing connection and re-establish a new one.

To cancel any changes on this page, click the Cancel button.

To return to the previous step of the configuration wizard, click the Back button.

To save these settings and proceed to the next step of the configuration wizard, click the Next button.

E-mail Servers

This page lets you define e-mail server parameters for the notification mailer. Some parameters are already set to required values and cannot be modified. You must set parameters marked with an asterisk (*) to appropriate values for your environment before you can run the notification mailer. A refresh icon identifies attributes that can be refreshed dynamically while the service component is running. If the notification mailer is currently running, then parameters marked with a refresh icon will be refreshed immediately when you select the Next button.

General

- **Mailer Node Name** - The node identifier name used by this notification mailer. The maximum length for a node name is eight characters. The node name cannot include any spaces or any of the following characters: left bracket ([), right bracket (]), slash (/), or at sign (@). The node name is included with the outgoing notification ID in outbound messages, and is used in inbound messages to identify the notification mailer that should process the messages. If you use the inbound and outbound thread count parameters to create notification mailers that are dedicated to either inbound or outbound processing, you should ensure that you assign the same node name to at least one outbound mailer and one inbound mailer, so that inbound mailer can process responses to messages sent by the outbound mailer. You can optionally assign the same node name to multiple mailers for load balancing purposes. However, each mailer that performs inbound processing for a node must have its own inbox. The default node name is WFMAIL.

  > **Note:** The node name for each node must be unique. However, multiple mailers can share the same node.

  If a particular notification message has the special #WFM_NODENAME message attribute defined, however, an outbound notification mailer will include the #WFM_NODENAME attribute value when sending the message, instead of the Mailer Node Name mailer parameter value.

- **Email Parser** - The Java class used to parse an incoming notification response e-mail formatted according to the templated response method and to create an XML document for the response. The notification mailer uses this parser when the Direct Response parameter is deselected. The default standard e-mail parser provided by Oracle Workflow is named oracle.apps.fnd.wf.mailer.TemplatedEmailParser. Usually you do not need to change this value.

  If you are not implementing inbound e-mail processing for this mailer, leave the default as a placeholder value.

  > **Note:** You do not need to change the value of the Email Parser parameter if you select the Direct Response parameter. The notification mailer automatically switches to the alternate e-mail parser when the Direct Response parameter is selected.

- **Alternate Email Parser** - The Java class used to parse an incoming notification response e-mail formatted according to the direct response method and to create an XML document for the response. The notification mailer uses this parser when the

Direct Response parameter is selected. The default alternate e-mail parser provided by Oracle Workflow is named oracle.apps.fnd.wf.mailer.DirectEmailParser. Usually you do not need to change this value.

If you are not implementing inbound e-mail processing for this mailer, leave the default as a placeholder value.

> **Note:** You do not need to change the value of the Alternate Email Parser parameter if you deselect the Direct Response parameter. The notification mailer automatically switches to the standard e-mail parser when the Direct Response parameter is deselected.

- **Expunge Inbox on Close** - Select this parameter to purge deleted messages from the inbox folder when the notification mailer closes this folder. If you do not select this parameter, copies of messages that were moved to the discard or processed folders remain in the inbox, in a deleted state, until you manually expunge them using your e-mail application.

Inbound E-mail Account

- **Inbound Protocol** - Oracle Workflow currently supports the IMAP protocol for inbound e-mail.

- **Inbound Server Name** - The name of the inbound mail server. Note that you must specify the actual host name for the server. Do not use `localhost` as the setting for this parameter. You can optionally specify the port number to use on that server. If you do not specify a port number, the notification mailer uses port 143 by default. Specify the server in the following format: `<server_name>[:<port_number>]`

  For example: `myimapserver.mycompany.com:143`

  If you are not implementing inbound e-mail processing for this mailer, enter a placeholder value.

- **Username** - The user name of the mail account that the notification mailer uses to receive e-mail messages.

  If you are not implementing inbound e-mail processing for this mailer, enter a placeholder value.

- **Password** - The password for the mail account specified in the Username parameter. The password value is masked as asterisks in the display and is stored in encrypted form.

  If you are not implementing inbound e-mail processing for this mailer, enter a placeholder value.

- **Inbox Folder** - The name of the folder from which the notification mailer receives inbound messages. This value is case-insensitive. The default value is `INBOX`. The inbox must be separate from the processed and discard folders. Each notification mailer that performs inbound processing should have its own separate inbox.

> **Note:** Usually, you use a dedicated mail account for notification mailer processing. If you want to use a mail account for the notification mailer that you also use for other purposes, you should create a folder in that account where you will place inbound messages destined for the notification mailer and specify that folder in the Inbox Folder parameter. Otherwise, the notification mailer will attempt to process all messages in the regular inbox and discard any messages that are not notification responses. If you do specify a separate folder to use as the notification mailer inbox folder, however, you must move messages from the regular inbox to that separate folder yourself. Depending on your mail program, you may be able to create a filter in the mail account to move such messages automatically. Use your e-mail client to create the separate folder. A notification mailer may not be able to access folders that were created using command line tools outside the e-mail client.

If you are not implementing inbound e-mail processing for this mailer, leave the default as a placeholder value.

- **Inbound Connection Timeout** - The maximum amount of time, in seconds, that the notification mailer will wait to establish a connection to the inbound server before timing out. The default inbound connection timeout period for a notification mailer is 120 seconds.

- **Inbound Message Fetch Size** - The maximum number of messages that the notification mailer can fetch from the inbox at one time. The default inbound message fetch size is 100 messages.

- **Maximum Ignore List Size** - The maximum number of notification IDs that the notification mailer can store in its ignore list, indicating that this notification mailer will make no further attempts to process them. For example, if the mailer encountered a connection error while processing a notification, that notification ID is temporarily added to the ignore list, and is then removed from the list the next time the inbox folder is successfully closed. The default maximum ignore list size is 1000. Usually you do not need to change this value.

  > **Note:** If the notification mailer finds additional messages to be ignored in the inbox when the ignore list is already full, the notification mailer removes the oldest notification IDs from the list and adds the new notification IDs instead.

- **Inbound SSL Enabled** - Select this parameter to enable the notification mailer to use SSL for connections to the IMAP server. Deselect this parameter to use non-SSL connections.

  > **Note:** When you enable SSL, the notification mailer connects to the IMAP server through port 993 by default. You can optionally specify a different port number along with the IMAP server name in the Inbound Server Name parameter.

  Before you can use SSL, you must also complete additional setup steps. See: Connecting to Mail Servers Through SSL, *Oracle Workflow Administrator's Guide*.

Outbound E-mail Account

- **Outbound Protocol** - Oracle Workflow currently supports the SMTP protocol for outbound e-mail.

- **Outbound Server Name** - The name of the outbound mail server. Note that you must specify the actual host name for the server. Do not use `localhost` as the setting for this parameter. You can optionally specify the port number to use on that server. If you do not specify a port number, the notification mailer uses port 25 by default. Specify the server in the following format: `<server_name>[:<port_number>]`

  For example: `mysmtpserver.mycompany.com:25`

  If you are not implementing outbound e-mail processing for this mailer, enter a placeholder value.

- **Username** - If the outbound SMTP server is configured to require authentication, enter the user name of the account that the notification mailer uses to connect to the SMTP server.

- **Password** - If the outbound SMTP server is configured to require authentication, enter the password for the account specified in the Username parameter. The password value is masked as asterisks in the display and is stored in encrypted form.

- **Test Address** - This parameter has been replaced by the override e-mail address, which is available through the Component Details page for a notification mailer. See: Reviewing Service Component Details, page 3-13.

- **Outbound Connection Timeout** - The maximum amount of time, in seconds, that the notification mailer will wait to establish a connection to the outbound server before timing out. The default outbound connection timeout period for a notification mailer is 120 seconds.

- **Outbound SSL Enabled** - Select this parameter to enable the notification mailer to use Secure Sockets Layer (SSL) for connections to the SMTP server. Deselect this parameter to use non-SSL connections.

> **Note:** When you enable SSL, the notification mailer connects to the SMTP server through port 465 by default. You can optionally specify a different port number along with the SMTP server name in the Outbound Server Name parameter.

Before you can use SSL, you must also complete additional setup steps. See: Connecting to Mail Servers Through SSL, *Oracle Workflow Administrator's Guide*.

E-mail Processing

- **Processed Folder** - The name of the mail folder where the notification mailer places successfully processed notification messages. This value is case-insensitive. The processed folder must be separate from the inbox and the discard folder.

  The default value for this parameter is `PROCESS`. If you enabled inbound processing in the Basic Configuration page and the mail account you specified did not already include a folder named `PROCESS`, Oracle Workflow automatically created a folder with this name in that account when you completed the basic notification mailer configuration.

  You can optionally specify the name of a different folder in this parameter. In this case, ensure that you use your e-mail client to create the folder. A notification mailer may not be able to access folders that were created using command line tools outside the e-mail client.

  > **Note:** The notification mailer does not perform any further operations on messages in the processed folder. You can review, back up, or delete these messages through your e-mail application if necessary.

  If you are not implementing inbound e-mail processing for this mailer, leave the default as a placeholder value.

- **Discard Folder** - The name of the mail folder where the notification mailer places incoming messages that are not recognized as notification messages. This value is case-insensitive. The discard folder must be separate from the inbox and the processed folder.

  The default value for this parameter is `DISCARD` If you enabled inbound processing in the Basic Configuration page and the mail account you specified did not already include a folder named `DISCARD`, Oracle Workflow automatically created a folder with this name in that account when you completed the basic notification mailer configuration.

  You can optionally specify the name of a different folder in this parameter. In this case, ensure that you use your e-mail client to create the folder. A notification mailer may not be able to access folders that were created using command line tools outside the e-mail client.

> **Note:** The notification mailer does not perform any further operations on messages in the discard folder. You can review, back up, or delete these messages through your e-mail application if necessary.

If you are not implementing inbound e-mail processing for this mailer, leave the default as a placeholder value.

- **Allow Forwarded Response** - Indicate whether to allow a user to respond by e-mail to an e-mail notification that has been forwarded from another role. This parameter is selected by default.

  - If Allow Forwarded Response is selected, the notification mailer never checks the "From" e-mail address of the notification response and always allows the response to be processed.

  - If Allow Forwarded Response is deselected, the notification mailer will check whether the "From" e-mail address of the notification response exactly matches the e-mail address of the recorded recipient role or the e-mail address of a user in that role. If the two e-mail addresses match exactly, meaning the notification was not forwarded or was forwarded according to a valid routing rule, the notification mailer treats the response as a valid response. If the two e-mail addresses do not match exactly, meaning the notification was simply forwarded using the e-mail Forward command, the notification mailer does not process the response and treats it as unsolicited mail.

    > **Note:** Note that there are limitations when you deselect Allow Forwarded Response. For example, suppose a notification is sent to a distribution list mail alias that does not have a user/role relationship in the Oracle Workflow directory service. If any user from the distribution list responds to the notification, the notification mailer will always treat that notification response as unsolicited mail, because the "From" e-mail address, which is an individual user's e-mail address, will never match the distribution list mail alias.

To cancel any changes on this page, click the Cancel button.

To return to the previous step of the configuration wizard, click the Back button.

To save these settings and proceed to the next step of the configuration wizard, click the Next button.

> **Note:** When you click the Next button, the configuration wizard validates the parameters you entered. If the inbound thread count is set to 1, the configuration wizard also verifies that it can connect to the e-mail account on the specified inbound mail server with the specified user name and password, and that the folders specified in the Processed Folder and Discard Folder parameters exist in that e-mail account. If the parameters are successfully validated, and the notification mailer is currently running, then Oracle Workflow Manager immediately refreshes the notification mailer with the new parameters.

Message Generation

This page lets you define message generation parameters for the notification mailer. Some parameters are already set to required values and cannot be modified. You must set parameters marked with an asterisk (*) to appropriate values for your environment before you can run the notification mailer. A refresh icon identifies attributes that can be refreshed dynamically while the service component is running. If the notification mailer is currently running, parameters marked with a refresh icon will be refreshed immediately when you select the Next button or the Finish button.

Send

- **From** - A value that appears in the From field of the message header of a notification e-mail. You can specify the From parameter value either as a display name only, or as a full RFC822-compliant address.

  - If you specify a display name only, the notification mailer adds the e-mail address from the Reply-to Address parameter to create a full RFC822-compliant address for the From message header. The full address is created in the following format: `"`*`Display Name`*`" <`*`reply_to_address`*`>`

  - If you specify a full RFC822-compliant address, the notification mailer uses only that From parameter value in the From message header, and does not include the Reply-to Address value.

  If a particular notification message has the special #WFM_FROM message attribute defined, however, the notification mailer will use the #WFM_FROM attribute value in the From field for that message, instead of the From parameter value.

  The default From parameter value for the seeded notification mailer service component is `Workflow Mailer`. For other notification mailers, if you selected the Inbound Processing parameter in the Basic Configuration page, Oracle Workflow by default sets the From parameter to the name portion of the reply-to address specified in the Basic Configuration page. For example, if the reply-to address is `Workflow@mycompany.com`, Oracle Workflow sets the From parameter to `Workflow`.

If you deselected the Inbound Processing parameter in the Basic Configuration page, Oracle Workflow by default sets the From parameter to `nobody@`*`<server_name>`*, where *`<server_name>`* is the name of the outbound SMTP mail server specified in the Basic Configuration page.

If you are not implementing outbound e-mail processing for this mailer, leave the default as a placeholder value.

- **Reply-to Address** - The address of the e-mail account that receives incoming messages, to which notification responses should be sent. This value must be a full RFC822-compliant e-mail address.

  If a particular notification message has the special #WFM_REPLYTO message attribute defined, however, the notification mailer will use the #WFM_REPLYTO attribute value as the reply address for that message, instead of the Reply-to Address parameter value.

  > **Note:** If the From parameter value is specified as a display name only, then the notification mailer also uses the reply-to e-mail address together with that display name to create a full RFC822-compliant address for the From field of the message header.

  If you deselected the Inbound Processing parameter in the Basic Configuration page, Oracle Workflow by default sets the Reply-to Address parameter to `nobody@`*`<server_name>`*, where *`<server_name>`* is the name of the outbound SMTP mail server specified in the Basic Configuration page. If you are not implementing inbound e-mail processing for this mailer, leave the default as a placeholder value.

- **HTML Agent** - The base URL that identifies the HTML agent that handles HTML notification responses. This URL is required to support e-mail notifications with HTML attachments. Usually the HTML agent specified here can match the value of the Applications Servlet Agent profile option; however, you can optionally specify a different HTML agent for a particular notification mailer. The HTML agent should be specified in the following format:

  ```
  http://<server_name:port>/OA_HTML/
  ```

  where *`<server_name:port>`* represents the server and TCP/IP port number on which your servlet agent accepts requests.

  > **Note:** The notification mailer can also still handle an HTML agent value in the previous format:
  >
  > ```
  > http://<server_name:port>/pls/wf
  > ```

  If a particular notification message has the special #WFM_HTMLAGENT message attribute defined, however, the notification mailer will use the

#WFM_HTMLAGENT attribute value as the HTML agent for that message, instead of the HTML Agent mailer parameter value.

- **Message Formatter** - Oracle Workflow uses the oracle.apps.fnd.wf.mailer.NotificationFormatter Java class to generate notification messages.

- **Framework User** - The numerical user ID for the user through which a notification mailer accesses Oracle Application Framework content for inclusion in e-mail notifications. The Framework user must have workflow administrator privileges in order to access the content for every user's notifications.

  The default value for this parameter is `0`, which is the user ID for the `SYSADMIN` user. This setting lets the notification mailer access Oracle Application Framework content through the `SYSADMIN` user, which is also the default workflow administrator role. If you change the Workflow System Administrator preference, check the Framework User parameter to ensure that the user accessed by the notification mailer has workflow administrator privileges. Set the Framework User parameter to a user that is a member of the Workflow System Administrator role, or, if you set the Workflow System Administrator preference to a responsibility, set the Framework User parameter to a user that has that responsibility. See: Setting Global User Preferences, *Oracle Workflow Administrator's Guide*.

  > **Note:** You can use the Workflow Mailer URL Access Tester page to test whether Oracle Application Framework content can be generated correctly for e-mail notifications. See: Testing Mailer URL Access, *Oracle Workflow Administrator's Guide*.

- **Framework Responsibility** - The numerical responsibility ID for the responsibility through which a notification mailer accesses Oracle Application Framework content for inclusion in e-mail notifications. The user specified in the Framework User parameter must have this responsibility assigned. The default value for this parameter is `20420`, which is the responsibility ID for the System Administrator responsibility.

- **Framework Application ID** - The numerical application ID for the application through which a notification mailer accesses Oracle Application Framework content for inclusion in e-mail notifications. The responsibility specified in the Framework Responsibility parameter must be assigned to this application. The default value for this parameter is `1`, which is the application ID for the System Administration application.

- **Framework URL Timeout** - The maximum amount of time, in seconds, that the notification mailer will wait to access a URL for Oracle Application Framework content before timing out. The default Framework URL timeout period for a notification mailer is 30 seconds.

- **Attach Images to Outbound Emails** - Select this parameter to attach any images referenced in HTML content included in a message, such as Oracle Application Framework content, to outbound notification e-mail messages. Deselect this parameter to display the image references as off-page URLs instead of attaching the images.

- **Attach Stylesheet to Outbound Email** - Select this parameter to attach any stylesheet referenced in HTML content included in a message, such as Oracle Application Framework content, to outbound notification e-mail messages. Deselect this parameter to display the stylesheet reference as a URL instead of attaching the stylesheet.

  > **Note:** E-mail clients vary in their support for stylesheet references within HTML content in the body of an e-mail. Some e-mail clients do not support references to a stylesheet that is attached to the e-mail, while others do not support any form of stylesheet references within HTML content at all. Consequently, attaching a stylesheet may not have the same effect in all e-mail clients.

- **Autoclose FYI** - Indicate whether this notification mailer automatically closes notifications that do not require a response, such as FYI (For Your Information) notifications, after sending the notifications by e-mail. This parameter is selected by default. If Autoclose FYI is deselected, all FYI notifications will remain open in the Worklist until users manually close these notifications.

- **Direct Response** - By default, notification mailers require a response format for plain text notifications called the templated response method. Select this parameter to use the direct response method instead.

  - With the templated response method, a notification mailer sends plain text notifications requiring a templated response to users with a notification preference of `MAILTEXT` or `MAILATTH`. Users must reply using a template of response prompts and enter their response values between the quotes following each prompt.

  - With the direct response method, a notification mailer sends plain text notifications requiring a direct response to users with a notification preference of `MAILTEXT` or `MAILATTH`. Users must enter their response values directly as the first lines of a reply.

    > **Note:** Responses that are generated automatically from an HTML-formatted notification or attachment must always use a response template, regardless of which response method you select.

  See: Workflow Open Mail (Templated) Message, *Oracle Workflow Administrator's*

Guide, Workflow Open Mail (Direct) Message, *Oracle Workflow Administrator's Guide*, To Respond to a Plain Text E-mail Notification Using Templated Response, *Oracle Workflow User's Guide*, To Respond to a Plain Text E-mail Notification Using Direct Response, *Oracle Workflow User's Guide*, and Example 'Respond' Message Attributes, *Oracle Workflow Developer's Guide*.

- **Reset NLS** - Indicate whether the notification mailer should convert the NLS codeset for a notification message according to the notification recipient's preferences before composing the message. This parameter is deselected by default. If Reset NLS is selected, the notification mailer will convert the message to the codeset listed in the WF_LANGUAGES table for the language and territory specified in the recipient's user preferences. If no preferred territory is specified, the notification mailer will use the codeset associated with the first entry it encounters for the user's preferred language. If neither a language nor a territory is specified in the user preferences, the notification mailer will use the codeset seeded in WF_LANGUAGES for the language AMERICAN and territory AMERICA. This parameter is relevant when there are several languages installed in the database and the character set of the user's e-mail client is not the same as the one specified for the database. For example, when a UTF8 database is used, the character set of e-mail clients used in Western Europe is generally 'Western (ISO-8859-1)'. In this case, selecting the Reset NLS parameter means that users who specify a Western European language such as French or German in their user preferences will receive any e-mail notification messages in the correct character set for the e-mail client.

  If a particular notification message has the special #WFM_RESET_NLS message attribute defined, however, the notification mailer will use the #WFM_RESET_NLS attribute value to determine whether or not to encode the e-mail to the preferred codeset for that message, instead of using the Reset NLS parameter value.

- **Inline Attachments** - Select this parameter to set the Content-Disposition MIME header to `inline` for attachments to notification messages, including the Notification Detail Link, HTML Message Body, Notification References containing attached URLs, and attached PL/SQL documents. Deselect this parameter to set the Content-Disposition MIME header to `attachment` for these attachments. For example, if your e-mail application cannot display HTML content such as the Notification Detail Link inline, deselect this parameter to display this link as an attachment instead. Note, however, that some e-mail clients may not support the Content-Disposition header, or may support it in varying ways. Consequently, the Inline Attachment setting may not always have the desired effect, depending on the e-mail clients with which users read their e-mail messages.

- **Send Warning for Unsolicited E-mail** - Select this parameter to allow the notification mailer to send back a warning message the first time it receives an unsolicited e-mail message from a particular e-mail address. Deselect this parameter to prevent the notification mailer from sending warning messages.

- **Send E-mails for Canceled Notifications** - Select this parameter to allow the notification mailer to send cancellation messages to users when previously sent notifications are canceled. Deselect this parameter to prevent the notification mailer from sending cancellation messages.

If you set up multiple notification mailers in the same Oracle E-Business Suite instance, you must set this parameter to the same setting for all the notification mailers.

Templates

This region lets you specify the message templates you want to use to generate e-mail notifications. The template for a particular type of e-mail notification determines the basic format of the notification, including what header information to include, and whether and where to include details such as the message due date and priority.

Oracle Workflow provides a set of standard templates in the System: Mailer item type, which are used by default. It is not recommended to modify the standard templates. However, you can customize the message templates used to send your e-mail notifications by creating your own custom message templates in the System: Mailer item type using the Workflow Builder, and assigning these templates to a particular notification mailer service component in this region. The templates assigned to a mailer override the default System: Mailer templates.

Additionally, you can create your own custom message templates in a custom item type using the Workflow Builder, and assign these templates to a particular notification in a workflow process by defining special message attributes. In this case the templates assigned to the notification override both the templates assigned to a mailer and the default System: Mailer templates.

If you are not implementing outbound e-mail processing for this mailer, leave the default templates as placeholder values.

- **Attached URLs** - The notification mailer uses this template to create the Notification References attachment for HTML-formatted notification messages that include URL attributes with Attach Content checked. The template must includes a list with links to each URL.

- **Outbound Closed Notification** - The notification mailer uses this template to inform the recipient that a previously sent notification is now closed.

- **Outbound Cancelled Notification** - The notification mailer uses this template to inform the recipient that a previously sent notification is canceled. You can optionally use the Send E-mails for Canceled Notifications parameter to specify whether or not the notification mailer should send Outbound Cancelled Notification messages.

- **Invalid Response Notification** - The notification mailer uses this template to inform a user that the user responded incorrectly to a notification. For example, if a response message from a user contains a valid notification ID (NID) line matching it with a notification, but does not contain any response value or contains an invalid response value, the notification mailer sends an Invalid Response Notification message to the user. This template must describe how to respond to the notification correctly.

- **Open Notification** - If you are using the default response method, which is templated response, the notification mailer uses this template to send open notifications that require a response. This message template must provide a response template for the recipient as well as instructions on how to use the response template.

  > **Note:** In addition to the default Workflow Open Mail (Templated) message template, Oracle Workflow also provides a predefined template called Workflow Open Mail (Outlook Express). This template is provided to accommodate e-mail applications such as Microsoft Outlook Express or other e-mail clients that cannot process the response links included in the HTML bodies of the Workflow Open Mail (Templated) and Workflow Open Mail (Direct) templates. If you use one of these e-mail clients, you can select the Workflow Open Mail (Outlook Express) message template to have HTML e-mail notifications include a link to the Notification Details Web page which lets users respond to the notification there.

If you are configuring this notification mailer for outbound message processing only and you are not implementing any corresponding inbound e-mail response processing, then you should set the Open Notification parameter to a message template that does not request a response by e-mail, but instead directs recipients to respond from the Notification Details Web page. For example, you can select the Workflow View From UI message template provided by Oracle Workflow, or create your own custom message template.

If you selected the Inbound Processing parameter in the Basic Configuration page, the Open Notification parameter is set to the Workflow Open Mail (Templated) message template by default. If you deselected the Inbound Processing parameter, the Open Notification parameter is set to the Workflow Open Mail (Outlook Express) message template by default.

> **Note:** The plain text version of the Workflow Open Mail (Outlook Express) message requests a response by e-mail. If you disable inbound processing, ensure that your users do not have a notification preference of MAILTEXT or MAILATTH. Alternatively, if you disable inbound processing and you want users to receive plain text notifications, specify a message template that directs recipients to respond from the Notification Details Web

page.

- **Open Notification (Direct Response Parsing)** - If you select the Direct Response parameter, the notification mailer uses this template to send open notifications that require a response. The response instructions in the plain text message body must describe how to reply using the direct response method. This message is used for notifications sent to performers with a notification preference of MAILTEXT or MAILATTH. The response instructions in the HTML-formatted message body must describe how to reply using the automatically generated response template. This message is used for notifications sent to performers with a notification preference of MAILHTML or MAILHTM2, and is also attached to notifications sent to performers with a notification preference of MAILATTH.

  > **Note:** Responses that are generated automatically from an HTML-formatted notification or attachment must always use a response template, regardless of which response method you select.

  > **Note:** If you are configuring this notification mailer for outbound message processing only and you are not implementing any corresponding inbound e-mail response processing, then you should set the Open Notification (Direct Response Parsing) parameter to a message template that does not request a response by e-mail, but instead directs recipients to respond from the Notification Details Web page. For example, you can select the Workflow View From UI message template provided by Oracle Workflow, or create your own custom message template.

  See: Workflow Open Mail (Templated) Message, *Oracle Workflow Administrator's Guide*, Workflow Open Mail (Direct) Message, *Oracle Workflow Administrator's Guide* , To Respond to a Plain Text E-mail Notification Using Templated Response, *Oracle Workflow User's Guide*, To Respond to a Plain Text E-mail Notification Using Direct Response, *Oracle Workflow User's Guide*, and Example 'Respond' Message Attributes, *Oracle Workflow Developer's Guide*.

- **Open FYI Notification** - The notification mailer uses this template to send notifications that do not require a response. The template must indicate that the notification is for your information (FYI) and does not require a response.

- **Outbound Summary Notification** - This template is no longer used.

- **Outbound Warning Notification** - The notification mailer uses this template to send a message to a user the first time it receives unsolicited mail from that user. For example, if a message from a user does not contain a notification ID (NID) line matching it with a notification, or contains an incorrectly formatted NID line, the notification mailer sends an Outbound Warning Notification message to the user. You can optionally use the Send Warning for Unsolicited E-mail parameter to specify whether or not the notification mailer should send Outbound Warning Notification messages.

- **Open Notification (More Information Request)** - The notification mailer uses this template to send a request for more information about a notification from one user to another user.

  > **Note:** If you use an e-mail application such as Microsoft Outlook Express that cannot process the response link included in the default Workflow Open Mail (More Information Request) message template, you can select an alternative template named Workflow More Information Request (Outlook Express) instead. In particular, if you set the Open Notification parameter to use the Workflow Open Mail (Outlook Express) message, then you should also set the Open Notification (More Information Request) parameter to use the Workflow More Information Request (Outlook Express) message.

- **Outbound HTML Summary Notification** - The notification mailer uses this template to send a summary of currently open workflow notifications to users and roles that have their notification preference set to SUMMARY or SUMHTML in the Oracle Workflow directory service.

To cancel any changes on this page, click the Cancel button.

To return to the previous step of the configuration wizard, click the Back button.

To save these settings and proceed to the next step of the configuration wizard, click the Next button.

To save these settings and proceed to the last step of the configuration wizard, click the Finish button.

> **Note:** When you click the Next or Finish button, the configuration wizard validates the parameters you entered. If the parameters are successfully validated, and the notification mailer is currently running, then Oracle Workflow Manager immediately refreshes the notification mailer with the new parameters.

Scheduling Events

This page lets you schedule events to control the running of the service component. The events are raised at the scheduled time by DBMS jobs. For a notification mailer service component, you can schedule the following events:

- Start
- Refresh
- Suspend
- Resume
- Stop
- Launch Summary Notifications

For each event, the list displays the event name, date and time when the event is first scheduled to be raised, the interval in minutes at which the event is reraised, and, for a Refresh event, any parameters to be refreshed. You can specify the following refreshable parameters, using the parameters' internal names, when you refresh the notification mailer.

- `PROCESSOR_IN_THREAD_COUNT` - Inbound Thread Count
- `PROCESSOR_OUT_THREAD_COUNT` - Outbound Thread Count
- `COMPONENT_LOG_LEVEL` - Log Level, specified as a numerical value
  - `1` - Statement
  - `2` - Procedure
  - `3` - Event
  - `4` - Exception
  - `5` - Error
  - `6` - Unexpected
- `EXPUNGE_ON_CLOSE` - Expunge Inbox on Close
- `ALLOW_FORWARDED_RESPONSE` - Allow Forwarded Response
- `FROM` - From
- `REPLYTO` - Reply-to Address
- `HTMLAGENT` - HTML Agent
- `ATTACH_IMAGES` - Attach Images to Outbound E-mails
- `ATTACH_STYLESHEET` - Attach Stylesheet to Outbound E-mail

- `AUTOCLOSE_FYI` - Autoclose FYI
- `RESET_NLS` - Reset NLS
- `INLINE_ATTACHMENT` - Inline Attachments
- `SEND_UNSOLICITED_WARNING` - Send Warning for Unsolicited E-mail
- `ATTACHED_URLS` - Attached URLs
- `CLOSED` - Outbound Closed Notification
- `CANCELED` - Outbound Cancelled Notification
- `OPEN_INVALID` - Invalid Response Notification
- `OPEN_MAIL` - Open Notification
- `OPEN_MAIL_DIRECT` - Open Notification (Direct Response Parsing)
- `OPEN_MAIL_FYI` - Open FYI Notification
- `SUMMARY` - Outbound Summary Notification
- `WARNING` - Outbound Warning Notification
- `OPEN_MORE_INFO` - Open Notification (More Information Request)
- `SUMHTML` - Outbound HTML Summary Notification

To schedule events:

- If no events are currently scheduled, click the Add a Row button to add a new row to the list of events and enter the information for the event.
  - Select the event for the command you want to schedule.
  - Select the date when you want the event to be raised first.
  - Select the hour and minute to specify the time on the specified date when you want the event to be raised first. The hour values are in a twenty-four hour format. For example, select 00 for midnight, or 23 for 11 PM.
  - If you want to raise the event periodically, enter the time interval in minutes at which you want to raise the event. If you do not specify a repeating interval, the event is raised only once.
  - If you choose the refresh event, you can optionally enter any parameters you want to include with the event in order to refresh the notification mailer

configuration parameters with those values when the event is raised. Specify the parameter names and values in the following format, separating the parameters with a colon (:): `internal_parameter_name=parameter_value`

For example: `PROCESSOR_OUT_THREAD_COUNT=3`

- To schedule another event, click the Add Another Row button and enter the information for the event.

- To remove an event, select the event and click the Remove button.

To cancel any changes on this page, click the Cancel button.

To return to the previous step of the configuration wizard, click the Back button.

To save these settings and proceed to the next step of the configuration wizard, click the Next button.

To save these settings and proceed to the last step of the configuration wizard, click the Finish button.

> **Note:** The configuration wizard verifies that an event is specified for every row in the list when you click the Next or Finish button. If you do not want to schedule another event, remove any empty rows before proceeding.

Tags

This page lets you enter patterns of text found in unusual messages and the status you want to assign to an inbound message if it contains any of those patterns. For example, unusual messages include bounced or returned messages and auto-reply messages such as those sent by vacation daemons, mass mailing lists, and so on. Since different mail systems vary in how they identify bounced, undeliverable, or otherwise invalid messages, you can use notification mailer tags to specify how your mail system identifies those stray messages and how you want the notification mailer to handle those messages should it come across them.

Oracle Workflow provides several predefined tags for text commonly found in undeliverable or auto-reply messages. For each tag, the list displays the pattern, which is the string of text to look for in the From line, Subject line, or body of the message, and the action, which is the mail status to assign to the message if that pattern is found. The notification mailer handles messages according to these mail status values, as follows:

- UNDELVRD - Moves the message to the discard folder and updates the notification's mail status to FAILED. Additionally, the notification preference of the recipient of the notification is updated to DISABLED. No error process is initiated for this notification activity. However, after correcting the issues that prevented the e-mail from being sent, you can reset the user's notification preference and then run the Resend Failed/Error Workflow Notifications program to re-enqueue failed notifications on the notification mailer's outbound queue. See: Handling Mailer Errors, *Oracle Workflow Administrator's Guide*.

- Unavailable - Moves the message to the discard folder and continues waiting for a reply to the notification since the notification's status is still OPEN, but its mail status is updated to UNAVAIL. This status is purely informative, as no further processing occurs with this notification.

- Ignore - Moves the message to the discard folder and continues waiting for a valid reply to the open notification. The notification's status is still OPEN and its mail status is still SENT.

You can define additional tags for other patterns you want the notification mailer to handle automatically.

- To add a new tag, click the Add Another Row button, enter the text pattern in the Pattern column, and select the status you want to assign to messages containing that pattern in the Action column.

- To remove a tag, select the tag and click the Remove button. You can only remove custom tags that you defined. You cannot remove predefined tags provided by Oracle Workflow.

> **Note:** It is important that you uniquely identify bounced messages and auto-replies by defining tags to distinguish them from normal responses. If you do not identify bounced and auto-reply messages, the notification mailer can mistake these as invalid responses, send an Invalid Response Notification message, and continue to wait for a reply. In both cases a perpetual loop would occur where the notification mailer continues sending out an 'Invalid' message and the 'Invalid' message bounces back or is auto-replied each time.

> **Note:** Only a message response that contains a notification ID can be handled through the FAILED and UNAVAIL mail statuses. If the notification mailer receives a message response that does not contain a notification ID, it moves the message response to the discard folder. If the Send Warning for Unsolicited E-mail parameter is selected, then for the first such message from a particular e-mail address, the notification mailer also sends an Outbound Warning Notification message to the sender to warn that it received unsolicited mail.

> **Note:** If a message response matches more than one pattern in the list of tags, the message is tagged with the status of the first tag it matches.

> That is, the notification mailer performs a top to bottom comparison against the tag list. Due to this behavior, you should prioritize your patterns listing the UNDELVRD tags first, followed by the Unavailable and then Ignore tags.

To cancel any changes on this page, click the Cancel button.

To return to the previous step of the configuration wizard, click the Back button.

To save these settings and proceed to the next step of the configuration wizard, click the Next button.

To save these settings and proceed to the last step of the configuration wizard, click the Finish button.

Test

This page lets you test the configuration for a notification mailer that performs outbound e-mail processing by sending sample notification messages. Select the recipient role to which the messages should be sent, and click the Send Test Message button.

> **Note:** To send a test message successfully, you must select a recipient role that either has a valid e-mail address defined, or that has members with valid e-mail addresses defined. The recipient role must also have a notification preference that includes individual e-mail notifications.
>
> If you set an override e-mail address for the notification mailer, the Test page displays that address. In this case the test message is sent to the override address rather than the e-mail address of the recipient role. However, you must still select a recipient role to enable the notification mailer to send the test messages. See: Reviewing Service Component Details, page 3-13.

Oracle Workflow sends two test messages to the recipient role: one message with content built using PL/SQL and one message with Oracle Application Framework content. Check the e-mail account for the recipient role to view the test messages and reply to them with the Acknowledge response. If you did not implement inbound e-mail processing for this mailer, use the Worklist pages to respond to the test messages after viewing the outbound messages in e-mail. After you acknowledge both test messages, Oracle Workflow sends a confirmation message to the same recipient role to show that the notification mailer successfully processed the inbound response e-mails.

If you do not receive the test messages or the response confirmation message, or if the message content does not appear correctly, check the notification mailer setup, including the mail servers and the mailer configuration parameters. In particular, if the Oracle Application Framework content does not appear correctly, check the Application Framework Agent and WF: Workflow Mailer Framework Web Agent profile options, as well as the Framework User, Framework Responsibility, Framework Application ID, and Framework URL Timeout parameters in the advanced configuration wizard. See: Setting Up a Notification Mailer, page 3-22 and Message Generation, page 3-47.

> **Note:** Oracle Workflow sends the test messages by launching the PLSQL/OAFwk Response Test Process in the System: Tests (WFTESTS) item type. This item type is stored in a file called wftstmlr.wft in the `$FND_TOP/import/<lang>` subdirectory. You can optionally use the Status Monitor to check the status of the test process.

To exit the advanced configuration wizard, click the Cancel button.

To return to the previous step of the configuration wizard, click the Back button.

To proceed to the next step of the configuration wizard, click the Next button.

To proceed to the last step of the configuration wizard, click the Finish button.

Review

This page lets you review the configuration parameter values that you set, the events that you scheduled, and the tags that you defined for this notification mailer service component.

- If you want to change any of these settings, return to the appropriate step in the configuration wizard to make your changes. To return to the previous step, click the Back button.
- To save these settings and finish the configuration, click the Finish button.

Agent Listeners

The Oracle Workflow Business Event System requires agent listeners to be scheduled to receive inbound event messages. An agent listener monitors a Business Event System agent for incoming messages and dequeues messages using the agent's queue handler. You should run agent listeners for your local inbound agents. Run PL/SQL agent listeners to process event subscriptions with a PL/SQL rule function in the database, and run Java agent listeners to process event subscriptions with a Java rule function in the middle tier.

When an event message is dequeued, the Event Manager begins subscription processing for the event. The Event Manager searches for and executes any active subscriptions by the local system to that event with a source type of External, and also any active subscriptions by the local system to the Any event with a source type of External. The agent listener exits after all event messages on the agent's queue have been dequeued.

The PL/SQL agent listener program is defined as a service component type in the Generic Service Component Framework. This framework helps to simplify and automate the management of background Java services.

Oracle Workflow provides several seeded agent listener service components to process messages on standard agents.

- Workflow Deferred Agent Listener - Handles messages on WF_DEFERRED to support deferred subscription processing. This service component is started automatically by its container.

- Workflow Deferred Notification Agent Listener - Handles notification messages on WF_DEFERRED to support outbound notification processing. This service component is started automatically by its container.

- Workflow Error Agent Listener - Handles messages on WF_ERROR to support error handling for the Business Event System. This service component is started automatically by its container.

- Workflow Inbound Notifications Agent Listener - Handles messages on WF_NOTIFICATION_IN to support inbound e-mail notification processing. This service component is started automatically by its container.

- ECX Inbound Agent Listener - Handles message on ECX_INBOUND to support Oracle XML Gateway processing. This service component must be started manually. For more information, see the *Oracle XML Gateway User's Guide*.

- ECX Transaction Agent Listener - Handles message on ECX_TRANSACTION to support Oracle XML Gateway processing. This service component must be started manually. For more information, see the *Oracle XML Gateway User's Guide*.

You cannot delete the seeded agent listeners or edit their names, assigned agents, correlation ID values, or containers. However, if necessary you can update other configuration parameters, schedule control events, or manually choose control commands to start, stop, suspend, resume, or refresh the agent listeners.

You can also optionally create additional agent listener service components. For example, you can configure agent listeners for other inbound agents that you want to use for event message propagation, such as the standard WF_IN and WF_JMS_IN agents, or any custom agents. You can also configure an agent listener that only processes messages on a particular agent that are instances of a specific event.

In addition to the parameters in the configuration wizard, for both seeded and custom PL/SQL agent listeners, you can optionally set the following internal agent listener parameters.

- `LISTENER_PROCESS_EVT_COUNT` - Lets you specify the maximum number of event messages that the agent listener can process each time it runs, before returning control to its service component container.

- `SQL_TRACE_LEVEL` - Lets you enable SQL tracing at various levels or disable SQL tracing for the agent listener.

- NAVIGATION_RESET_THRESHOLD - Lets you reset the agent listener's navigation through waiting messages to include newly arrived messages, so that new high priority messages are processed sooner.

Use the afsvcpup.sql script to set these parameters. See: Scheduling Listeners for Local Inbound Agents, *Oracle Workflow Administrator's Guide* and To Set Internal Agent Listener Parameters, *Oracle Workflow Administrator's Guide*.

If you create custom agent listener service components, you can either assign them to the seeded container for agent listeners, named Workflow Agent Listener Service, or, based on the volume to be handled by the seeded container, you can also choose to create your own custom containers.

Before the seeded agent listener service components can run, the Workflow Agent Listener Service container which manages them must be first be started. You should ensure that this container is running. If you create your own custom containers for custom service components, ensure that those containers are running as well. Use the Service Instances page to start each container as a service instance in Generic Service Management (GSM). When the Workflow Agent Listener Service container is running, it automatically starts the Workflow Deferred Agent Listener, Workflow Deferred Notification Agent Listener, Workflow Error Agent Listener, and Workflow Inbound Notifications Agent Listener.

Agent Listener Configuration Wizard

The agent listener configuration wizard lets you configure an agent listener service component by defining general and detail attributes and scheduling control events. You can use the configuration wizard to configure a new agent listener service component, or to edit the configuration of an existing agent listener service component.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Service Components status icon > (B) Create > (B) Continue

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Service Components status icon > (B) Edit

Define

This page lets you define general attributes for the service component. Some attributes are already set to required values and cannot be modified. You must set attributes marked with an asterisk (*) to appropriate values for your environment before you can run the service component.

- **ID** - When you edit a previously created service component, the configuration wizard displays the identifier for the service component.

- **Status** - When you edit a previously created service component, the configuration wizard displays the status of the service component.

- **Name** - The name of the service component. This name must be unique.

- **Startup Mode** - Select Automatic, Manual, or On-Demand as the startup mode for the service component.

- **Container Type** - The container type to which this service component belongs, which is always Oracle Applications Generic Service Management (Oracle Applications GSM).

- **Inbound Agent** - The Business Event System agent that you want to monitor for inbound event messages.

- **Outbound Agent** - Leave this field blank. Agent listener service components do not use an outbound agent.

- **Correlation ID** - Optionally specify the Oracle Advanced Queuing (AQ) correlation ID of the event messages that you want the agent listener to process. The AQ correlation ID for an event message in the Business Event System is usually specified in the following format:

  ```
  <event name>
  ```

  Consequently, by specifying a correlation ID in this attribute, you can dedicate the agent listener to listen only for messages that are instances of the specified event. You can also specify a partial value to listen for messages that are instances of any event whose name begins with the specified value.

  For example, the seeded Workflow Deferred Notification Agent Listener has an AQ correlation ID of `oracle.apps.wf.notification.%`, meaning that this agent listener handles only notification event messages on the WF_DEFERRED agent. However, the Workflow Deferred Agent Listener, Workflow Error Agent Listener, and Workflow Inbound Notifications Agent Listener do not have any correlation ID specified so that they can process all event messages on their respective agents.

  > **Note:** The AQ correlation ID is different than the correlation ID contained within the WF_EVENT_T event message structure.

To cancel the configuration without saving any changes, click the Cancel button.

To save these settings and proceed to the next step of the configuration wizard, click the Next button.

Details

This page lets you define detail attributes for the service component. You must set attributes marked with an asterisk (*) to appropriate values for your environment before you can run the service component. A refresh icon identifies attributes that can be refreshed dynamically while the service component is running.

- **ID** - When you edit a previously created service component, the configuration wizard displays the identifier for the service component.

- **Status** - When you edit a previously created service component, the configuration wizard displays the status of the service component.

- **Name** - The configuration wizard displays the name defined for the service component.

- **Container** - The container to which the service component will belong. Oracle Workflow provides a container called Workflow Agent Listener Service for agent listener service components.

- **Maximum Idle Time** - If you selected the On-Demand startup mode for the service component, enter the maximum time in minutes that the service component can remain idle before it is stopped. An on-demand component that is stopped in this way will be restarted by its container when it is needed again to process new messages.

- **Max Error Count** - The number of consecutive errors the service component can encounter before its container stops it and changes its status to Stopped with Error. If an error is resolved and processing can continue, the error count is reset. The default value for the maximum error count is 10.

- **Inbound Thread Count** - Set the inbound processing thread count to 1 (one) or higher to enable inbound message processing with this agent listener. Set the inbound thread count to 0 (zero) to disable this agent listener. The default value is 1. If this agent listener receives a high volume of inbound messages, you can set the inbound thread count to a higher value to increase throughput.

- **Outbound Thread Count** - Leave this parameter set to the default value of 0 (zero). Agent listener service components do not perform outbound message processing.

- **Log Level** - Select the level of detail for the information you want to record in the service component container log. The recommended log level, which is also the default value, is Error. Usually the log level only needs to be changed if you want to record additional detailed information for debugging purposes. You can choose the following levels:

  - 1 - Statement

  - 2 - Procedure

  - 3 - Event

  - 4 - Exception

  - 5 - Error
  - 6 - Unexpected

- **Processor Read Wait Timeout** - Specify the amount of time in seconds that the service component's processing thread continues to wait, after reading the last message from its assigned queue, before timing out. If another message is received before this time expires, that message is processed and the timeout period begins again. If the timeout period expires and no more messages have been received, the service component stops reading and its sleep time begins. The default read timeout period for an agent listener is 0 (zero) seconds.

- **Processor Min Loop Sleep** - Specify the minimum sleep time in seconds during which the service component waits, after its read timeout period expires, before it checks its queue for messages again. The default minimum sleep time for an agent listener is 120 seconds.

- **Processor Max Loop Sleep** - Specify the maximum sleep time in seconds if you want to increase the sleep time between read attempts when no messages are received. If you specify a maximum sleep time that is greater than the minimum sleep time, then the service component initially waits for the minimum sleep time after it finishes reading messages from its queue. If no messages are read in subsequent attempts, then the sleep time between read attempts gradually increases until the maximum sleep time is reached. Increasing the sleep time can help enhance performance if messages are received infrequently. You can also specify 0 (zero) for this parameter to indicate that the sleep time should not be increased. In this case, the service component always waits for the minimum sleep time between read attempts. The default value for an agent listener is 0 (zero).

- **Processor Error Loop Sleep** - Specify the sleep time in seconds during which the service component waits, after an error occurs, before it attempts to begin processing again. The default error sleep time for an agent listener is 60 seconds.

- **Processor Close on Read Timeout** - Select this parameter to specify that the service component should close its connections after its read timeout period expires, when its sleep time begins. Deselect this parameter to specify that the connections should remain open until the processing thread stops.

To cancel any changes on this page, click the Cancel button.

To return to the previous step of the configuration wizard, click the Back button.

To save these settings and proceed to the next step of the configuration wizard, click the Next button.

To save these settings and proceed to the last step of the configuration wizard, click the Finish button.

Scheduling Events

This page lets you schedule events to control the running of the service component. The events are raised at the scheduled time by DBMS jobs. For an agent listener service component, you can schedule the following events:

- Start
- Refresh
- Suspend
- Resume
- Stop

For each event, the list displays the event name, date and time when the event is first scheduled to be raised, the interval in minutes at which the event is reraised, and, for a refresh event, any parameters to be refreshed. You can specify the following refreshable parameters, using the parameters' internal names, when you refresh the agent listener.

- `PROCESSOR_IN_THREAD_COUNT` - Inbound Thread Count
- `COMPONENT_LOG_LEVEL` - Log Level, specified as a numerical value
  - 1 - Statement
  - 2 - Procedure
  - 3 - Event
  - 4 - Exception
  - 5 - Error
  - 6 - Unexpected

To schedule events:

- If no events are currently scheduled, click the Add a Row button to add a new row to the list of events and enter the information for the event.
  - Select the event for the command you want to schedule. Oracle Workflow provides events to let you start, stop, refresh, suspend, or resume the service component.
  - Select the date when you want the event to be raised first.
  - Select the hour and minute to specify the time on the specified date when you

want the event to be raised first. The hour values are in a twenty-four hour format. For example, select 00 for midnight, or 23 for 11 PM.

  - If you want to raise the event periodically, enter the time interval in minutes at which you want to raise the event. If you do not specify a repeating interval, the event is raised only once.

  - If you choose the refresh event, you can optionally enter any parameters you want to include with the event in order to refresh the agent listener configuration parameters with those values when the event is raised. Specify the parameter names and values in the following format, separating the parameters with a colon (:):
    `internal_parameter_name=parameter_value`

    For example: `PROCESSOR_IN_THREAD_COUNT=1`

- To schedule another event, click the Add Another Row button and enter the information for the event.

- To remove an event, select the event and click the Remove button.

To cancel any changes on this page, click the Cancel button.

To return to the previous step of the configuration wizard, click the Back button.

To save these settings and proceed to the next step of the configuration wizard, click the Next button.

To save these settings and proceed to the last step of the configuration wizard, click the Finish button.

> **Note:** The configuration wizard verifies that an event is specified for every row in the list when you click the Next or Finish button. If you do not want to schedule another event, you should remove any empty rows before proceeding.

Review

This page lets you review the configuration parameter values that you set and the events that you scheduled for this service component.

- If you want to change any of these settings, return to the appropriate step in the configuration wizard to make your changes. To return to the previous step, click the Back button.

- To save these settings and finish the configuration, click the Finish button.

Java Agent Listeners

The Oracle Workflow Business Event System requires agent listeners to be scheduled to receive inbound event messages. An agent listener monitors a Business Event System agent for incoming messages and dequeues messages using the agent's queue handler. You should run agent listeners for your local inbound agents. Run PL/SQL agent listeners to process event subscriptions with a PL/SQL rule function in the database, and run Java agent listeners to process event subscriptions with a Java rule function in the middle tier.

When an event message is dequeued, the Event Manager begins subscription processing for the event. The Event Manager searches for and executes any active subscriptions by the local system to that event with a source type of External, and also any active subscriptions by the local system to the Any event with a source type of External. The agent listener exits after all event messages on the agent's queue have been dequeued.

The Java agent listener program is defined as a service component type in the Generic Service Component Framework. This framework helps to simplify and automate the management of background Java services.

Oracle Workflow provides several seeded Java agent listener service components to process messages on standard agents.

- Workflow Java Deferred Agent Listener - Handles messages on WF_JAVA_DEFERRED to support deferred subscription processing in the middle tier. This service component is started automatically by its container.

- Workflow Java Error Agent Listener - Handles messages on WF_JAVA_ERROR to support error handling for the Business Event System in the middle tier. This service component is started automatically by its container.

- Web Services IN Agent - Handles messages on WF_WS_JMS_IN to support inbound Web service message processing. This service component must be started manually.

You can optionally update the configuration of the Workflow WebServices In listener or delete this service component if necessary. You cannot delete the Workflow Java Deferred Agent Listener and Workflow Java Error Agent Listener or edit their names, assigned agents, correlation ID values, or containers. However, if necessary you can update other configuration parameters, schedule control events, or manually choose control commands to start, stop, suspend, resume, or refresh these Java agent listeners.

You can also optionally create additional Java agent listener service components. For example, you can configure Java agent listeners for other inbound agents that you want to use for event message propagation in the middle tier, such as custom agents. You can also configure a Java agent listener that only processes messages on a particular agent that are instances of a specific event.

In addition to the parameters in the configuration wizard, for both seeded and custom Java agent listeners, you can optionally set an internal agent listener parameter named `NAVIGATION_RESET_THRESHOLD`. This parameter lets you reset the agent listener's navigation through waiting messages to include newly arrived messages, so that new high priority messages are processed sooner. Use the `afsvcpup.sql` script to set this parameter. See: Scheduling Listeners for Local Inbound Agents, *Oracle Workflow Administrator's Guide* and To Set Internal Agent Listener Parameters, *Oracle Workflow Administrator's Guide*.

If you create custom Java agent listener service components, you can either assign them to the seeded container for agent listeners, named Workflow Agent Listener Service, or, based on the volume to be handled by the seeded container, you can also choose to create your own custom containers.

Before the seeded Java agent listener service components can run, the Workflow Agent Listener Service container which manages them must be first be started. You should ensure that this container is running. If you create your own custom containers for custom service components, ensure that those containers are running as well. Use the Service Instances page to start each container as a service instance in Generic Service Management (GSM). When the Workflow Agent Listener Service container is running, it automatically starts the Workflow Java Deferred Agent Listener and Workflow Java Error Agent Listener.

Java Agent Listener Configuration Wizard

The Java agent listener configuration wizard lets you configure a Java agent listener service component by defining general and detail attributes and scheduling control events. You can use the configuration wizard to configure a new Java agent listener service component, or to edit the configuration of an existing Java agent listener service component.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Service Components status icon > (B) Create > (B) Continue

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Service Components status icon > (B) Edit

Define

This page lets you define general attributes for the service component. Some attributes are already set to required values and cannot be modified. You must set attributes marked with an asterisk (*) to appropriate values for your environment before you can run the service component.

- **ID** - When you edit a previously created service component, the configuration wizard displays the identifier for the service component.

- **Status** - When you edit a previously created service component, the configuration wizard displays the status of the service component.

- **Name** - The name of the service component. This name must be unique.

- **Startup Mode** - Select Automatic, Manual, or On-Demand as the startup mode for the service component.

- **Container Type** - The container type to which this service component belongs, which is always Oracle Applications Generic Service Management (Oracle Applications GSM).

- **Inbound Agent** - The Business Event System agent that you want to monitor for inbound event messages.

- **Outbound Agent** - Leave this field blank. Java agent listener service components do not use an outbound agent.

- **Correlation ID** - Optionally specify the Oracle Advanced Queuing (AQ) correlation ID of the event messages that you want the Java agent listener to process. The AQ correlation ID for an event message in the Business Event System is usually specified in the following format:

  ```
  <event name>
  ```

  Consequently, by specifying a correlation ID in this attribute, you can dedicate the Java agent listener to listen only for messages that are instances of the specified event. You can also specify a partial value to listen for messages that are instances of any event whose name begins with the specified value.

  The seeded Java agent listeners do not have any correlation ID specified so that they can process all event messages on their respective agents.

  > **Note:** The AQ correlation ID is different than the correlation ID contained within the WF_EVENT_T event message structure.

To cancel the configuration without saving any changes, click the Cancel button.

To save these settings and proceed to the next step of the configuration wizard, click the Next button.

Details

This page lets you define detail attributes for the service component. You must set attributes marked with an asterisk (*) to appropriate values for your environment before you can run the service component. A refresh icon identifies attributes that can be refreshed dynamically while the service component is running.

- **ID** - When you edit a previously created service component, the configuration wizard displays the identifier for the service component.

- **Status** - When you edit a previously created service component, the configuration wizard displays the status of the service component.

- **Name** - The configuration wizard displays the name defined for the service component.

- **Container** - The container to which the service component will belong. Oracle Workflow provides a container called Workflow Agent Listener Service for Java agent listener service components.

- **Maximum Idle Time** - If you selected the On-Demand startup mode for the service component, enter the maximum time in minutes that the service component can remain idle before it is stopped. An on-demand component that is stopped in this way will be restarted by its container when it is needed again to process new messages.

- **Max Error Count** - The number of consecutive errors the service component can encounter before its container stops it and changes its status to Stopped with Error. If an error is resolved and processing can continue, the error count is reset. The default value for the maximum error count is 10.

- **Inbound Thread Count** - Set the inbound processing thread count to 1 (one) or higher to enable inbound message processing with this Java agent listener. Set the inbound thread count to 0 (zero) to disable this Java agent listener. The default value is 1. If this Java agent listener receives a high volume of inbound messages, you can set the inbound thread count to a higher value to increase throughput.

- **Outbound Thread Count** - Leave this parameter set to the default value of 0 (zero). Java agent listener service components do not perform outbound message processing.

- **Log Level** - Select the level of detail for the information you want to record in the service component container log. The recommended log level, which is also the default value, is Error. Usually the log level only needs to be changed if you want to record additional detailed information for debugging purposes. You can choose the following levels:

  - 1 - Statement

  - 2 - Procedure

  - 3 - Event

  - 4 - Exception

  - 5 - Error

  - 6 - Unexpected

- **Processor Read Wait Timeout** - Specify the amount of time in seconds that the service component's processing thread continues to wait, after reading the last message from its assigned queue, before timing out. If another message is received before this time expires, that message is processed and the timeout period begins again. If the timeout period expires and no more messages have been received, the service component stops reading and its sleep time begins. The default read timeout period for a Java agent listener is 10 seconds.

- **Processor Min Loop Sleep** - Specify the minimum sleep time in seconds during which the service component waits, after its read timeout period expires, before it checks its queue for messages again. The default minimum sleep time for a Java agent listener is 5 seconds.

- **Processor Max Loop Sleep** - Specify the maximum sleep time in seconds if you want to increase the sleep time between read attempts when no messages are received. If you specify a maximum sleep time that is greater than the minimum sleep time, then the service component initially waits for the minimum sleep time after it finishes reading messages from its queue. If no messages are read in subsequent attempts, then the sleep time between read attempts gradually increases until the maximum sleep time is reached. Increasing the sleep time can help enhance performance if messages are received infrequently. You can also specify 0 (zero) for this parameter to indicate that the sleep time should not be increased. In this case, the service component always waits for the minimum sleep time between read attempts. The default maximum sleep time for a Java agent listener is 60 seconds.

- **Processor Error Loop Sleep** - Specify the sleep time in seconds during which the service component waits, after an error occurs, before it attempts to begin processing again. The default error sleep time for a Java agent listener is 60 seconds.

- **Processor Close on Read Timeout** - Select this parameter to specify that the service component should close its connections after its read timeout period expires, when its sleep time begins. Deselect this parameter to specify that the connections should remain open until the processing thread stops.

To cancel any changes on this page, click the Cancel button.

To return to the previous step of the configuration wizard, click the Back button.

To save these settings and proceed to the next step of the configuration wizard, click the Next button.

To save these settings and proceed to the last step of the configuration wizard, click the Finish button.

Scheduling Events

This page lets you schedule events to control the running of the service component. The events are raised at the scheduled time by DBMS jobs. For a Java agent listener service component, you can schedule the following events:

- Start
- Refresh
- Suspend
- Resume
- Stop

For each event, the list displays the event name, date and time when the event is first scheduled to be raised, the interval in minutes at which the event is reraised, and, for a refresh event, any parameters to be refreshed. You can specify the following refreshable parameters, using the parameters' internal names, when you refresh the Java agent listener.

- `PROCESSOR_IN_THREAD_COUNT` - Inbound Thread Count
- `COMPONENT_LOG_LEVEL` - Log Level, specified as a numerical value
  - `1` - Statement
  - `2` - Procedure
  - `3` - Event
  - `4` - Exception
  - `5` - Error
  - `6` - Unexpected

To schedule events:

- If no events are currently scheduled, click the Add a Row button to add a new row to the list of events and enter the information for the event.
  - Select the event for the command you want to schedule. Oracle Workflow provides events to let you start, stop, refresh, suspend, or resume the service component.
  - Select the date when you want the event to be raised first.
  - Select the hour and minute to specify the time on the specified date when you want the event to be raised first. The hour values are in a twenty-four hour format. For example, select 00 for midnight, or 23 for 11 PM.

  - If you want to raise the event periodically, enter the time interval in minutes at which you want to raise the event. If you do not specify a repeating interval, the event is raised only once.

  - If you choose the refresh event, you can optionally enter any parameters you want to include with the event in order to refresh the Java agent listener configuration parameters with those values when the event is raised. Specify the parameter names and values in the following format, separating the parameters with a colon (:): `internal_parameter_name=parameter_value`

    For example: `PROCESSOR_IN_THREAD_COUNT=1`

- To schedule another event, click the Add Another Row button and enter the information for the event.

- To remove an event, select the event and click the Remove button.

To cancel any changes on this page, click the Cancel button.

To return to the previous step of the configuration wizard, click the Back button.

To save these settings and proceed to the next step of the configuration wizard, click the Next button.

To save these settings and proceed to the last step of the configuration wizard, click the Finish button.

> **Note:** The configuration wizard verifies that an event is specified for every row in the list when you click the Next or Finish button. If you do not want to schedule another event, you should remove any empty rows before proceeding.

Review

This page lets you review the configuration parameter values that you set and the events that you scheduled for this service component.

- If you want to change any of these settings, return to the appropriate step in the configuration wizard to make your changes. To return to the previous step, click the Back button.

- To save these settings and finish the configuration, click the Finish button.

Web Services Outbound

You can use Web services in Oracle Workflow to initiate outbound Web service requests and to accept inbound Web service requests.

When Web service messages are dequeued by the Oracle E-Business Suite, they are transmitted by the Web service outbound component.

The Web services outbound program is defined as a service component type in the Generic Service Component Framework. This framework helps to simplify and automate the management of background Java services.

Oracle Workflow provides a seeded Web services outbound component named Web Services OUT Agent to process messages on the standard WF_WS_JMS_OUT queue, which is a Business Event System agent. This service component must be started manually. You can optionally update its configuration if necessary.

You can also optionally create additional Web services outbound components. For example, you can configure a Web services outbound component that only processes messages on a particular agent or queue.

If you create custom Web services outbound components, you can either assign them to the seeded container for Web services outbound components, named Workflow Document Web Services Service, or, based on the volume to be handled by the seeded container, you can also choose to create your own custom containers.

Before the seeded Web services outbound component can run, the Workflow Document Web Services Service container which manages it must be first be started. You should ensure that this container is running. If you create your own custom containers for custom service components, ensure that those containers are running as well. Use the Service Instances page to start each container as a service instance in Generic Service Management (GSM).

> **Note:** Inbound Web service messages are processed by a seeded service component of type Java agent listener, named Workflow Web Services In.

Web Services Outbound Configuration Wizard

The Web services outbound configuration wizard lets you configure a Web services outbound service component by defining general and detail attributes and scheduling control events. You can use the configuration wizard to configure a new Web services outbound service component, or to edit the configuration of an existing Web services outbound service component.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Service Components status icon > (B) Create > (B) Continue

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Service Components status icon > (B) Edit

Define

This page lets you define general attributes for the service component. Some attributes are already set to required values and cannot be modified. You must set attributes marked with an asterisk (*) to appropriate values for your environment before you can run the service component.

- **ID** - When you edit a previously created service component, the configuration wizard displays the identifier for the service component.
- **Status** - When you edit a previously created service component, the configuration wizard displays the status of the service component.
- **Name** - The name of the service component. This name must be unique.
- **Startup Mode** - Select Automatic, Manual, or On-Demand as the startup mode for the service component.
- **Container Type** - The container type to which this service component belongs, which is always Oracle Applications Generic Service Management (Oracle Applications GSM).
- **Inbound Agent** - Leave this field blank. Web services outbound components do not use an inbound agent.
- **Outbound Agent** - The agent/queue that you want to monitor for outbound Web services messages.

To cancel the configuration without saving any changes, click the Cancel button.

To save these settings and proceed to the next step of the configuration wizard, click the Next button.

Details

This page lets you define detail attributes for the service component. You must set attributes marked with an asterisk (*) to appropriate values for your environment before you can run the service component. A refresh icon identifies attributes that can be refreshed dynamically while the service component is running.

- **ID** - When you edit a previously created service component, the configuration wizard displays the identifier for the service component.
- **Status** - When you edit a previously created service component, the configuration wizard displays the status of the service component.
- **Name** - The configuration wizard displays the name defined for the service component.
- **Container** - The container to which the service component will belong. Oracle Workflow provides a container called Workflow Document Web Services Service for Web services outbound components.

- **Maximum Idle Time** - If you selected the On-Demand startup mode for the service component, enter the maximum time in minutes that the service component can remain idle before it is stopped. An on-demand component that is stopped in this way will be restarted by its container when it is needed again to process new messages.

- **Max Error Count** - The number of consecutive errors the service component can encounter before its container stops it and changes its status to Stopped with Error. If an error is resolved and processing can continue, the error count is reset. The default value for the maximum error count is 10.

- **Inbound Thread Count** - Leave this parameter set to the default value of 0 (zero). Web services outbound components do not perform inbound message processing.

- **Outbound Thread Count** - Specify the number of outbound processing threads you want to execute simultaneously with this Web services outbound component, depending on the volume of outbound messages you need to send. Specify 0 (zero) to disable this Web services outbound component. The default value is 1 (one).

- **Log Level** - Select the level of detail for the information you want to record in the service component container log. The recommended log level, which is also the default value, is Error. Usually the log level only needs to be changed if you want to record additional detailed information for debugging purposes. You can choose the following levels:

  - 1 - Statement

  - 2 - Procedure

  - 3 - Event

  - 4 - Exception

  - 5 - Error

  - 6 - Unexpected

- **Processor Read Wait Timeout** - Specify the amount of time in seconds that the service component's processing threads continue to wait, after reading the last message from the assigned queue, before timing out. If another message is received before this time expires, that message is processed and the timeout period begins again. If the timeout period expires and no more messages have been received, the service component stops reading and its sleep time begins. The default read timeout period for a Web services outbound component is 10 seconds.

- **Processor Min Loop Sleep** - Specify the minimum sleep time in seconds during which the service component waits, after its read timeout period expires, before it checks its queue for messages again. The default minimum sleep time for a Web services outbound component is 5 seconds.

- **Processor Max Loop Sleep** - Specify the maximum sleep time in seconds if you want to increase the sleep time between read attempts when no messages are received. If you specify a maximum sleep time that is greater than the minimum sleep time, then the service component initially waits for the minimum sleep time after it finishes reading messages from its queue. If no messages are read in subsequent attempts, then the sleep time between read attempts gradually increases until the maximum sleep time is reached. Increasing the sleep time can help enhance performance if messages are received infrequently. You can also specify 0 (zero) for this parameter to indicate that the sleep time should not be increased. In this case, the service component always waits for the minimum sleep time between read attempts. The default maximum sleep time for a Web services outbound component is 60 seconds.

- **Processor Error Loop Sleep** - Specify the sleep time in seconds during which the service component waits, after an error occurs, before it attempts to begin processing again. The default error sleep time for a Web services outbound component is 60 seconds.

- **Processor Close on Read Timeout** - Select this parameter to specify that the service component should close its connections after its read timeout period expires, when its sleep time begins. Deselect this parameter to specify that the connections should remain open until the processing thread stops.

To cancel any changes on this page, click the Cancel button.

To return to the previous step of the configuration wizard, click the Back button.

To save these settings and proceed to the next step of the configuration wizard, click the Next button.

To save these settings and proceed to the last step of the configuration wizard, click the Finish button.

Scheduling Events

This page lets you schedule events to control the running of the service component. The events are raised at the scheduled time by DBMS jobs. For a Web services outbound component, you can schedule the following events:

- Start

- Refresh

- Suspend

- Resume

- Stop

For each event, the list displays the event name, date and time when the event is first scheduled to be raised, the interval in minutes at which the event is reraised, and, for a refresh event, any parameters to be refreshed. You can specify the following refreshable parameters, using the parameters' internal names, when you refresh the Web services outbound component.

- `PROCESSOR_OUT_THREAD_COUNT` - Outbound Thread Count
- `COMPONENT_LOG_LEVEL` - Log Level, specified as a numerical value
  - `1` - Statement
  - `2` - Procedure
  - `3` - Event
  - `4` - Exception
  - `5` - Error
  - `6` - Unexpected

To schedule events:

- If no events are currently scheduled, click the Add a Row button to add a new row to the list of events and enter the information for the event.
  - Select the event for the command you want to schedule. Oracle Workflow provides events to let you start, stop, refresh, suspend, or resume the service component.
  - Select the date when you want the event to be raised first.
  - Select the hour and minute to specify the time on the specified date when you want the event to be raised first. The hour values are in a twenty-four hour format. For example, select 00 for midnight, or 23 for 11 PM.
  - If you want to raise the event periodically, enter the time interval in minutes at which you want to raise the event. If you do not specify a repeating interval, the event is raised only once.
  - If you choose the refresh event, you can optionally enter any parameters you want to include with the event in order to refresh the Web services outbound configuration parameters with those values when the event is raised. Specify the parameter names and values in the following format, separating the parameters with a colon (:):
    `internal_parameter_name=parameter_value`

For example: `PROCESSOR_OUT_THREAD_COUNT=3`

- To schedule another event, click the Add Another Row button and enter the information for the event.
- To remove an event, select the event and click the Remove button.

To cancel any changes on this page, click the Cancel button.

To return to the previous step of the configuration wizard, click the Back button.

To save these settings and proceed to the next step of the configuration wizard, click the Next button.

To save these settings and proceed to the last step of the configuration wizard, click the Finish button.

> **Note:** The configuration wizard verifies that an event is specified for every row in the list when you click the Next or Finish button. If you do not want to schedule another event, you should remove any empty rows before proceeding.

Review

This page lets you review the configuration parameter values that you set and the events that you scheduled for this service component.

- If you want to change any of these settings, return to the appropriate step in the configuration wizard to make your changes. To return to the previous step, click the Back button.
- To save these settings and finish the configuration, click the Finish button.

Background Engines

Background engine processes serve three purposes in Oracle Workflow: to handle activities deferred by the Workflow Engine, to handle timed out notification activities, and to handle stuck processes.

When the Workflow Engine initiates and performs a process, it completes all necessary activities before continuing to the next eligible activity. In some cases, an activity can require a large amount of processing resource or time to complete. Oracle Workflow lets you manage the load on the Workflow Engine by setting up supplemental engines to run these costly activities as background tasks. In these cases, the costly activity is deferred by the Workflow Engine and run later by a background engine. The main Workflow Engine can then continue to the next available activity, which may occur on some other parallel branch of the process.

A background engine must also be set up to handle timed out notification activities. When the Workflow Engine comes across a notification activity that requires a response, it calls the Notification System to send the notification to the appropriate performer, and then sets the notification activity to a status of 'NOTIFIED' until the performer completes the notification activity. Meanwhile, a background engine set up to handle timed out activities periodically checks for 'NOTIFIED' activities and whether these activities have time out values specified. If a 'NOTIFIED' activity does have a time out value, and the current date and time exceeds that time out value, the background engine marks that activity as timed out and calls the Workflow Engine. The Workflow Engine then resumes by trying to execute a <timeout> transition activity.

Additionally, a background engine must be set up to handle stuck processes. A process is identified as stuck when it has a status of ACTIVE, but cannot progress any further. For example, a process could become stuck in the following situations:

- A thread within a process leads to an activity that is not defined as an End activity but has no other activity modeled after it, and no other activity is active.

- A process with only one thread loops back, but the pivot activity of the loop has the On Revisit property set to Ignore.

- An activity returns a result for which no eligible transition exists. For instance, if the function for a function activity returns an unexpected result value, and no default transition is modeled after that activity, the process cannot continue.

The background engine sets the status of a stuck process to ERROR:#STUCK and executes the error process defined for it.

You can define and start up as many background engines as you like to check for deferred and timed out activities.

Background engines can be restricted to handle activities associated with specific item types, and within specific cost ranges. A background engine runs until it completes all eligible activities at the time it was initiated. Generally, you should set the background engine up to run periodically.

Ensure that you have at least one background engine that can check for timed out activities, one that can process deferred activities, and one that can handle stuck processes. At a minimum, you need to set up one background engine that can handle both timed out and deferred activities as well as stuck processes. Generally, you should run a separate background engine to check for stuck processes at less frequent intervals than the background engine that you run for deferred activities, normally not more often than once a day. Run the background engine to check for stuck processes when the load on the system is low.

Running Background Engines

You run a background engine by submitting the Workflow Background Process concurrent program (FNDWFBG). When you start a new background engine, you can restrict the engine to handle activities associated with specific item types, and within specific cost ranges. You can submit the Workflow Background Process concurrent program several times to schedule different background engines to run at different times.

- To submit a request for the Workflow Background Process concurrent program, choose Background Engines from the Submit Request For pull-down menu in the Workflow System status page and click the Go button.

- To view Workflow Background Process concurrent requests, click the Background Engines status icon in the Workflow System status page.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go

Parameters

When you submit the Workflow Background Process concurrent program, specify the following parameters.

- **Item Type** - Specify an item type to restrict this engine to activities associated with that item type. If you do not specify an item type, the engine processes any activity regardless of its item type.

- **Minimum Threshold** - Specify the minimum cost that an activity must have for this background engine to execute it, in hundredths of a second.

- **Maximum Threshold** - Specify the maximum cost that an activity can have for this background engine to execute it, in hundredths of a second. By using Minimum Threshold and Maximum Threshold you can create multiple background engines to handle very specific types of activities. The default values for these arguments are null so that the background engine runs activities regardless of cost.

- **Process Deferred** - Specify whether this background engine checks for deferred activities. Setting this parameter to Yes allows the engine to check for deferred activities.

- **Process Timeout** - Specify whether this background engine checks for activities that have timed out. Setting this parameter to Yes allows the engine to check for timed out activities.

- **Process Stuck** - Specify whether this background engine checks for stuck processes. Setting this parameter to Yes allows the engine to check for stuck processes.

> **Note:** Make sure you have a least one background engine that can check for timed out activities, one that can process deferred activities, and one that can handle stuck processes. At a minimum, you need to set up one background engine that can handle both timed out and

deferred activities as well as stuck processes.

Viewing Concurrent Requests

When you view the Workflow Background Process concurrent requests, the Search Results page shows standard request detail information for these requests. For each request, the list displays the request ID, program short name, description, application short name, phase, status, requester, duration, wait time, and submission date. Click a column heading to sort the list by that column.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Background Engines status icon

- To show the details for a request if they are hidden, click the Show link in the Details column. Oracle Applications Manager displays details about the request depending on the status of the request. You can also perform actions, such as placing a hold on a request, canceling a request, viewing diagnostic information, viewing manager details, viewing logs, or viewing request output, by clicking the corresponding button. The actions that are available depend on the status of the request.

- To hide the details for a request if they are shown, click the Hide link in the Details column.

- To search for concurrent requests with different criteria, click the New Search button or click one of the Quick Search links.

- To modify the search criteria from this search, click the Modify Search button.

- To add the information from this page to your support cart, click the Add to Support Cart button.

Purging Workflow Data

The Oracle Applications Manager console helps you easily maintain the Oracle Workflow and Oracle XML Gateway database tables. Oracle Workflow and Oracle XML Gateway access several tables that can grow quite large with obsolete workflow information that is stored for all completed workflow processes, as well as obsolete information for XML transactions. The size of these tables and indexes can adversely affect performance. These tables should be purged on a regular basis, using the Purge Obsolete Workflow Runtime Data concurrent program.

This program purges obsolete runtime information associated with work items, including status information, any associated notifications, and, if the ECX: Purge ECX data with WF profile option is set to `Y`, any associated Oracle XML Gateway transactions. By default, it also purges obsolete design information, such as activities that are no longer in use and expired ad hoc users and roles, and obsolete runtime information not associated with work items, such as notifications that were not handled through a workflow process and, if the ECX: Purge ECX data with WF profile option is set to Y, Oracle XML Gateway transactions that were not handled through a workflow process. You can optionally choose to purge only core runtime information associated with work items for performance gain during periods of high activity, and purge all obsolete information as part of your routine maintenance during periods of low activity.

> **Note:** This program does not delete ad hoc users or roles whose expiration date is null. To ensure that ad hoc users and roles are purged in a timely fashion after they are no longer needed, estimate how long they should be active and specify an appropriate expiration date when you call *WF_DIRECTORY.CreateAdHocUser()*, *WF_DIRECTORY.CreateAdHocRole()*, or *WF_DIRECTORY.CreateAdHocRole2()* to create them.

To preserve electronic signature evidence for future reference, this program by default does not delete any notifications that required signatures or their associated signature information. If you do not need to maintain signature evidence, you can choose to delete signature-related information as well.

> **Note:** You can also use the Purge Obsolete ECX Data concurrent program to purge Oracle XML Gateway transactions according to Oracle XML Gateway-specific parameters. For information about this program and about the ECX: Purge ECX data with WF profile option, see: Purge Obsolete ECX Data Concurrent Program, *Oracle XML Gateway User's Guide* and Purge Obsolete Workflow Runtime Data Concurrent Program, *Oracle XML Gateway User's Guide*.

Workflow Purge

The Workflow Purge page shows summary information about the next scheduled and last completed purge requests and about completed work items.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Purge status icon

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Related Links > Throughput > Work Items

To view work items with a different status, choose the status you want from the View pull-down menu and click the Go button. You can view items with the following statuses:

- Completed Work Items
- Active Work Items

- Deferred Work Items
- Suspended Work Items
- Errored Work Items

Requests Summary

This region displays summary information about the next scheduled and last completed Purge Obsolete Workflow Runtime Data concurrent requests.

- To show information in this region if it is hidden, click the Show link.
- To hide information in this region if it is shown, click the Hide link.

Next Scheduled

For the next scheduled Purge Obsolete Workflow Runtime Data concurrent request, Oracle Workflow Manager displays the request ID, requestor, status, requested start time, wait time, and parameters.

Last Completed

For the last completed Purge Obsolete Workflow Runtime Data concurrent request, Oracle Workflow Manager displays the request ID, requestor, status, completed time, duration, and parameters.

To view the log file for the request, click the Request Log link.

Completed Work Items

This region displays the distribution of completed work items across different item types.

- To show information in this region if it is hidden, click the Show link
- To hide information in this region if it is shown, click the Hide link.
- This region displays the date and time when the work item statistics were last updated. To refresh this information, click the refresh icon. See: Gathering Oracle Workflow Statistics, page 3-2.

For each work item type in the Completed Work Items list, Oracle Workflow Manager displays the work item type name, the persistence type, the retention period in days, the number of completed work items of that type, and the number of items of that type that are available for purging. Click any column heading to sort the list by that column.

- To filter the item types displayed in the list, select an item type property and an operator from the Filter pull-down menus, enter a filter value in the text field, and click the Go button. You can filter by the following properties:

  - Work item type display name
  - Work item type internal name
  - Persistence type
  - Retention period
  - Number of completed work items of this type
  - Number of items of this type available for purging

- To view details for work items of a particular item type, either click the item type link in the Work Item Type column, or select the item type and click the View Details button.

Submitting the Purge Program

You perform purging by submitting the Purge Obsolete Workflow Runtime Data concurrent program (FNDWFPR). You can enter restrictions to specify the data that you want to purge.

- To submit a request for the Purge Obsolete Workflow Runtime Data concurrent program, either click the Purge button in the Completed Work Items region of the Workflow Purge page, or choose Purge from the Submit Request For pull-down menu in the Workflow System status page and click the Go button.

- To view Purge Obsolete Workflow Runtime Data concurrent requests, click the View Purge Requests button in the Completed Work Items region of the Workflow Purge page.

Parameters

When you submit the Purge Obsolete Workflow Runtime Data concurrent program, specify the following parameters.

- **Item Type** - Specify the item type to purge. Leave this field blank to purge the runtime data for all item types.

- **Item Key** - Specify the item key to purge. The item key is a unique identifier for an item within an item type. Leave this field blank to purge the runtime data for all items of the specified item type.

- **Age** - Specify the minimum age of data to purge, in days, if you are purging items with a Temporary persistence type. The default is 0 days.

- **Persistence Type** - Specify the persistence type of the data you want to purge, either Permanent or Temporary. The default is Temporary.

- **Core Workflow Only** - Enter 'Y' to purge only obsolete runtime data associated with work items, or 'N' to purge all obsolete runtime data as well obsolete design data. The default is 'N'.

- **Commit Frequency** - Enter the number of records to purge before the program commits data. To reduce rollback size and improve performance, set this parameter to commit data after a smaller number of records. The default is 500 records.

  > **Note:** After performing a commit, the program resumes purging work items with the next subsequent begin date. In some cases, if additional items have the same begin date as the last item that was purged before a commit, the program may not purge all eligible items. To purge these remaining work items, simply rerun the program.

- **Signed Notifications** - Enter 'N' to preserve signature evidence, including notifications that required electronic signatures and their associated signature information. Enter 'Y' to purge signature-related information. The default is 'N'.

Viewing Concurrent Requests

When you view the Purge Obsolete Workflow Runtime Data concurrent requests, the Search Results page shows standard request detail information for these requests. For each request, the list displays the request ID, program short name, description, application short name, phase, status, requestor, duration, wait time, and submission date. Click a column heading to sort the list by that column.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Purge status icon > (B) View Purge Requests

- To show the details for a request if they are hidden, click the Show link in the Details column. Oracle Applications Manager displays details about the request depending on the status of the request. You can also perform actions, such as placing a hold on a request, canceling a request, viewing diagnostic information, viewing manager details, viewing logs, or viewing request output, by clicking the corresponding button. The actions that are available depend on the status of the request.

- To hide the details for a request if they are shown, click the Hide link in the Details column.

- To search for concurrent requests with different criteria, click the New Search button or click one of the Quick Search links.

- To modify the search criteria from this search, click the Modify Search button.

- To add the information from this page to your support cart, click the Add to Support Cart button.

Completed Work Item Details

This page shows details about completed work items of a particular item type.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Purge status icon > (B) View Details

To view work items with a different status, choose the status you want from the View pull-down menu and click the Go button. You can view items with the following statuses:

- Completed Work Items

- Active Work Items

- Deferred Work Items

- Suspended Work Items

- Errored Work Items

Completed Work Items Stage Summary

This region displays the distribution of completed work items that ended at various activity stages within the workflow process. For each activity stage, the list displays the activity internal name and result, and the number of completed work items that ended at that stage. Click any column heading to sort the list by that column.

- By default, the list shows completed work items that ended within the last 30 days. To view completed work items that ended within a different period, enter a number of days in the Filter: End Date Within Last _ Days option and click the Go button.

- To view details about the work items that ended at a particular activity stage, either click the activity stage link in the Work Item Activity Stage column, or select the activity stage and click the View Details button.

Completed Work Item Activity Details

This page shows details about completed work items that ended at a particular activity stage within a particular item type.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Purge status icon > (B) View Details > (B) View Details

To view work items with a different status, choose the status you want from the View pull-down menu and click the Go button. You can view items with the following statuses:

- Completed Work Items
- Active Work Items
- Deferred Work Items
- Suspended Work Items
- Errored Work Items

Oracle Workflow Manager displays a list of all completed work items of the selected item type that ended at the selected activity stage. By default, the list shows completed work items that ended within the last 30 days. For each work item, the list displays the internal name of the activity at which the work item ended, the activity start date, end date, user assigned to perform the activity, and item key. Click any column heading to sort the list by that column.

- To filter the work items displayed in the list, select an activity property from the Filter pull-down menu, enter a filter value in the text field, and click the Go button. You can filter by the following properties:
  - Internal name of the activity at which the work item ended
  - Start date within a specified number of days
  - End date within a specified number of days
  - User assigned to perform the activity
  - Item key of the work item
- To launch the Workflow Monitor for a work item, select the work item and click the Launch Workflow Monitor button.

  > **Note:** If you perform an action in the Workflow Monitor that changes the status of the work item, then you must refresh your Oracle Workflow Manager web page in order to see the updated information.

Workflow Control Queue Cleanup

Oracle Workflow contains a standard Business Event System agent named WF_CONTROL, which is associated with a standard queue that is also named WF_CONTROL. This queue has a payload type of JMS Text message. The

WF_CONTROL agent is used for internal processing only, and is not meant for customer use. You should not place custom event messages on this queue.

The Generic Service Component Framework uses WF_CONTROL to handle control events for containers and service components, such as notification mailer or agent listener service components. WF_CONTROL is also used for other Oracle E-Business Suite internal processing.

You do not need to schedule propagation for the WF_CONTROL agent, because the middle tier processes that use WF_CONTROL dequeue messages directly from its queue. However, the subscribers to the WF_CONTROL queue need to be cleaned up periodically. A concurrent program named Workflow Control Queue Cleanup is automatically scheduled to perform this cleanup for you.

When a middle tier process for Oracle E-Business Suite starts up, it creates a JMS subscriber to the queue. Then, when an event message is placed on the queue, a copy of the event message is created for each subscriber to the queue. If a middle tier process dies, however, the corresponding subscriber remains in the database. For more efficient processing, you should ensure that WF_CONTROL is periodically cleaned up by removing the subscribers for any middle tier processes that are no longer active. The Workflow Control Queue Cleanup concurrent program sends an event named oracle.apps.wf.bes.control.ping to check the status of each subscriber to the WF_CONTROL queue. If the corresponding middle tier process is still alive, it sends back a response. The next time the cleanup program runs, it checks whether responses have been received for each ping event sent during the previous run. If no response was received from a particular subscriber, that subscriber is removed.

The recommended frequency for performing cleanup is every twelve hours. In order to allow enough time for subscribers to respond to the ping event, the minimum wait time between two cleanup runs is thirty minutes. If you run the procedure again less than thirty minutes after the previous run, it will not perform any processing.

Running Workflow Control Queue Cleanup

You perform Workflow control queue cleanup by submitting the Workflow Control Queue Cleanup concurrent program (FNDWFBES_CONTROL_QUEUE_CLEANUP). This program does not require any parameters. This concurrent program is scheduled to run every twelve hours by default, which is the recommended frequency for performing cleanup. You can optionally submit this program with a different schedule if you want to perform cleanup at a different frequency.

- To submit a request for the Workflow Control Queue Cleanup concurrent program, choose Control Queue Cleanup from the Submit Request For pull-down menu in the Workflow System status page and click the Go button.

- To view Workflow Control Queue Cleanup concurrent requests, click the Control Queue Cleanup status icon in the Workflow System status page.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go

Viewing Concurrent Requests

When you view the Workflow Control Queue Cleanup concurrent requests, the Search Results page shows standard request detail information for these requests. For each request, the list displays the request ID, program short name, description, application short name, phase, status, requester, duration, wait time, and submission date. Click a column heading to sort the list by that column.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Control Queue Cleanup status icon

- To show the details for a request if they are hidden, click the Show link in the Details column. Oracle Applications Manager displays details about the request depending on the status of the request. You can also perform actions, such as placing a hold on a request, canceling a request, viewing diagnostic information, viewing manager details, viewing logs, or viewing request output, by clicking the corresponding button. The actions that are available depend on the status of the request.

- To hide the details for a request if they are shown, click the Hide link in the Details column.

- To search for concurrent requests with different criteria, click the New Search button or click one of the Quick Search links.

- To modify the search criteria from this search, click the Modify Search button.

- To add the information from this page to your support cart, click the Add to Support Cart button.

Active Work Items

The Active Work Items page shows the distribution of active work items across different item types. All work items that do not have an end date are counted as Active work items, including deferred, suspended, and errored work items as well as running work items.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Workflow Metrics > Work Items > Active

To view work items with a different status, choose the status you want from the View pull-down menu and click the Go button. You can view items with the following statuses:

- Completed Work Items

- Active Work Items

- Deferred Work Items
- Suspended Work Items
- Errored Work Items

The page displays the date and time when the work item statistics were last updated. To refresh this information, click the refresh icon. See: Gathering Oracle Workflow Statistics, page 3-2.

For each work item type, the Active Work Items page displays the work item type name and the number of active work items of that type. Click any column heading to sort the list by that column.

- To filter the item types displayed in the list, select an item type property and an operator from the Filter pull-down menus, enter a filter value in the text field, and click the Go button. You can filter by the following properties:
  - Work item type display name
  - Work item type internal name
  - Number of active work items of this type

To view details about active work item activities within a particular item type, either click the item type link in the Work Item Type column, or select the item type and click the View Details button.

Active Work Item Activities

This page shows details about active work item activities within a particular item type. Active work item activities include only activities with a status of Active, Waiting, or Notified.

> **Note:** Only activities with a status of Active, Waiting, or Notified are included in this page. Activities with a status of Deferred, Suspended, or Error are not included in this page, although the work items to which they belong are counted as Active work items. You can use the View pull-down menu to view details for activities with a status of Deferred, Suspended, or Error.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Workflow Metrics > Work Items > Active > (B) View Details

To view work items with a different status, choose the status you want from the View pull-down menu and click the Go button. You can view items with the following statuses:

- Completed Work Items
- Active Work Items
- Deferred Work Items
- Suspended Work Items
- Errored Work Items

Active Work Items Stage Summary

This region displays the distribution of active work items that are currently at various activity stages within the workflow process, if the activity has a status of Active, Waiting, or Notified. For each activity stage, the list displays the activity internal name and the number of active work items at that stage. Click any column heading to sort the list by that column.

- By default, the list shows active work items that started within the last 30 days. To view active work items that started within a different period, enter a number of days in the Filter: Start Date Within Last _ Days option and click the Go button.
- To view details about the work items at a particular activity stage, either click the activity stage link in the Work Item Activity Stage column, or select the activity stage and click the View Details button.

Active Work Item Activity Details

This page shows details about active work item activities of a particular activity stage within a particular item type. Active work item activities include only activities with a status of Active, Waiting, or Notified.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Workflow Metrics > Work Items > Active > (B) View Details > (B) View Details

To view work items with a different status, choose the status you want from the View pull-down menu and click the Go button. You can view items with the following statuses:

- Completed Work Items
- Active Work Items
- Deferred Work Items
- Suspended Work Items
- Errored Work Items

Oracle Workflow Manager displays a list of all active activities of the selected stage for work items of the selected item type. Active work item activities include only activities with a status of Active, Waiting, or Notified. By default, the list shows active work items that started within the last 30 days. For each activity, the list displays the activity internal name, start date, due date, user assigned to perform the activity, and item key of the work item. Click any column heading to sort the list by that column.

- To filter the work items displayed in the list, select an activity property from the Filter pull-down menu, enter a filter value in the text field, and click the Go button. You can filter by the following properties:
  - Internal name of the active activity
  - Start date within a specified number of days
  - Due date within a specified number of days
  - User assigned to perform the activity
  - Item key of the work item
- To abort all work items in the list, click the Abort All button. If you have filtered the list, only the work items currently displayed in the list are aborted.
- To suspend all activities in the list, click the Suspend All button. If you have filtered the list, only the work items currently displayed in the list are suspended.
- To abort a single work item, select the activity you want and click the Abort button.
- To suspend a single activity, select the activity you want and click the Suspend button.
- To launch the Workflow Monitor for a work item, select the activity you want and click the Launch Workflow Monitor button.

  > **Note:** If you perform an action in the Workflow Monitor that changes the status of the work item, such as aborting the work item, then you must refresh your Oracle Workflow Manager web page in order to see the updated information.

Deferred Work Items

The Deferred Work Items page shows the distribution of deferred work items across different item types. An abnormal number of activities with a deferred status may indicate that there are not enough background engines available.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go >

Workflow Metrics > Work Items > Deferred

To view work items with a different status, choose the status you want from the View pull-down menu and click the Go button. You can view items with the following statuses:

- Completed Work Items
- Active Work Items
- Deferred Work Items
- Suspended Work Items
- Errored Work Items

The page displays the date and time when the work item statistics were last updated. To refresh this information, click the refresh icon. See: Gathering Oracle Workflow Statistics, page 3-2.

For each work item type, the Deferred Work Items page displays the work item type name and the number of deferred work items of that type. Click any column heading to sort the list by that column.

- To filter the item types displayed in the list, select an item type property and an operator from the Filter pull-down menus, enter a filter value in the text field, and click the Go button. You can filter by the following properties:
  - Work item type display name
  - Work item type internal name
  - Number of deferred work items of this type
- To view details for work items of a particular item type, either click the item type link in the Work Item Type column, or select the item type and click the View Details button.

Deferred Work Item Details

This page shows details about deferred work items of a particular item type.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Workflow Metrics > Work Items > Deferred > (B) View Details

To view work items with a different status, choose the status you want from the View pull-down menu and click the Go button. You can view items with the following statuses:

- Completed Work Items

- Active Work Items
- Deferred Work Items
- Suspended Work Items
- Errored Work Items

Deferred Work Items Stage Summary

This region displays the distribution of deferred work items that are currently at various activity stages within the workflow process. For each activity stage, the list displays the activity internal name and the number of deferred work items at that stage. Click any column heading to sort the list by that column.

- By default, the list shows active work items that started within the last 30 days. To view deferred work items that started within a different period, enter a number of days in the Filter: Start Date Within Last _ Days option and click the Go button.
- To view details about the work items at a particular activity stage, either click the activity stage link in the Work Item Activity Stage column, or select the activity stage and click the View Details button.

Deferred Work Item Activity Details

This page shows details about deferred work items that are currently at a particular activity stage within a particular item type.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Workflow Metrics > Work Items > Deferred > (B) View Details > (B) View Details

To view work items with a different status, choose the status you want from the View pull-down menu and click the Go button. You can view items with the following statuses:

- Completed Work Items
- Active Work Items
- Deferred Work Items
- Suspended Work Items
- Errored Work Items

Oracle Workflow Manager displays a list of all deferred activities of the selected stage for work items of the selected item type. By default, the list shows deferred work items that started within the last 30 days. For each activity, the list displays the activity internal name, start date, due date, user assigned to perform the activity, and item key of the work item. Click any column heading to sort the list by that column.

- To filter the work items displayed in the list, select an activity property from the Filter pull-down menu, enter a filter value in the text field, and click the Go button. You can filter by the following properties:
  - Internal name of the deferred activity
  - Start date within a specified number of days
  - Due date within a specified number of days
  - User assigned to perform the activity
  - Item key of the work item
- To abort all work items in the list, click the Abort All button. If you have filtered the list, only the work items currently displayed in the list are aborted.
- To suspend all activities in the list, click the Suspend All button. If you have filtered the list, only the work items currently displayed in the list are suspended.
- To abort a single work item, select the activity you want and click the Abort button.
- To suspend a single activity, select the activity you want and click the Suspend button.
- To launch the Workflow Monitor for a work item, select the activity you want and click the Launch Workflow Monitor button.

> **Note:** If you perform an action in the Workflow Monitor that changes the status of the work item, such as aborting the work item, then you must refresh your Oracle Workflow Manager web page in order to see the updated information.

Suspended Work Items

The Suspended Work Items page shows the distribution of suspended work items across different item types.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Workflow Metrics > Work Items > Suspended

To view work items with a different status, choose the status you want from the View pull-down menu and click the Go button. You can view items with the following statuses:

- Completed Work Items
- Active Work Items
- Deferred Work Items
- Suspended Work Items
- Errored Work Items

The page displays the date and time when the work item statistics were last updated. To refresh this information, click the refresh icon. See: Gathering Oracle Workflow Statistics, page 3-2.

For each work item type, the Suspended Work Items page displays the work item type name and the number of suspended work items of that type. Click any column heading to sort the list by that column.

- To filter the item types displayed in the list, select an item type property and an operator from the Filter pull-down menus, enter a filter value in the text field, and click the Go button. You can filter by the following properties:
  - Work item type display name
  - Work item type internal name
  - Number of suspended work items of this type
- To view details for an item type, either click the item type link in the Work Item Type column, or select the item type and click the View Details button.

Suspended Work Item Details

This page shows details about all suspended work items of a particular item type.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Workflow Metrics > Work Items > Suspended > (B) View Details

To view work items with a different status, choose the status you want from the View pull-down menu and click the Go button. You can view items with the following statuses:

- Completed Work Items
- Active Work Items
- Deferred Work Items
- Suspended Work Items

- Errored Work Items

Suspended Work Items Stage Summary

This region displays the distribution of suspended work items that are currently at various activity stages within the workflow process. For each activity stage, the list displays the activity internal name and the number of suspended work items at that stage. Click any column heading to sort the list by that column.

- To view suspended work items that started within a specific period, enter a number of days in the Filter: Start Date Within Last _ Days option and click the Go button.
- To view details about the work items at a particular activity stage, either click the activity stage link in the Work Item Activity Stage column, or select the activity stage and click the View Details button.

Suspended Work Item Activity Details

This page shows details about all suspended work items at a particular activity stage within a particular item type.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Workflow Metrics > Work Items > Suspended > (B) View Details > (B) View Details

To view work items with a different status, choose the status you want from the View pull-down menu and click the Go button. You can view items with the following statuses:

- Completed Work Items
- Active Work Items
- Deferred Work Items
- Suspended Work Items
- Errored Work Items

Oracle Workflow Manager displays a list of all suspended activities of the selected stage for work items of the selected item type. For each activity, the list displays the activity internal name, start date, due date, user assigned to perform the activity, and item key of the work item. Click any column heading to sort the list by that column.

- To filter the work items displayed in the list, select an activity property from the Filter pull-down menu, enter a filter value in the text field, and click the Go button. You can filter by the following properties:
  - Internal name of the suspended activity

  - Start date within a specified number of days

  - Due date within a specified number of days

  - User assigned to perform the activity

  - Item key of the work item

- To abort all work items in the list, click the Abort All button. If you have filtered the list, only the work items currently displayed in the list are aborted.

- To resume all activities in the list, click the Resume All button. If you have filtered the list, only the work items currently displayed in the list are resumed.

- To abort a single work item, select the activity you want and click the Abort button.

- To resume a single activity, select the activity you want and click the Resume button.

- To launch the Workflow Monitor for a work item, select the activity you want and click the Launch Workflow Monitor button.

  > **Note:** If you perform an action in the Workflow Monitor that changes the status of the work item, such as aborting the work item, then you must refresh your Oracle Workflow Manager web page in order to see the updated information.

Errored Work Items

The Errored Work Items page shows the distribution of errored work items across different item types.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Workflow Metrics > Work Items > Error

To view work items with a different status, choose the status you want from the View pull-down menu and click the Go button. You can view items with the following statuses:

- Completed Work Items

- Active Work Items

- Deferred Work Items

- Suspended Work Items

- Errored Work Items

The page displays the date and time when the work item statistics were last updated. To refresh this information, click the refresh icon. See: Gathering Oracle Workflow Statistics, page 3-2.

For each work item type, the Errored Work Items page displays the work item type name and the number of errored work items of that type. Click any column heading to sort the list by that column.

- To filter the item types displayed in the list, select an item type property and an operator from the Filter pull-down menus, enter a filter value in the text field, and click the Go button. You can filter by the following properties:
  - Work item type display name
  - Work item type internal name
  - Number of errored work items of this type
- To view details for an item type, either click the item type link in the Work Item Type column, or select the item type and click the View Details button.

Errored Work Item Details

This page shows details about all errored work items of a particular item type.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Workflow Metrics > Work Items > Error > (B) View Details

To view work items with a different status, choose the status you want from the View pull-down menu and click the Go button. You can view items with the following statuses:

- Completed Work Items
- Active Work Items
- Deferred Work Items
- Suspended Work Items
- Errored Work Items

Errored Work Items Stage Summary

This region displays the distribution of errored work items that are currently at various activity stages within the workflow process. For each activity stage, the list displays the activity internal name and the number of errored work items at that stage. Click any column heading to sort the list by that column.

- To view errored work items that started within a specific period, enter a number of days in the Filter: Start Date Within Last _ Days option and click the Go button.

- To view details about the work items at a particular activity stage, either click the activity stage link in the Work Item Activity Stage column, or select the activity stage and click the View Details button.

Errored Work Item Activity Details

This page shows details about all errored work items at a particular activity stage within a particular item type.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Workflow Metrics > Work Items > Error > (B) View Details > (B) View Details

To view work items with a different status, choose the status you want from the View pull-down menu and click the Go button. You can view items with the following statuses:

- Completed Work Items

- Active Work Items

- Deferred Work Items

- Suspended Work Items

- Errored Work Items

Oracle Workflow Manager displays a list of all errored activities of the selected stage for work items of the selected item type. For each activity, the list displays the activity internal name, start date, due date, user assigned to perform the activity, and item key of the work item. Click any column heading to sort the list by that column.

- To filter the work items displayed in the list, select an activity property from the Filter pull-down menu, enter a filter value in the text field, and click the Go button. You can filter by the following properties:
    - Internal name of the errored activity
    - Start date within a specified number of days
    - Due date within a specified number of days
    - User assigned to perform the activity
    - Item key of the work item

- To abort all work items in the list, click the Abort All button. If you have filtered the list, only the work items currently displayed in the list are aborted.
- To retry all activities in the list, click the Retry All button. If you have filtered the list, only the work items currently displayed in the list are retried.
- To abort a single work item, select the activity you want and click the Abort button.
- To retry a single activity, select the activity you want and click the Retry button.
- To launch the Workflow Monitor for a work item, select the activity you want and click the Launch Workflow Monitor button.

  > **Note:** If you perform an action in the Workflow Monitor that changes the status of the work item, such as aborting the work item, then you must refresh your Oracle Workflow Manager web page in order to see the updated information.

  > **Note:** You can also use the Retry Errored Workflow Activities concurrent program to retry multiple errored activities for a particular item type at once. See: Retry Errored Workflow Activities (FNDWFRET), *Oracle Workflow Administrator's Guide*.

Agents

The Agent Activity page shows the distribution of event messages with different statuses on different Business Event System agents in your instance of Oracle Workflow.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Workflow Metrics > Agent Activity

The page displays the date and time when the agent activity statistics were last updated. To refresh this information, click the refresh icon. See: Gathering Oracle Workflow Statistics, page 3-2.

For each agent, the list displays the agent name as well as the number of event messages on that agent with the following statuses: Ready, Waiting, Processed, Expired, and Undeliverable. Click any column heading to sort the list by that column.

- To view queue details for an agent, click the agent link in the Agent column.
- To view details about the messages being held on an agent, select the agent and click the Search Agent Entry Details button.

> **Note:** The Agent Activity page displays event messages on the WF_ERROR agent according to their explicitly assigned status on the WF_ERROR queue, unlike the Agent Activity graph in the Workflow System Status page which summarizes all messages on the WF_ERROR agent in an Error status.

If an inbound agent has an abnormally large number of messages with a status of Ready, you may need to check the status of the agent listener processing message for that agent, or create a new agent listener service component for that agent. Similarly, if an outbound agent has an abnormally large number of messages with a status of Ready, you may need to check the status of the propagation schedule for that agent's queue, or schedule propagation if necessary.

Agent Queue Details

The Agent Details page displays the following details for the queue associated with an agent:

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Workflow Metrics > Agent Activity > agent link

- Owner - The owner of the queue.
- Name - The name of the queue.
- Queue Table - The name of the table in which the queue data resides.
- Queue ID - The object number of the queue.
- Queue Type - The type of the queue.
- Maximum Retries - The maximum number of attempts that is allowed when dequeuing a message from the queue.
- Retry Delay - The time interval between retry attempts, when dequeuing a message from the queue.
- Enqueue Enabled - Whether the queue is enabled for enqueuing.
- Dequeue Enabled - Whether the queue is enabled for dequeuing.
- Retention - The time interval during which processed messages are retained in the queue.
- User Comments - Descriptive comments about the queue.

After reviewing the agent queue details, choose the OK button to return to the Agent Activity page.

Message Details

The Search Queue page lets you search for messages being held on a particular agent and review details about those messages. This page displays different message details depending on the payload type of the agent's queue.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Workflow Metrics > Agent Activity > (B) Search Agent Entry Details

WF_EVENT_T and SYS.AQ$_JMS_TEXT_MESSAGE

This page lets you review messages on queues with a payload type of WF_EVENT_T, such as the standard WF_ERROR or WF_DEFERRED queues, or SYS.AQ$_JMS_TEXT_MESSAGE, such as the standard WF_CONTROL queue.

Enter filter criteria to locate the messages you want to review and click the Go button. You can filter by the following message properties:

- Internal event name
- Event key
- Correlation ID used to associate a message with other related messages
- Enqueue date either within the last seven days or prior to the last seven days
- Dequeue date either within the last seven days, prior to the last seven days, or on any date
- Status

Oracle Workflow Manager displays the event messages on the queue for the selected agent that match your filter criteria. For each message, the list displays the event name, event key, correlation ID, event parameters, From System that sent the message, To System that received the message, date the message was sent, error message, error stack, and the message status.

The list also includes any messages on the exception queue associated with the selected queue. Messages are transferred from a user queue to the associated exception queue if Oracle Advanced Queuing cannot retrieve or process them for some reason. For more information, see: Oracle Streams AQ Exception Handling, *Oracle Streams Advanced Queuing User's Guide and Reference*.

> **Note:** Each queue table contains one default exception queue that is shared by all the user queues in that queue table. When you search for messages on a particular queue, the search result list includes all messages on the associated exception queue as well, regardless of the user queue from which they originated. Consequently, if you create

more than one user queue in the same queue table, the search result list may display exception messages that originated from other queues than the queue you selected.

- To review the event data for a message as an XML document, choose the message details icon in the View XML column.

  Note: The message details icon is disabled if the event data for a message is empty.

- To add the information from this page to your support cart, click the Add to Support Cart button.

SYSTEM.ECXMSG

This page lets you review messages on queues with a payload type of SYSTEM.ECXMSG, including the standard Oracle XML Gateway ECX_INBOUND and ECX_OUTBOUND queues.

Enter filter criteria to locate the messages you want to review and click the Go button. You can filter by the following message properties:

- Transaction type
- Document number
- Party site ID
- Correlation ID used to associate a message with other related messages
- Enqueue date either within the last seven days or prior to the last seven days
- Dequeue date either within the last seven days, prior to the last seven days, or on any date
- Status

Oracle Workflow Manager displays the messages on the queue for the selected agent that match your filter criteria. For each message, the list displays the message type, message standard, transaction type and subtype, document number, party ID, party site ID, party type, protocol type, protocol address, first, second, third, fourth, and fifth attributes, and the message status.

- To review the XML document for a message, choose the message details icon in the View XML column.

> **Note:** The message details icon is disabled if the XML document for a message is empty.

- To add the information from this page to your support cart, click the Add to Support Cart button.

SYSTEM.ECX_INENGOBJ

This page lets you review messages on queues with a payload type of SYSTEM.ECX_INENGOBJ, including the standard Oracle XML Gateway ECX_IN_OAG_Q queue.

Enter filter criteria to locate the messages you want to review and click the Go button. You can filter by the following message properties:

- Message ID
- Correlation ID used to associate a message with other related messages
- Enqueue date either within the last seven days or prior to the last seven days
- Dequeue date either within the last seven days, prior to the last seven days, or on any date
- Status

Oracle Workflow Manager displays the messages on the queue for the selected agent that match your filter criteria. For each message, the list displays the message ID, debug mode, and the message status.

To add the information from this page to your support cart, click the Add to Support Cart button.

Queue Propagation

You should schedule propagation for your local outbound agents to send event messages to their destinations. You can schedule Oracle Advanced Queueing (AQ) propagation for agents that use the SQLNET protocol by the following methods:

- Use the Distributed Database Management feature to manage AQ through Oracle Enterprise Manager. See: Oracle Enterprise Manager Support, *Oracle Streams Advanced Queuing User's Guide and Reference*.
- Run the DBMS_AQADM.Schedule_Propagation API in SQL*Plus. See: DBMS_AQADM, *Oracle Database PL/SQL Packages and Types Reference*.

If you want to use the standard WF_OUT and WF_JMS_OUT agents or custom agents for event message propagation, ensure that you schedule propagation for those agents. You do not need to schedule propagation for the WF_CONTROL or WF_NOTIFICATION_OUT agents, however, because the middle tier processes that use WF_CONTROL dequeue messages directly from its queue, and a notification mailer sends messages placed on the WF_NOTIFICATION_OUT queue.

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Related Links > Configuration > Queue Propagation

Queue Propagation

Use the Queue Propagation page to review the database initialization parameters required for queue propagation, as well as the existing propagation schedules for Business Event System agents in your instance of Oracle Workflow.

Database Initialization Parameters for Queue Propagation

For each parameter, this list shows the parameter name, actual parameter value, recommended value, and description. If the actual value does not match the recommended value, the recommended value is marked with a warning indicator icon.

The JOB_QUEUE_PROCESSES parameter defines the number of job queue processes for your instance. Oracle Workflow requires job queue processes to handle propagation of Business Event System event messages by AQ queues. The recommended number of processes for Oracle Workflow is ten or more.

> **Note:** In Oracle Database 10*g* and higher, you do not need to set the AQ_TM_PROCESSES parameter.

Queue Schedules

For each propagation schedule, the list displays the outbound queue, destination database link, job queue process executing the schedule, whether the schedule is enabled or disabled, and the error date and error message of the last unsuccessful execution. Click any column heading to sort the list by that column.

If no process is allocated to execute the schedule, you may need to increase the JOB_QUEUE_PROCESSES database initialization parameter to ensure that processes are available for propagation.

To view details for a propagation schedule, either click the queue link in the Queue column, or select the schedule and click the View Details button.

Queue Propagation Details

The Queue Propagation Details page displays the following details for a propagation schedule:

Navigation: Applications Dashboard > (pull-down menu) Workflow Manager > (B) Go > Related

Links > Configuration > Queue Propagation > (B) View Details

- Destination - The destination database link.

- Process Name - The name of the job queue process executing this schedule.

- Enabled - `Y` if this schedule is enabled or `N` if the schedule is disabled. The schedule will not be executed if it is disabled.

- Last Error Date - The date of the last unsuccessful execution.

- Last Error Time - The time of the last unsuccessful execution.

- Last Error Message - The error message of the last unsuccessful execution.

- Schema - The schema that owns the queue.

- Session ID - The session ID (SID, SERIAL#) of the job executing this schedule; NULL if not currently executing.

- Propagation Window - The duration in seconds of the propagation window.

- Maximum Bytes - The maximum number of bytes propagated during a propagation window.

- Failures - The number of times that execution of the schedule failed. If the number of failures reaches 16, the schedule will be disabled.

- Latency - The latency time in seconds that specifies how long to wait, after all messages have been propagated, before rechecking the queue for new messages to the destination. The latency represents the maximum wait time during the propagation window for a message to be propagated after it is enqueued.

- Next Run Date - The date at which the next propagation window of this schedule will be started.

- Next Run Time - The time at which the next propagation window of this schedule will be started, in HH:MI:SS format.

- Current Start Date - The date at which the current propagation window of this schedule was started.

- Current Start Time - The time at which the current propagation window of this schedule was started, in HH:MI:SS format.

- Instance - The cluster database instance number executing the schedule.

- Start Date - The date when propagation should be started, in the default date format.

- Start Time - The time when propagation should be started, in HH:MI:SS format.
- Last Run Date - The date of the last successful execution.
- Last Run Time - The time of the last successful execution, in HH:MI:SS format.
- Total Time - The total time, in seconds, spent by the system in executing this schedule.
- Total Number - The total number of messages propagated in this schedule.
- Total Bytes - The total number of bytes propagated in this schedule .
- Maximum Number - The maximum number of messages propagated during a propagation window.
- Average Number - The average number of messages propagated during a propagation window.
- Average Size - The average size of a propagated message, in bytes.
- Average Time - The average time, in seconds, to propagate a message.

4

Monitoring Oracle E-Business Suite

Overview of Monitoring Oracle E-Business Suite

Using Oracle Applications Manager (OAM), you can monitor components of your Oracle E-Business Suite instance.

For more information on setting up OAM, as well as other features, see the *Oracle E-Business Suite System Administrator's Guide - Configuration.*

The Applications Dashboard

The Applications Dashboard provides a "snapshot" of your Oracle E-Business Suite system. Information is grouped under the following tabs: Overview, Performance, Critical Activities, Diagnostics, Business Flows, Security, and Software Updates.

For information on Software Updates, see: Software Updates, *Oracle E-Business Suite Patching Procedures*.

From the Dashboard you can navigate to the Site Map, or use the drop-down menu to navigate to any of the following pages:

- Application Services
- Configuration - Overview
- Forms Sessions
- Database Status
- Applied Patches
- Patch Wizard
- Workflow Manager

Oracle Applications Manager uses the collection program OAM Applications Dashboard Collection (short name: FNDOAMCOL) to gather the information displayed. The default repeat interval for this program is 10 minutes. To immediately regather the data and update the display for a particular region, click the corresponding Refresh icon. If the OAM Applications Dashboard Collection request is not running when you log in to the Oracle Applications Manager, a request will be submitted automatically under your username.

> **Note:** The status of Web Components is collected manually from the Dashboard.

Overview

This page provides an overview of the general status of your system. It includes the following regions:

Applications System Status

Use this region to view the status of each host machine in your system. The display shows which services are installed on which host machine and the statuses of these services.

Services displayed that represent more than one service component (such as Forms) indicate the status of the worst-case component. For example, if the Forms Listener is down, but the other Forms components are running, the down status will be indicated on this page.

The Database, Concurrent Processing, Forms, and Web status indicators drill down to the Applications System Status page where you can view the status of each individual service.

- Host - the host name.
- Platform - the host's operating system.
- Admin - indicates whether the Admin server has been installed on the host machine.
- Database - indicates the status of the database instance installed on the host machine.
- Concurrent Processing- indicates the status of the Internal Concurrent Manager and the services managed by the ICM.
- Forms - indicates the status of the Forms Server components: Forms Listener, Metrics Server, Metrics Client, and OAM Generic Collection Service.

- Web - indicates the status of the Apache Web Listener.

Configuration Changes

The purpose of this region is to alert you to system-level changes that have occurred in the last 24 hours. Use this data to help diagnose sudden changes in the functioning of your applications system.

To see the list of Patches Applied, click on the number to drill down to the Patch Summary page.

To see the list of Site Level Profile Options, click on the number to drill down to the Site Level Profile Settings page.

To see the list of Applications Context Files Edited, click on the number to drill down to the Applications Configuration Parameters page. Changes made to context files can impact your overall processing configuration and the functioning of business processes.

System Alerts

This region lists the number of system alerts in the categories listed below. If your system is functioning well, there should be no new alerts reported. When an alert of a particular type first occurs, it is counted as a new alert. It remains new until the status is manually changed by the administrator. If an alert of the same type occurs again while the original alert is still in open or new status, it is counted as a new occurrence.

- New Alerts - alerts that have not yet been acknowledged by the administrator. An alert is acknowledged when it is manually moved from a status of "New" to a status of "Open" or "Closed."

- New Occurrences - additional occurrences of alerts that are in new status.

- Open Alerts - all alerts that are in an open status. An alert must be manually moved from the new to open status.

- Open Occurrences - all occurrences of alerts that are currently open. Click on the number for any of these to drill down to the System Alerts and Metrics page.

Web Components Status

This region lists the status of the web components. Status values may be "Up," "Down," or "Warning".

The status of each Web component is determined by testing the corresponding URL as defined in the component's Web agent profile option. The Warning status will be displayed if the profile option is not set. Otherwise, a status of Up or Down will be returned based on the success of the URL test. The profile options are listed with their corresponding components below.

- PL/SQL Agent - Uses profile option APPS_WEB_AGENT (Applications Web Agent). Look for errors in the Apache error log ($LOG_HOME/ora/10.1.3/Apache).

- Servlet Agent - Uses profile option APPS_SERVLET_AGENT (Apps Servlet Agent). If down, the Self-Service Framework-based Applications will not function, as well as all other servlet-based features. Look for errors in the Apache error and access logs (see above for location). Also, execute the Servlet Ping from the System Administration Diagnostics menu.

- JSP Agent - Uses profile option APPS_SERVLET_AGENT (Apps Servlet Agent). If down, execute the JSP Ping from the System Administration Diagnostics menu.

- JTF - Uses profile option APPS_SERVLET_AGENT (Apps Servlet Agent).

- Discoverer (if installed) - Uses profile option ICX_DISCOVERER_VIEWER_LAUNCHER (ICX: Discoverer Viewer Launcher). If down, you will not be able to run BIS reports.

- Personal Homepage - Uses profile option APPS_SERVLET_AGENT (Apps Servlet Agent). If down, you cannot log on through the Personal Homepage.

- TCF - Uses profile option APPS_SERVLET_AGENT (Apps Servlet Agent). If down, try running the AOL/J Diagnostic or the Servlet Ping utilities from the System Administration Diagnostics menu.

Applications System Status

This page lists each Applications Server and its status. Each server type expands to display the host name, which expands to display the status of each server component.

Navigation: Applications Dashboard (Overview page) > (drill down on) Database, Concurrent Processing, Forms, or Web column (under Applications System Status)

- Administration

- Database- expands to display the instance name and status. Drill down on the instance name to display the Database Status Details page. Concurrent Processing - expands to display concurrent managers and services controlled by the Internal Concurrent Manager. These expand to display the instances of the managers and services and their statuses. Drill down on the instance names to display the Service Instances page.

- Forms - expands to display the Forms server components: the Forms Listener, the Metrics Server, the Metrics Client, and the OAM Generic Collection Service. The component names expand to display the service instances. Drill down on the instance name to display the Service Instances page.

- Web - expands to display the web component: the Apache Web Listener. The component name expands to display the service instance name. Drill down on the instance name to display the Service Instances page.

Click on the Focus icon for an item to display only its status and the status of its children.

Applications Dashboard - Performance

The Performance region lists Activity and System Throughput indicators. Each of the values listed for Activity and System Throughput links to the related detail page.

Activity

- Forms Sessions - the number of running Forms sessions. Drills down to the Forms Sessions page.
- Database Sessions - the number of active database sessions. Clicking the value runs the Show Active Database Sessions request and returns the results page.
- Running Concurrent Requests - drills down to the Search for Requests Results page showing all currently running requests.
- Service Processes - drills down to the System Activity page. Service processes include all concurrent manager processes and all processes managed by the ICM. If you have set up your system to have other services managed by the GSM, those services are included as well.
- Services Up - the number of service instances whose target services match the actual services. Services Down - the number of service instances whose target services do not match the actual services.
- Invalid Database Objects - drills down to the Invalid Database Objects page displaying the search results for invalid objects owned by the APPS schema.
- Unsent Workflow E-Mail

System Throughput (last 24 hours)

- Completed Concurrent Requests - the percentage of concurrent requests submitted in the last 24 hours that have completed.
- Sent Workflow E-Mail - the percentage of Workflow e-mail sent successfully.

Applications Dashboard - Critical Activities

The Critical Activities region lists concurrent programs that perform maintenance activities. The programs are grouped by activity type and by application. To display only a particular group, click the group's **Focus** icon.

To add or delete a program to the critical activities list, click the **Modify Monitored Program List** button to access the Modify Monitored List page.

To change the frequency that a monitored program is run, click the **Update Frequency** button.

For each critical activity, the following are displayed:

- Program Name - Drills down to the Activity Summary page showing work metrics for those programs that have been instrumented to compute them.
- Request ID - The last run request ID. Drills down to display the request in the concurrent request Search Results screen.
- Last Run Date
- Outcome - indicates the completion status of the request.
- Oracle Recommended Frequency - The frequency that Oracle recommends a critical program be run (if applicable).
- On Schedule (Oracle Recommended) - indicates whether the Oracle recommended schedule has been met (if applicable).
- Onsite Frequency - the frequency that the program is currently scheduled to run. To change the frequency, use the Update Frequency button to access the Update Frequency for Monitored Critical Activities page.
- On Schedule (Onsite Frequency) - indicates whether the onsite schedule has been met.
- Success Rate - the percentage of completed requests that completed with a status of normal. Drill down on the value to display a success rate chart showing completion status percentage rates of Normal, Warning, and Error. Mouse over the chart to display the numeric values.

Modify Monitored List

Navigation: Applications Dashboard > Critical Activities (B) Modify Monitored Program List

Use this page to add or remove programs to the critical activities list.

To add a program to the Monitored list, select the program from the Not Monitored list and click the Move shuttle button.

To add all programs from the Monitored list, click the **Move All** shuttle button.

To remove a program from the Monitored list, select the program from the Monitored list and click the **Remove** shuttle button.

To remove all programs from the Monitored list, click the **Remove All** shuttle button.

Click **OK** to apply your changes.

Update Frequency for Monitored Critical Activities

Navigation: Applications Dashboard > Critical Activities (B) Update Frequency

Use this screen to update the frequency that your critical activity programs are run.

The following are listed for each critical activity program:

- Program Name
- Application
- Program Type
- Oracle Recommended Frequency - the run frequency recommended by Oracle (if applicable).
- Onsite Frequency - the frequency that the program is currently scheduled to run. To change the run schedule for a program, update the **Onsite Frequency** field and click **OK**. Note that this is the target frequency and may not be the frequency that the program actually runs. Monitor the success of the target frequency with the On Schedule (Onsite Frequency) field on the Applications Dashboard - Critical Activities page.

Critical Activities - Activity Summary

Navigation: Applications Dashboard > Critical Activities > [Program Name]

This page displays work metrics for those maintenance programs that have been instrumented to compute them. The display can be filtered by the table name or value.

- Name - the name of the table that will be purged by the program.
- Value - the number of rows in the table that will be purged if the program is run.

Applications Dashboard - Business Flows

Oracle Applications Manager allows you to monitor and support business flows within Oracle E-Business Suite. User-defined key business flows are correlated with the system components responsible for the execution of those flows.

Navigation: Applications Dashboard > Business Flows tab

From the OAM console you can:

- View the hierarchical representation of the business flows.

- Monitor system alerts, errored requests, and errored work items for a business flow.

- View the setup status for the business flows and associated subflows.

The Key Business Flows region displays the current listing of business flows, with these columns:

- Status - Indicates the setup status of the business flow. Business flows that are not fully set up are listed as unavailable

- Edit

To create a new business flow, click **Create**. Click View Details for a selected business flow to view additional information for that business flow. Click the **Edit** icon for a selected business flow to update it.

Create or Edit a Business Flow

Use these pages to create or edit a business flow.

Navigation: Applications Dashboard > Business Flows tab > Create (B) or Edit icon for a selected business flow

Enter a name and description for the business flow.

Enter in a child flow or component for the business flow. Choose from the following:

- New Business Flow - If you select New Business Flow you are prompted for a name and description of the new business flow. You can later update the new subflow with children of its own.

- Existing Business Flow - You are prompted to choose a business flow from a list of values.

- Work Item Type - You are prompted to choose a workflow item type from a list of values.

- Component - Select from Concurrent Program, Service, Form or Function. You are prompted for a component name from a list of values.

View Business Flow Details

This page displays details for a selected business flow.

Navigation: Applications Dashboard > Business Flows tab > View Details (B) for selected business flow

Subflows and components of the business flow are shown in hierarchical format. You can expand or collapse nodes on the hierarchical tree.

Business Flow Monitoring and Setup

Maintain your business flow monitoring from this page.

Navigation: Setup (global icon) > Business Flows (side navigation)

Schedule Requests

OAM provides the following concurrent program to help you maintain your business flow setup. Schedule requests for the concurrent program from the link provided.

- Metrics Refresh - schedule requests for the OAM: KBF Metrics Rollup Program to update the setup status of your business flows.

Setup Monitoring

For each of the business flows listed, you can view whether monitoring is enabled and enable or disable monitoring.

Select a business flow and click Update to enable or disable monitoring. Click **View Details** to view if monitoring is enabled.

Applications Dashboard - Security

Information on this page helps you detect and diagnose security issues on your Oracle E-Business Suite System.

Navigation: Applications Dashboard > Security (tab)

Click the **Manage Security Options** button to manage SQL*Net access for your middle-tier hosts.

Security Alerts

Security Alerts can be raised either at runtime by the application code, or at the failure of security-related diagnostic tests. The table is organized by severity, which can be Critical, Error, or Warning. It provides numerical counts of new and open alerts. Where enabled, you can drill down on the numerical links to view and manage the details of an alert and any associated diagnostic test reports. Alert details and test reports can be added to the Support Cart.

Security Test Failures

This table shows security-related diagnostic tests that failed when they were executed. The table specifies the most recent time that the test failed, and provides links that open detailed test reports. For a specific test, clicking the **Diagnose** icon will re-execute the test -- this is useful to verify that the error still exists. For a specific application, clicking the Diagnose icon allows you to re-execute all failed tests in that application for the chosen security level.

Resources

Links to security-related documents on My Oracle Support are located here. Documents include:

- Best Practices for Securing Oracle E-Business Suite
- Oracle Support Services Security Alert - Frequently Asked Questions
- Security Announcements and Notes

Security-Related Tests

You can manage Oracle E-Business Suite Diagnostics tests from the dashboard.

For more information on Oracle E-Business Suite Diagnostics, see: *Oracle Diagnostics Framework User's Guide*.

Manage Security Options

Use this button to access Security Options.

Managing SQL*Net Access from Middle-Tier Hosts

These pages allow you to restrict SQL*Net access to the database from your middle-tier hosts. If you enable the SQL*Net Access security option, you can select which hosts have SQL*Net access to the database. If you disable the SQL*Net Access security option, then all middle-tier hosts have SQL*Net access to the database.

View SQL*Net Access

Use the View SQL*Net Access page to see how SQL*Net Access is currently configured for your middle-tier hosts.

Navigation: Applications Dashboard > Security (tab) > Manage Security Options (B)

If the Manage SQL*Net Access security option is disabled, a message here indicates that it is disabled. All hosts have SQL*Net access to the database in this case.

If this feature is enabled, the table of hosts indicates which hosts have SQL*Net access and which do not.

> **Note:** In order for the information on this page to be accurate, the following steps must be run in addition to enabling or disabling the Manage SQL*Net security option:
>
> - Run AutoConfig on the database tier
> - Bounce the TNS Listener

The table shows the hosts that have SQL*Net access and includes the following columns:

- Name
- Platform
- Oracle Applications Host - Indicates whether the host is an Oracle E-Business Suite host or not. Application services (Concurrent Processing, Oracle Forms, Web, Admin, and Database services) can run on Oracle E-Business Suite hosts.

Enable SQL*Net Access

Use the Manage SQL*Net Access wizard to enable or disable SQL*Net access to the middle-tier hosts. You can register a new host and grant it access as well from this wizard.

Disable SQL*Net Access

When you disable the SQL*Net Access security option, you allow SQL*Net access to the database from your middle-tier hosts.

Applications Dashboard Collection

Oracle Applications Manager uses the program OAM Applications Dashboard Collection (short name: FNDOAMCOL) to gather the information displayed on the Dashboard under the Overview and the Performance tabs.

The Dashboard Collection Program can selectively enable and disable monitoring of various metrics, and to raise alerts for services when the service has a specified status. The Dashboard Collection Program can collect data for a metric and then raise an alert when a metric reaches a specified threshold. Note that for most components, you can collect data for monitoring purposes in two different ways: (1) through the Dashboard Collection Program, or (2) manually refreshing the data from a Dashboard page.

Metrics for the following data can be monitored for the following using the Dashboard Collection Program. In addition, data for web components can be collected manually in the dashboard.

Activity

- Forms Sessions
- Database Sessions
- Running concurrent requests
- Service processes
- Services up

- Services down
- Invalid database objects
- Unsent Oracle Workflow e-mail

Configuration changes (made in the last 24 hours)

- Patches applied
- Site level profile options
- Applications context files edited

System Alerts

- New alerts
- New occurrences of an alert
- Open alerts

Alerts can be raised for the following services. When a service attains a specified status, an alert is raised.

- Service instances listed under Applications System Status
- Web Components

System Throughput (in the last 24 hours)

- Completed concurrent requests
- Sent Oracle Workflow e-mail

Additional Monitoring in Oracle Applications Manager

From the Monitoring tab on the OAM Site Map, you can access these utilities.

Service Instances for the Forms Listener

Navigation: Site Map > Monitoring > Forms (under Availability)

This page lists the service instances for the Forms Listeners. From this page you can edit information for a selected service instance. You can also view its status, view processes, and view information on its Forms Runtime Processes. Also, you can start, stop, abort, or restart the instance.

SQL Activity

Navigation: Site Map > Monitoring > SQL Activity (under Performance)

This page provides data regarding SQL Activity:

- SQL_HASH
- Physical Reads
- Logical Reads
- Total Sorts
- Execs
- Total Loads
- Load

For more information on these columns, see the Oracle database documentation.

Concurrent Request Runaways

Main Navigation Path: Site Map > Monitoring (subtab) > Performance (heading) > Concurrent Request Runaways (link)

System performance can potentially be affected by database sessions that should have ended when their corresponding concurrent requests were canceled, but for some reason did not.

If any such database sessions are currently active, they will be reported on this page. The table supplies context information for each session: request ID, AUDSID, program, user name, start time, phase, status, Oracle SPID, and PID. You can delete a session by selecting it in the table and clicking Terminate. You can drill down on the links in the request ID, AUDSID, program, and user name columns to view the respective details.

Forms

The following information is shown:

Forms Sessions

Navigation: Site Map - Monitoring > Forms Sessions (under Current Activity)

This page shows information on the current forms sessions. Every open form has its own database session, or "form session."

The profile option "Sign-On:Audit Level" should be set to 'Form' to use this feature. If this profile option is not set to 'Form', the Forms Sessions table will show an empty table even when there are active forms sessions.

To filter the display by Form Name, Username, Responsibility, or Application, make the appropriate selection from the drop-down menu, enter the search string in the field provided, and click Go.

The following data is shown for each session:

- Form Name
- AUDSID - The auditing session ID. Click on the value to drill down to the Database Session information page.
- RTI_PID - The runtime instance process ID. Click on the value to drill down to the Forms Sessions for Process ID page.
- Username
- Responsibility
- Application
- LRs (Session Logical Reads) - Input/output (I/O) is one of the most expensive operations in a database system. SQL statements that are I/O-intensive can monopolize memory and disk use and cause other database operations to compete for these resources. To prevent single sources of excessive I/O, Oracle lets you limit the logical data block reads per call and per session. Logical data block reads include data block reads from both memory and disk. The limits are set and measured in number of block reads performed by a call or during a session.
- PRs (Physical Reads) - The total number of data blocks read from the disk for the session.
- CPU
- PGA (Session Program Global Area memory) - The PGA is a memory buffer that contains data and control information for a server process. A PGA is created by Oracle when a server process is started. The information in a PGA depends on the configuration of Oracle
- UGA - User Global Area memory used by the session.
- Duration - in HH:MM:SS

Click on the **Session Details** button or the AUDSID to view database information for the selected forms session.

Use the **Diagnostics On/Off** button to turn on or off the Forms Runtime Diagnostics (FRD) for the runtime process. If this button is disabled, make sure your Forms patchset level is 12 or higher (that is, 6.0.8.20 or higher) and then set the environment variable

FORMS60_OAM_FRD for the Forms Listener process.

Forms Sessions for Process ID

If you click on the RTI_PID from the Forms Session window, or if you click on the PID from the Forms Runtime Processes window you will see the fields described above as well as the following data for the Process ID:

- Client IP Address
- Server Host Name
- CPU Time
- Memory Usage (KB)
- Diagnostics (On/Off)
- Log File Name

Use the **View Diagnostics** button to view the Forms Runtime Diagnostics (FRD) log file. The log file can be added to the Support Cart.

Forms Runtime Processes

Navigation: Site Map - Monitoring > Forms Runtime Processes (under Current Activity)

This page shows information about Forms runtime processes. You must first register and start a service instance of the OAM Generic Collection Service to collect this information. The Generic Collection Service must be running for the information to be collected.

You can filter your view by Node or Username.

The following columns are shown for each session:

- PID - The ID of the runtime process for the user session. Click this value to drill down to the Forms Sessions for Process ID page.
- Node
- Port - The Apache port of the servlet listener, if any.
- Memory (KB) - The memory used by the runtime process in kilobytes. For HP and AIX platforms, this is the virtual memory size. For all other platforms, this is the resident set size.
- CPU
- Duration

- Client IP Address - The IP address of the client machine used to connect to the Forms Services.
- Username - The database username used by the Forms application for the user session.
- Diagnostics - On/Off
- Last Update Time

Use the Upload button to refresh the data on this page.

Use the Terminate button to end a selected process.

Click on the Sessions button or click on the PID to view the Forms Sessions for Process ID page.

This page also shows the runtime processes from the Forms Servlet Listener, if any. The Port column for such processes indicates the Apache Listener port.

Forms Listener versus Forms Listener Servlet

The Forms Listener is a process running on a specific port on the server machine. When the connection between the client and the Forms runtime process is established, the client and the runtime process requires that the connection be persistent.

The Forms Listener Servlet is a Java servlet running in a servlet engine. The Web server routes the client requests for the Forms Listener Servlet directly to the servlet instance. Because the web server acts like the end point for the client, the other server machines and ports are no longer exposed to the firewall.

In the Forms Runtime Processes page, the node name and the port are shown for each runtime process. You can distinguish between the Forms Listener process and Forms Listener Servlet process by examining the port numbers. For the Forms Listener process, the port is the Forms server machine port. For the Forms Listener Servlet process, the port is the web server port.

System Activity (Activity Monitors)

Navigation: Site Map > Activity Monitors (under Activity)

This region displays information on the system's activity.

A Database Sessions graph displays the number of database sessions related to the following:

- Login sessions
- Oracle E-Business Suite forms sessions
- Services

- Requests

A Concurrent Requests graph displays the number of requests with the following statuses:

- Pending
- Running
- Waiting on a lock
- Inactive
- Completed in the last hour

Click on the bar for any status to drill down to more information on requests of each status.

Database Session Information

Navigation: Site Map - Monitoring > Forms Sessions (under Current Activity) > (B) Session Details

This page displays detailed information about the selected database session. Click **Terminate** to end the database session.

Summary

- Form or Service Name
- Username
- Responsibility

Instance Attributes

- Logon Time
- Serial Number
- OS PID
- Status
- Session ID
- Oracle SPID
- User

- SQL Hash - If the value shown is a link, you can click on it to view a page showing the SQL statement that is currently executing, as well as an execution plan for the statement. For more information on execution plans, see the Oracle database documentation.

Client Attributes

- OS User
- Machine
- Process
- Terminal

Application Attributes

- Module
- Module Hash
- Action
- Program

Session Wait Information

- Event
- Wait Time
- Timeouts
- Average Wait
- Total Wait
- Maximum Wait

Tracing Options

Set the trace options to the level desired. Options available are:

- Normal Trace
- Trace with Waits
- Trace Off

- Trace with Binds
- Trace with Binds and Waits

Click **Apply** to apply any changes made to the Tracing Options. Click **View Trace** to view the current trace information.

Current Activity

The following information is shown:

Invalid Objects

Navigation: Site Map > Monitoring > Invalid Objects (under Current Activity)

This page lists invalid objects in the database. To remove invalid objects, you can compile the APPS schema (for invalid objects in the APPS schema) or run a script provided with the database (for other invalid objects). See the *Maintaining Oracle E-Business Suite Documentation Set* for more information on compiling objects.

Forms Runaway Processes

Navigation: Site Map > Monitoring (subtab) > Current Activity (heading) > Forms Runaway Processes (link) Overview

You can also access this page by clicking the **View Runaways** button on the Forms Runtime Processes page.

Running Oracle E-Business Suite requires the creation of many system-level processes. On occasion, processes can behave incorrectly and have a negative impact on system performance. In Oracle Applications Manager, you can:

- Configure thresholds (maximum memory size, maximum CPU percent, maximum duration in minutes) for tracking runaway processes. These settings take immediate effect as soon as you click Apply. These settings are used to raise system alerts on the Applications Dashboard.
- See the user name and IP address of runaway processes.
- Terminate processes.
- See the parameters of the OAM Generic Collection Service (the background process which runs on all Forms nodes).
- Open the associated log file.

You can define memory, CPU, and duration thresholds. Memory refers to process memory size, resident set size, or total virual memory size based on the platform. On a UNIX system, CPU refers to the cumulative execution time of the process. On a Windows NT system, CPU is, CPMemory - Process memory size, Kb, resident set size or total virtual memory size based on the platform. CPU - On UNIX, it is the percentage of CPU use. If the system has both UNIX and Windows NT nodes, then CPU refers to the percentage of CPU use. In all cases Duration refers to the total time elapsed since a connection was established.

The default values of the thresholds are as follows:

- Maximum memory: 1.0 MB
- Maximum CPU: 25%
- Maximum duration: 20.0 minutes

Applications Usage

Navigation: Site Map > Monitoring (tab) > Applications Usage Reports (under Usage)

The Applications Usage page contains links to the following pages:

- Products Installed
- Applications Users Per Module Summary
- Page Access Tracking and Sign-On Audit: Configuration, Reports
- Applications Usage Reports: Purchase Lines Processed, Order Entry Lines Processed, and more

Products Installed

Navigation:

Applications Systems > (B) Configuration > Products Installed

or

Applications Systems > (menu) Applications Usage > (B) Go > Products Installed

This page lists the following information for Oracle E-Business Suite products:

- Application Short Name
- Application Name
- Version
- Status- A product's status can be Installed, Shared, or Inactive. Installed indicates that the product has been licensed and installed. The Shared status is used for products that other products are dependent upon. Products that are neither Installed nor Shared have anInactive status.

Application Users Per Module Summary

Navigation: *All Applications Systems > (pull down menu) Applications Usage > (B) Go > Application Users Per Module Summary*

This page lists the following information for Oracle E-Business Suite modules:

- Application Short Name
- Module Name
- Count - number of current users

You can view details for a particular module by selecting its radio button on the left and clicking the **View Details** button. This takes you to a page that lists the following:

- Module Name
- User Name
- Description of User
- Creation Date of User
- Last Log On Date

Click **Show All** to see a format suitable for printing that lists all users. Within the Show All format, click on **Show Set** to see the table format of the list.

Page Access Tracking and Sign-On Audit

Page Access Tracking and Sign-on Audit tracks the accesses of Oracle E-Business Suite JSPs and Oracle Forms for usage pattern analysis and performance statistics. The Reports screen displays the complete flow of accesses across technology stacks within a user session. It also aggregates collected metrics and display summary statistics.

Applications Usage Reports

Use these reports to collect information on specific applications usage. Your License Management Services analyst may ask you to collect such information, or you can use these reports for your own monitoring.

The following reports can generate information on various licensing metrics in a time period you specify. However, for the purposes of License Management, a twelve (12) month period is used.

Purchase Line Items Processed (iSupplier Portal, Purchasing Intelligence, and iProcurement)

These reports generate information for the licensing metric Purchase Line. Purchase Line is defined as the total number of purchase line items processed by the application during a 12 month period. Multiple purchase lines may be created on either a requisition or purchase order or may be automatically generated by other Oracle E-Business Suite programs. For iProcurement, Purchase Lines are counted as all line items on an approved requisition created in iProcurement. For iSupplier Portal and Purchasing Intelligence, Purchase Lines are counted as the line items on purchase orders processed through each of those applications. This does not include communication on the same Purchase Order. For each application, you may not exceed the licensed number of Purchase Lines during any 12-month period unless you acquire additional Purchase Line licenses from us. You may acquire a different number of Purchase Line licenses for each program (Number of Purchase Lines for iProcurement could be a smaller number than for iSupplier Portal).

For iSupplier Portal, use the Suppliers script to generate a list of suppliers and their IDs. You can then use this information when running the Purchase Line Items Processed report for iSupplier Portal.

Order Entry Lines Processed (Order Management)

This report is used for the licensing metric Order Line, which is defined as the total number of order entry line items processed by the program during a 12 month period. Multiple order entry line items may be entered as part of an individual customer order or quote and may also be automatically generated by the Oracle Configurator. You may not exceed the licensed number of Order Lines during any 12 month period.

Expense Reports Processed (Internet Expenses)

This report is used for the licensing metric Expense Report, which is defined as the total number of expense reports processed by the iExpenses during a 12 month period. You may not exceed the licensed number of Order Lines during any 12 month period.

Invoice Line Items Processed (Accounts Receivables)

This report is used for the licensing metric Invoice Line, which is defined as the total number of invoice line items processed by the program during a 12 month period. You may not exceed the licensed number of Invoice Lines during any 12 month period unless you acquire additional Invoice Line licenses from us.

Custom Reporting Utilities - SQL Extensions

Use this page to run seeded and custom scripts.

Navigation: Site Map > SQL Extensions (under Others)

Click on the icon in theFocus column to display only those reports from the selected group.

Use the **Hide/Show** icon next to the group name to hide or display the reports contained in the group.

The following columns are shown for each report:

- Name - Click on the name of the report to display the report details.
- Description
- Protected - A "locked" icon indicates that a password is required to submit the report.
- Run Report - Click on the icon in this column to run the report. If a password or parameters are required, the SQL File Detailspage will display. Otherwise, the output of the report will display in the Results page.

Use the **Reload** button to reload the displayed reports from the metadata file.

Adding Custom Scripts to the SQL Extensions Page

You can have your custom scripts automatically discovered by Oracle Applications Manager and available to run from the SQL Extensions page.

1. Create a new SQL script. Multiple SQL statements are allowed within the same file. For example: a report called "Get Sysdate": sysdate.sql
2. Create a directory called /custom/sql for your custom SQL files under <APPL_TOP>/admin. Your directory structure should look like <APPL_TOP>/admin/custom/sql.
3. Copy your SQL files to <APPL_TOP>/admin/custom/**sql** directory.
4. Now log in to Oracle Applications Manager and navigate to Site Map > SQL Extensions.
5. The discovered SQL files will be under the "DefaultC" group.

After the files are discovered, you can customize the grouping, protection, and execution method of these scripts.

Customizing Automatically Discovered Scripts

To customize the grouping, protection, report format, or drill-downs for your automatically discovered scripts, you must edit **oamcustext.amx** located under <APPL_TOP>/admin/custom/xml.

For each discovered script, the oamcustext.amx file will contain an entity similar to the following example that defines the grouping, protection, and report format:

<cReport type="SQL" group="DefaultC">

<title>sysdate.sql</title> <script name="sysdate.sql" protected="yes" execMode="SQLPLUS" parameters="unknown">

</script>

```
</cReport>
```

To move your report to a different group

You can change the group that your report displays under.

1. In the oamcustext.amx file, change the value of "group" to the name of the group you want your report to appear in. For example, to change the group to "Custom Reports", the result would be:

   ```
   <cReport type="SQL" group="Custom Reports">

   <title>sysdate.sql</title>

   <script name="sysdate.sql" protected="yes" execMode="SQLPLUS"

   parameters="unknown">

   </script>

   </cReport>
   ```

2. Log in to Oracle Applications Manager and navigate to the SQL Extensions page (Site Map > SQL Extensions).

3. Click the **Reload** button to reload the metadata. Your script will appear under the new group.

To change the protection on your report

You can change the password protection that is set on your report.

1. In the oamcustext.amx file set the value of "protected" to "yes", if you want password protection enabled on your script. Set it to "no" to remove password protection. For example, to set the protection to "no", the result would be:

   ```
   <cReport type="SQL" group="Custom Reports">

   <title>sysdate.sql</title>

   <script name="sysdate.sql" protected="no" execMode="SQLPLUS"
   parameters="unknown">

   </script>

   </cReport>
   ```

2. Log in to Oracle Applications Manager and navigate to the SQL Extensions page (Site Map > SQL Extensions).

3. Click the **Reload** button to reload the metadata. Your script will appear with the "unlocked" icon.

To change the report format

1. In the oamcustext.amx file set the value of "execMode" to "SQLPLUS" text format, or set it to JDBC for HTML format. For example, to set the report format to HTML, the result would be:

   ```
   <cReport type="SQL" group="Custom Reports">
   <title>sysdate.sql</title>
   <script name="sysdate.sql" protected="no" execMode="JDBC"
   parameters="unknown">
   </script>
   </cReport>
   ```

2. Log in to Oracle Applications Manager and navigate to the SQL Extensions page (Sitemap > SQL Extensions).

3. Click the **Reload** button to reload the metadata.

To provide drill-downs from the results of your script

For reports defined in HTML format, you can provide drill-downs from the results of your script to other Oracle Applications Manager pages. Currently drill-downs are supported for requests based on REQUEST_ID and database session information based on AUDSID.

Example:

Suppose your SQL script returns REQUEST_ID as the first column of the report, you can link it to the Request Details page as follows:

1. Ensure that execMode="JDBC"

2. Add the following to the entry for your SQL script:

   ```
   <keyColumns>
   <column position="1" key="REQUEST_ID"/>
   </keyColumns>
   ```

Here, position="1" indicates that the REQUEST_ID column is the first column reported by your select statement. Currently the possible values for the key attribute are REQUEST_ID and AUDSID.

The new full entry for your SQL script will look like the following:

```
<cReport type="SQL 'group="Custom Reports">
<title>sysdate.sql</title> <script name="sysdate1.sql" protected="no" execMode="JDBC"
parameters="unknown">
```

```
</script>
<keyColumns>
<column position="1" key="REQUEST_ID"/>
</keyColumns>
</cReport>
```

Troubleshooting

- If you try to execute a SQL script and encounter the following error message:

  An error has occurred!

  <filename>(No such file or directory)

  The SQL file does not exist under <APPL_TOP>/admin/custom/sql. Make sure you have copied the file into this directory.

- If your SQL script takes input parameters, ensure that you provide the parameters one per line in the **Input Parameters** text field. The result will contain errors if you do not provide the necessary parameters.

Details of Report

Navigation: Site Map > SQL Extensions >(select report name)

This page displays information based on the report definition. Information may include:

- Description
- Report Format - HTML or Text
- Applications Schema Password - If the report is password-restricted, enter the password here.
- Input Parameters - Enter any required or optional parameters.

You can run the report from this window by clicking the **Run Report** button.

Report Results

Navigation: Site Map > SQL Extensions (Run Report)

The contents and format of this page will vary depending on the report run.

Report results returned in HTML allow you to filter the report by a specific Column value.

Use the **Refresh** button to rerun a report from this page.

Click **Add to Support Cart** to add your report results to the Support Cart.

System Alerts, Metrics, and Logs

Overview of System Alerts, Metrics, and Logs

The System Alerts, Metrics, and Logs screens provide information that can help you diagnose potential problems. For example, configuration issues, overdue routine maintenance tasks, and invalid data can cause serious problems requiring either an automated response or manual intervention.

Oracle E-Business Suite applications can report these potential problems as system alerts to Oracle Applications Manager. These alerts can then be tracked in OAM, and administrators can classify alerts as open or closed, as well as keep notes on the steps taken to resolve underlying problems.

In addition, some problems may be more easily detected through external analysis of performance metrics. External analysis allows for easier comparison of current and historical metric values, consideration of metrics from multiple products and components, and end-user defined exception triggers. Such exceptions could include decreasing transaction throughput for a component or excessive completion times for a business process.

System Alerts

Navigation: Site Map > >Monitoring > System Alerts (under Current Activity)

Components in an Applications System such as concurrent programs, forms, service instances, or functions can post exception messages during specific error conditions as defined by the developer of the component. The term "System Alert" denotes a grouping of such exceptions having the same message. The term "Occurrence" is used to denote each member exception of such a group. Each alert is associated with a Severity (Critical, Error or Warning) and a Category (System or Product).

This page shows a summary of the system alerts as well as a list of new alerts.

Alerts are classified by Severity level:

- Critical - the alert indicates that an important business flow is impeded, or that a large number of users is affected.

- Error - the alert indicates a less severe, more isolated issue.

- Warning - the alert indicates that there may be a negative impact on users or business processes.

Alerts are also marked as New or Open. "New" indicates that the alert has just been posted in the system. "Open" indicates the alert is being resolved.

In the Summary region, Alerts are grouped according to their severity and status of New or Open. The New or Open column indicates how many alerts of the given severity exist. You can click on the number to drill down to details on the alerts.

When a new exception is posted, if an alert already exists with the same message and is in New or Open state, then the new exception is considered an occurrence of the existing alert. If an alert with the same message does not exist then a new one is created (with the state New) and this exception becomes the first occurrence of this alert. A notification is also sent to subscriptions for the newly created alert.

You can change the state of alerts (along with the associated occurrences) in OAM. You can change the state of a new alert to Open to indicate the exception has been acknowledged and the problem is being resolved. Once the problem is resolved you can change the state of the alert to Closed. You can also add notes to alerts; for example, to indicate how the problem was resolved.

You can search for alerts, search for occurrences, and view the notification setup for alerts using the buttons provided.

System Alert Flood Control

Oracle Applications Manager provides the System Alerts feature to inform system administrators of potential problems in Oracle E-Business Suite. For the Oracle Application Object Library messages logged at the level of Unexpected, OAM can raise system alerts. Ideally, system administrators should actively look at these alerts and close them once issue is resolved. However if for some reason, the alerts are not closed, too many new system alerts can flood the system with alerts, occurrences, business events, and notifications. Oracle E-Business Suite provides a mechanism to control the count of new system alerts to avoid a system alert flood.

By default, the system will raise only 500 new alerts. Once this limit is reached for new system alerts, no new alerts or notifications will be raised and a message will be displayed on System Alert and Metric page. To re-enable the alerting, a system administrator should change the status of existing new alerts from OAM. Oracle E-Business Suite also allows system administrators to change the default threshold by using the System Alert Setup button from System Alert and Metrics page can access this page. From the setup page you can also change the number of occurrences per alert. By default only 50 occurrences per alert is logged.

The setup page also provides control to enable the system alert for a particular severity. If critical severity is selected, only critical alerts will be logged. "None" selection will disable the system alert completely and no new alert will be raised.

System Alert Details

This page displays the details associated with a particular system alert. This page includes the summary information for the alert such as severity, category, state, creation date, and the exception message. The occurrences table summarizes the individual occurrences for this alert. You can select an occurrence and click **View Details** to drill down to the context details for an individual occurrence.

From this page, you can also change the state of the alert as well as navigate to the **Add**

Notes page to add notes to the alert.

Search Alerts

This page allows you to search for alerts by Severity, Category, State and Posted Date. The search results are displayed in the same tabular format as in the New Alerts section in the **System Alerts** page. You can also add notes or change the state of the alerts displayed in the results table.

To search for occurrences from this page, click **Search Occurrences**.

Search Occurrences

This page allows the user to search for occurrences of alerts by various criteria. The query criteria are categorized into the following groups:

- System Alert - The criteria in this section pertain to the alert to which the occurrence belongs.
- Component - The criteria in this section pertain to the component that logged the occurrence.
- User and Responsibility - The criteria in this section pertain to the user and responsibility that used the component that generated the alert.
- Database Session - The criteria in this section pertain to the database session associated with the transaction during which the exception was logged.
- Others - Additional criteria related to the occurrence.

From the results table on this page, users can drill down to view the context details for each occurrence. In addition, the users can also drill down to view the details for the alert to which each occurrence belongs.

To search for alerts from this page, click **Search Alerts**.

System Alert Occurrence Details

This page displays the entire context information associate with an individual alert occurrence. This page is divided into the following three sections:

- **Summary** - This section displays information associated with the alert to which the occurrence belongs.
- **Context** - This section displays all the context information and is further categorized into the following subsections:
  - **Component** - Name and application of the component that posted the alert occurrence.

  - **User and Responsibility** - Username, responsibility, and application for the user who ran the Component that posted the alert occurrence.

  - **Database Session** - Database session ID, database instance, session module, and session action associated with the database session for the transaction during which the alert was posted.

  - **Others** - Miscellaneous information such as session ID, node, security group, processes ID, thread ID (if applicable) and JVM ID (if applicable).

- The third section on this page varies based on the type of the transaction during which the alert occurrence was posted. The following types are possible:

  - **Concurrent Request** - Request ID, concurrent program name, a link to the request log, and a link to the output file are available if the transaction is a concurrent request. You can use the Request ID link to drill down to the request details. In addition, you can drill down to view related system logs to view other log messages that were posted during the same transaction.

  - **Concurrent Process** - If the transaction type was a concurrent process (belonging to a service instance), the service instance name, concurrent process ID, and a link to the manager log can be viewed from this section.

  - **Form** - If the transaction was from a Form, the form name is displayed in this section.

  - **ICX** - If the transaction was of type ICX, then the ICX transaction ID is displayed in this section.

  In addition, regardless of the transaction type, users can also drill down to view related system logs to view other log messages that were posted during the same transaction.

System Metrics

Navigation: Site Map > Monitoring > System Alerts (under Current Activity) > Metrics (tab)

Not all exception conditions can be immediately detected directly within an Oracle E-Business Suite component, but are best detected through external analysis. Some are detected by measuring certain criteria, such as decreasing transaction throughput for a component or excessive completion times for a business process. External analysis allows for easier comparison of current and historical metric values, consideration of metrics from multiple products and components, and end-user defined exception triggers. These exceptions are analogous to "events" in Oracle Enterprise Manager where the use specifies the specific conditions that will trigger an alert.

Simple Search Metrics

You can search for metrics based on **Application**, **Component**, **Posted After** date, or **Posted Before** date.

Advanced Search Metrics

Click on the **Advanced Search** button to search for metrics based on detailed criteria.

This page allows the users to search for metrics based on the context information associated with the metrics. The query criteria are categorized into the following groups:

- **Metrics** - The criteria in this section pertain to the metric itself such as metric code, metric value and date on which the metric was posted.
- **Component** - These criteria pertain to the component that logged the metric.
- **User and Responsibility** - These criteria pertain to the user and responsibility that used the component that generated the metric.
- **Database Session** - These criteria pertain to the database session associated with the transaction during which the metric was logged.
- **Others** - This group contains miscellaneous criteria such as node, security group, process ID, Thread ID, and JVM ID.

From the results table, users can drill down to view the context details for each metric.

System Metrics Results Table

The System Metrics results table shows information on:

- **Component** - the application component. A component is a functional unit, such as a concurrent program, form, or Web Application function.
- **Application** - the owning application of the metric.
- **Metric Code** - the internal name of the metric.
- **Value** - the value of the metric.
- **Metric Type** - the data type of the metric.
- **Time** - the time the metric was taken.

System Metric Details

This page shows the following:

Summary

- Metric Code
- Metric Type
- Metric Value
- Time Posted

Context

- Component:
    - Name
    - Application
- Database Session
    - AUDSID
    - DB Instance
    - Session Module
    - Session Action
- User and Responsibility
    - User
    - Responsibility
    - Application
- Others
    - Session ID
    - Node
    - Security Group
    - Process ID
    - Thread ID
    - JVM ID

Request Summary

- Request ID - Click on the request ID to view details for the request.
- Request Log - Click **View** to view the request log.
- Program Name - the program name.
- Output file - click **View** to view the output file.

System Logs

Navigation: Site Map > Monitoring > Logs (under Current Activity)

System Logs are messages that are logged by Oracle E-Business Suite system components.

Log messages contain a comprehensive set of context information and are useful for pinpointing and diagnosing system problems. They can have the following levels (listed from most serious to least serious):

- 6 - Unexpected: Used for the failure reporting of internal unhandled software failures. Example: Failed to place order due to NullpointerException
- 5 - Error: Used for the failure reporting of external end user errors. Example: Invalid username/password
- 4 - Exception: Used for the failure reporting of internal handled software failures. Example: User Session timed out
- 3 - Event: Used for high-level progress reporting. Example: Order placed successfully
- 2 - Procedure: Used for API-level progress reporting. Example: Entering or exiting an API
- 1 - Statement: Used for low-level progress reporting. Example: Processing records within an API

The system logs screens allow you to work with log messages that have been saved to the database. Please note that if logging has been configured to store messages in a middle tier file, such log messages will not be visible on the UI screens. Also, if a log message would normally raise a system alert but the message is sent to a file instead of the database, then the system alert will not be raised.

The following topics describe how to work effectively with the system logs screens:

- Performing a Simple Search

- Performing an Advanced Search
- Working With Search Results
- Viewing Log Message Details
- Setting Up Logging

Performing a Simple Search

In a simple search, you can search for log messages based on the following criteria:

- Posted After date

  The default value is today's date.

- Posted Before date

  The default value is tomorrow's date.

- Component Application
- Component
- Module
- Level

Enter values into the fields as desired and click **Go** to perform a search.

Performing an Advanced Search

To run an advanced search, click the **Advanced Search** button. You can use any combination of the following search criteria:

- Logged From
- Logged To

  The default time interval is from 12:00 AM today to 12:00 AM tomorrow.

- Application
- Responsibility
- User
- Log Level
- Module

- Message
- Host
- Java Virtual Machine
- Database Session ID
- Security Group
- Database Instance

On this page, the LOVs only display values that are reflected in existing log messages. For example, the User LOV only shows users who are specified in one or more log messages. It does not show the entire list of Oracle E-Business Suite users. Furthermore, the LOVs are also filtered by any other search criteria you have entered on the page.

Optionally, you can perform searches that depend on the Component Type. In the Component region, select a Type from the drop-down list. The page will refresh to offer additional search fields. For example, for Concurrent Programs, you can search by Concurrent Program Application or Concurrent Program Name.

Working with Search Results

Viewing Search Results

When you perform a search, the System Log Summary table shows how many log messages were returned and how many are at each log level.

Individual log messages are listed in the System Log Details table. For each log message, the sequence number, module, log level, user, and time are displayed. You can drill down on an individual message or on a user to view details.

Downloading Search Results

To download all returned log messages, click the Download All button. (This includes the full range of log messages, not only those displayed on the current page.) The downloadable file is a comma-delimited CSV file.

To download your choice of currently displayed log messages, select them in the table and click the Download button.

Additionally, you can save all search results by clicking the **Add to Support Cart** button.

Viewing Log Message Details

Summary

- Module: The unit of code specified in the FND_LOG API call. A module might be a PL/SQL stored procedure, a C file, or a Java class.
- Level

- Time Posted

- Message Text

Context

- Component: Name, Application

- User and Responsibility: User, Responsibility, Application

- Database Session: AUDSID, DB Instance

- Others: Session ID, Node, Security Group, Process ID, Thread ID, JVM ID

Request Summary

- Request ID

- Request Log

- Program Name

- Output File

Attachment

In the Attachment region, additional context information (such as environment variables or file versions) may be available in some cases.

Optionally, you can add this page to the Support Cart.

Setting Up Logging

Navigation: Site Map > Monitoring > Logs (under Current Activity) > Log Setup (button)

On the Log Setup screen, you can configure logging according to user, responsibility, application, or site. Additionally, you can view any Java System Property settings for the current JVM that may be active. Note that Java System Property settings override all other settings.

Setting Up Logging for Users, Responsibilities, or Applications

The following procedure explains how to set up logging for a particular user. The steps are the same for responsibilities or applications. Note that user settings override responsibility settings, responsibility settings override application settings, and application settings override site settings. In the table, null values indicate that the setting is to be inherited from the next higher profile level.

1. If the User table is not currently displayed, then click the icon to show it.

2. If there is a blank User Name field, then click the flashlight icon to select a user name. If there is not a blank User Name field, then click the **Add Another Row** button to add an empty row to the table, then select a user name.

3. In the Log Enabled field, select null, Yes, or No. A null value means that the setting will be inherited from a higher level profile value.

4. In the Log Level field, select a log level. Log messages greater than or equal to the specified level will be stored.

5. (Optional) In the Midtier Log File Name field, type in a valid middle-tier file path. If this field is blank, then log messages will be stored in the database. Note: Server PL/SQL messages are always logged to the database.

6. (Optional) In the Module field, enter the module for which you want to enable logging. For example, "fnd%".

7. Click Apply to save your work.

Setting Up Logging for a Site

The following procedure explains how to set up logging for your entire site.

1. In the Log Enabled field, select null, Yes, or No. (A null value means that the setting will be inherited from a higher level profile value.)

2. In the Log Level field, select a log level. Log messages greater than or equal to the specified level will be stored. It is strongly recommended that you choose 4 - Exception, 5 - Event, or 6 - Unexpected. Significant system performance issues may arise if logging is enabled at less than 4 - Exception.

3. (Optional) In the Midtier Log File Name field, type in a valid middle-tier file path. If this field is blank, then log messages will be stored in the database. Note: Server PL/SQL messages are always logged to the database.

4. (Optional) In the Module field, enter the module for which you want to enable logging. For example, "fnd%".

5. Click **Apply** to save your work.

5

Administering Oracle E-Business Suite Secure Enterprise Search

Overview of Oracle E-Business Suite Secure Enterprise Search

Oracle E-Business Suite Secure Enterprise Search is a centralized, secure search vehicle with consistent user interfaces throughout the Oracle E-Business Suite. By leveraging Oracle Secure Enterprise Search (SES), Oracle E-Business Suite Secure Enterprise Search enables a powerful keyword search on applications content in a faster, user-friendly way without compromising on the security and context sensitive information.

Before users can search on applications content, searchable objects must be set up first, constructed with secure context, and indexed into a full text search engine by Oracle SES in order to be ready for query. To accomplish this goal, Oracle E-Business Suite Secure Enterprise Search uses a flexible mechanism to help analyze these searchable objects, group related objects into categories, and build security rules around them for easier, secure search and fast result display.

In fact, searchable objects are business objects that are made available for text search. For example, a purchase order is a searchable object that can be defined as a set of searchable properties or business attributes along with its relationship to other searchable objects. This abstraction allows searchable objects to be bound to different context at run time and grouped into searchable categories.

Searchable objects are created with searchable attributes. These attributes allow the objects to be indexed, applied with security rules, and displayed with structured search results. Before users query, a search administrator grants appropriate data access privileges to users to secure application sensitive data from unauthorized access before deploying these objects to an Oracle SES instance.

At crawl time, the Oracle SES search engine starts a crawling job for a specific business object type. Based on a object type, searchable business objects or attributes get retrieved, indexed, and stored in the Oracle SES index store.

At query time, when a user performs a search through the centralized user interface, he or she is actually searching against a preindexed store which contains numerous objects or metadata that has been preprocessed with indexes at crawl time. The search engine queries the results enforced by security rules and constructs the hits returning as search results displayed to the user.

Key features of Oracle E-Business Suite Secure Enterprise Search include:

- A centralized global search capability provides user rich experience of searching text across the entire Oracle E-Business Suite.
- It allows you to search structured and unstructured data like attachment through business categories and further narrow down your search results by business entities or attributes.
- Security context defined at multiple levels controls the accessibility of application sensitive data to only authorized users.
- It leverages extensive search capabilities provided by Oracle SES to search application content in a secure and user-friendly way.
- It provides pluggable search region capability which allows a specific searchable object to be embedded in a page for context sensitive search.
- A search administrator can proactively control and manage crawling schedules and statuses using the administrative pages.
- It provides multiple language support allowing application users to perform internationalized searches.

To have a better understanding of Oracle E-Business Suite Secure Enterprise Search, the following topics are discussed in this section:

- Terms and Definitions, page 5-2
- Architecture Overview, page 5-4
- Design Time, page 5-6
- Crawl Time, page 5-7
- Query Time, page 5-13

Oracle E-Business Suite Secure Enterprise Search Related Terms and Definitions

To better understand and administer Oracle E-Business Suite Secure Enterprise Search, this section provides relevant terminologies and their definitions used in Oracle E-Business Suite Secure Enterprise Search.

Searchable Objects

Searchable objects are business objects that are made available for text search; they are used in an abstract way for exposing business data to search engines. For example, a purchase order as a searchable object would be defined as a set of searchable properties and its relationship to other searchable objects.

Search Category

Related searchable objects can be grouped into a search category and it is also called a searchable group.

Oracle E-Business Suite Secure Enterprise Search leverages Role-Based Access Control (RBAC) model to associate searchable groups with permission sets and grant the group access privileges to authorized users.

Search Context

The binding information could be specific to a search engine. In order to make the search service open, Oracle E-Business Suite Secure Enterprise Search needs to abstract out the search engine internals and makes search engine a service that can be replaced by one another at the deploy time.

Search context is an application within which search services will be provided for searchable objects.

Search Engine

Search engine is an application or service that encapsulates the need of text search on a resource. It uses a number for well-defined sub modules to perform the necessary tasks. For Oracle E-Business Suite Secure Enterprise Search, Oracle SES is the search engine that makes search service feasible.

Crawler

Crawlers are software agents used by a search engine to retrieve content for a given data source.

Indexer

An indexer is a software module that is used by a search engine to create an index from each crawled document.

Once indexes are created for a particular data source, they are available for search through a set of Web Service APIs (Searcher interface).

Searcher

A searcher is a software module that allows external users to query into pre crawled and indexed stores. It is responsible for matching keywords and predicates to documents, and then return them to the user.

Security Plug-in

To help protect unauthorized access to application information, security plug-in is used to enforce search security at the object level. Security plug-in is a Java class that implements the security methods to generate the access control list (ACL) for a document and to fetch Security Keys for a user.

An ACL is a list of permissions attached to an object specifying who or what is allowed to access the object and what operations are allowed to be performed. Oracle SES authorization plug-in works on the basis of the ACL-based security model and Security Keys for a document to authorize users or revoke the access to a search result.

User Authorization Cache (UAC)

This Oracle SES feature provides a framework allowing the Security Keys for a particular user, a specific data source, or a search object in Oracle E-Business Suite can be cached in Oracle SES.

By leveraging this framework from Oracle SES, when a user performs a search, the UAC is first looked up for the availability of the Security Keys for that user. If the keys are not found, then the Security Keys will be fetched synchronously during the query.

Query Rewrite

Query rewrite is a feature offered through a plug-in component that can rewrite the query to reflect current user context such as security before the query is sent to a search engine.

Data Security

Data security is a generic authorization model used by many applications within the Oracle E-Business Suite. It controls what users can see on application data through security grants.

Function Security

Function security is the basic access control in Oracle E-Business Suite. It restricts user access to individual menus and menu options within the system regardless of which application data in the row.

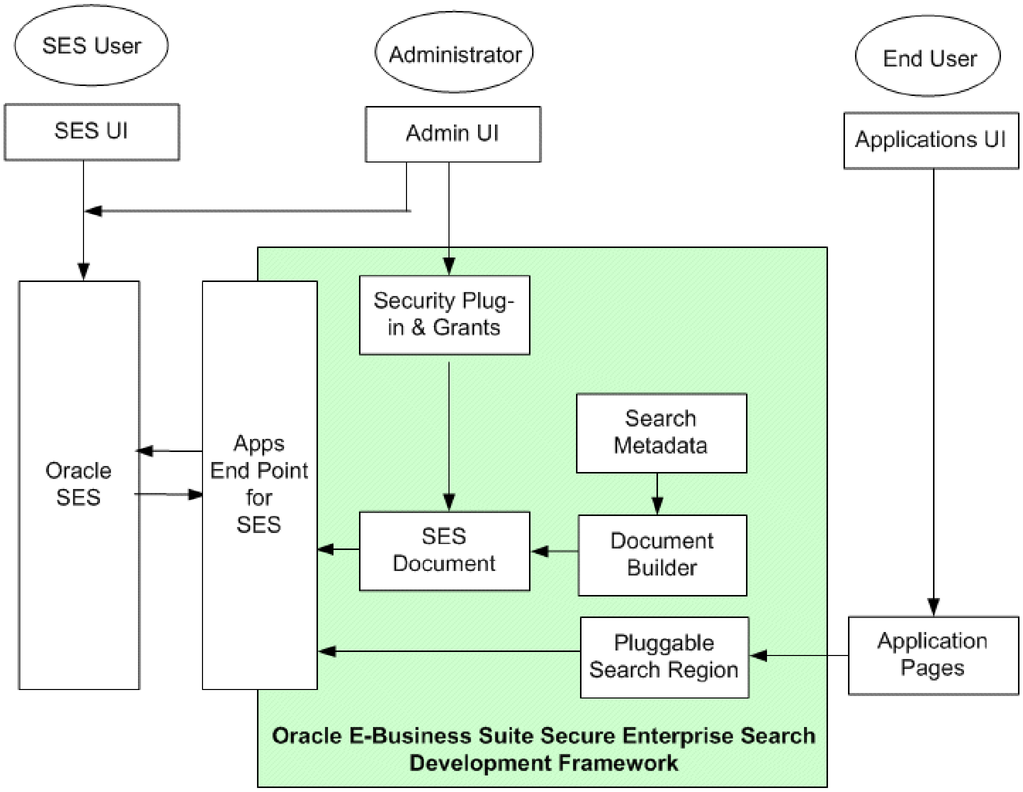
Oracle E-Business Suite Secure Enterprise Search uses the function security feature to guard the application content access through the menus and responsibilities assigned to each application user.

Architecture Overview

Oracle E-Business Suite Secure Enterprise Search development framework establishes searchable objects from search metadata. This search metadata is then used during crawl time to conduct searches and store data, and used during query time to qualify results.

The following architecture diagram illustrates how metadata is used in defining searchable objects, and the interaction between Oracle E-Business Suite Secure Enterprise Search and Oracle SES:

Architecture Diagram



Business objects with searchable attributes become searchable metadata. Oracle E-Business Suite Secure Enterprise Search utilizes SES Document Builder to construct this searchable metadata or object which may contain complex business structure into a flattened searchable document. This document is also known as SES Document.

A search administrator creates security grants through roles or responsibilities, and necessary security plug-ins to secure searchable objects.

The search administrator or system administrator configures the necessary Oracle SES proxy parameters and setup tasks both in Oracle E-Business Suite Secure Enterprise Search and Oracle SES. This enables Oracle SES to crawl Oracle E-Business Suite (EBS), and Oracle E-Business Suite to query Oracle SES.

When an application user performs a search through application interfaces, a query is executed by invoking a search against a preindexed search store in SES.

Design Time

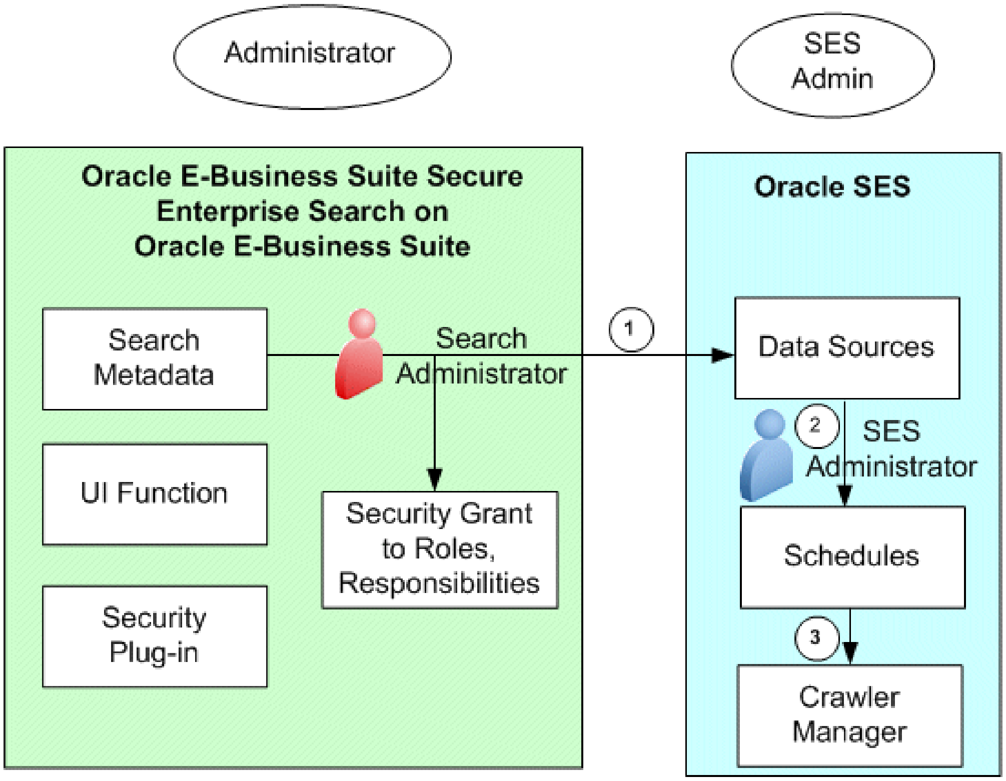
During the design phase, searchable objects with searchable attributes are created in Search Modeler and loaded to Oracle E-Business Suite as search metadata. These attributes allow searchable objects to be indexed, applied with security rules, and displayed with structured search results.

The search administrator grants appropriate data access privileges to users through roles or responsibilities to secure application sensitive data from unauthorized access before or after deploying objects to Oracle SES; the Oracle SES administrator then manages crawling schedules so that deployed data sources can be crawled for a specific object type and indexed.

> **Note:** Once searchable objects are deployed, crawling schedules are automatically created along with data sources in Oracle SES. For more information on how to manage crawling schedules, see Administering Crawls in Oracle SES, page 5-66.

The following diagram illustrates the interaction flow during the design time:

Design Time Process Diagram



1. The search administrator creates security grants to users through roles or responsibilities before or after deploying searchable objects to Oracle SES as data sources.

2. The Oracle SES administrator manages crawling schedules that contain data sources.

3. The crawler manager picks the data source for crawl based on the schedules.

For more information about how to create searchable objects in Search Modeler, see Creating Searchable Objects, *Oracle E-Business Suite Search Modeler User's Guide* available from My Oracle Support Knowledge Document 781366.1, Search Modeler 1.1 for Oracle E-Business Suite Readme.

Crawl Time

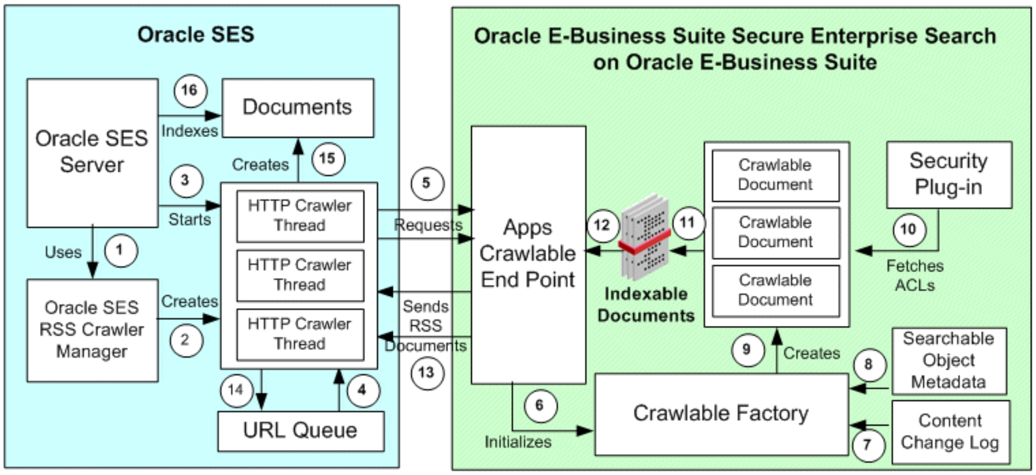
To produce satisfying search results in a timely fashion, crawling and indexing are essential tasks to a successful search. At crawl time, crawling is done by several distributed crawlers. Oracle SES crawler is a Java process activated by a set schedule. When activated, the crawler spawns a configurable number of processor threads that fetch information from various sources and index the documents. This index is used for searching sources.

Some crawlers are designed to crawl Oracle E-Business Suite users and provide user documents to Oracle SES. Oracle SES in turn invokes its authorization plug-in to generate document security access keys for each user crawled pertaining to the Oracle E-Business Suite source type and caches these keys for the authorized users and specific searchable objects or data sources. When a user performs a search, these previously cached security access keys will be used which provides a quick search result with security enforced.

Crawl Time for Indexable Documents

After searchable objects are deployed to Oracle SES as data sources contained in crawling schedules, Oracle SES starts crawling jobs in the Oracle E-Business Suite. A "crawlable" Oracle E-Business Suite means a secure end point that has been made crawlable to Oracle SES. This allows application data to be crawled and indexed into an Oracle SES store. The following diagram illustrates the interaction flow of Oracle SES crawler tasks:

Crawl Time Interaction Diagram for Indexable Documents



1. Oracle SES initializes RSS Crawler Manager.

2. Oracle SES Crawler Manager spawns and initializes a preconfigured number of crawler threads.

3. Oracle SES Starts the crawlers.

   Note: The crawler maps links and analyzes relationships. Whenever the crawler encounters embedded non-HTML, or non-textual documents during the crawling, it automatically detects the document type and filters and indexes the document.

4. Crawler threads pick up crawlable URLs from the URL Queue. URL Queue is populated using controlFeed mechanism as described in step 5.

5. Crawler threads contact Oracle E-Business Suite Crawling End Point, which is a servlet registered in `oafm` container.

   The requests come as post requests with URL parameters as in `http(s)://<ebs apache host>:<web host>/webservices/AppSearch/[ConfigFeed | ControlFeed | DataFeed]/Search Object Name>?user<ebs user having FND_SEARCH_CRAWLER resp>&password=<password>`.

   > **Note:** ConfigFeed and ControlFeed are crawling mechanisms to generate crawlable URLs in multiple batches of preconfigured sizes, so that crawling can proceed in parallel. These are used to generate the initial "URL Queue" in Oracle SES.
   >
   > DataFeed is the actual crawling request, which has been illustrated in the diagram.

6. Once the Oracle E-Business Suite Crawlable End Point receives the crawling requests, it initializes the Crawlable Factory whose purpose is to fetch the content from Oracle E-Business Suite database.

   Please note that Crawlable Factory is also responsible for splitting the original application content large data set into smaller work units through AD Parallel Update package, and then crawling the units in parallel by using the multi-thread crawling mechanism provided by Oracle SES.

   > **Note:** The Crawlable Factory is the place where an initial crawl taken place. The initial crawl refers to the first time a searchable object is crawled.

7. Content change log provides application changes that are indexed to the Crawlable Factory.

8. Search metadata is loaded to the Crawlable Factory.

9. Crawlable Factory creates crawlable documents, which conform to some schema provided by the indexing vendor.

10. While creating indexable documents, the Access Control List (ACL) is fetched for each document using the search plug-in associated with the searchable object definition. The `getAcl()` and `getSecureAttrAcl()` methods of the search

plug-in are invoked to generate the ACLs.

For more information about security plug-in, see Search Security Plug-ins, page 5-37.

11. Documents are ready to be consumed by a search/indexing engine.

12. Oracle E-Business Suite crawler threads pick the documents.

13. The indexable documents which are in the form of a RSS feed are passed to Oracle SES through the Oracle E-Business Suite End Point URL in response to the crawling request mentioned in step 5.

    These documents conform to Oracle SES crawlable schema and should have following information:

    - Metadata
    - Content to be indexed
    - Dependent document URLs (such as actionable links, attachments, or related documents or links)

14. On retrieving the document, Oracle SES indexing engine analyzes the RSS feed received from Oracle E-Business Suite and places the neighboring URLs into the URL Queue.

    Typically the neighboring URLs in Oracle E-Business Suite are the attachment fetch URLs.

15. Oracle SES indexing engine transforms the documents in Oracle SES readable format by extracting keywords.

16. Finally indexing process indexes the documents.

    Indexed documents are stored in the precrawled index store in Oracle SES.

Crawl Time for User Authorization Cache Source

To reduce the search response time of synchronously fetching Security Keys for an authorized user during user query, cached Security Keys for a particular user and a searchable object or data source are precrawled and stored in Oracle SES and then used directly at query time. This solution by using cached access keys to authorize a document access privilege for a user at query time is leveraged from Oracle SES User Authorization Cache (UAC) feature. For more information about this feature, see User Authorization Cache, page 5-57.

> **Note:** To protect sensitive application data from unauthorized access,

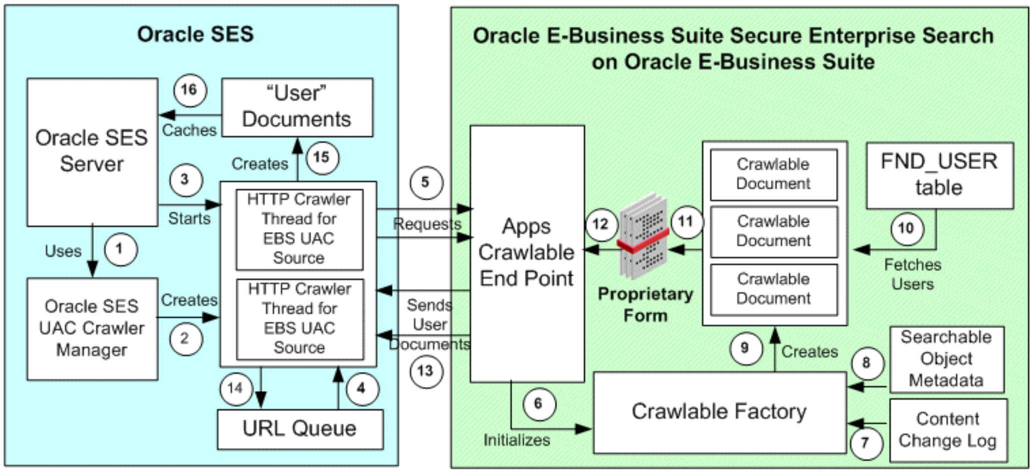
Access Control List (ACL) and Security Keys are generated through a security plug-in that is attached to a searchable object to enforce security at the object level.

An ACL is a list of permissions attached to an object specifying who or what is allowed to access the object and what operations are allowed to be performed. Security Keys are generated for a user to match the prebuilt ACLs to access specific documents based on user privileges.

For more information about security plug-in, see Search Security Plug-ins, page 5-37.

The following diagram illustrates the interaction flow of Oracle SES crawler tasks for Oracle E-Business Suite "User Authorization Cache" (UAC) source:

Crawl Time Interaction Diagram for User Authorization Cache Source



This interaction diagram for UAC source is similar to the crawling tasks for indexable documents. The major differences between these two are highlighted as follows:

- UAC Crawler Manager is initialized to preconfigure the crawler threads specifically for Oracle E-Business Suite UAC source type (step 2).

- While creating documents for User Crawl, crawlable instances use FND_USER, which is the source of Oracle E-Business Suite users. This holds true for Single Sign-On integrated Oracle E-Business Suite instances as well (step 10).

- Oracle E-Business Suite End Point URL responds to the crawling request mentioned in step 5 by sending the user documents, which are XML-based documents conforming to a mutually agreed upon schema.

  Oracle E-Business Suit calculates the total number of users satisfying user list criteria mentioned in Oracle SES. If the number is less than the profile value defined in the *FND: Search Crawl Batch Size* profile option, it directly gives user list to Oracle SES. Otherwise, it gives a 'User Control Feed' which in turn is used again by Oracle SES to create final user list feeds. (step 13).

- On retrieving the document, Oracle SES indexing engine analyzes the XML feed received from Oracle E-Business Suite and places the neighboring URLs into the URL Queue (step 14).

- Finally Oracle SES engine caches the Oracle E-Business Suite users. The precrawled UAC sources are stored in Oracle SES (step 16).

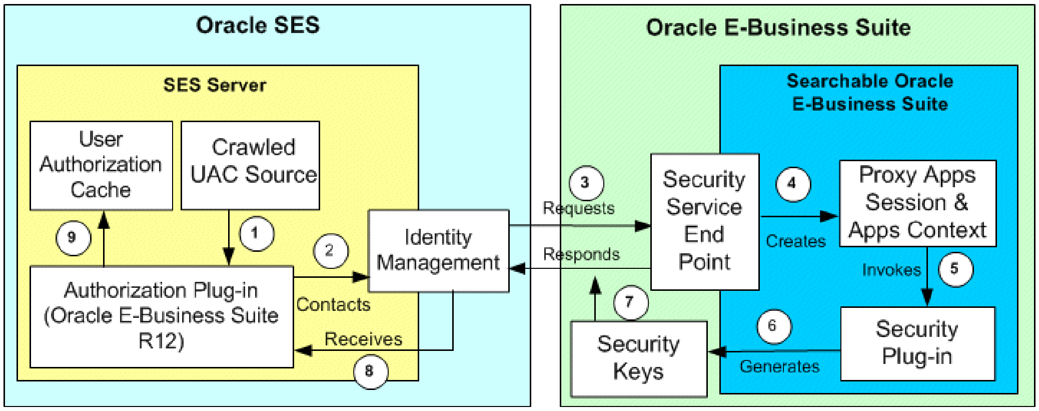
This crawling process generates a list of Oracle E-Business Suite users for whom the Security Keys need to be cached in Oracle SES for the predefined "User Authorization Cache" source type.

Fetching Security Keys Offline

In order to provide quick search results back to a user and eliminate possible time-outs of fetching Security Keys simultaneously during query due to complex application logic of deriving the keys, by leveraging the User Authorization Cache framework from Oracle SES, the user Security Keys can be generated as an offline process.

The following diagram illustrates the interaction flow for fetching Security Keys offline:

Interaction Diagram for Fetching Security Keys Offline



1. The crawled UAC source retrieves users and associated data sources from Oracle E-Business Suite.

   Based on each user and data source, the authorization plug-in is invoked

2. Authorization plug-in contacts Identity Management to initiate the Security Key fetch process.

3. Identity Management plug-in sends a request to the Oracle E-Business Suite Security Service End Point to fetch the Security Keys for an Oracle E-Business Suite

user and a data source (i.e. search object in Oracle E-Business Suite).

The request is in the form: `http://<ebs server>:<port>/AppSearch/SecurityService?user=<proxy user>&password=<proxy password>`.

An XML message containing the user for whom the Security Keys are requested and the search object name is posted.

4. Security establishes the proxy session and applications context. The credential is verified for the proxy user name and password, which Oracle SES posts with the request.

   The session is trusted or updated on behalf of the actual search user for whom the Security Keys have been requested.

5. The search plug-in is invoked by the Security Service End Point to generate the Security Keys. It is executed in the same proxy session.

6. The `getSecurityKeys( )` and `getSecureAttrKeys( )` methods are executed to generate the Security Keys for the proxy context.

   Since the context is always incomplete, security plug-ins have to be aware of such scenarios.

7. Security Service End Point responds to the request mentioned in step 3 by sending the Security Keys for the requested user.

8. The authorization plug-in receives the Security Keys.

9. Security Keys are cached for a given user and a specific search object or data source.

Query Time

When an application user performs a search from the centralized search user interfaces, the user actually queries from a preindexed store in Oracle SES.

It is important to note that searchable group security rule and search plug-in security are enforced for a user query. For the searchable group security, not every searchable group can be seen or displayed to a user. Only those who have the group access privileges can find the group names displayed from the list of values for search selection. For search plug-in security, it can be used at crawl time and query time to fetch ACLs and generate Security Keys to protect unauthorized access to application data.

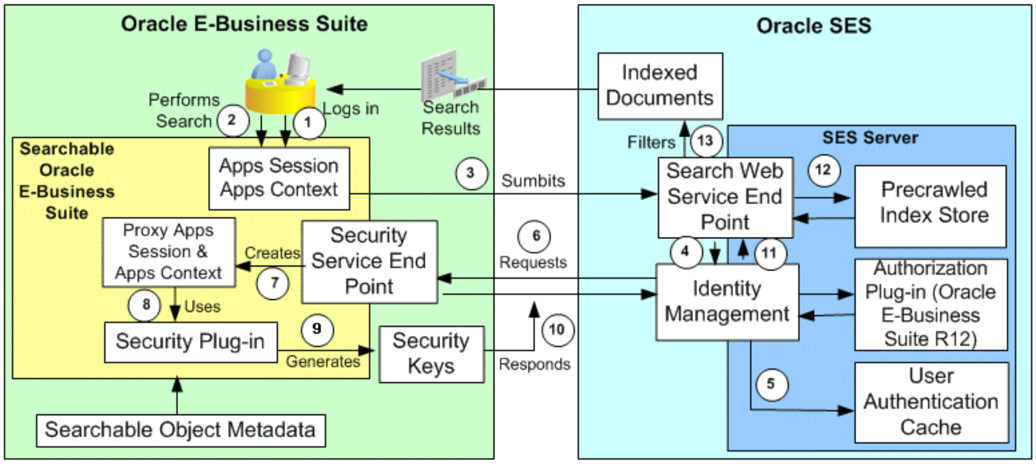
For information on how to secure searchable objects through searchable group security and security plug-in, see Securing Searchable Objects, page 5-32. For information on how to perform a search, see *Oracle E-Business Suite User's Guide*.

Query from Oracle E-Business Suite

You can perform a search from the Oracle E-Business Suite centralized search user interfaces.

The following diagram illustrates the query time interaction flow when performing a search through Oracle E-Business Suite:

Query Time Interaction Flow from Oracle E-Business Suite


Oracle E-Business Suite
Performs Search
2
Logs in
1
Search Results
Searchable Oracle E-Business Suite
Apps Session Apps Context
3
Sumbits
Proxy Apps Session & Apps Context
Creates
Security Service End Point
7
6
Requests
8
Uses
Security Plug-in
9
Generates
Security Keys
10
Responds
Searchable Object Metadata
Oracle SES
Indexed Documents
Filters
13
SES Server
Search Web Service End Point
12
Precrawled Index Store
4
11
Identity Management
Authorization Plug-in (Oracle E-Business Suite R12)
5
User Authentication Cache

1. A user logs on to Oracle E-Business Suite. A proxy session is created along with the initialization of applications context for the user.

   The applications context may be incomplete at this stage depending on whether the user has selected a responsibility or not.

2. The user accesses the Oracle E-Business Suite Secure Enterprise Search toolbar and submits a search query within the same session and context.

3. The query is submitted to the Oracle SES client APIs, which are hosted within Oracle E-Business Suite. The Oracle SES client APIs in turn make Web service calls to the Search Web Service End Point published by Oracle SES server.

   The Web service call includes the search keywords, filters if any, and user information amongst the most important parameters.

4. Once the search service is invoked, Oracle SES contacts the Identity Manager.

   Identity Management is set up as part of the configuration for the integration between Oracle E-Business Suite and Oracle SES. Oracle SES has specific identity manager for Oracle E-Business Suite Release 12. This Identity Manager configuration needs Oracle E-Business Suite Security Service End Point and a proxy application user name and password to establish a proxy session.

   For setup configuration for Oracle SES integration, see Setting Up Oracle E-Business

Suite Secure Enterprise Search for Oracle SES Integration, page 5-25.

5. If a User Crawler initiates at the crawl time, the Security Keys for a user, data source, or searchable object can be retrieved offline and cached in Oracle SES.

   Oracle SES first looks up the Security Keys for the object and logged-in user in User Authentication Cache (UAC).

   - If a match is found and the cache is usable, proceed to Step 12.

   - If there is no match found, proceed to the next Step 6.

   For more information on this feature, see User Authorization Cache, page 5-57.

6. Identity Manager requests Security Key information for the search user from the Security Service End Point. The Security Service End Point is registered as a servlet in `oafm` container.

7. Once the Security Service End Point receives a request for Security Keys, it initializes a proxy session. The proxy username/password credential is verified for the request. The session is then trusted or updated on behalf of the actual search user for whom the Security Keys have been requested.

   > **Note:** The proxy applications context may be incomplete since the responsibility information may or may not be there. Therefore, a special plug-in mechanism is provided to create the complete context information. For more information about the plug-in mechanism, see Understanding Security Logic and General Plug-in Mechanism, page 5-41.

8. The search plug-in is invoked in the same proxy session by the Security Service End Point to generate the Security Keys.

9. The `getSecurityKeys()` and `getSecureAttrKeys()` methods of the search plug-in are executed to generate the Security Keys for the proxy context.

   Since the context may be incomplete, security plug-ins have to be aware of such scenarios.

10. The Security Service End Point responds to the request mentioned in Step 5 by sending the Security Keys for the search user. The request-response happens over HTTP protocol.

    Oracle SES ensures that it does not wait indefinitely for the response to complete by setting a time-out on the request.

    > **Note:** The time-out value is configurable. This is done to ensure

responsiveness of the overall search solution.

11. The search service receives the authorization keys from Identity Management.

12. Search service retrieves indexed documents from the index store as per the search criteria given.

13. Indexed documents are filtered by Oracle SES after applying the Security Keys/Authorization Keys. This way, only the authorized documents are retrieved for the search user. The filtered indexed documents are returned to the query user for viewing and further action.

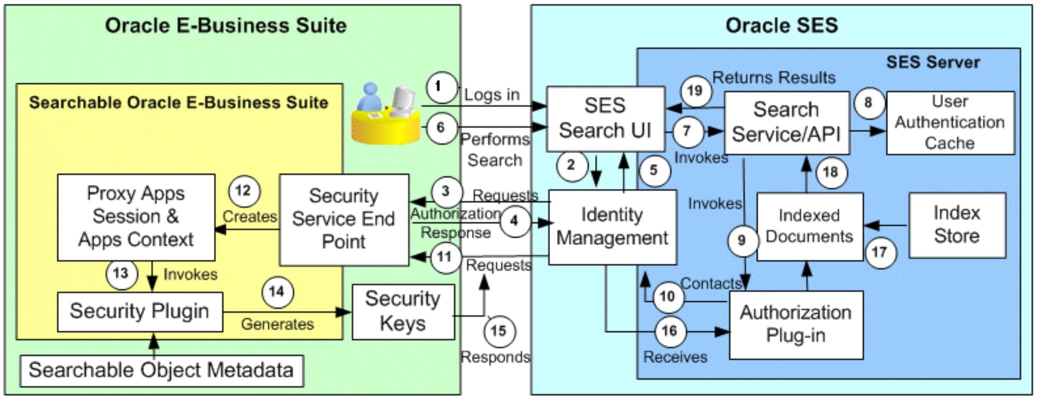
Query from Oracle SES

If an Oracle E-Business Suite user tries to log on and performs a search through the Oracle SES search user interface instead, the user's login credentials need to be authenticated first. At this stage, user login validation does not require any search plug-in.

Once the login is authenticated, the user can perform a search in the Oracle SES search UI with similar query time architecture as query in the Oracle E-Business Suite.

The following diagram illustrates the query time interaction flow when performing a search through Oracle SES:

Query Time Interaction Flow from Oracle SES



1. An Oracle E-Business Suite user attempts to sign in to Oracle SES Search UI using Oracle E-Business Suite username and password.

2. Oracle SES contacts Identity Manager to verify the user credentials.

3. Identity Manager sends an authentication request to the Security Service End Point of Oracle E-Business Suite. The request is sent over HTTP protocol.

It is typically of the form `http(s)://<ebs server>:<port>/webservices/AppSearch/SecurityService`. An XML message containing the exact authentication service requested is posted.

4. The Security Service End Point validates the login credentials and responds to the request by sending another XML message.

5. Identity Manager parses the response message and sends the success or failure response to the Oracle SES Search UI.

6. After successful login, the user submits a search query. It may consist of keywords, filters, and other search criteria.

7. Upon receiving the search request, Oracle SES invokes an appropriate search service or API.

8. If a User Crawler initiates at the crawl time, the Security Keys for a user, data source, or searchable object can be retrieved offline and cached in Oracle SES.

   Oracle SES first looks up the Security Keys for the object and logged-in user in User Authentication Cache (UAC).

   - If a match is found and the cache is usable, proceed to Step 17.

   - If there is no match found, proceed to the next Step 9.

   For more information on this feature, see User Authorization Cache, page 5-57.

9. The search service in turn invokes the authorization plug-in to get the Security Keys for the current search user.

10. Authorization plug-in contacts the Identity Manager to fetch the Security Keys.

11. Identity Manager requests Security Key information for the search user from the Security Service End Point. This is done over HTTP. The request message contains the proxy username and password, which is stored in Oracle SES as part of the configuration.

12. Security establishes the proxy session and applications context. The proxy username/password credential is verified for the request from Oracle SES. The session is then trusted or updated on behalf of the actual search user for whom the Security Keys have been requested.

    Note: Please note that the proxy applications context is always incomplete since the responsibility information may not be there while logging into Oracle SES. This is the major difference between searching from Oracle E-Business Suite and searching from Oracle

SES Search user interface.

13. The search plug-in is invoked in the same proxy session by the Security Service End Point to generate the Security Keys.

14. The `getSecurityKeys()` and `getSecureAttrKeys()` methods of the search plug-in are executed to generate the Security Keys for the proxy context.

    Since the context is always incomplete, security plug-ins have to be aware of such scenarios.

15. The Security Service End Point responds to the request mentioned in Step 5 by sending the Security Keys for the search user. The request-response happens over HTTP protocol.

    Oracle SES ensures that it does not wait indefinitely for the response to complete by setting a time-out on the request.

    > **Note:** The time-out value is configurable. This is done to ensure responsiveness of the overall search solution.

16. The authorization plug-in receives the Security Keys for the query user.

17. The Oracle SES search service or API retrieves indexed documents from index store, matching the search keywords and filters.

18. Indexed documents are filtered by the Security Keys retrieved for the query user.

19. Filtered search results are returned back to the query user.

Performing Administrative and Setup Tasks

Since all searchable objects are precrawled and indexed in the Oracle SES index store before a search invokes, a search administrator or system administrator must perform administrative setup tasks. These tasks include enabling searches in the E-Business Suite, creating a search administrator who is responsible for setting up, and configuring Oracle E-Business Suite Secure Enterprise Search for Oracle SES integration.

This section includes the following topics:

- Creating a Search Administrator, page 5-19
- Setting Up Oracle E-Business Suite Secure Enterprise Search, page 5-19
- Setting Up Oracle E-Business Suite Secure Enterprise Search for Oracle SES Integration, page 5-25

Creating a Search Administrator

To have Oracle E-Business Suite Secure Enterprise Search work properly, a search administrator must be set up first in order to configure and maintain administrative tasks before users can perform searches on applications data.

> **Note:** It is important to know that a search administrator is not only responsible for configuring and setting up essential tasks, but also responsible for managing crawling schedules and administering crawls in Oracle SES which are typically not performed by a system administrator. It is highly recommended that you create a new user (such as sesadmin/welcome) for that role, instead of using an existing system administrator user (sysadmin/sysadmin) assigned with necessary responsibilities. For more information, see *Oracle E-Business Suite Secure Enterprise Search Best Practices, Release 12*, My Oracle Support Knowledge Document 744820.1.

Use the following steps to create a search administrator:

1. Create a user (such as `sesadmin/welcome`) who will be the search administrator.
2. Assign the following responsibilities to the user `sesadmin/welcome`:
   - Application Search Administrator responsibility (FND_SEARCH_ADMIN)
   - FND Search Crawler responsibility (FND_SEARCH_CRAWLER)

Once a search administrator is created, the same user name and password information (such as sesadmin/welcome) will be entered in the Application Search Administration page as part of the setup parameters for Oracle SES Integration, as well as entered in the Oracle SES administrative pages to validate and authenticate users for secured searches on Oracle E-Business Suite or add secure federated searches.

For detailed configuration and setup steps, see Configuring Search Proxy Parameters for Oracle SES, page 5-28 and Performing Setup Steps in Oracle SES, page 5-30.

Setting Up Oracle E-Business Suite Secure Enterprise Search

Setup Overview

Oracle E-Business Suite Secure Enterprise Search is comprised of database, middle-tier, and UI components. It also relies on external dependencies to have the function work properly. Before setting up Oracle E-Business Suite Secure Enterprise Search and performing administrative tasks, a search administrator or system administrator must first understand the product dependencies and the integration between Oracle SES.

Product Dependencies

Oracle E-Business Suite Secure Enterprise Search has dependencies on the following products in order to have its features work properly:

- **Oracle Secure Enterprise Search (SES)**

  Oracle E-Business Suite Secure Enterprise Search relies on an external search engine to provide text search capability, and this search function is provided by Oracle SES.

- **AD Parallel**

  Oracle E-Business Suite Secure Enterprise Search utilizes the AD Parallel Update package to facilitate the crawlable factory in expediting the performance of an initial crawl which usually involves a large set of data.

- **OA Framework**

  Oracle E-Business Suite Secure Enterprise Search depends on OA Framework to enable the reusable search region displayed in the OA Home page.

  > **Note:** Since Oracle E-Business Suite Secure Enterprise Search can embed reusable search regions either in the OA Home Page or as a plug-in, the OA Home Page is dependent on Oracle E-Business Suite Secure Enterprise Search as well.

- **Function Security**

  Oracle E-Business Suite Secure Enterprise Search uses function security to guard the application content access through the menus and responsibilities assigned to an application user.

- **Data Security**

  Oracle E-Business Suite Secure Enterprise Search uses data security to control what users can see on the application data through security grants. Only authorized users can view searchable objects.

  > **Note:** The security access to searchable objects are also implemented through the Role-Based Access Control Security for Oracle E-Business Suite Secure Enterprise Search, page 5-33.

- **Web Service Technology Stack**

  Oracle E-Business Suite Secure Enterprise Search forms query and performs a search against Oracle SES through Web Service Technology Stack.

Setup Tasks

Since all searchable objects are precrawled and indexed in the Oracle SES index store before a search is invoked, a search administrator or system administrator needs to perform general setup tasks in Oracle E-Business Suite and search-related setup tasks both in Oracle E-Business Suite Secure Enterprise Search and Oracle SES administrative pages.

This section contains the following topics:

- Enabling Searches in Oracle E-Business Suite, page 5-21
  - Setting Language Preferences, page 5-21
  - Setting Profile Options, page 5-21
  - Assigning FND Search Crawler Responsibility to an FND User, page 5-24
  - Performing Personalization Setup Steps, page 5-24
- Setting Up Oracle E-Business Suite Secure Enterprise Search for Oracle SES Integration, page 5-25
  - Configuring Search Parameters for Oracle SES, page 5-28
  - Performing Setups in Oracle SES, page 5-30

Enabling Searches in Oracle E-Business Suite

The setup steps in Oracle E-Business Suite include the following tasks:

- Setting language preferences
- Setting profile options
- Assigning the FND Search Crawler responsibility to an FND user
- Performing personalization setup steps for displaying the Enterprise Search region

Setting Language Preferences

To have the search and result displayed in your preferred language, a search administrator must set a default language in the General Preferences page if it is not English.

For information on how to set language preferences, refer to Set Preferences section, Getting Started with Oracle E-Business Suite chapter, *Oracle E-Business Suite User's Guide* for details.

Setting Profile Options

Oracle E-Business Suite Secure Enterprise Search uses profile options to define necessary setup parameters so that searches can be enabled in the Oracle E-Business Suite. These profiles determine the following features:

- The availability of the Oracle E-Business Suite Secure Enterprise Search feature

- The valid URL for an external Oracle SES instance access
- The version of Oracle SES to be used for integrating with Oracle E-Business Suite Secure Enterprise Search
- The timeout value in seconds for an FND user logging into Oracle SES for query

  > **Note:** A valid FND user indicates that the user's application login information such as user name and password must be stored in the FND_USER table.

- The timeout value in seconds for an administrator logging into Oracle SES for administrative tasks
- The site-wide batch size used by AD Parallel for crawling

The following table lists the profile options used in Oracle E-Business Suite Secure Enterprise Search:

Profile Option	Description	Required	Default Value
FND: Search Enabling Flag	Use this site level profile option to control whether Oracle SES integration is enabled for the site. Oracle E-Business Suite Secure Enterprise Search must have it set to Yes indicating this feature is enabled.	Yes	N

Profile Option	Description	Required	Default Value
FND: Search Engine URL	Use this site level profile option to specify a valid URL with the format `http://<hostname>:<portnumber>` for an external Oracle SES instance to which query will be made against. This profile value must be provided if the site is Oracle SES enabled.	Yes	N/A
FND: Search SES Version	Use this site level profile option to specify a valid version of Oracle SES for integrating with Oracle E-Business Suite Secure Enterprise Search. The profile value should have minimum two characters, and the first two characters should be digits (such as 10.1.8.4, 11.1.2, 11G).	Yes	No default value for this option. However, if this profile is not set, Oracle SES version 10.1.8.4 will be considered.
FND: Search Session Timeout Value for Query	Use this site level profile option to control the timeout value in seconds for an FND user logging into Oracle SES. The session expires if this amount of time passes since the last activity by the user.	Yes	1200

Profile Option	Description	Required	Default Value
FND: Search Session Timeout Value for Admin Tasks	Use this site level profile option to control the timeout value in seconds for an administrator logging into Oracle SES. The session expires if this amount of time passes since the last activity by the administrator.	Yes	1200
FND: Search Crawl Batch Size	This profile allows application administrators to set the site-wide batch size used by AD Parallel.	Yes	1000

Assigning the FND Search Crawler Responsibility to an FND User

The FND Search Crawler responsibility must be assigned to an FND user and its user name and password must also be provided in the search administrative page before synchronizing applications metadata with Oracle SES. If the user information changes, you must update it and synchronize the data again.

Performing Personalization Setup Steps for Displaying the Enterprise Search Region

To ensure that the Enterprise Search region appears on top of the Oracle E-Business Suite Home page, you need to perform the following personalization steps:

1. Log in to Oracle E-Business Suite with the system administrator's user name and password.

2. Select the Functional Administrator responsibility from the Navigator menu.

3. Select the Personalization tab and the Application Catalog subtab to open the Application Catalog page.

4. In the Search region, enter `/oracle/apps/fnd/search/webui` in the Document Path field as the search criteria and click **Go**.

   All document names that match the search criteria should be displayed in the search result table.

5. Click the **Personalize Page** icon for the `/oracle/apps/fnd/search/webui/AppsSearchRG` document name listed in

the result table to open the Choose Personalization Context page.

6. Enter 'Applications Home Page' (OAHOMEPAGE) in the Set Function field and click **Apply** to open the Personalization Region page for your document.

7. In the Personalization Structure region, select the **Personalize** icon for the Row Layout field to open the Personalize Row Layout page.

8. Set the rendered property to 'true' at the 'Function: Applications Home Page' level.

9. Navigate back to the Home page after applying the personalization change.

10. Review if the Enterprise Search region is getting rendered on the Oracle E-Business Suite Home page.

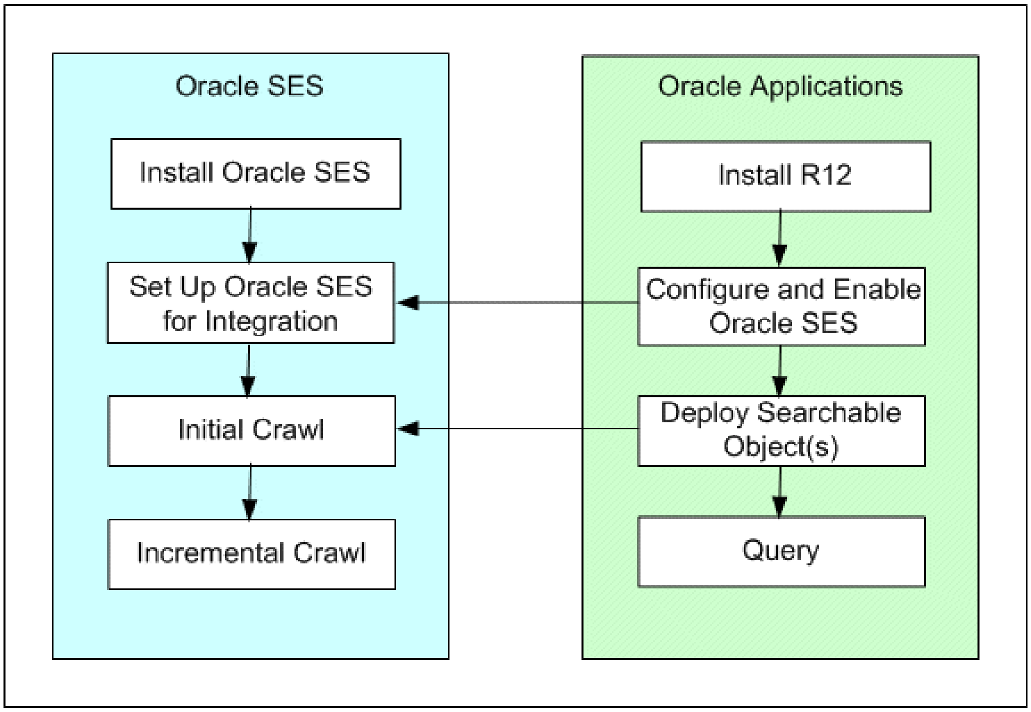
11. Perform a search by entering search criteria and click **Go** to verify if the search result is displayed in the search result page.

Setting Up Oracle E-Business Suite Secure Enterprise Search for Oracle SES Integration

To have seamless integration with Oracle SES, after enabling searches in Oracle E-Business Suite, the system administrator or search administrator must perform configuration tasks in Oracle E-Business Suite Secure Enterprise Search and Oracle SES.

The following diagram illustrates the high-level integration flow for Oracle E-Business Suite and Oracle SES integration:

Oracle SES and Oracle E-Business Suite Integration Workflow



After the installation of Oracle SES and Oracle E-Business Suite, search related metadata and business objects must be created and made it available in Oracle SES; metadata and relevant security rules are implemented and employed by Oracle E-Business Suite. To make the search available in Oracle E-Business Suite, necessary setup tasks must be performed in Oracle E-Business Suite, Oracle E-Business Suite Secure Enterprise Search, and Oracle SES.

For example, these tasks include setting language preferences and profile options for the applications to enable Oracle E-Business Suite Secure Enterprise Search, configuring search proxy parameters to facilitate remote access to Oracle SES, and performing administrative setup steps in Oracle SES for integration.

With appropriate setup and configuration between Oracle SES and Oracle E-Business Suite Secure Enterprise Search, searchable objects can be successfully deployed to Oracle SES instance, and initial and incremental crawls can be launched in Oracle SES. Users can perform queries from Oracle E-Business Suite against a precrawled index store in Oracle SES.

> **Important:** For troubleshooting frequently encountered issues during installation and setups, see *Oracle E-Business Suite Secure Enterprise Search Troubleshooting Guidelines, Release 12*, My Oracle Support Knowledge Document 726239.1 for details.

This section covers the following setup tasks in Oracle E-Business Suite Secure Enterprise Search and Oracle SES:

1. Installing Oracle E-Business Suite Secure Enterprise Search, page 5-27

   This section provides installation information so that Oracle E-Business Suite Secure Enterprise Search can integrate with Oracle SES.

2. Configuring Search Proxy Parameters for Oracle SES, page 5-28

   This step includes setting administrative proxy and query proxy parameters, such as user name, password, and timeout value in seconds for an administrator and a valid FND user to access a remote Oracle SES instance.

3. Performing Setup Steps in Oracle SES, page 5-30

   To ensure the seamless integration between Oracle E-Business Suite Secure Enterprise Search and Oracle SES, the system administrator or search administrator must perform additional setup steps in Oracle SES. These steps include setting up connections between Oracle SES and an identify management system, and adding federation entities to Oracle SES.

Installing Oracle E-Business Suite Secure Enterprise Search

Oracle E-Business Suite Secure Enterprise Search is released with Oracle E-Business Suite and Oracle Secure Enterprise Search (SES). To have it installed properly, perform the following installation steps:

1. Install or upgrade your instance to Oracle E-Business Suite Release 12.1.3.

2. Install Oracle SES 11.1.2 from Oracle Technology Network (OTN) page (http://www.oracle.com/technology/), or upgrade to Oracle SES 11.1.2 from Oracle SES 10.1.8.4.

   Refer to *Oracle Secure Enterprise Search Installation and Upgrade Guide* 11*g* Release 1 (11.1.2.0.0) for installation details and upgrade information from Oracle SES 10.1.8.4 to Oracle SES 11.1.2.

   Oracle SES can be integrated with Oracle E-Business Suite Release 12.1.3. The minimum supported version of Oracle SES in this 12.1.3 release is SES 11.1.2. To have a successful integration with SES 11.1.2, a few mandatory Oracle SES one-off patches need to be applied. Refer to *Installing Oracle E-Business Suite Secure Enterprise Search, Release 12*, My Oracle Support Knowledge Document 462377.1 for details.

   > **Note:** Oracle SES 11.1.2 uses two separate JVMs for running the crawler and search applications. The crawler is run using Sun JRE whereas the search application is run using JRockit JRE. Both JREs are available under `$ORACLE_HOME` of Oracle SES installation. If

> Oracle E-Business Suite is on SSL enabled environment, when integrating with Oracle SES 11.1.2 instance, the Oracle E-Business Suite SSL certificate has to be imported into both the Oracle SES keystores (JRE truststores) using keytool.

Remember the port and 'eqsys' password during the installation. This information will be used later in configuring Oracle E-Business Suite Secure Enterprise Search to enable Oracle SES integration.

> **Note:** Since Oracle SES defaults to TNS database port 1521 during the installation and it does not appear to be changeable, when trying to install Oracle SES, you must have port 1521 free in order to have Oracle SES successfully installed in your system.

Once you complete the installation for both Oracle E-Business Suite and Oracle SES, you must also perform administrative setup tasks both in Oracle SES and Oracle E-Business Suite Secure Enterprise Search to configure the system.

See:

- Configuring Search Proxy Parameters for Oracle SES, page 5-28
- Performing Setup Steps in Oracle SES, page 5-30

For more installation information, see *Installing Oracle E-Business Suite Secure Enterprise Search, Release 12*, My Oracle Support Knowledge Document 462377.1 for details.

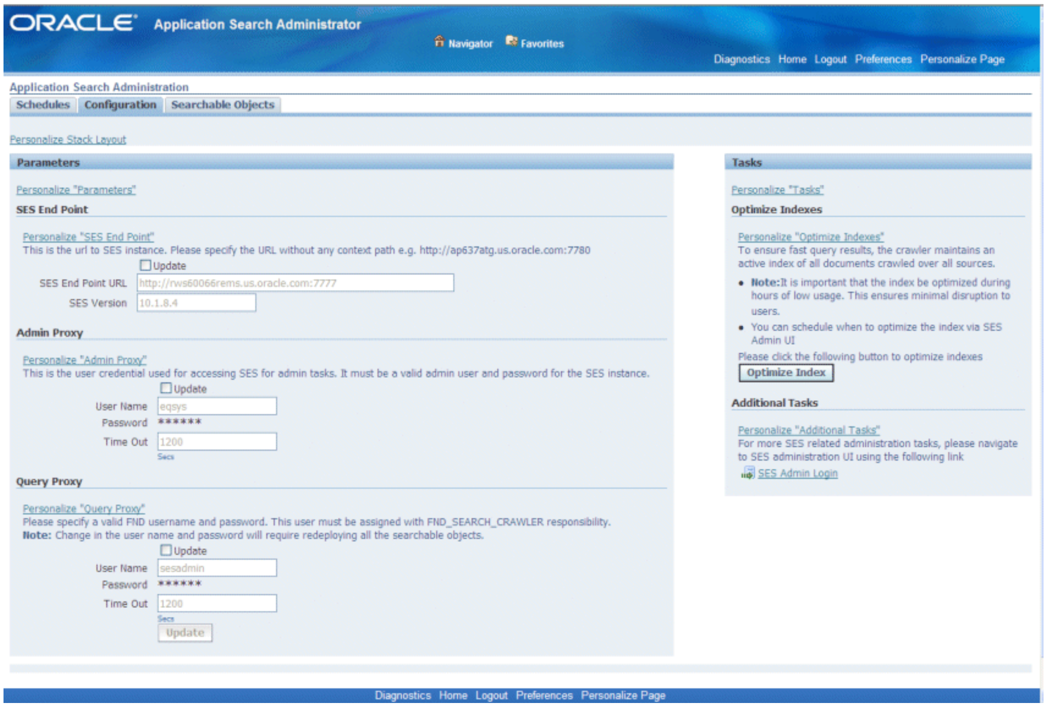
To ensure that the Enterprise Search region appears on top of the Oracle E-Business Suite Home page, perform the personalization steps mentioned earlier. See: Performing Personalization Setup Steps, page 5-24.

Configuring Search Proxy Parameters in the Configuration Tab

Use the Configuration tab to set proxy parameters to enable Oracle SES instance access. This includes setting proxy parameters for an administrator and a valid FND user who has the FND Search Crawler responsibility.

> **Important:** Changes in the proxy parameters including user name and password will require redeploying all searchable objects. If these objects have been crawled, then redeployment will not make data updates in Oracle SES. To resynchronize Oracle SES data, you must manually delete the data source of the same name in Oracle SES first, and then redeploy the objects.

Configuring Parameters to Access Oracle SES


ORACLE
Application Search Administrator
Navigator
Favorites
Diagnostics Home Logout Preferences Personalize Page
Application Search Administration
Schedules
Configuration
Searchable Objects
Personalize Stack Layout

Parameters

Personalize "Parameters"

SES End Point

Personalize "SES End Point"

This is the url to SES instance. Please specify the URL without any context path e.g. http://ap637atg.us.oracle.com:7780

□ Update

SES End Point URL	http://rws60066rems.us.oracle.com:7777
SES Version	10.1.8.4

Admin Proxy

Personalize "Admin Proxy"

This is the user credential used for accessing SES for admin tasks. It must be a valid admin user and password for the SES instance.

□ Update

User Name	eqsys
Password	******
Time Out	1200 Secs

Query Proxy

Personalize "Query Proxy"

Please specify a valid FND username and password. This user must be assigned with FND_SEARCH_CRAWLER responsibility.

Note: Change in the user name and password will require redeploying all the searchable objects.

□ Update

User Name	sesadmin
Password	******
Time Out	1200 Secs

Tasks

Personalize "Tasks"

Optimize Indexes

Personalize "Optimize Indexes"

To ensure fast query results, the crawler maintains an active index of all documents crawled over all sources.

- **Note:**It is important that the index be optimized during hours of low usage. This ensures minimal disruption to users.
- You can schedule when to optimize the index via SES Admin UI

Please click the following button to optimize indexes

Additional Tasks

Personalize "Additional Tasks"

For more SES related administration tasks, please navigate to SES administration UI using the following link

SES Admin Login

Use the following steps to configure search proxy parameters for an administrator and a valid FND user:

1. Log on to Oracle E-Business Suite with the Application Search Administrator responsibility and select the Application Search Administration link from the Navigator window.

2. From the Application Search Administration window, select the Configuration tab.

3. Specify the following information in the SES End Point region:

   - SES End Point URL: Enter an URL address with the format `http://<hostname>:<portnumber>`, such as `http://my.host.com:portnumber` in this field. This is an external Oracle SES instance to which query will be made against.

     If you have the FND: Search Engine URL profile value defined, then you should see the URL value populated automatically.

     To update this field, select the **Update** check box in the SES End Point region to enter new URL address. Click **Update** at the bottom of the page to save your change.

   - SES Version: Enter an appropriate Oracle SES version that your system will be integrated with. It should have minimum two characters, and the first two characters should be digits, such as 10.1.8.4, 11.1.2, or 11g.

Values entered here will be stored in the 'FND: Search SES Version' profile option.

4. Specify the administrative proxy parameters including User Name, Password, and Time Out values in the Admin Proxy region.

   The Time Out value field can be populated automatically if you set the 'FND: Search Session Timeout Value for Admin Tasks' profile value.

   > **Note:** To integrate Oracle E-Business Suite Secure Enterprise Search with Oracle SES, you need to set the Admin Proxy section as follows:
   >
   > - User Name: `eqsys`
   > - Password: Use the same password (such as `Oracle10g`) for `eqsys` user name when you installed the Oracle SES.
   > - Time Out: 1200 secs

   To update these fields, select the **Update** check box in the Admin Proxy region to make the changes. Click **Update** at the bottom of the page to save your change.

5. Specify the query proxy parameters including User Name, Password, and Time Out values for a valid FND user with the FND Search Crawler responsibility. This query user name and password is usually set to the system administrator `sysadmin/welcome` or search administrator `sesadmin/welcome` who has appropriate search responsibilities.

   Like the Admin Proxy region, the Time Out value field can be populated automatically if you set the 'FND: Search Session Timeout Value for Query' profile value.

   To update these fields, select the **Update** check box in the Query Proxy region to make the changes. Click **Update** at the bottom of the page to save your work.

   > **Important:** Once you change the query proxy parameters, the Oracle SES instance needs to be restarted to reflect the changes.

Performing Setup Steps in Oracle SES

Oracle E-Business Suite Secure Enterprise Search integrates with Oracle Secure Enterprise Search (SES) to provide powerful text search features. It allows Oracle SES to crawl application content and return results for query.

To ensure its seamless integration with Oracle SES, the search administrator needs to perform the following administrative tasks in Oracle SES after completing necessary setup steps in Oracle E-Business Suite Secure Enterprise Search:

1. Log on to the Oracle SES administrative user interface using `http://<hostname>:<portnumber>/search/admin`. You can also access it from the **SES Admin Login** link in the Configuration tab of the Oracle E-Business Suite Secure Enterprise Search administrative page.

2. Select the Global Settings tab from the Secure Enterprise Search page to configure the following settings:

   - Select **Identity Management Setup** from the System section to set up connections between Oracle SES and an identity management system to validate and authenticate users for secured searches.

     Select `oracle.search.plugin.security.identity.ebs.EBSIdentityPluginMgr` from the Available Identity Plug-in region and click **Activate**.

     In the Activate Identity Plug-in page, enter the following parameter values to define the selected Identity Plug-in settings for all authentication and validation activity in Oracle SES:

     - HTTP endpoint for authentication: Enter an end point URL for Oracle E-Business Release 12 authentication, such as `http://my.host.com:port/webservices/AppSearch/SecurityService`.

     - User ID: Enter the search administrator's user name that you created earlier. See: Creating a Search Administrator, page 5-19.

     - Password: Enter the search administrator's login password.

     Click **Finish** to return to the Global Settings page.

   - Select **Federation Trusted Entities** from the Search section to add federation entities. Oracle SES uses these entities to provide secure federated searches.

     In the Federation Trusted Entities page, enter the following information:

     - Entity Name: Enter the search administrator's user name that you created earlier. See: Creating a Search Administrator, page 5-19.

     - Entity Password: Enter the search administrator's login password.

     - Select the **Use Entity Plug-in for authentication** check box to authenticate through the active identity plug-in.

     Click **Add** to return to the Global Settings page.

   - Select the **Crawler Configuration** link from the Sources section to ensure the crawler logging setting is appropriate.

In the Crawler Logging region, ensure the crawler log file directory path including log file name defined in the Crawler Log File Directory field is less than the supported length of 100 characters for Oracle SES 11.1.2 integration.

Click **Apply**.

3. Restart both Oracle SES and Oracle E-Business Suite instances.

   Important: You must make sure that the `search.properties` file in Oracle SES server is also properly configured. Use the following steps to set the time in milliseconds to wait for security filter refresh task to finish during query processing:

   1. Locate the `search.properties` file in `$ORACLE_HOME/search/webapp/config` directory.

   2. Set the security filter refresh task wait time value: `sec_filter_refresh_wait_time=20000`

For more information on Oracle SES integration setup steps, see the *Oracle Secure Enterprise Search Administrator's Guide* for details.

Securing Searchable Objects

Security is the most critical feature that is designed to guard application content from unauthorized access. To ensure that the right person has access to appropriate data at the right time, searchable objects or metadata must be enforced by security rules before they can be made available for search within the Oracle E-Business Suite.

Oracle E-Business Suite Secure Enterprise Search provides a flexible mechanism to enforce and secure searchable objects without compromising on the data integrity and content sensitivity. To effectively manage search security both at the group and object levels, and reduce the search response time, the following security mechanisms are used in enabling Oracle E-Business Suite Secure Enterprise Search:

- **Role-Based Access Control (RBAC) Security**, page 5-33

  With RBAC security model, search security can be enforced at the group level through security grants. This section discusses the Role-Based Access Control (RBAC) security model and steps in creating security grants to ensure the application content sensitive data is only accessed by authorized people.

- **Search Security Plug-ins**, page 5-37

  Security plug-ins provide another layer of security control at the object level. A security plug-in can be added to a searchable object at the design time; it can also be used at crawl time to fetch ACLs and generate Security Keys offline or at query time if needed to protect unauthorized access to application data. Sample security plug-ins are also described in this section.

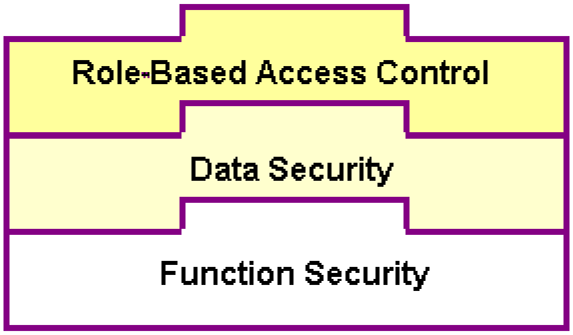
- **User Authorization Cache**, page 5-57

  User Authorization Cache (UAC) feature allows previously cached Security Keys for a specific user and a searchable object or data source to be used at query time. This greatly reduces the search response time and provides a quick result with security enforced. When a user performs a search, the cached information is first examined to look up the query user or an object. If the match is found, the associated keys will be compared with the pre-built ACLs to authorize or revoke the document access privileges. In case there is no match found, then the Security Keys are fetched synchronously.

Role-Based Access Control (RBAC) Security

Oracle E-Business Suite Secure Enterprise Search uses Role-Based Access Control (RBAC) security to secure searchable objects through roles, and user access to applications data is determined by the roles granted to the user. This approach builds upon Data Security and Function Security, but it goes beyond both of them.

Role-Based Access Control Security



Function security is the base layer of access control in Oracle E-Business Suite. It restricts user access to individual menus and menu options within the system, but it does not restrict access to the data contained within those menus. Data security provides access control on the application data, and the actions a user can perform on the data. With data security, users can be restricted by security rules to access or view only certain types of data on the screen once they have selected a menu while an administrator can have more data access to the same page.

With RBAC, access control is defined through roles, and a role can be configured to consolidate the responsibilities, permissions, function and data security policies that users require to perform a specific task. This solution simplifies mass updates of user permissions because changes can be done through roles which inherit the new sets of permissions automatically. Based on the job functions, each role can be assigned a specific permission or permission set if needed. For example, a sales organization may include 'Sales Representative', 'Sales Manager', and 'Sales Support' roles. The 'Sales Manager' role would include a permission set allowing the manager role to perform a job function for both the representative and support roles.

By leveraging the concept of permission sets, Oracle E-Business Suite Secure Enterprise Search allows related searchable objects to be grouped and sequenced to construct searchable groups; these searchable groups are associated with a function role and then they are assigned to users through security grants. When a user logs on to the E-Business Suite and performs a search, Oracle E-Business Suite Secure Enterprise Search filters the secured searchable objects based on the grant and displays the list to the user who has authorized privileges.

For example, Oracle E-Business Suite Secure Enterprise Search uses search function security to provide a permission on searchable objects and then grant to different roles. When a searchable object 'purchase order' is defined, in order for a user to search on this purchase order object, she or he must have been assigned to a role that holds a grant of purchase order access permission. Once the user logs on the applications, she or he should be able to see the purchase order displayed from the searchable object list for search selection.

For more information on Data Security, Function Security, and RBAC security models, see *Oracle E-Business Suite System Administrator's Guide - Security* for details.

Creating Security Grants

To secure application data access to a user with right privileges, the system administrator or search administrator needs to administer the security grant which includes:

1. Create Objects, page 5-34

2. Create Permissions, page 5-35

3. Create Permission Sets, page 5-36

4. Grant Permission Sets, page 5-36

Prerequisites: Please note that the system or search administrator needs to have Functional Developer role to create objects, permissions, and permission sets, as well as the Functional Administrator role to create grants.

To create security grants:

Creating Objects

1. Log on to Oracle E-Business Suite with the Functional Developer responsibility.

2. From the Security tab, click the Objects subtab, and select **Create Object**.

3. Enter the following fields to create an object:

   - Name: Enter a display name.

   - Code: Enter a name, such as `WF_SEARCHABLE_NTF`.

   - Application Name: Select an application name.

   - Database Object: This must be `FND_OBJECTS`.

   - Description: Enter a proper description for the object you want to create.

   - Column: Select the first column name as `CRAWL_CRAWLABLE`. The Type field populated automatically with `VARCHAR2`.

4. Click **Apply**.

5. Select the Object Instance Set tab and click **Create Instance Set**.

6. Enter the following information to create an instance set:

   - Name: Enter a display name for the instance set.

   - Code: Enter a code.

   - Description: Enter a proper description for the instance set.

   - Predicate: Enter a predicate.

Creating Permissions

1. Log in with the Functional Developer responsibility. From the Security tab, select the Permissions subtab and click **Create Permission**.

2. Enter the following fields to create a permission:

   - Name: Enter a name for the permission, such as WF: Searchable Notifications.

     > **Note:** The permission name entered here will be displayed as a searchable object name in the Narrow By region which allows you to refine your search from the Search Results page. For more information on how to use Oracle E-Business Suite Secure Enterprise Search, see *Oracle E-Business Suite User's Guide*.

   - Code: Enter a standard code, such as `WF_SEARCHABLE_NTF`.

- Description: Enter a proper description for the permission.

- Object Name: Select the object you created in the previous steps.

- Add to Permission Set: Select a permission set for this field if you have a permission set created.

3. Click **Apply**.

Creating Permission Sets

1. Log in with the Functional Developer responsibility. From the Security tab, select the Permission Sets subtab and click **Create Permission Set**.

2. Enter the following fields to create a permission set:

   - Name: Enter a name for the permission set, such as ATG Searchables.

     > **Note:** If you are authorized to have the security access to the permission set name you entered here, when you perform a search on the Oracle E-Business Suite Home Page or a product home page, you should find this permission set name displayed from the business category drop-down list for your selection. For more information on how to use Oracle E-Business Suite Secure Enterprise Search, see *Oracle E-Business Suite User's Guide*.

   - Code: Enter a standard code, such as `SESG_WF_NTF`.

     > **Important:** Your permission set must be prefixed with `SESG`.

   - Description: Enter a proper description for the permission set.

3. Click **Add Another Row** and enter the following information:

   - Permission: Select a permission you created earlier, such as WF: Searchable Notifications.

   - Add more permissions as appropriate.

4. Click **Apply**.

Granting Permission Sets

This process requires the 'Functional Administrator' role to create grants.

1. Log in with the Functional Administrator responsibility. From the Security tab,

select the Grants subtab and click **Create Grant**.

2. Enter the following fields in the Create Grant: Define Grant page:
   - Name: Enter a name for the grant, such as ATG Searchables Grant.
   - Description: Enter a proper description for the grant.
   - Enter proper information in the Effective From and Effective To fields.
3. Enter the following information in the Security Context region:
   - Grantee Type: Select a proper grantee type, such as Group of Users.
   - Grantee: Enter System Administrator.
4. Click **Next**.
5. In the Set region, select a permission set to grant, such as ATG Searchables and click **Next**.
6. Review the grant details and click **Apply**.

Search Security Plug-ins

In addition to securing your search at the group level through security grants, Oracle E-Business Suite Secure Enterprise Search uses security plug-in to strengthen security further down to the object level. Since searchable objects are the key elements in the crawling mechanism, this type of security mechanism can be easily implemented and enforced at crawl time and even can be dynamically executed during user query. Its flexible, object-based security plug-in feature can effectively guard and protect application sensitive data such as HRMS employee data, General Ledger data in a legal entity from unauthorized access or transactions across organizations if in a multiple-organization environment.

Security plug-in is a Java class that implements security methods to support custom or user-defined security rules at the object level and in turn to secure your search.

At design time, a security plug-in can be added to a searchable object during the object creation through the metadata-based Search Modeler user interface.

At crawl time, while creating indexable documents, two search methods (`getAcl()` and `getSecureAttrAcl()`) of the plug-in associated with the object definition are invoked to generate the access control list (ACL) for each document.

> **Note:** An ACL is a list of permissions attached to an object specifying who or what is allowed to access the object and what operations are allowed to be performed.

> Oracle SES authorization plug-in works on the basis of the ACL-based security model and Security Keys for a document to authorize users or revoke the access to a search result. Through the authorization plug-in implementation of Oracle E-Business Suite connector in Oracle SES, all searches within Oracle E-Business Suite can be authorized and leveraged from the SES search engine.

At query time, when a user performs a search, different sets of search methods (`getSecurityKeys()` and `getSecureAttrKeys()`) of the plug-in are executed to generate the **Security Keys** for the user in order to match the pre-built ACLs. Any matched indexed documents will then be retrieved for the user. Unmatched or unauthorized documents get dynamically filtered out in the process.

Security Keys and User Authorization Cache (UAC)

To reduce the search response time of fetching Security Keys simultaneously during user query, User Authorization Cache (UAC) framework in Oracle SES is leveraged to allow Security Keys to be generated as an offline process if a User Crawler initiates at the crawl time.

This user crawling process generates a list of Oracle E-Business Suite users for whom the Security Keys needs to be cached in Oracle SES. Security Keys are then generated against the user list by executing (`getSecurityKeys()` and `getSecureAttrKeys()`) methods of the plug-in. These generated keys for a given user and a specific searchable object or data source are cached as User Authorization Cache and will be looked up during user query to see if any match for a given source and user and whether the cache is usable.

For more information about User Authorization Cache feature and how it works, see User Authorization Cache, page 5-57.

How to add a search security plug-in to an object, see Creating Searchable Objects, *Oracle E-Business Suite Search Modeler User's Guide* available from My Oracle Support Knowledge Document 781366.1, Search Modeler 1.1 for Oracle E-Business Suite Readme.

This section includes the following topics:

- How Security Plug-in Works, page 5-39
- Understanding Security Logic and General Plug-in Mechanism, page 5-41
- ACL-based Secuirty, page 5-43
- Query Rewrite Security, page 5-45
- Supporting Security Models with Search Plug-ins, page 5-49
- Other Considerations, page 5-55

How Security Plug-in Works

To effectively guard application content from unauthorized access and support various business requirements within Oracle E-Business Suite, security plug-in mechanism is implemented to ensure the search security and context sensitive information only accessible to appropriate users.

This section highlights and further explains the roles of security plug-in from crawl and query different perspectives. It includes the following topics:

- Crawl Time to Generate ACLs, page 5-39
- Query Time to Generate Security Keys, page 5-39

Crawl Time to Generate ACLs

Security plug-ins are used to fetch ACLs at crawl time.

When Oracle E-Business Suite Crawlable End Point receives crawl requests from Oracle SES crawler threads, the Crawlable Factory is initialized to fetch the indexable content from Oracle E-Business Suite database and create crawlable documents. While creating indexable documents, the security plug-in associated with the searchable object definition will be used through the invocation of the `getAcl()` and `getSecureAttrAcl()` methods to generate ACLs for the documents.

At this time, these indexable documents in the form of RSS feed is ready to be consumed. Oracle E-Business Suite crawler threads pick up the documents; the Crawlable End Point sends them back to the SES indexing engine as crawling responses. The SES indexing engine will then analyze the documents and transform them into indexed documents with readable format.

Query Time to Generate Security Keys

At query time, security plug-ins are used to generate Security Keys for the query user.

Query through Oracle E-Business Suite

When a user performs a search through the Oracle E-Business Suite user interface, a search session is created and the applications context is also initialized for the user. The applications context may be incomplete at this stage depending on if the user has selected a responsibility or not after logging on to the Oracle E-Business Suite.

> **Note:** Applications context information is required for application users to perform certain business transactions or to be used in security plug-in to generate the ACLs and Security Keys for the users. It contains username, responsibility, responsibility application, and security group information.

When the query is submitted to the SES client APIs, the APIs in turn invoke the Web service calls in the Oracle SES server. To ensure the user is authorized for a search, Oracle SES first looks up the previously cached Security Keys for the object and logged-in user in User Authentication Cache (UAC). If a match is found and the cache is usable, the associated keys will be used to compare the pre-built ACLs. Any matched indexed documents will be retrieved for the user. If no match is found, Identity Manager in Oracle SES requests Security Keys for the user through Security Service End Point. A proxy session is initialized to verify the credentials of the proxy username and password required by Oracle SES for the user. This proxy session is trusted or updated on behalf of the actual search user for whom the security keys have been requested.

Please note that the proxy applications context may be incomplete since the search can be performed either with or without the responsibility information. To generate Security Keys for the user in order to perform certain business transactions or activities that require full applications context information, you must extend the `oracle.apps.fnd.search.impl.ContextSecurable` plug-in class to create the complete context information. For more information about the plug-in mechanism, see Understanding Security Logic and General Plug-in Mechanism, page 5-41.

Security plug-in is also invoked by the Security Service End Point to generate the Security Keys through the execution of the `getSecurityKeys()` and `getSecureAttrKeys()` methods for the proxy content.

Once the Security Keys are generated, the Security Service End Point sends the keys back in response to the earlier request from Identity Manager. This request-response happens over HTTP protocol.

To ensure that it does not wait indefinitely for the response to complete, Oracle SES can set a timeout message on the request. The timeout value is configurable.

Query through Oracle SES

When an Oracle E-Business Suite user performs a search through the Oracle SES user interface, the security checks can be performed in the following two stages:

1. Login Security Authentication: This stage validates the user's login credentials through Oracle SES without security or authorization plug-ins.

2. Search Security Authorization: This stage begins when a user submits a search query after successful login. Search plug-in is used in the same way as described in querying through Oracle E-Business Suite that is to generate Security Keys for the query user.

   > **Note:** The major difference between searching from within Oracle E-Business Suite and from Oracle SES Search UI is that while searching from the Oracle SES Search UI, the proxy applications context is always incomplete since the responsibility information may not be there.
   >
   > If certain business transactions or activities that require full applications context information, you must extend the `oracle.apps.fnd.search.impl.ContextSecurable` plug-in class to create the complete context information. For more

information about the plug-in mechanism, see Understanding Security Logic and General Plug-in Mechanism, page 5-41.

The user query is submitted to the SES client APIs which in turn invoke the Web service calls in the Oracle SES server. To ensure the user is authorized for a search, Oracle SES first looks up the previously cached Security Keys for the object and logged-in user in User Authentication Cache (UAC). If a match is found and the cache is usable, the associated keys will be used to compare the pre-built ACLs. Any matched indexed documents will be retrieved for the user. If no match is found, authorization plug-in contacts the Identity Manager to fetch the Security Keys. Identity Manager sends a request message containing the proxy username and password to Oracle E-Business Suite Security Service End Point. Security End Point establishes the proxy session and Applications Context. After the user credential (proxy username and password) is verified, the proxy session is trusted or updated on behalf of the actual search user for whom the Security Keys have been requested.

Security plug-in is invoked by the Security Service End Point to generate the Security Keys through the execution of the `getSecurityKeys()` and `getSecureAttrKeys()` methods for the proxy content.

Once the Security Keys are generated, the Security Service End Point sends the keys back in response to the earlier request from Identity Manager. Authorization plug-in receives the Security Keys for the search user.

Use Security Keys to Match the Pre-built ACLs

Oracle SES search service or APIs retrieve indexed documents from index store, matching the search keywords and filters. Indexed documents with pre-built ACLs are filtered by the Security Keys retrieved for the search user. Filtered search results are returned back to the query user. Unmatched or unauthorized documents get dynamically filtered out in the process.

Understanding Security Logic and General Plug-in Mechanism

Implementing Security Logic

Oracle E-Business Suite Secure Enterprise Search provides security through an interface. Once implemented, various methods of this interface can be called at different stages to enforce the security on the content of a searchable object. Each searchable object can have a plug-in Java class, nominated at design time through the Search Modeler user interface. If this class implements the `Securable` interface, the rules implemented by this class are enforced on the searchable object.

This `Securable` interface security plug-in Java class includes the following security methods:

- **isAclEnabled**

Crawlers use this method to determine if a document is ACL guarded or not. The `getAcl()` and `getSecurityKeys()` methods are called only when this method returns a value of *true*.

- **getAcl**

  This method returns a list of tokens as access control during crawl time to extract each doc with ACL. This method is called for every document before they are sent to Oracle SES for indexing. The string value must be uppercase, alphanumeric, and not longer than 30 characters. This list is used as a predicate when the query is sent to Oracle SES. For example, if you return a string value of "XYZ123ABC", then only the person who holds the key "XYZ123ABC" can access this document, which is then returned by the `getSecurityKeys()` method.

- **getSecurityKeys**

  This method returns an array of keys that the user holds at the time the query is made. You can get the session user from search context that is passed into this method. This method is called only once per session.

- **getSecureAttrAcl**

  In some cases, ACLs may be related to an attribute of the searchable object. If this is true, then you must specify which attribute of the searchable object is a secure attribute. When it is specified and the `Securable` interface is implemented by its plug-in, this method is called for each secure attribute of each document. This method returns a list of ACL for secure attributes at crawl time. It uses the same rules as for `getAcl()`, except it is associated with a particular attribute. This method is paired with `getSecureAttrKeys()` as `getSecurityKeys()` is with `getAcl()`.

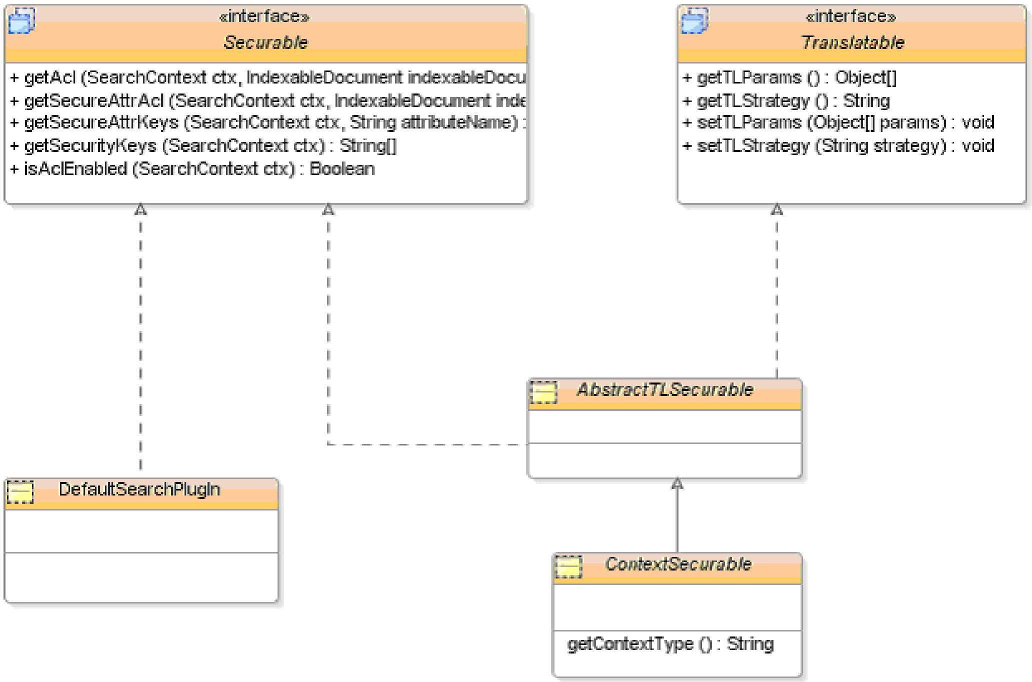
- **getSecureAttrKeys**

  This method is called for each secure attribute per session. It returns a match string list based on the user's access.

General Security Plug-in Mechanism

Certain security plug-ins not only provide `Securable` feature, but also provide `translation` feature to searchable attribute. The relationship between `Securable` interface, `translation` interface, and other associated Java classes is illustrated in the following plug-in class hierarchy diagram:

General Plug-in Class Hierarchy Diagram


«interface»
Securable
+ getAcl (SearchContext ctx, IndexableDocument indexableDocu
+ getSecureAttrAcl (SearchContext ctx, IndexableDocument inde
+ getSecureAttrKeys (SearchContext ctx, String attributeName) :
+ getSecurityKeys (SearchContext ctx) : String[]
+ isAclEnabled (SearchContext ctx) : Boolean
«interface»
Translatable
+ getTLParams () : Object[]
+ getTLStrategy () : String
+ setTLParams (Object[] params) : void
+ setTLStrategy (String strategy) : void
AbstractTLSecurable
DefaultSearchPlugIn
ContextSecurable
getContextType () : String

- `oracle.apps.fnd.search.AbstractTLSecurable`: It is an abstract Java class which supports translation of Searchable and Displayed attribute names. Any business requirement which requires the displayed attribute names to be translated should extend this class.

- `oracle.apps.fnd.search.impl.ContextSecurable`: It is an abstract Java class which can have the full applications context information in order to generate the ACLs and Security Keys. Any plug-in business logic which would require full applications context should extend this class. It is imperative that any subclass of `ContextSecurable` plug-in class has to implement translations as well.

- `oracle.apps.fnd.search.impl.DefaultSearchPlugIn`: It is a concrete Java class which secures the search results based on whether the search user has access to the target UI function or not. This Java class (and any of its subclass) does not support translation of attribute names and full applications context.

ACL-based Security

An access control list (ACL) is a list of permissions attached to an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object.

In the ACL-based security, each entry in the list specifies a subject and an operation. For example, the entry (Alice, delete) on the ACL for file WXY gives Alice permission to delete file WXY. Each crawled entry is associated with a locker, which is created in the form of an ACL. Both the locker and the content get indexed in Oracle SES.

When a user performs a search on an object in Oracle E-Business Suite, the system first checks the list for an applicable entry in order to decide whether to proceed with the query.

When crawled, the `getAcl()` method for each document is called by the crawler and it returns an ACL, which is indexed by Oracle SES along with the document.

Please note that the ACL-based security approach can also be used at query time along with `getSecureAttrKeys()` for additional security based on secure attributes. For more information, see Supporting Security Models with Search Plug-ins, page 5-49.

A Security Example with ACL-based Security

In this example, the ACL is a list of responsibilities that have access to functions in `FND_FORM_FUNCTIONS`. Resolving this relationship requires some complex logic and a number of tables including `FND_MENUS` and `FND_MENU_ENTRIES`.

Function ID	Name	Content	ACL
1	Edit	Oracle Workflow	10 20
2	Update	Oracle Test	10
3	Create	Oracle Financial	30
4	Delete	Oracle Personnel	40

At query time, a search user needs to acquire key(s) for a secure searchable object. In this example, it is a list of responsibilities assigned to the user. The `getSecurityKeys()` method returns this list when it is called. The query is rewritten with the key(s) and posted to Oracle SES. (This is the equivalent of adding security predicates to a query in SQL before hitting the database table).

The user SYSADMIN logs in and issues a query search on the content *Oracle*. Before hitting Oracle SES, the `getSecureAttrKeys()` method is called with the proper user context and returns a list of responsibilities assigned to SYSADMIN, which is "10", "20", and "30". The query is rewritten as:

```
(ACL_KEY: 10 OR 20 or 30) AND content: oracle
```

Using the above example, this query returns the following:

Function ID	Name	Content	ACL
1	Edit	Oracle Workflow	10 20

Function ID	Name	Content	ACL
2	Update	Oracle Test	10
3	Create	Oracle Financials	30

This approach incurs some cost at crawl time because it calls the `getAcl()` method for each row in `FND_FORM_FUNCTIONS`. However, this is acceptable if the underlying table is relatively small.

> **Tip:** In this example, there are approximately 40,000 records in `FND_FORM_FUNCTIONS` and it takes about ten minutes to crawl the entire table.

Query Rewrite Security

By leveraging the searchable attribute feature, Query Rewrite provides another layer of security mechanism during user query to secure application content.

To use this Query Rewrite security, one or more searchable object attributes have to be marked as "Secured" at design time during object creation so that the `getSecurityKeys()` method of the search plug-in can be invoked for each "Secured" attribute at the time of user query.

At crawl time, since the secure attribute concept is used in this mechanism, no access control list will be generated during crawl for the documents of a searchable object.

At query time, when a user performs a search, the user acquires key(s) for a secure object to authenticate the operation based on the applications context. Oracle SES fetches the run-time keys for the user by invoking `getSecurityKeys()` method for each secure attribute, and returns a list of Security Keys for the user to access the secure object. The query is rewritten with keys and posted to Oracle SES. This query rewrite concept is similar to add security predicates to a query in SQL before hitting the database table. As a result, only proper data for the authorized user will be returned as the search result, but the entire query rewritten process is transparent to the user.

For example, a Purchase Order should be visible only to the buyer who places the order. With this design principle, `BUYER_ID` acting as an identifier should be marked as a secure attribute and it should be associated with the document of Purchase Order searchable object during the design time to secure the order content. When a user searches for "laptop docking station" related purchase orders, the query will be rewritten with the predicate, `BUYER_ID = "<buyer id of user>"`. This approach reinforces the secured object Purchase Order and only allows the person who places the order to have the relevant UI and order access privileges.

Tip: Query rewrite method should be used when the number of keys is limited in number. If the number of keys is higher, use ACL method instead.

With the query oriented approach, you nominate one or more attributes as secure attributes for each searchable object. For example, the `BUYER_ID` can be a secure identifier for a purchase order.

At query time, (before searching Oracle SES), a `getSecureAttrKeys()` method is called for each secure attribute such as `BUYER_ID`. The `getSecureAttrKeys()` method implementation should map the number of IDs that the current user has access to.

Note: The query only returns results that the user has access to.

When using this approach, there is no need to form Access Control Lists (ACLs) and security is basically enforced at query time, which means there is less risk of security data being out of date. However, this approach does not work if a user has too many keys. To rewrite a query that has thousands of keys is unrealistic. In order for this approach to perform you must provide a way to limit the number of keys returned by `getSecureAttrKeys()`.

Tip: When there is no clear way to limit keys, or it is too expensive to resolve keys at query time, you should use the crawl oriented approach.

A Security Example with ACL with Query Rewrite

The ACL-based security approach can also be used at query time along with `getSecureAttrKeys()` for additional security based on secure attributes.

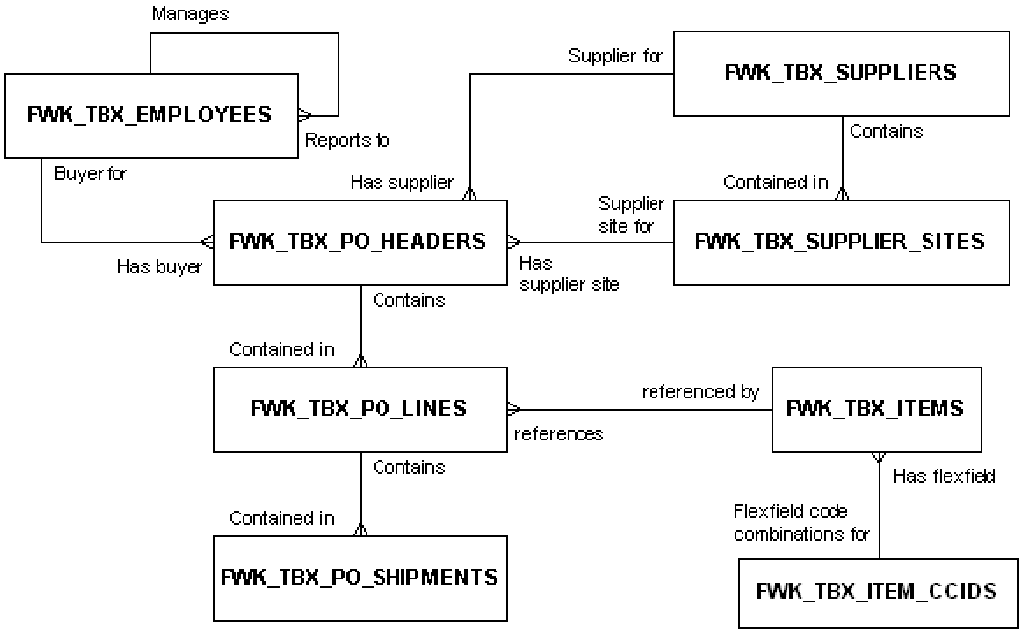
Security Rule Based on Employee Hierarchy

Take purchase orders as an example to explain the security mechanism that combines both ACL-based security and Query Rewrite security.

Purchase orders are usually owned by the user (employee) who initiates the purchase, and the employee hierarchy is usually used as the rule for its visibility to others. For example, an employee can access only his or her own purchase orders, whereas a manager can access the purchase orders he or she owns and those that are initiated by his or her reportees.

The following diagram illustrates a typical entity relationship for a purchase order.

Purchase Order Entity Relationships



The following list of attributes have been selected for displaying:

Entity	Attribute
FWK_TBX_PO_HEADERS	HEADER_ID (PK)
	STATUS_CODE
	DESCRIPTION
	BUYER_ID (FK)
FWK_PO_LINES	LINE_ID (PK)
	HEADER_ID (FK)
	ITEM_ID (FK)
	ITEM_DESCRIPTION
FWK_TBX_ITEMS	ITEM_ID (PK)
	ITEM_DESCRIPTION

Entity	Attribute
FWK_TBX_EMPLOYEE	EMPLOYEE_ID (PK) FIRST_NAME LAST_NAME EMAIL_ADDRESS MANAGER_ID

To use Query Rewrite security, you should mark the BUYER_ID attribute as a "Secured" attribute. The content is then indexed in Oracle SES during crawl time without an ACL.

The following is a sample listing of purchase orders that are initiated by different employees. Employees *adillon* and *bcarey* report to *ekane*, *ekane* reports to *rlavery*, and *rlavery* reports to *khart*.

Header ID	Status Code	Description	Content	BUYER_ID
1	Open	Dell Computer	Oracle Workflow	12 (adillon)
2	Closed	Apple, Inc	Oracle SES	13 (khart)
3	Open	Oracle	Oracle Test	14 (ekane)
4	Approved	Microsoft	Oracle Financial	15 (bcarey)
5	Approved	Oracle	Oracle	13 (khart)
6	Closed	Dell Computer	Oracle Framework	10 (rlavery)
7	Open	Oracle	Oracle Personnel	14 (ekane)

At query time, an authenticated user acquires a key, or keys, via the `getSecureAttrKeys()` method. This method passes applications context information along with the secure attribute such as BUYER_ID. It returns a list of keys to access purchase orders. The query is rewritten with the keys and posted to Oracle SES.

Using the above list of purchase orders, if the user *ekane* performs a keyword search on 'Oracle', she would have the keys 12, 14, and 15. The results would be:

Header ID	Status Code	Description	Content	BUYER_ID
1	Open	Dell Computer	Oracle Workflow	12 (adillon)
3	Open	Oracle	Oracle Test	14 (ekane)
4	Approved	Microsoft	Oracle Financial	15 (bcarey)
7	Open	Oracle	Oracle Personnel	14 (ekane)

If *adillon* performs the same search only one row is returned. However, this approach becomes more complicated when the head of a real department performs a search because they own the entire hierarchy and may have thousands of keys. For this case you can add logic in the `getSecureAttrKeys()` method so that only a specific number of keys or levels of hierarchy is returned.

Supporting Security Models with Search Plug-ins

To secure sensitive application data from authorized access and support complex security needs within Oracle E-Business Suite, Oracle E-Business Suite Secure Enterprise Search provides seeded security search plug-ins. These plug-ins are pre-built public Java classes which support well-known application security models. With the flexible plug-in security mechanism, users can search and navigate to appropriate transaction pages with security enforced to obtain needed information.

Oracle E-Business Suite Secure Enterprise Search supports the following security models with seeded search plug-ins:

- Business Group Based Security Search
- Legal Entity Based Security Search
- Organization Based Security Search
- Employee Hierarchy Based Security Search

Common Security Features of Seeded Search Plug-ins

Although these seeded search plug-ins are provided for various business reasons to secure sensitive application data, they all have the following common security features:

- **Designed Based on ACL and Query Rewrite Security Models**

  All these four seeded search plug-ins are designed based on both the ACL and Query Rewrite security models. As a result, the `isAclEnabled()` method must return "true" in order for the `getAcl()` and `getSecurityKeys()` methods to be called later on during the crawl and query.

- *Crawl Time ACL Implementation*

  In order to fetch ACLs while creating indexable documents at crawl time, the `getAcl()` and `getSecureAttrAcl()` methods of the plug-in have to be implemented.

  Additionally, the `getAcl()` method should extend the DefaultSearchPlugIn concrete Java class (`oracle.apps.fnd.search.impl.DefaultSearchPlugIn`), so that the access to specific target UI function can be securely enforced. For more information about DefaultSearchPlugIn, see Understanding Security Logic and General Plug-in Mechanism, page 5-41.

- *Query Time Security Key Implementation*

  At query time, after a query user's credential (proxy username and password) is verified and updated in response to a request of the user security validation, the `getSecurityKeys()` method should be simply invoked with super class implementation, and the `getSecureAttrKeys()` method returns the list of matched business groups that the query user has access to.

- **A Secure Attribute Needed for Query Rewrite**

  A *secure attribute* is needed to implement the Query Rewrite security mechanism.

  A searchable object contains a number of database tables or views; each table or view contains a number of columns that are bound to business data. While defining a searchable object through Search Modeler, you can select needed columns for each selected table name (entity) for your object. These table columns are called *attributes* that can be indexed for search. If an attribute contains certain feature that can be used to secure documents during search, then this attribute can be considered as a secure attribute. For example, the `BUSINESS_GROUP_ID` column that acts as a Business Group identifier can be a *secure attribute* for HR tables.

  At query time, in order for query engine to generate Security Keys, (before searching Oracle SES) the `getSecureAttrKeys()` method is called for each *secure attribute* such as `BUSINESS_GROUP_ID`. The `getSecureAttrKeys()` method then returns a number of Business Group IDs that the query user has access to. As a result, the query to Oracle SES is rewritten.

  "Secured" and "Stored" Attribute

  To ensure the security check of each search plug-in can be enforced, all seeded plug-ins must contain an unique, secure table column (attribute) as a secure identifier. To differentiate the "secure" feature from other attributes, the attribute property "Secured" should be selected while defining a searchable object in Search Modeler. An attribute marked with "Secured" property indicates that this attribute can be used for securing the document using search plug-in. Additionally, select "Stored" property for the attribute. This indicates that this attribute can be stored in Oracle SES.

> **Note:** If an attribute is marked not "stored", it cannot be displayed in the search result summary.
>
> Other available attribute properties can be like "displayed", "title", "Is attachement", etc. For more attribute property information, see Creating Searchable Objects, *Oracle E-Business Suite Search Modeler User's Guide* available from My Oracle Support Knowledge Document 781366.1, Search Modeler 1.1 for Oracle E-Business Suite Readme.

For example, to ensure business group based security, Business Group Search Plug-in will require that the search object definition should have `BUSINESS_GROUP_ID` attribute, which should be marked at least "Stored" and " Secured".

For more information about ACL and Query Rewrite security models, see ACL-based Secuirty, page 5-43 and Query Rewrite Security, page 5-45.

In addition to the common security features, each search plug-in contains various security requirements and secure attribute information. They are further explained in the following sections:

- Business Group Based Security Search, page 5-51
- Legal Entity Based Security Search, page 5-53
- Organization Based Security Search, page 5-53
- Employee Hierarchy Based Security Search, page 5-54

Business Group Based Security Search

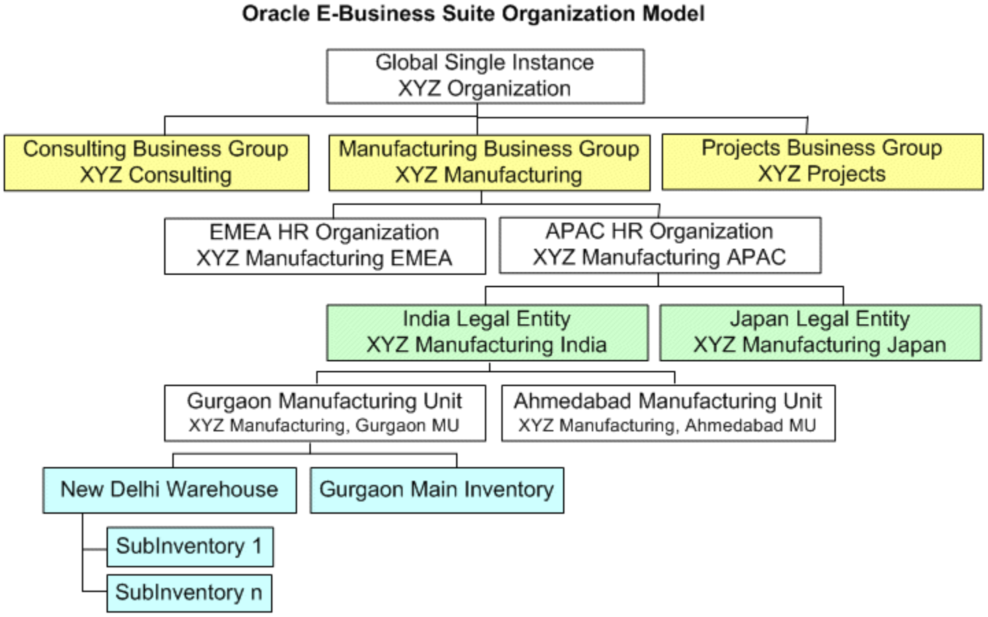
A good example of this type of security model is Oracle E-Business Suite Core HRMS system.

- **Security Requirements:** A Business Group is an organization that is set up and configured in Oracle Human Resources. It is the highest level classification in the organization hierarchy of the Oracle E-Business Suite, and it often relates to country-specific legislation. It may correspond to your entire enterprise or to a major grouping such as a subsidiary or operating division. If your payroll tax and employment authorities permit it, you can group employees of different registered companies together for reporting.

  In this security model, data within a business group is only visible to members of that business group. Even an HRMS superuser (e.g. HR Director) can only see data pertaining to the same business group.

  For example, an XYZ Organization has Consulting, Manufacturing, and Projects business groups. Consulting business group data can only be seen by the Consulting group members, not by the Manufacturing and Projects group members.

Oracle E-Business Suite Organization Model



To secure the group data access only limited to the associated group members while retrieving search results, data is striped in the HRMS tables using `BUSINESS_GROUP_ID` identifier.

- **Business Group Search Plug-in (** `oracle.apps.fnd.search.impl.BusinessGroupSearchPlugin`**) Java Class:** Use this seeded business group search plug-in to secure search results depending on the search user's access to one or more HRMS Business Groups. This search plug-in must extend the DefaultSearchPlugIn concrete Java class (`oracle.apps.fnd.search.impl.DefaultSearchPlugIn`) to ensure that the secure access to the target UI function is also validated.

- **Secure Attribute:** Since a secure attribute is needed to implement the Query Rewrite security mechanism, all HRMS tables are striped with `BUSINESS_GROUP_ID` column, which acts as a Business Group identifier.

  Since a secure attribute is needed to implement the Query Rewrite security mechanism, all HRMS tables are striped with `BUSINESS_GROUP_ID` column, which acts as a Business Group identifier.

  This plug-in requires that the search object definition should have `BUSINESS_GROUP_ID` attribute, which should be marked at least "Stored" and " Secured".

Legal Entity Based Security Search

- **Security Requirements:** Legal Entity in the Oracle E-Business Suite corresponds closely to "company" in the legal world. It has the right to own property, the right to trade, and the responsibility to comply with appropriate laws. You can store information about a registered company or other real world legal entity in the "legal entity".

  The Ledger represents an accounting representation for an organization that is accountable in a self-contained way. A ledger owner might be a legal entity. Thus, the General Ledger (GL) application in Oracle E-Business Suite secures data at Legal Entity level.

  To secure GL data during search, Legal Entity level security needs to be enforced by using the `LEDGER_ID` identifier in GL tables while retrieving search results.

- **Legal Entity Search Plug-in (** `oracle.apps.fnd.search.impl.LegalEntitySearchPlugin`**) Java class:** Use this legal entity search plug-in to restrict search results by the legal entities, which are accessible to the query user.

  Similar to the business group search plug-in, this legal entity search plug-in must extend the DefaultSearchPlugIn concrete Java class (`oracle.apps.fnd.search.impl.DefaultSearchPlugIn`) to ensure that the secure access to the target General Ledger UI function is also validated.

- **Secure Attribute:** Since a secure attribute is needed to implement the Query Rewrite security mechanism, all GL tables are striped with `LEDGER_ID` column, which acts as an unique identifier as a business group identifier does to a business group security model.

  This plug-in requires that the search object definition should have `LEDGER_ID` attribute, which should be marked at least "Stored" and "Secured".

Organization Based Security Search

Oracle E-Business Suite supports the concepts of multiple organizations as well as "Multiple Organizations Access Control (MOAC)" security model.

- **Security Requirements:** *Multiple Organizations* can be sets of books, business groups, legal entities, operating units, or inventory organizations. You can define multiple organizations and the relationships between them through a single installation of Oracle E-Business Suite.

  Operating Units (OUs) are good examples of multiple organizations and they are often identified with security. (The "Manufacturing Units" mentioned in the Oracle E-Business Suite Organization Model diagram in the Business Group Based Security Search, page 5-51 closely resemble the multiple organizations.)

  With MOAC security model, users are given access to the data they handle though "responsibilities". A responsibility is associated with a specific OU, or with several OUs. By securing application data in this way, users can access and process transaction only for the particular operating unit or set of operating units to which they have been granted access. In other words, data pertaining to one organization is normally not visible to another organization unless the user has permission to transact across organizations.

While performing a search on such objects, the organization level data security needs to be enforced through `ORG_ID` identifier for a wide variety of business entities including Purchase Orders, Sales Orders, Payables Invoices, Receivables Invoices, etc.

- **Organization Search Plug-in (** `oracle.apps.fnd.search.impl.OrganizationSearchPlugin`**) Java Class:** Use this organization search plug-in to restrict search results by organizations, which are accessible to the query user.

  Similar to the business group search plug-in, this legal entity search plug-in must extend the DefaultSearchPlugIn concrete Java class (`oracle.apps.fnd.search.impl.DefaultSearchPlugIn`) to ensure that the secure access to the target UI function associated with organizations is also validated.

- **Secure Attribute:** Since a secure attribute is needed to implement the Query Rewrite security mechanism, most Oracle Financial applications tables (e.g. AP, AR, FA etc.) are striped with `ORG_ID` column, which acts as an unique identifier as a business group identifier does to a business group security model.

  This plug-in requires that the search object definition should have `ORG_ID` attribute, which should be marked at least "Stored" and "Secured".

Employee Hierarchy Based Security Search

This type of security model secures data based on employee hierarchy. Good examples can be iExpense, iProcurement, and iLearning within Oracle E-Business Suite. These application modules search on a particular employee's expenses, procurement, and training information based on employee hierarchy.

- **Security Requirements:** Based on the employee hierarchy, data for a particular employee is only visible within his reporting hierarchy. Therefore, while performing a search on such object, search results have to be secured through an unique person identifier.

- **Employee Hierarchy Search Plug-in (** `oracle.apps.fnd.search.impl.EmployeeHierarchySearchPlugin`**) Java Class:** Use this organization search plug-in to restrict search results by employee hierarchy in an organization, which are accessible to the query user.

  Similar to other seeded search plug-ins, this legal entity search plug-in must extend the DefaultSearchPlugIn concrete Java class (`oracle.apps.fnd.search.impl.DefaultSearchPlugIn`) to ensure that the secure access to the target UI function associated with organizations is also validated.

- **Secure Attribute:** Since a secure attribute is needed to implement the Query Rewrite security mechanism, most applications which require employee hierarchy, refer to `PER_ALL_PEOPLE_F` table. The `PERSON_ID` column is the unique person identifier (along with effective dates).

  This plug-in requires that the search object definition should have `PERSON_ID` attribute, which should be marked at least "Stored" and "Secured".

Other Considerations

Oracle E-Business Suite Secure Enterprise Search allows various security rules to be added to secure your searchable objects and application content. However, there are some security limitations and performance need to be considered.

Limitations

If you have more than one security attribute implemented, the principle is that both security rules must be satisfied. This may prevent some use cases from working.

For example, purchase orders are allowed to be seen by buyer, approver, and accountant. However, the accountant is actually a role which can be held by different people at different times, while the buyer and approver are recognized by their employee Ids. If this case occurs, set the emp_id as a secure attribute. This way, when `getSecureAttrAcl` for `emp_id` is called, the `buyer_id` is returned along with a list of responsibilities that are granted to access purchase order. The logic is paired with `getSecureAttrKeys`, which basically returns the buyer's direct employee Id as well as their responsibilities.

Performance

Since a search plug-in is used both during crawl and query, it adds overhead to performance in various times of the object life cycle. This is especially true in `getAcl` and `getSecureAttrAcl` since these methods are called row by row.

Crawl Time Performance

For crawl time performance, there are two possible expensive operations when crawling a searchable object:

- Get Content

  Get content implies JDBC calls to collect information to form indexable documents for Oracle SES to index. The performance of this operation depends on how well the view objects are defined, and how complex a searchable object is.

  For example, if a searchable object assembles a large set of objects, such as a purchase order, it will take time to crawl because each document will need to source data from a number of tables (views).

- Get Acl

  Get ACL is performed on a row-by-row basis by definition because each document will have different ACLs. For a complex security model, `getAcl` might involve multiple database trips. This could incur a high cost and should be carefully balanced with query time performance in order to achieve overall performance.

Query Time Performance

Security also has impact on query time performance. This is due to the fact that for a securable searchable object, the query must be rewritten with access keys by calling `getSecurityKeys`. This function call usually involves database calls.

For example, during query execution, Oracle SES authorization plug-in mechanism contacts Oracle E-Business Suite Security Service End Point over HTTP protocol. The Security Service End Point is used to authenticate an Oracle E-Business Suite user and generate the Security Keys for the query user. The Security Service End Point is implemented as a servlet and registered as "AppSearch" servlet in `oafm` container. Therefore, any security service request is subject to the risk of HTTP Timeout. That is when Oracle SES authorization plug-in mechanism contacts the Security Service in Oracle E-Business Suite, the request has to be completed within a predefined amount of time.

As a guideline, the HTTP time-out value should be set to 30000 milliseconds. The time taken to execute the search plug-in is quite proportional to the overall execution time of a query. Hence for a responsive application, the order of execution has to be classified as follows:

1. Simple plug-in execution: 5000 milliseconds

2. Medium complexity plug-in execution: 10000 milliseconds

3. Complex plug-in execution: 20000 milliseconds

Please note that this has to irrespective of the data volume, which a customer might encounter. Query time performance normally has higher priority than crawl time performance. It must be balanced on a case-by-case basis.

> **Note:** During query, Oracle SES fetches the runtime keys for the current application user using `getSecurityKeys()` or `getSecureAttrKeys()`. Oracle SES waits for a predetermined but configurable amount of time for these methods to retrieve the results. In case of a timeout, Oracle SES assumes the security keys are null for the current user and caches them. Most of the cases, it results in getting no search hits. This is one of the foremost reasons of not getting desired search results.

Improving Query Time Performance Using Cache

Please note that query time performance can be greatly improved by using previously cached security access keys stored in Oracle SES for a particular user, data source, or object. This greatly reduces the query response time of synchronously fetching the

Security Keys for a user or gets timed out if the cache exists. For more information on how to use this feature, see User Authorization Cache, page 5-57.

User Authorization Cache

User Authorization Cache (UAC) framework provides a mechanism allowing the security access keys for a particular user, a specific data source, or a searchable object in Oracle E-Business Suite can be precrawled, cached, and stored in Oracle SES.

By leveraging this UAC feature from Oracle SES 11.1.2, when a user performs a search, instead of fetching the access keys synchronously for that user or object during user query, the previously cached Security Keys will be first looked up in SES for the availability of the keys for that user or object. If a match is found and the cache is usable, the associated keys will be used to compare with the pre-built ACLs. Any matched indexed documents will then be retrieved for the user. Unmatched or unauthorized documents get dynamically filtered out in the process. If there is no match found, the Security Keys will then be fetched and built security filters synchronously during the query. Any matched indexed documents based on the Security Keys and ACLs will be retrieved for the user.

> **Note:** Although Oracle SES 11.1.2 contains UAC feature, UAC for Oracle E-Business Suite will be fully enabled in a later release of Oracle SES. Full benefits of UAC will be visible only until then.

By using the previously cached keys to authorize or revoke the document access privilege (in contrast of generating the keys real time during user query), this feature greatly reduces the search response time and in turn provides quick search results with security enforced.

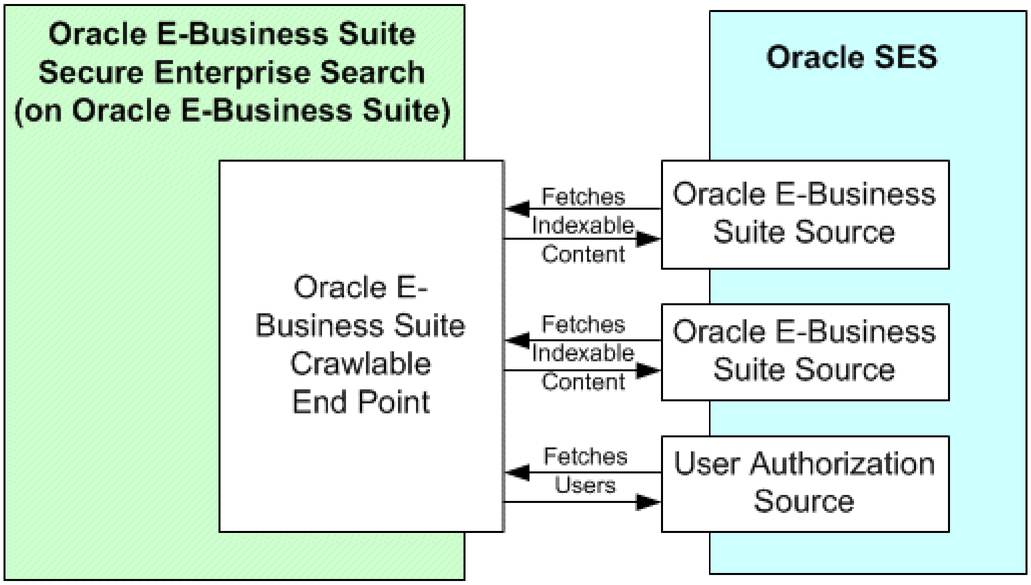
> **Note:** Security Keys are generated through the execution of the `getSecurityKeys()` and `getSecureAttrKeys()` methods of a security plug-in. For more security plug-in information, see Search Security Plug-ins, page 5-37.

How Does User Authorization Cache Work

To enable UAC feature, a specific User Crawler should be initialized to crawl Oracle E-Business Suite users and provides User documents to Oracle SES while other crawlers are for crawling and indexing searchable documents.

The following diagram illustrates the high level crawler tasks:

Crawler Interaction Flow


Oracle E-Business Suite
Secure Enterprise Search
(on Oracle E-Business Suite)
Oracle E-Business Suite Crawlable End Point
Oracle SES
Fetches Indexable Content
Oracle E-Business Suite Source
Fetches Indexable Content
Oracle E-Business Suite Source
Fetches Users
User Authorization Source

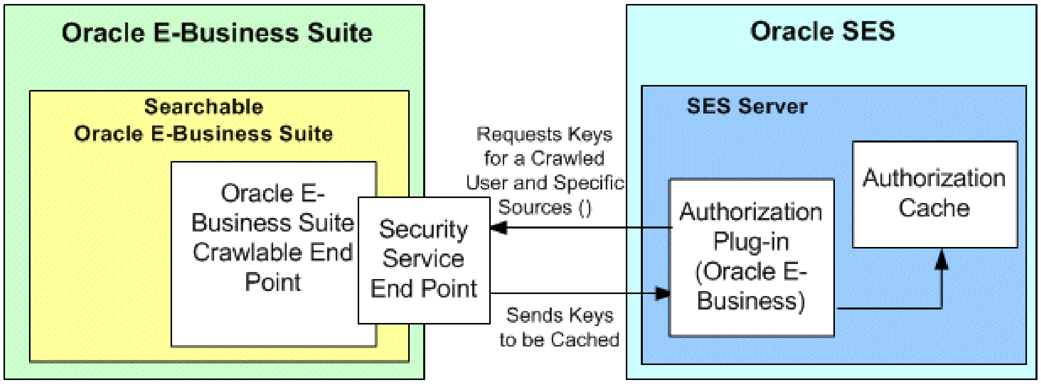
The User Crawler process generates a list of Oracle E-Business Suite users for whom the Security Keys need to be cached in Oracle SES for the predefined "User Authorization Cache" source type. See Defining and Updating UAC Source, page 5-59.

Fetching Security Keys Offline

In order to provide quick search results back to a user and eliminate possible time-outs of fetching Security Keys simultaneously during query due to complex application logic of deriving the keys, the user Security Keys can be generated as an offline process.

The following diagram illustrates the high level authorization cache population flow:

Authorization Cache Population High Level Flow Diagram


Oracle E-Business Suite
Searchable
Oracle E-Business Suite
Oracle E-Business Suite Crawlable End Point
Security Service End Point
Requests Keys for a Crawled User and Specific Sources ()
Sends Keys to be Cached
Oracle SES
SES Server
Authorization Plug-in (Oracle E-Business)
Authorization Cache

When a list of Oracle E-Business Suite user documents is generated by the User Crawler, Oracle SES invokes its Authorization Plug-in to contact Identity Management to fetch the Security Keys. This is done by sending a request for the keys of a crawled user and a specific data source to Oracle E-Business Suite Security Service End Point. The Service End Point in turn invokes the search plug-in to generate the Security Keys which is executed in the same proxy session where the user credential (username and password) is verified. The `getSecurityKeys()` and `getSecureAttrKeys()` methods of a search plug-in are executed to generate the Security Keys. The Service End Point sends the generated keys for a given user and a specific searchable object or data source to be cached to the Authorization Plug-in and have them cached and stored in Oracle SES.

Using Cached Keys for Query Time

When a user performs a search, these previously cached Security Keys will be examined first in Oracle SES to see if the cache exists for a given source and user, as well as whether the cache is usable.

- If a match is found and the cache is usable, the associated keys will be used to compare with the pre-built ACLs. Any matched indexed documents will be retrieved for the user.

- If there is no match found, the Security Keys will be fetched real time during the query and built security filters. Any matched indexed documents based on the Security Keys and ACLs will be retrieved for the user. Unmatched or unauthorized documents get dynamically filtered out in the process.

  Please note that the user authentication cache is populated only when the User Crawler gets executed at the crawl time. If the Security Keys are fetched synchronously during user query, the cache will not be populated.

Defining and Updating UAC Source

In order to crawl Oracle E-Business Suite users in a source system, a special "User Authorization Cache" source type should be defined.

Creating UAC Source

For Oracle E-Business Suite which has seamless integration with Oracle SES, whenever any searchable object is deployed either from Oracle E-Business Suite or from Search Modeler for the first time, one source of "User Authorization Cache" type will be transparently created. This source will have the following information:

Parameter Name	Value
Name	Oracle E-Business Suite UAC
Type	User Authorization Cache

Parameter Name	Value
User Search Query	" " **Note:** Query expression defines the set of users to be crawled. For example, `a*` means to crawl all users whose names begin with the letter `a`, and null value (`*`) means to crawl all Oracle E-Business Suite users. The SES Administrator can enter comma separated user names in wild card format, for example, `OPERATIONS, BPALMER, SYSADMIN*`. The names entered will be preserved during successive deployment of objects.
Source names for which security attributes should be crawled	This parameter will have comma separated values of Sources already deployed. These source names will be automatically updated on deployment of objects.

The above information lets Oracle SES know about the Oracle E-Business Suite "Sources" for a specific user for which the security keys need to be fetched. In other words, the UAC source maps users with the sources whose security keys need to be cached.

Updating UAC Source

Any searchable object deployed subsequently will automatically update the "Source names for which security attributes should be crawled" parameter value to include the name of the source currently being deployed.

Manually Updating UAC Source

However, in case a "User" crawl is in progress while such deployment is attempted, the update to the UAC source might fail. Therefore, a Search Administrator might have to manually add the source name later on.

To manually update the UAC source, log on to Oracle SES and select Sources tab. For Source Type, select "User Authorization Cache" and then click the Update icon. The Update User-Defined Source page is displayed allowing you to update the source information.

Managing the UAC Crawling Schedules

A Search Administrator needs to schedule the crawling job of "E-Business Suite UAC" source at a regular interval to fulfill your business needs.

How to set the crawling frequency and manage crawling schedules, see Administering Crawls in Oracle SES, page 5-66 and Managing Crawling Schedules, page 5-73.

Administering Searchable Objects

Searchable objects are business objects that are made available for text search; they are used in an abstract way for exposing business data to search engines. For example, a purchase order as a searchable object would be defined as a set of searchable properties and its relationship to other searchable objects. Oracle E-Business Suite Secure Enterprise Search uses this abstraction concept to group objects in a logical way at runtime.

To secure all searchable objects containing sensitive application context only exposed to appropriate users before they are deployed to Oracle SES, and to effectively manage and administer data sources after the deployment, system administrator or search administrator needs to perform the following tasks:

1. Securing Searchable Objects Using Security Grants, page 5-61

   Before deploying searchable objects to Oracle SES and making them available to users, these objects must be secured first. By leveraging the concept of the Role-Based Access Control (RBAC) security model, administrators can create security grants to ensure the application content sensitive data is only accessed by authorized people.

2. Deploying Searchable Objects to Oracle SES, page 5-62

   Once searchable objects are ready to be deployed, the system administrator or search administrator can deploy them to the Oracle SES instance. Since not all searchable objects can be successfully deployed to Oracle SES, deployment guidelines and additional tasks are described in this section.

3. Administering Crawls in Oracle SES, page 5-66

   Once searchable objects are deployed to the Oracle SES instance, the crawling schedules by default are automatically created in Oracle SES and visible in the Oracle E-Business Suite. The system administrator or search administrator must first manually edit the default schedules with desired crawling frequencies and start the initial crawl.

Securing Searchable Objects Using Security Grants

As soon as a searchable object is created and patched into Oracle E-Business Suite, it is crawlable in Oracle SES. To make it available for users to search without compromising the data integrity and content sensitivity, the security context must be constructed around the searchable object first. By leveraging the Role-Based Access Control (RBAC) security model, Oracle E-Business Suite Secure Enterprise Search provides a flexible solution that can easily embed application security into a full text search service, and this solution allows only authorized users with appropriate access privileges to search on or view applications data against a preindexed Oracle SES store.

For more information about the RBAC model and how to create security grants, see Role-Based Access Control (RBAC) Security, page 5-33.

Deploying Searchable Objects to Oracle SES

Once searchable objects are ready to be deployed to the Oracle SES instance that you set up earlier in the Configuration tab, the system administrator or search administrator can deploy a single object or deploy all objects simultaneously from a search.

The deployment process can create the following items in Oracle SES:

- Create a data source for each deployed searchable object
- Create a 'Oracle E-Business Suite Release 12' data source type associated with each data source
- Create a schedule per data source
- Create all source groups

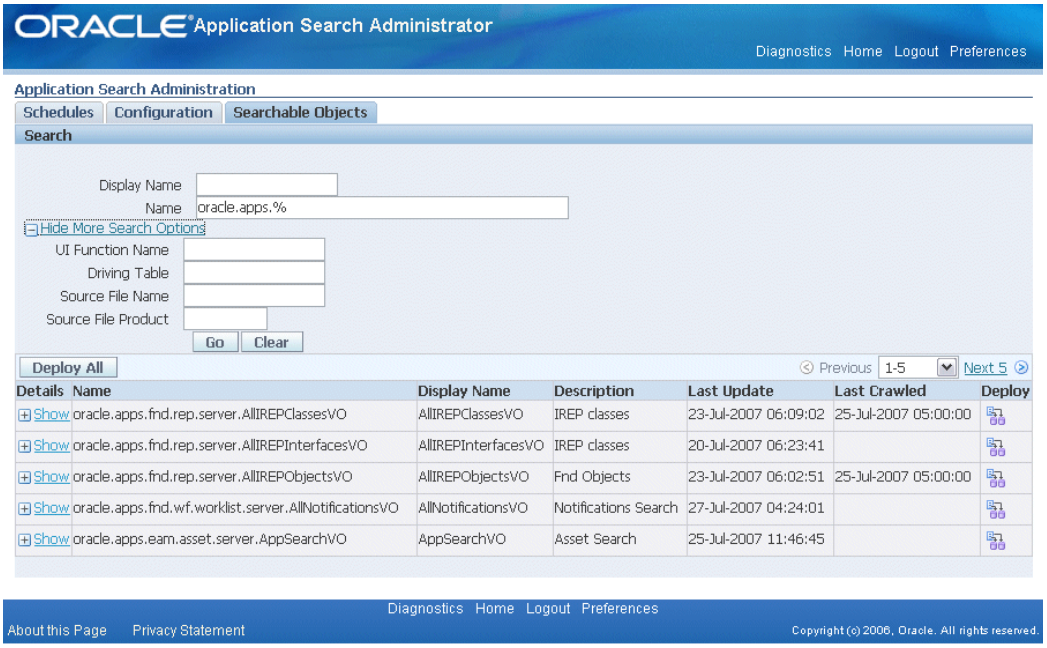
  This creation includes a source group per data source, and a source group per permission set.

> **Important:** Once searchable objects are deployed to Oracle SES, default schedules for each searchable object are created automatically in Oracle SES, but they are set to have a manual launch for the initial crawl. A system administrator or search administrator must manually edit the default schedule by setting up crawling frequency through the use of the administrative page in Oracle SES and starting the initial crawl. Otherwise, the initial crawl will not be automatically started. For more information on setting up crawling frequency and starting an initial crawl, see Administering Crawls, page 5-66.

Please note that this synchronization process with an Oracle SES instance can only deploy the objects that have never been deployed to Oracle SES. Once they are deployed, any future deployment will not update the Oracle SES instance unless you manually delete the data source of the same name in Oracle SES and redeploy it again. Also, if you change the proxy user name and password, business objects that have already been crawled cannot be updated or resynchronized with the Oracle SES instance.

For more details on deployment, see Deployment Concepts and Guidelines in Oracle SES, page 5-64.

Deploying Searchable Objects


ORACLE Application Search Administrator
Diagnostics Home Logout Preferences
Application Search Administration
Schedules
Configuration
Searchable Objects
Search

Display Name

Name oracle.apps.%

UI Function Name

Driving Table

Source File Name

Source File Product

Go
Clear
Deploy All
Previous 1-5 Next 5

Details	Name	Display Name	Description	Last Update	Last Crawled	Deploy
Show	oracle.apps.fnd.rep.server.AllREPClassesVO	AllREPClassesVO	IREP classes	23-Jul-2007 06:09:02	25-Jul-2007 05:00:00	
Show	oracle.apps.fnd.rep.server.AllREPInterfacesVO	AllREPInterfacesVO	IREP classes	20-Jul-2007 06:23:41		
Show	oracle.apps.fnd.rep.server.AllREPObjectsVO	AllREPObjectsVO	Fnd Objects	23-Jul-2007 06:02:51	25-Jul-2007 05:00:00	
Show	oracle.apps.fnd.wf.worklist.server.AllNotificationsVO	AllNotificationsVO	Notifications Search	27-Jul-2007 04:24:01		
Show	oracle.apps.eam.asset.server.AppSearchVO	AppSearchVO	Asset Search	25-Jul-2007 11:46:45		

Diagnostics Home Logout Preferences
About this Page
Privacy Statement
Copyright (c) 2006, Oracle. All rights reserved.

To deploy searchable objects:

1. Log on to Oracle E-Business Suite with the Application Search Administrator responsibility and select the Application Search Administration link from the Navigator window.

2. From the Application Search Administration window, select the Searchable Objects tab.

3. Enter simple search criteria in the Search region, such as Display Name and Name fields. Click **Go** to execute the search.

   Optionally, click the **Show More Search Options** link to enter more search criteria, such as UI Function Name, Driving Table, Source File Name, and Source File Product fields.

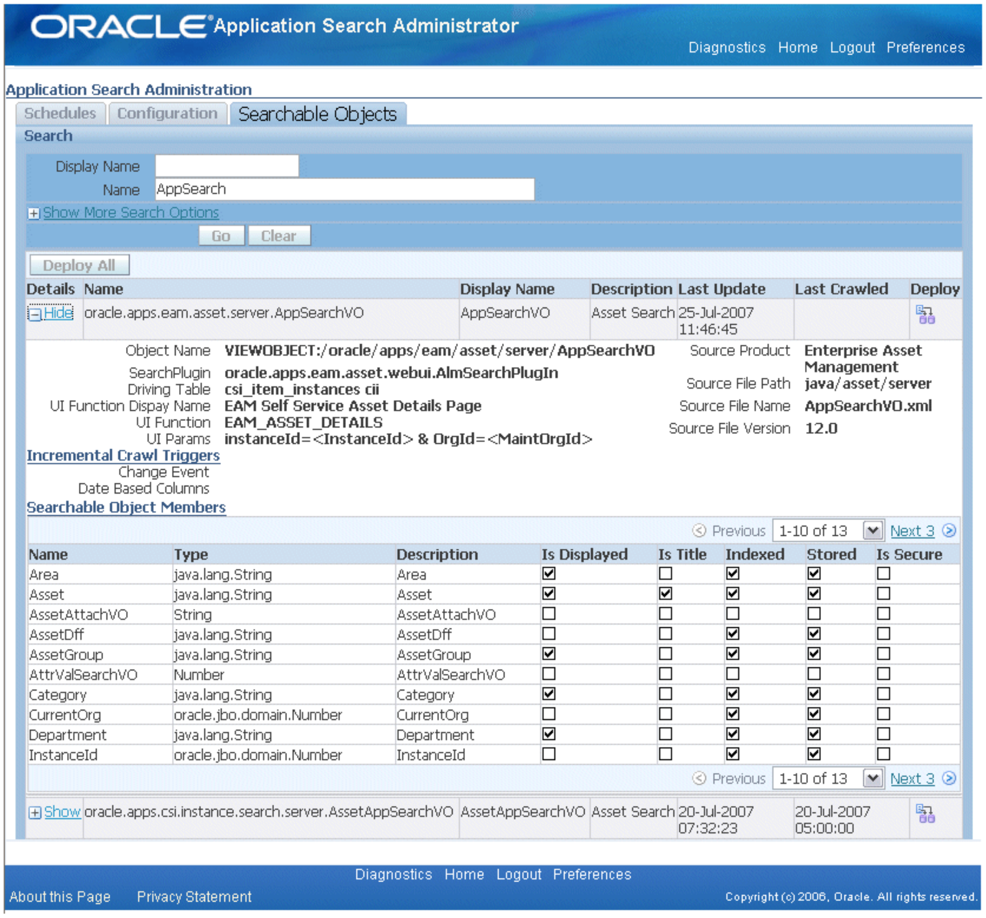
4. From the search result table, you can choose one searchable object you want to deploy to an Oracle SES instance and click the **Deploy** icon for the object.

5. Click **Deploy All** to deploy all the objects from the result table.

   > **Note:** The selection of **Deploy All** is to deploy all the objects from the search result to an Oracle SES instance, and this would mean a reload of Oracle SES references.

6. Click the **Show** link for an object to view the object details. These details include the searchable object's properties information and detailed breakdown for each object member's attributes whether it is displayed, titled, indexed, stored, or secured.

Displaying Searchable Object Details



ORACLE Application Search Administrator
Diagnostics Home Logout Preferences
Application Search Administration
Schedules Configuration Searchable Objects
Search

Display Name

Name AppSearch

Show More Search Options
Go Clear
Deploy All

Details	Name	Display Name	Description	Last Update	Last Crawled	Deploy
Hide	oracle.apps.eam.asset.server.AppSearchVO	AppSearchVO	Asset Search	25-Jul-2007 11:46:45		

Object Name	VIEWOBJECT:/oracle/apps/eam/asset/server/AppSearchVO
SearchPlugin	oracle.apps.eam.asset.webui.AlmSearchPlugIn
Driving Table	csi_item_instances cii
UI Function Dispay Name	EAM Self Service Asset Details Page
UI Function	EAM_ASSET_DETAILS
UI Params	instanceId=<InstanceId> & OrgId=<MaintOrgId>
Source Product	Enterprise Asset Management
Source File Path	java/asset/server
Source File Name	AppSearchVO.xml
Source File Version	12.0

Incremental Crawl Triggers

Change Event

Date Based Columns

Searchable Object Members

Name	Type	Description	Is Displayed	Is Title	Indexed	Stored	Is Secure
Area	java.lang.String	Area	☑	□	☑	☑	□
Asset	java.lang.String	Asset	☑	☑	☑	☑	□
AssetAttachVO	String	AssetAttachVO	□	□	□	□	□
AssetDff	java.lang.String	AssetDff	□	□	☑	☑	□
AssetGroup	java.lang.String	AssetGroup	☑	□	☑	☑	□
AttrValSearchVO	Number	AttrValSearchVO	□	□	□	□	□
Category	java.lang.String	Category	☑	□	☑	☑	□
CurrentOrg	oracle.jbo.domain.Number	CurrentOrg	□	□	☑	☑	□
Department	java.lang.String	Department	☑	□	☑	☑	□
InstanceId	oracle.jbo.domain.Number	InstanceId	□	□	☑	☑	□

Details	Name	Display Name	Description	Last Update	Last Crawled	Deploy
Show	oracle.apps.csi.instance.search.server.AssetAppSearchVO	AssetAppSearchVO	Asset Search	20-Jul-2007 07:32:23	20-Jul-2007 05:00:00	

Diagnostics Home Logout Preferences
About this Page Privacy Statement
Copyright (c) 2006, Oracle. All rights reserved.

Click the **Hide** link to close the detailed view.

Deployment Concepts and Guidelines in Oracle SES

In addition to deploying searchable objects to an Oracle SES instance, the system administrator or search administrator must be aware of the following concepts and may need to perform additional tasks if necessary:

- Data sources
- Crawling schedules
- Data source groups

Data Sources

A data source is one kind of data that you might want to search on. For example, if your data is in Web pages, then Web source is your data source. In other words, it is a particular end point where data can be retrieved. Each data source has a data type associated with it, such as Oracle E-Business Suite 12. Searchable objects contain many business attributes and these attributes can be retrieved and indexed for a given data source type during crawling.

Since the deploy process will only synchronize objects that they have never been deployed to an Oracle SES instance, if an object has been deployed, any future deployment for the same object will not update the instance unless you manually delete the data source of the same name in the instance and then deploy it again. Also, if you change the proxy user name and password, business objects that have already been crawled cannot be resynchronized with the Oracle SES instance.

Deployment Guidelines

Use the following guidelines to have searchable objects successfully deployed to the Oracle SES instance:

- If a data source of the same name does not exist, create the data source with new parameters.

- If a data source is created, you can only delete the data source if it is not crawled and create the data source with new parameters.

- If a data source exists and has been crawled already, do not delete the source or create a new one. Instead, you need to manually update the data source parameters in the Oracle SES administrative pages and redeploy it from the E-Business Suite.

  To access the Oracle SES administrative user interfaces, select the Configuration tab in the Applications Search Administration page. In the Tasks region, click the **SES Admin Login** link under the Additional Tasks section to navigate to the Oracle SES administrative user interfaces. In the Oracle SES instance, use the Home tab and the Source subtab to edit or create data sources. For more information on data source creation and parameters, see the *Oracle Secure Enterprise Search Administrator's Guide* for details.

Crawling Schedules for Searchable Objects

Once searchable objects are deployed to Oracle SES, default schedules for each searchable object are generated automatically in Oracle SES, but they are set to have manual launch the initial crawl. It is very important that system administrator or search administrator must manually edit the default schedule by setting up crawling frequency through the use of the administrative page in Oracle SES and starting the initial crawl. Otherwise, the initial crawl will never be automatically started. See: Administering Crawls in Oracle SES, page 5-66

During the data deployment process, if the data source gets created, the existing schedule will be deleted and a new one should be created. However, for a data source that has been crawled already, its schedule will not be recreated.

Data Source Groups

A data source group is a concept used in Oracle SES to group a number of crawled indexes for an aggregated search. For each searchable object, a default data source group is created with the same name which includes only the data source for this object.

To enable Oracle SES to perform searches on groups, all the groups that have been created in the E-Business Suite application instance should have corresponding source groups created in the Oracle SES instance as well.

For example, for each permission set that starts with `SESG`, a data source group will also be created and populated with Oracle SES references. The permissions included in the permission set that is linked to a searchable object will have their data sources included in the group.

For example, a **permission set `SESG_SEARCH_CRM`** includes the following permissions:

- **ServiceRequest** permission (contains 'ServiceRequest' searchable object)
- **Customer** permission (contains 'Customer' searchable object)
- **Contract** permission (contains 'Contract' searchable object)

Oracle E-Business Suite Secure Enterprise Search uses this mechanism to allow an application user to perform text search in a searchable group and refine or narrow down the search result using the searchable objects contained in the group:

- Each individual searchable object within the group `SESG_SEARCH_CRM`:
  - ServiceRequest
  - Customer
  - Contract

For more information on permission sets used in building security context, see Securing Searchable Objects Using Security Grants, page 5-61.

Administering Crawls in Oracle SES

Crawling schedules define the frequency at which the index is updated with information about each source. Once searchable objects are deployed to Oracle SES, crawling schedules are automatically created along with the data sources in Oracle SES and visible in the Oracle E-Business Suite. However, these automatically created crawling schedules have the crawling frequency type set to the default value 'Manual Launch' which requires you to manually start the initial crawl. Otherwise, these schedules will never be started automatically.

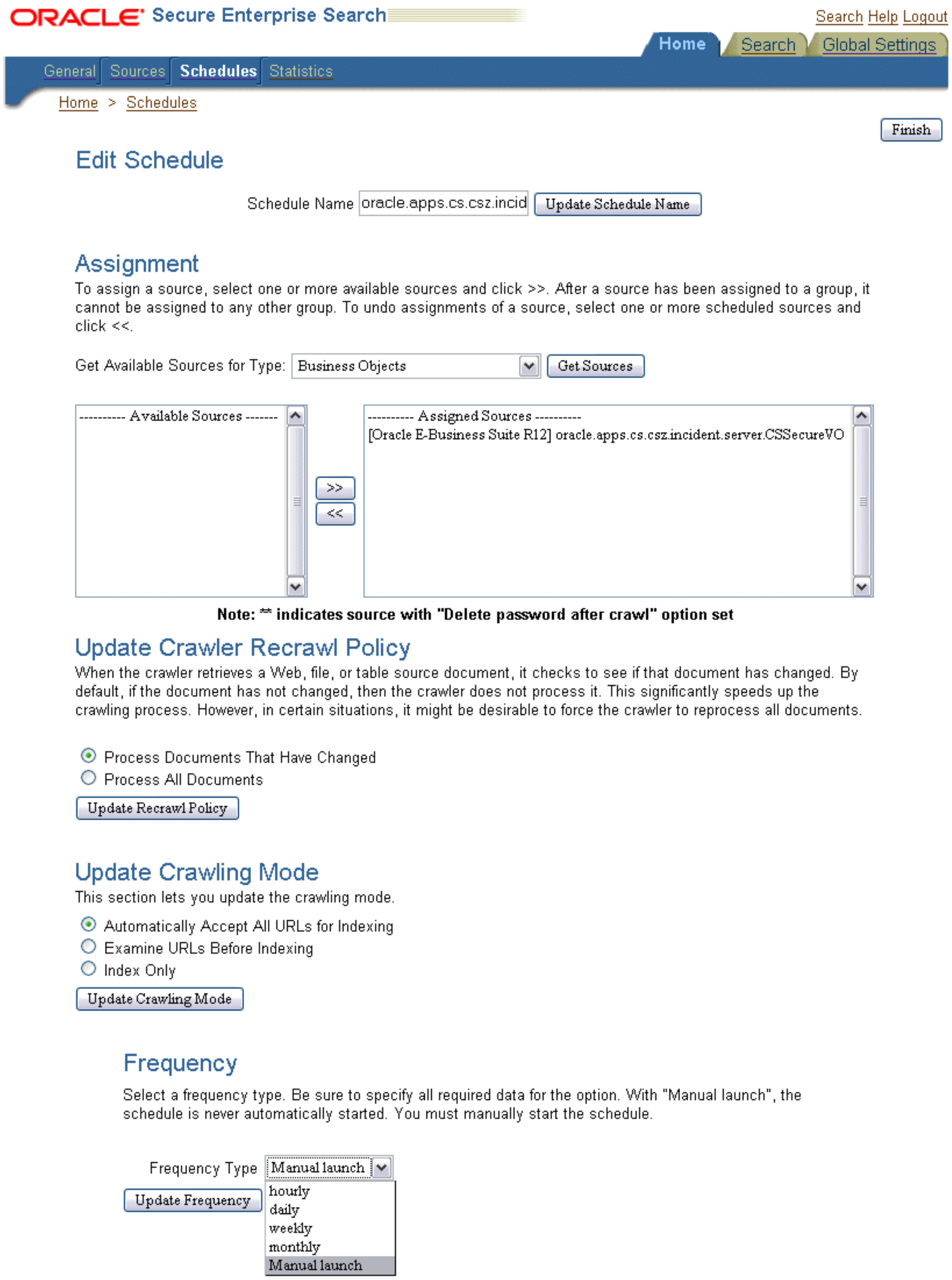
> **Note:** The initial crawl refers to the first time a searchable object is crawled. Since it usually involves a large set of data, it is highly

recommended that an initial crawling job should be scheduled by a low bandwidth job in non-peak hours.

To have fast performance on initial crawl, Oracle E-Business Suite Secure Enterprise Search uses the AD Parallel Update package to help split the large data set into smaller work units, and crawl the units in parallel by using the multi-thread crawling mechanism provided by Oracle SES.

If you want the source or index updated more frequently after the initial crawl is completed, you can update the crawling frequency for a schedule in the Edit Schedule page through the Oracle SES administrative UI.

Setting Crawling Frequency



Edit Schedule

Schedule Name: oracle.apps.cs.csz.incid [Update Schedule Name]

Assignment

To assign a source, select one or more available sources and click >>. After a source has been assigned to a group, it cannot be assigned to any other group. To undo assignments of a source, select one or more scheduled sources and click <<.

Get Available Sources for Type: Business Objects [Get Sources]

---------- Available Sources -------

---------- Assigned Sources ----------
[Oracle E-Business Suite R12] oracle.apps.cs.csz.incident.server.CSSecureVO

Note: ** indicates source with "Delete password after crawl" option set

Update Crawler Recrawl Policy

When the crawler retrieves a Web, file, or table source document, it checks to see if that document has changed. By default, if the document has not changed, then the crawler does not process it. This significantly speeds up the crawling process. However, in certain situations, it might be desirable to force the crawler to reprocess all documents.

● Process Documents That Have Changed
○ Process All Documents

[Update Recrawl Policy]

Update Crawling Mode

This section lets you update the crawling mode.

● Automatically Accept All URLs for Indexing
○ Examine URLs Before Indexing
○ Index Only

[Update Crawling Mode]

Frequency

Select a frequency type. Be sure to specify all required data for the option. With "Manual launch", the schedule is never automatically started. You must manually start the schedule.

Frequency Type: Manual launch

To set crawling frequency in Oracle SES administrative page from Oracle E-Business Suite Secure Enterprise Search:

1. Log on to Oracle E-Business Suite with the Applications Search Administrator

responsibility.

2. Select the Configuration tab and click the **SES Admin Login** link from the Tasks region. This opens the Oracle SES login page.

3. Enter the user name and password you defined for an administrator in order to access an Oracle SES instance.

4. In Oracle SES, select the Home tab and Schedules subtab to access the Crawler Schedules page.

5. Select a schedule name and click the **Edit** icon to see the Edit Schedules page.

6. The selected schedule name is populated automatically in the Schedule Name field. You can select another schedule to update it if you want.

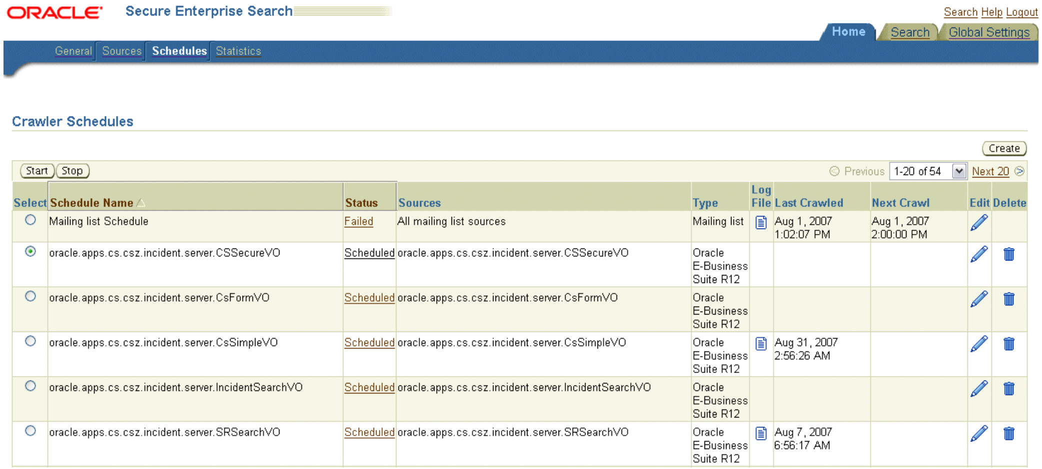
7. Leave the Assignment and Update Crawler Recrawl Policy regions unchanged with the default values.

8. In the Update Crawling Mode region, leave the **Automatically Accept All URLs for Indexing** radio button selected. This selection crawls and indexes all URLs in the source. It also extracts and indexes any links found in those URLs. If the URL has been crawled before, then it will be reindexed only if it has changed.

9. In the Frequency region, change the frequency type from the default 'Manual Launch' to daily, hourly, weekly, or monthly. Click **Update Frequency**.

10. Click **Finish** to save your changes.

Starting an Initial Crawl



Crawler Schedules

Select	Schedule Name	Status	Sources	Type	Log File	Last Crawled	Next Crawl	Edit	Delete
○	Mailing list Schedule	Failed	All mailing list sources	Mailing list	🗎	Aug 1, 2007 1:02:07 PM	Aug 1, 2007 2:00:00 PM	✎	
●	oracle.apps.cs.csz.incident.server.CSSecureVO	Scheduled	oracle.apps.cs.csz.incident.server.CSSecureVO	Oracle E-Business Suite R12				✎	🗑
○	oracle.apps.cs.csz.incident.server.CsFormVO	Scheduled	oracle.apps.cs.csz.incident.server.CsFormVO	Oracle E-Business Suite R12				✎	🗑
○	oracle.apps.cs.csz.incident.server.CsSimpleVO	Scheduled	oracle.apps.cs.csz.incident.server.CsSimpleVO	Oracle E-Business Suite R12	🗎	Aug 31, 2007 2:56:26 AM		✎	🗑
○	oracle.apps.cs.csz.incident.server.IncidentSearchVO	Scheduled	oracle.apps.cs.csz.incident.server.IncidentSearchVO	Oracle E-Business Suite R12				✎	🗑
○	oracle.apps.cs.csz.incident.server.SRSearchVO	Scheduled	oracle.apps.cs.csz.incident.server.SRSearchVO	Oracle E-Business Suite R12	🗎	Aug 7, 2007 6:56:17 AM		✎	🗑

To start, stop, or delete a crawl in Oracle SES:

1. Log on to Oracle E-Business Suite with the Applications Search Administrator responsibility.

2. Select the Configuration tab and click the **SES Admin Login** link from the Tasks region. This opens the Oracle SES login page.

3. Enter the user name and password you defined for an administrator in order to access an Oracle SES instance.

4. In Oracle SES, select the Home tab and Schedules subtab to access the Crawler Schedules page.

5. Select a schedule name that you want to start the initial crawl and click **Start**. If you want to stop an existing crawl, select the schedule name and click **Stop** or click **Delete** to delete a schedule.

6. To update a schedule, select a schedule name and click **Edit**. See: To set crawling frequency in the Oracle SES administrative page from Oracle E-Business Suite Secure Enterprise Search, page 5-68.

7. To view a schedule status, click the link in the Status column, such as scheduled, disabled, launching, or failed, to see the schedule details.

8. Click the **Log File** icon to see detailed crawler settings and status.

9. Click **Create** to manually create a new schedule.

For more information on managing crawling schedules in Oracle SES, see the *Oracle Secure Enterprise Search Administrator's Guide* for details.

Testing Oracle E-Business Suite Secure Enterprise Search Setups

Use the following sections to validate whether you have successfully set up the Oracle E-Business Suite Secure Enterprise Search:

- Validate General Setups, page 5-71
- Test Deployment, page 5-71
- Test Schedules, page 5-72
- Test Searches, page 5-72

Validating General Setups

Use the following steps to validate general setups in Oracle E-Business Suite Secure Enterprise Search:

1. Test whether you have set the FND: Search Enabling Flag profile value to Yes. If it is not set to Yes, crawling should be disabled.

2. Assign the FND Search Crawler (SES_SEARCH_CRAWLER) responsibility and Application Search Administrator responsibility to a system administrator or search administrator. This administrator must be a valid FND user used as a proxy user for query.

3. Ensure you have set the correct value for the proxy parameters. To verify, log on to Oracle E-Business Suite with the Application Search Administrator responsibility, and select Configuration tab to view your setup parameters.

   Use the **Update** check box to reset SES admin proxy and query proxy. For example, set SES admin proxy with user name `egsys` and password `Oracle10g`; query proxy with user name `sysadmin` and password `welcome`. The query user name must be a valid FND user with FND Search Crawler responsibility.

   > **Important:** Once you change the query proxy parameters, the SES instance needs to be restarted to reflect the changes.

Testing Deployment

Use the following steps to test whether you can deploy an object:

1. Log on to Oracle E-Business Suite with the Application Search Administrator responsibility.

2. Select the Searchable Objects tab and search for the object that you want to deploy.

3. Select the object to be deployed and click the **Deploy** icon.

Testing Schedules

Once searchable objects are deployed to the Oracle SES instance, you should be able to find their corresponding schedules automatically created in Oracle SES. Use the Oracle SES instance to start the crawling schedules.

Use the following steps to test crawling schedules whether they work properly:

1. Log on to the Oracle SES administrative page through the Configuration tab in the Application Search Administration page.

2. Select the Home tab and Schedules subtab. Refresh the page and you should be able to see the schedule for object you just deployed.

3. Select the schedule and click **Start** to observe the schedule status change for the selected schedule. Refresh the page if necessary to view the status updates.

Testing Searches

Once the setup tasks are completed, application users with appropriate privileges should be able to perform searches within the Oracle E-Business Suite.

Use the following steps to perform searches:

1. From the home page of the Oracle E-Business Suite, select a searchable group form the search drop-down list.

2. Enter a keyword in the text field, such as 'oracle' and click **Go**.

   You should be able to find the search results populated in the results region.

Additional Administrative Tasks

In addition to setting up necessary tasks for Oracle E-Business Suite Secure Enterprise Search to ensure its seamless integration with Oracle SES, and performing administrative tasks to secure and deploy searchable objects, the system administrator and search administrator also need to perform the following tasks to proactively manage crawling schedules and optimize indexes:

- Managing Crawling Schedules, page 5-73

- Optimizing Indexes, page 5-75

Managing Crawling Schedules

Once searchable objects are deployed, crawling schedules are automatically created along with data sources in Oracle SES. After an initial crawl is completed, subsequent incremental crawls are scheduled and can be executed automatically triggered by business events, date changes, or crawling frequency, as well as other necessary manual crawls.

When a crawling job starts, each crawler retrieves business objects of a given type and then pushes the retrieved objects to be indexed by Oracle SES indexers. Finally, these objects with indexes are stored in the Oracle SES index store for user queries.

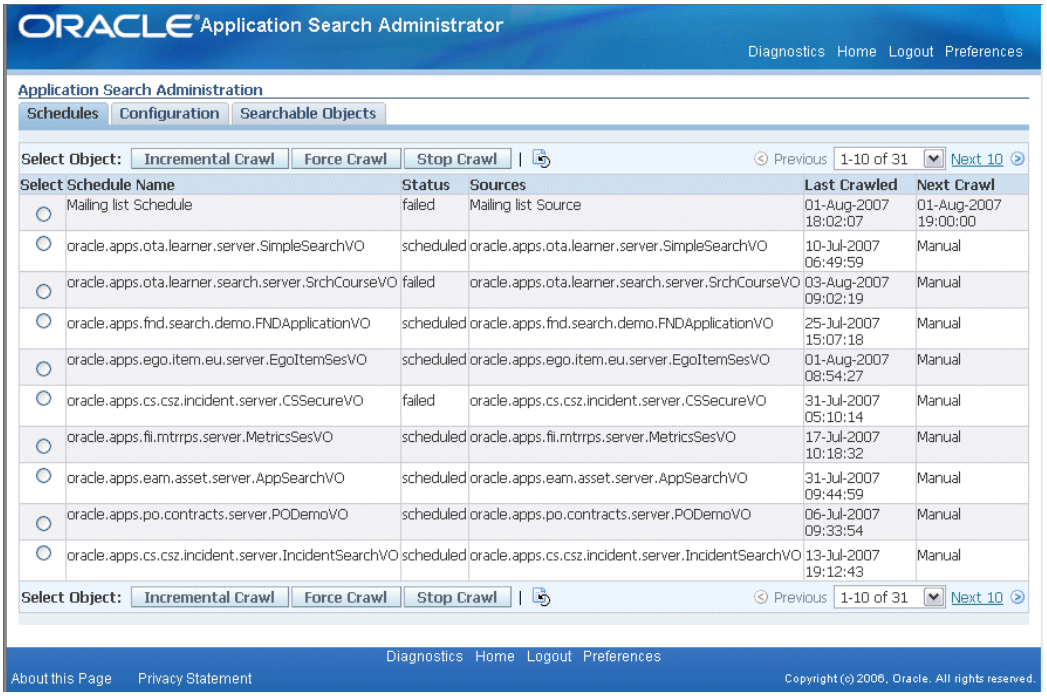
For example, a searchable object, such as a purchase order, may have source data from a number of tables (views), such as product description, employee e-mail address, and so on. When these fields change, the last updated date for the purchase order is also updated. In this way, when a scheduled crawl is performed, the purchase order gets reindexed and stored in the Oracle SES index store.

Oracle E-Business Suite Secure Enterprise Search allows the administrator to proactively manage the crawling schedules in the following ways:

- View the latest crawling status, last crawled, and next crawling schedule for a given schedule
- Stop a manual crawling job
- Recrawl all the data for a selected schedule
- Create an incrementally crawling job for a selected schedule once the initial crawling is completed
    - The initial crawl refers to the first time a searchable object is crawled. Since it usually involves a large set of data, it is highly recommended that an initial crawling job should be scheduled by a low bandwidth job in non-peak hours.

      To have fast performance on initial crawl, Oracle E-Business Suite Secure Enterprise Search uses the AD Parallel Update package to help split the large data set into smaller work units, and crawl the units in parallel by using the multi-thread crawling mechanism provided by Oracle SES.
    - The incremental crawl refers to crawling the data to the original data source after the initial crawl.

Managing Crawling Schedules



Select	Schedule Name	Status	Sources	Last Crawled	Next Crawl
○	Mailing list Schedule	failed	Mailing list Source	01-Aug-2007 18:02:07	01-Aug-2007 19:00:00
○	oracle.apps.ota.learner.server.SimpleSearchVO	scheduled	oracle.apps.ota.learner.server.SimpleSearchVO	10-Jul-2007 06:49:59	Manual
○	oracle.apps.ota.learner.search.server.SrchCourseVO	failed	oracle.apps.ota.learner.search.server.SrchCourseVO	03-Aug-2007 09:02:19	Manual
○	oracle.apps.fnd.search.demo.FNDApplicationVO	scheduled	oracle.apps.fnd.search.demo.FNDApplicationVO	25-Jul-2007 15:07:18	Manual
○	oracle.apps.ego.item.eu.server.EgoItemSesVO	scheduled	oracle.apps.ego.item.eu.server.EgoItemSesVO	01-Aug-2007 08:54:27	Manual
○	oracle.apps.cs.csz.incident.server.CSSecureVO	failed	oracle.apps.cs.csz.incident.server.CSSecureVO	31-Jul-2007 05:10:14	Manual
○	oracle.apps.fii.mtrrps.server.MetricsSesVO	scheduled	oracle.apps.fii.mtrrps.server.MetricsSesVO	17-Jul-2007 10:18:32	Manual
○	oracle.apps.eam.asset.server.AppSearchVO	scheduled	oracle.apps.eam.asset.server.AppSearchVO	31-Jul-2007 09:44:59	Manual
○	oracle.apps.po.contracts.server.PODemoVO	scheduled	oracle.apps.po.contracts.server.PODemoVO	06-Jul-2007 09:33:54	Manual
○	oracle.apps.cs.csz.incident.server.IncidentSearchVO	scheduled	oracle.apps.cs.csz.incident.server.IncidentSearchVO	13-Jul-2007 19:12:43	Manual

To manage crawling schedules:

1. Log on to Oracle E-Business Suite with the Application Search Administrator responsibility and select the Application Search Administration link from the Navigator window.

2. From the Application Search Administration window, select the Schedules tab.

3. From the Schedules page, you can view the crawling details for a given schedule including schedule name, crawling status, source, last crawled, and next crawling schedule.

4. To view the latest schedule details, click the **Refresh Crawler Schedules** icon to get the schedule refreshed.

5. To create incremental crawling schedules, select a schedule name by clicking the **Select** radio button and click **Incremental Crawl** to have the next crawling schedule created in the Next Crawl field.

   Incremental crawling can be raised by a business event or a date change to a searchable object since the last time it was crawled.

6. To stop an existing crawling job, after selecting a schedule name, click **Stop Crawl** to stop the crawling job for the selected schedule.

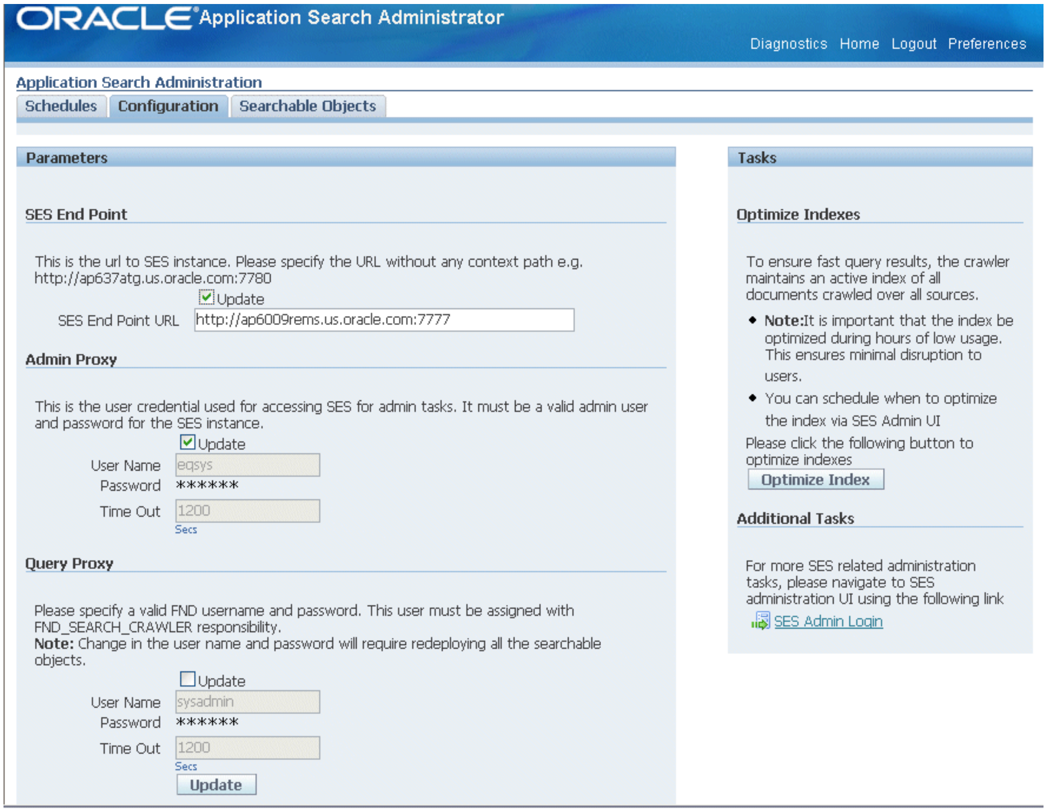
7. To recrawl all the data for a selected schedule, click **Force Crawl**.

Optimizing Indexes

Crawlers maintain active indexes of all documents crawled over all sources. To reduce fragmentation from crawls and increase the speed of searches, the administrator needs to create schedules for optimizing indexes through the Oracle SES administrative pages.

Oracle E-Business Suite Secure Enterprise Search also facilitates the index optimization performed in Oracle SES through a request.

Optimzing Indexes



SES End Point

This is the url to SES instance. Please specify the URL without any context path e.g. http://ap637atg.us.oracle.com:7780

☑ Update

SES End Point URL: http://ap6009rems.us.oracle.com:7777

Admin Proxy

This is the user credential used for accessing SES for admin tasks. It must be a valid admin user and password for the SES instance.

☑ Update

User Name: eqsys
Password: ******
Time Out: 1200 Secs

Query Proxy

Please specify a valid FND username and password. This user must be assigned with FND_SEARCH_CRAWLER responsibility.
Note: Change in the user name and password will require redeploying all the searchable objects.

☐ Update

User Name: sysadmin
Password: ******
Time Out: 1200 Secs

Update

Optimize Indexes

To ensure fast query results, the crawler maintains an active index of all documents crawled over all sources.

- **Note:**It is important that the index be optimized during hours of low usage. This ensures minimal disruption to users.
- You can schedule when to optimize the index via SES Admin UI

Please click the following button to optimize indexes

Optimize Index

Additional Tasks

For more SES related administration tasks, please navigate to SES administration UI using the following link

SES Admin Login

To optimize indexes:

1. Log on to Oracle E-Business Suite with the Application Search Administrator responsibility and select the Application Search Administration link from the Navigator window.

2. From the Application Search Administration window, select the Configuration tab.

3. Click **Optimize Index** in the Optimize Indexes section. This raises an optimization request to Oracle SES and the indexes get optimized.

Important: In order to have minimal disruption to users, it is highly recommended that the index optimization should be done during hours of low usage.

For more information on optimizing indexes in Oracle SES, see the *Oracle Secure Enterprise Search Administrator's Guide* for details.

Error Messages

The following is a list of seeded error messages that Oracle E-Business Suite Secure Enterprise Search uses to notify or alert users when violations occur in interacting with the Oracle SES engine or during query:

Error Message Code	Description
FND_SEARCH_SECURITY	This message occurs when security rules are violated by a query. The query module will terminate the process and throw security exception along with this message. Parameters in this message might include current FND user name. User-specified filters in a secured attribute is a security error. For example, you can enter keyword "oracle" to query. However, if you query on "EMP_ID:dlam content:oracle", an error message is returned because 'EMP_ID' is a secured attribute.
FND_SEARCH_TOO_MANY_ENTRIES	This message occurs when the query engine is to perform a post-query row-by-row process and there were too many rows. The query engine might perform some heuristic actions or throw an exception to the API user.
FND_SEARCH_SYNTAX_ERROR	This message occurs when the query syntax does not conform with Oracle SES. The query engine might rewrite the query.
FND_SEARCH_SES_ERROR	This message relays any potential error originating from Oracle SES when Oracle E-Business Suite Secure Enterprise Search interacts with the Oracle SES engine.

The following table lists the error message type for the types of errors that occur during the integration with Oracle SES engine or query:

Error Message Type	Description
FND_SEARCH_0001	Indicates search engine general errors.
FND_SEARCH_0002	Indicates security errors.
FND_SEARCH_0003	Indicates crawl time errors.
FND_SEARCH_0004	Indicates metadata errors.
FND_SEARCH_0005	Indicates query errors.

6

Technology Inventory Utility

Technology Inventory Utility

This chapter describes the *Technology Inventory Utility* that was introduced in Oracle E-Business Suite Release 12. This command-line utility generates reports that list the installed technology stack components and versions on the various nodes of a Release 12 Oracle E-Business Suite system. The reports can be generated in either HTML (the default) or text format. Separate reports are generated for the database and application tiers.

Since there are major differences in technology components between Release 11*i* and Release 12, this utility will also be useful for those who wish to become familiar with the components and versions employed by Release 12.

Running the Technology Inventory Utility

The Technology Inventory Utility generates a consolidated report that summarizes the version levels of all installed technology stack components.

Set your Oracle E-Business Suite environment, then run one of the following commands:

On UNIX:

Application tier:

```
perl $FND_TOP/patch/115/bin/TXKScript.pl
-script=$FND_TOP/patch/115/bin/txkInventory.pl
-txktop=$APPLTMP
-contextfile=$CONTEXT_FILE
-appspass=apps
-outfile=$APPLTMP/Report_Inventory.html
```

Database tier:

```
perl $ORACLE_HOME/appsutil/bin/TXKScript.pl
-script=$ORACLE_HOME/appsutil/bin/txkInventory.pl
-txktop=$ORACLE_HOME/appsutil/temp
-contextfile=$CONTEXT_FILE
-appspass=apps
-outfile=$ORACLE_HOME/appsutil/temp/Report_Inventory.html
```

> **Note:** To generate the report in text format, append `-reporttype=text` to the relevant command, and change the outfile name to have a .txt suffix instead of a .html suffix.

On Windows:

Application tier:

```
perl %FND_TOP%\patch\115\bin\TXKScript.pl
-script=%FND_TOP%\patch\115\bin\txkInventory.pl
-txktop=%APPLTMP%
-contextfile=%CONTEXT_FILE%
-appspass=apps
-outfile=%APPLTMP%\Report_Inventory.html
```

Database tier:

```
perl %ORACLE_HOME%\appsutil\bin\TXKScript.pl
-script=%ORACLE_HOME%\appsutil\bin\txkInventory.pl
-txktop=%ORACLE_HOME%\appsutil\temp
-contextfile=%CONTEXT_FILE%
-appspass=apps
-outfile=%ORACLE_HOME%\appsutil\temp\Report_Inventory.html
```

> **Note:** To generate the report in text format, append `-reporttype=text` to the relevant command, and change the outfile name to have a .txt suffix instead of a .html suffix.

Parameters

The following table describes the parameters for the utility:

Parameter	Usage
txktop	Temporary working directory used by perl modules. Required parameter.
contextfile	Location of the Applications context file. If not specified, default is picked from environment.
appspass	APPS schema password. If not specified, default password is used.

Parameter	Usage
outputfile	Location of the report being generated. If not specified, the default location is $APPLTMP/TXK.

Output from the Technology Inventory Utility

The report generated on both the application and database tiers has the following common header:

Parameter	Usage
Date	Date on which report was generated.
Hostname	Details of host on which report was generated.
Enabled Services	Services enabled on the host where report was generated (application tier only).
Instance	Name of the instance.
Platform	OS name of the host where report was generated.
OS	OS release version of the host where report was generated.
DB Host	Details of the host where database is located.
Context File	Location of the context file specified when the report was generated.
Report File	Location of the report that was generated.
XML Definition File	Lists actions executed to obtain the contents of the report.

The contents of the main report reflect the role of the node on which the utility is run: Database, Web, Forms, or Concurrent Processing.

Database Tier

For example, the report for the database might include:

Database Service Properties (apps1.company.com):

Technology Component/Property	Component Version/Value
Database version from dbms_utility	10.2.0.2.0
JOB_QUEUE_PROCESSES database parameter	2
UNDO_MANAGEMENT database parameter	AUTO
Amount of temporary tablespace in MB assigned to the APPS schema	3724
UTL_RECOMP package is found in the database.	TRUE
Number of CPUs	4
PARALLEL_MAX_SERVERS database parameter	8
O7_DICTIONARY_ACCESSIBILITY database parameter	FALSE
SYSTEM tablespace size in MB	11668
RAC-enabled	FALSE
Oracle Database 11g patchset version	11.1.0.6.0

Application Tier

Examples of the sections of the Application Tier report follow.

Web Services Node

The report for a Web services node might include:

HTTP Service Properties (apps2.company.com):

Technology Components / Properties	Component Version/Value
Oracle Application Server version	10.1.3.0.0
Sun JDK Client version	1.5.0_10
JDK version on HTTP server node	1.5.0_08
Oracle JDBC driver version using JAVA API (oracle.jdbc.driver.OracleDriver)	10.2.0.2.0
Oracle AOL/J version	Roll Up Patch J
Oracle BC4J version	10.1.3.39.81
Oracle BI Beans version	3.1.1.5
Oracle HTTP Client version	10h
Java Object Cache	10.1.3
Oracle JRAD libraries version	10.1.3
Oracle MDS version	9.0.6.0.0_22
OA Framework version	12.0.0
Oracle Help Web version	2.0.8
Oracle XML driver version	10.1.3.0.0
Oracle UIX version	2_3_6
OJSP version	10.1.3.0.0
JDK version used by AD utilities on HTTP server node	1.5.0_08
Number of symbolic links found under directories served by Oracle HTTP server	0

Technology Components / Properties	Component Version/Value
DB client (RSF) library version in OracleAS 10.1.3 Oracle Home	10.1.0.2.0
Version of OWA packages	10.1.2.0.0
Package OWA_MATCH exists in SYS schema	TRUE

Forms Services Node

The report for a Forms services node might include:

Forms Service Properties (apps2.company.com):

Technology Components / Properties	Component Version/Value
Developer 10g version	10.1.2.0.2
DB client (RSF) library version in OracleAS 10.1.2 Oracle Home	10.1.0.5.0
Forms runtime configuration from Applications context file	socket
JDK version used by AD utilities on Forms node	1.5.0_08
Oracle Application Server patchset version	10.1.2.0.2

Concurrent Processing Node

The report for a Concurrent Processing (CP) server node might include:

Concurrent Processing Service Properties (apps2.company.com):

Technology Components / Properties	Component Version/Value
JDK version on Concurrent Processing node	1.5.0_08
JDK version used by AD Utilities on Concurrent Processing node	1.5.0_08

Code Inventory of the OracleAS 10.1.2 Oracle Home and the OracleAS 10.1.3 Oracle Home

This report also lists each one-off patch and its date and time of application to the OracleAS 10.1.2 Oracle Home or OracleAS 10.1.3 Oracle Home

Future Directions

A future release of Oracle E-Business Suite will build on the Inventory Utility to validate the components in use.

7

Diagnostics and Repair in Oracle Applications Manager

Diagnostics in Oracle Applications Manager

Oracle Applications Manager allows you to run diagnostic utilities from the Diagnostics and Repair tab on the OAM Site Map.

Diagnostic Utilities

Debug Workbench

Navigation Path: Site Map > Diagnostics and Repair (tab) > Diagnostics (heading) > Debug Workbench (link)

Overview

The Debug Workbench enables you to centrally control and monitor the debugging of Oracle E-Business Suitecomponents. Using the Debug Workbench, you can set up debug rules for system components and view the debug information that has been collected.

The Debug Workbench can be launched from Oracle Applications Manager and from the Standard Request Submission (SRS) form using the button **Debug Options...** By default, this button is disabled. To enable this button, set the Concurrent: Allow Debugging profile option to Y.

Using the Main Debug Workbench Screen

On the main Debug Workbench screen, a table lists summary information (Rule ID, Component Name, and so on) for the debug rules that exist on the system. On this screen, you can:

- Filter the table by component type (Concurrent Programs, Forms).
- Create debug rules.
- Search for past executions of debug rules.
- Delete a debug rule.

Creating Debug Rules

You create debug rules to collect debug information about specific system components.

To create a new debug rule, use the following procedure:

1. On the main Debug Workbench screen, click the **Create** button. This launches a multi-step flow of screens that guide you through the rule-making process.
2. Choose the component type that you want to debug. Optionally, you can enter a comment to describe the rule.
3. Choose the component instance.
4. You must set up at least one debug option. Debug options such as logging level, PL/SQL profiler, SQL trace, and Reports trace are available. For a given rule, you can select any combination of available debug option values.
5. Specify the context and schedule of the rule. You can set a rule to execute for a specific responsibility or user, and to execute either during a specific span of time or for a certain number of repetitions.
6. Review your work and click the **Finish** button to save the new rule.

The new rule will appear on the main Debug Workbench screen.

Client System Analyzer Data Collections

Main Navigation Path: Site Map > Diagnostics and Repair (subtab) > Diagnostics (heading) > Client System Analyzer Data Collections (link)

Overview

In Oracle Applications Manager, you can view the data that has been collected by the Client System Analyzer. For more information about using the Client System Analyzer from the Oracle E-Business Suite, see My Oracle Support Knowledge Document 277904.1.

Tasks

You can perform the following tasks on the main Client System Analyzer Data Collections page:

- Click the refresh icon to update the data displayed in the table.
- Filter the table by user name. To do so, select the desired operator (is, contains, starts with, ends with) from the drop-down list, type a search term into the text box, and click **Go**.
- Select one or more rows of data collections and add them to the Support Cart.
- Select one or more rows of data collections and delete them.
- Sort the table by user name by clicking the Applications User Name column header.
- Sort the table by collection date by clicking the Collection Date column header.
- Click an icon in the View column to see the details of a particular data collection.
- Click the **Add to Support Cart** button to add the page itself to the Support Cart.

Data Collection Details

The default set of collected data is organized into categories as follows.

- Client Identification Information
  - OS user name
  - Host name
  - Domain
  - IP address
- Network Configuration and Performance Information
  - Latency
  - Bandwidth
  - Subnet
- Browser and Java Information
  - Browser type

  - JVM vendor
  - JVM version
  - Proxy information
- Hardware Information
- CPU Information
- OS Information
  - OS name
  - OS vendor
  - Base version
  - Update level
- OS Components
- OS Properties
- OS-Registered Software

Troubleshooting Wizards

Oracle Applications Manager provides several wizards:

- Concurrent Manager Recovery
- Service Infrastructure
- Generic Collection Service (GCS) and Forms Monitoring Wizard
- CP Signature

Concurrent Manager Recovery

Navigation: Site Map - Diagnostics and Repair > Concurrent Manager Recovery (under Troubleshooting Wizards)

Use this feature when the Internal Concurrent Manager fails to start.

Click the **Run Wizard** button to start the recovery process. You cannot run this process if the Internal Concurrent Manager is currently running.

If you encounter any problems, each wizard screen can be added to the Support Cart.

Step 1- Active Managers with a Database Session

This screen lists all managers that must be stopped before proceeding with the recovery.

Listed for each manager are:

- CP ID - The Concurrent Program ID.
- Manager - The manager name.
- Node - The node on which the manager is running.
- DB Session ID - Drills down to the Database Session Details screen.
- Session Status
- OS ID
- Started At - The time at which the manager was started.
- Running Request - Drills down to display the request in the Advanced Search for Requests page.

You may want to wait for any requests that are running to complete before you execute the shutdown. Drill down on the Running Request to view it.

Click **Shutdown** to shut down all the listed managers, and then click the **Refresh** icon to verify that they were shut down. If a manager fails to shut down from this page, you can drill down to the **Database Session Details** page and use the **Terminate** button to end the session from there. Return to the **Concurrent Manager Recovery** screen and refresh the page to verify all managers have been shut down before proceeding to the next step.

Step 2 - Managers Deemed Active but Without Database Session

Any processes listed here must be terminated before continuing. Because these processes have lost their database sessions, they must be manually terminated from the command line. Refer to your operating system documentation for instructions on terminating a process from the command line.

After terminating the processes, click **Update** to mark the processes as no longer active in the database table. Click the **Refresh** icon to verify that all processes have been terminated.

Listed for each process are:

- CP ID
- Manager

- Node
- OS PID
- Started At

Step 3 - Reset Conflict Resolution

Click the **Reset** button to reset the listed requests for conflict resolution. This action changes requests that are in a Pending/Normal phase and status to Pending/Standby. Click the **Refresh** icon to verify that all requests have been reset.

You can drill down on the Request ID to view the request in the **Advanced Search for Requests** screen.

Listed for each request are:

- Request ID
- Program
- User

Step 4 - Requests that are Orphaned

This page lists the requests that do not have a manager. If any requests have Active Sessions listed, drill down on the session ID and terminate the session from the **Database Session Details** screen. Return to the Concurrent Manager Recovery screen and click the **Refresh** icon to verify that the session is no longer active.

Listed for each request are:

Request ID - Drills down to display the request in the **Advanced Search for Requests** page.

- Parent ID
- Program
- User
- Phase
- Status
- Active Session

Concurrent Manager Recovery Summary

The summary page lists the information collected from the previous steps. After reaching this page, you should be able to restart your Internal Concurrent Manager. If you cannot, retry starting the Internal Concurrent Manager with DIAG=Y, refresh the summary page, add it to the Support Cart with the log files, and send them to Oracle Support.

Log Files Collected - Click on the log file name to view it. The log files can be added to the Support Cart.

Report Summary

- Active Managers with a Database Session
- Managers Deemed Active but Without a Database Session
- Reset Conflict Resolution
- Requests that are Orphaned

Service Infrastructure

Navigation: Site Map > Diagnostics and Repair > Service Infrastructure (under Troubleshooting Wizards)

Using the Service Infrastructure diagnostic wizard, you can examine existing Generic Service Management data to determine potential problems, and update the data to eliminate the issues.

Click **Run Wizard** to begin using the wizard.

Step 1: Active Nodes without a Service Manager

This screen lists any active nodes without a registered service manager. Concurrent processing requires a registered Service Manager on every registered node. If you need to register service managers for the listed nodes, you can click on the **Register** button to do so.

Step 2: Active Concurrent Processing Nodes without an Internal Monitor

This screen lists any concurrent processing nodes that need a registered Internal Monitor. Click the **Register** button to register Internal Monitors for any listed nodes.

Step 3: Service Managers without Active Nodes

This screen lists service managers and Internal Monitors that are registered for deactivated or nonexistent nodes. If you do not plan on using these nodes in the future, these managers, including the Internal Monitor, can be disabled. Click the **Disable** button to disable the managers for a node.

Step 4: Active Nodes with Inactive Service Managers

All active nodes should have active service managers. This screen lists active nodes without active service managers. Click the **Activate** button to activate service manager definitions for the listed nodes.

Step 5: Enabled Service Instances without Workshifts

This screen shows service instances without any workshifts defined. You can add the Standard workshift to the listed service instances using the **Add Workshifts** button.

Step 6: All Nodes should be Uppercased (for Service Instances)

This screen lists any service instances that are assigned to a node that does not have an uppercase name. Use the **Uppercase** button to change the names of the listed nodes to uppercase.

Step 7: All Nodes should be Uppercased (for Processes)

This screen lists any processes on nodes that do not have an uppercase name. Use the **Uppercase** button to change the names of the listed nodes to uppercase.

Service Infrastructure Summary

This screen shows a summary of the data found for each of the previous screens, as well as any changes you made.

Configuration and Log files are listed first. Two log files and two configuration files are listed for each node. You can click on the name of the file to view it and add it to the Support Cart. You can add all the files to the Support Cart using the **Add All Files to Support Cart** button.

Generic Collection Service (GCS) and Forms Monitoring Wizard

Navigation Path: Site Map > Diagnostics and Repair (tab) > Troubleshooting Wizards (heading) > GCS and Forms Monitoring (link)

Overview

The GCS and Forms Monitoring wizard helps you troubleshoot the OAM Generic Collection Service.

Prerequisites

The wizard cannot be launched unless the Internal Concurrent Manager (ICM) is up and running.

Running the Wizard

Click **Run Wizard** to start the wizard. The steps in the wizard are as follows:

1. If necessary, register the OAM Generic Collection Service on all listed nodes.

2. If necessary, enable the OAM Generic Collection Service on all listed nodes.

3. If necessary, activate the OAM Generic Collection Service on all listed nodes.

4. See the registration of the Forms Listener.

5. If necessary, enable the Forms Listener on all listed nodes.

6. If necessary, set the Sign-On Audit level to "FORM".

7. See a summary screen where you can view a log file and add files to the Support Cart.

CP Signature

The CP Signature Wizard collects information regarding the current status of concurrent processing on the system.

Navigation: Site Map > Diagnostics and Repair > CP Signature

This wizard collects information on the following:

- Configuration status for Parallel Concurrent Processing, Real Application Clusters, and Generic Service Management
- Registered nodes
- Concurrent processing package versions
- Concurrent processing package errors
- Concurrent processing profile options
- Service instances that could be managed by concurrent processing
- Concurrent processing processes
- Request processing manager specialization rules
- Request Conflict Resolution
- Concurrent request processing statistics
- Recent requests to run the Purge Concurrent Request and/or Manager Data program

Support Cart

The Support Cart feature allows you to save Oracle Applications Manager pages with their data and then zip them up in a file to send to Oracle Support. Oracle Support can then view your pages in the Oracle Applications Manager display format.

When you click the **Add to Support Cart** button, the page is added to the Support Cart. If you have filtered or sorted the data, your manipulated view is submitted.

For example, these are some of the pages with the Support Cart feature:

- Configuration Overview
- Site Level Profile Settings
- Recommended/Mandatory Initialization Parameters
- ICM Environment
- Products Installed
- Invalid Objects
- Concurrent Manager Recovery
- Report Results
- All log files

To view the contents of the Support Cart, click on the **Support Cart** global button.

Click **Save Cart** to save the contents to a zip file that you can send to Oracle Support.

Any contents of the cart that are not saved are automatically deleted when you log out of Oracle Applications Manager.

To restore a saved cart, click **Restore Cart** to browse your directory for the saved cart.

To restore a cart file, select a cart file from the list displayed, or use Browse to select a file from the directory. Then click **Restore**.

Support Cart Contents

Description

Enter a TAR Number and additional details for the Support Cart Contents.

Applications Signature

The Support Cart can collect a standard set of information regarding your E-Business Suite system. Oracle Support requires this information when logging a technical assistance request (TAR).

To collect this information, click **Collect**.

In the **Generic** region, information is collected on:

- Product information - For each product, the version, current patch level, and status (for example, "Installed") is shown.
- Database parameters - The init.ora parameter settings.
- Patches - For each individual patch applied, the patch number, type (for example, "

Patch Set" or "Maintenance Pack"), and application timestamp is shown.

- Topology - This page includes data about all the nodes of the applications infrastructure. For each node, it collects information about the operating system and the different services running on that node.

- Database version

Click the **View** icon to view these pages. If you want to delete a page, select it and click the **Delete** button. Clicking **Collect** again will collect information for all four pages again.

In the **Nodes** region, you can specify to include or exclude output and log files for specific nodes as well.

Other Information Collected

Pages that you save using the **Add to Support Cart** button are listed under this tab.

Oracle Applications Manager Log

This page displays the log file generated by Oracle Applications Manager.

Navigation: Site Map > Administration > Applications Manager Log (under Others)

The current message level of the log is shown. To change the level, select the desired option and click **Go**.

> **Note:** Changing the log level from this page will only be effective until the servlet is restarted. For a persistent setting, the log level initialization parameter must be changed in zone.properties. The parameter is: oracle.apps.oam.logger.level
>
> For example:
>
> servlet.weboam.initArgs=oracle.apps.oam.logger.level=USER
>
> Bounce Apache/Jserv for your changes to zone.properties to take effect.

The possible settings are:

- USER - includes messages related to Oracle Applications Manager initialization routines, trace information about the error message, and any diagnostic messages related to customizations or extensions that have been added.

- SUPPORT - includes the User level messages and additional information useful to support for diagnosing problems (for example, configuration setting details, prerequisite patch-related issues, and module-related information).

- DEV - (Development) includes trace information related to code paths (for example, "Inside method A") and any code-related information that could be useful to the developer to diagnose a problem. This level also includes performance-related log messages.

The default is USER.

The log can be added to the Support Cart.

8

Patching and Maintenance with Oracle Applications Manager

Patching and Maintenance Tools

Oracle Applications Manager provides several features to help with patch management. With OAM, you can easily determine which patches have been applied to your system, including the individual patches included in mini-packs, maintenance packs, and merged patches. You can also examine the patched files on a system and find all of the patches that altered a given files. For each patch applied, OAM can show the individual actions taken by the individual patch drivers.

The Patch Wizard recommends patches for your Oracle E-Business Suite system. The wizard takes patch data downloaded from Oracle, analyzes that data against your specific system, and recommends patches based on your preferences. The wizard can also analyze individual patches, identify any prerequisites missing on the system, and show the impact that the patches would have on the system in terms of affected applications, files, and other areas. Additionally, the wizard can download multiple patches from Oracle and merge them into a single patch.

Oracle Applications Manager can also be used to monitor current and previous executions of Applications DBA (AD) utilities.

To schedule required maintenance, you can use the Manage Downtime feature. As soon as a downtime is scheduled, users are notified of the upcoming period during which the system will not be available. During the scheduled downtime, Oracle E-Business Suite will be unavailable, but certain users will be allowed to log in to Oracle Applications Manager in order to monitor maintenance activity.

Patch Impact Analysis

The Patch Impact Analysis page shows the impact of the patch if applied to your system.

For information for this page, see: Patch Impact Analysis (AD), *Oracle E-Business Suite Maintenance Utilities*.

Managing Downtime in Restricted Mode

Restricted Mode

In Restricted Mode, only valid database users are allowed to login into OAM via a special URL, and are allowed to access a limited set of features. The database role AD_MONITOR_ROLE has access to all the required database objects for Restricted Mode features. However, a valid database user who does not have the AD_MONITOR_ROLE may have further limited access to OAM functionality based on the database objects to which this user has access. Monitoring in-progress AD utilities is the only feature that is accessible.

How to Implement Restricted Mode

1. Schedule the system downtime and notify end users of the upcoming downtime. Use OAM to schedule the downtime. See: Manage Downtime Schedules - Overview, page 8-3.

2. Complete the required one-time setup steps required to monitor patching progress. Ensure that you have enabled the monitoring user account by unlocking the ad_monitor account with the following command:

   ```
   alter user ad_monitor account unlock;
   ```

   Then log in to SQL*Plus as the user ad_monitor. The default password is 'lizard'. Reset the password.

3. Shut down Apache and all other all Oracle E-Business Suite services. Use the standard AD script:

   ```
   $INST_TOP/admin/scripts/adstpall.sh <apps user>/<apps password>
   ```

4. Enable Maintenance Mode for your system.

   To do this, run adadmin and select Option 5 =>Change Maintenance Mode, then Option 1 => Enable Maintenance Mode.

5. Run the command:

   ```
   $FND_TOP/bin/txkrun.pl -script=ChangeApacheMode -contextfile=<Path
   and name of the context file> -mode=Restrict
   ```

6. Start Oracle HTTP Server and oacore OC4J:

   ```
   $INST_TOP/admin/scripts/adapcctl.sh start
   ```

   ```
   $INST_TOP/admin/scripts/adoacorectl.sh start
   ```

7. Begin applying patch(es). Run adpatch (hotpatch=n).

8. To monitor patching progress, launch Restricted Mode in OAM using the OAM Restricted Mode URL:

   http://hostname:port/OA_HTML/weboamLocal/oam/oamServlet

9. Log in as ad_monitor with the new password.

10. You are now in OAM Restricted Mode, and can access patching utilities from the Maintenance tab of the Site Map: Navigate to Site Map > Maintenance, Patching and Utilities > Timing Reports.

11. Confirm the end of scheduled downtime in OAM upon patch completion.

    From within OAM in Restricted Mode, navigate to Site Map > Maintenance > Patching and Utilities > Manage Downtime Schedules. Click the **Mark Complete** button. Confirm that you wish to change the downtime status to Complete.

12. Now switch the system back to normal mode. Run adadmin and select Option 5 => Change Maintenance Mode, then Option 2 => Disable Maintenance Mode.

13. Stop Oracle HTTP Server and oacore OC4J:

    ```
    $INST_TOP/admin/scripts/adapcctl.sh stop
    $INST_TOP/admin/scripts/adoacorectl.sh stop
    ```

14. Run the following command:

    ```
    $FND_TOP/bin/txkrun.pl -script=ChangeApacheMode –contextfile=<Path
    and name of the context file> -mode=Normal
    ```

15. Restart all services:

    ```
    $INST_TOP/admin/scripts/adstrtal.sh <user/password>
    ```

For more information on AutoConfig and the AD scripts, see the *Maintaining Oracle E-Business Suite Documentation Set*.

Manage Downtime Schedules - Overview

Navigation: Site Map > Maintenance > Manage Downtime Schedules (under Patching and Utilities)

Use these pages to manage downtime for maintenance.

Scheduled Downtimes

This region shows downtime periods scheduled for the future.

Previous Downtimes

This region shows previously scheduled downtime periods. Downtime periods that were canceled before they were scheduled to start are included here.

Schedule Downtime

Use this page to set up your downtime schedule and messages.

Downtime

This information appears in the Scheduled Downtime Details screen shown to users while the system is down.

Enter the following:

- Name
- Start Date and Time
- Expected End Date and Time
- Contact Information - You can enter a name, email address, etc. in this free-text field.
- Downtime Status URL
- Downtime Message - This message is displayed to users who try to log in while the system is down. You can use the default message provided, a message defined in Message Dictionary, or enter your own message.
  - Default message
  - Message Dictionary - you can use a Message Dictionary message by specifying its name.
  - Message Text - Directly enter your own message here.

Warning

Warning information is displayed to users before the downtime actually starts. Enter the following:

- Warning Start Date and Time
- Warning Message - Options are similar to those for the Downtime Message above.

Downtime Details

Navigation: Site Map > Maintenance > Manage Downtime Schedules (under Patching and Utilities) > [Selected Downtime] Details

This page shows you the details for a downtime that were entered in when the downtime was scheduled. Notes can be added on an ongoing basis.

Purging in Oracle Applications Manager

Navigation: Site Map > Maintenance > (Critical Activities) Setup and Monitor

Purge programs help reduce the amount of transient data stored in an Oracle E-Business Suite system. Periodically purging unneeded data helps to:

- Reduce system downtime for upgrades
- Decrease backup times
- Increase storage efficiency
- Improve system performance

Oracle E-Business Suite has several concurrent programs defined as purge programs. These programs can then be added to the Critical Activities by navigating to the Setup link. These features can then be run from the Critical Activities Monitor link.

9

License Manager

License Manager

License Manager is a utility that registers additional products, country-specific functionalities, and languages for your Oracle E-Business Suite system. Once you have contacted your Oracle sales representative, or set up your new license agreements online through the Oracle Store, you are ready to register your new products, country-specific functionalities or languages using License Manager. License Manager does not set up license agreements or determine pricing, but the registration procedure makes new components accessible to all Oracle E-Business Suite utilities.

License Manager also provides a set of reports that allows you to determine the products, country-specific functionalities and languages that are registered on your Oracle E-Business Suite system.

The main License Manager page contains three main licensing links and five report links. The licensing pages are:

- Products
- Country-specific Functionalities
- Languages

The five report links that provide licensing details about your Oracle E-Business Suite system are:

- Licensed Products
- Shared Products
- Country-specific Functionalities
- Languages

- Summary

License Section

This section contains links to license products, country-specific functionalities, and languages.

License Products

Clicking the Products link in the License section of the License Manager main page opens the License Products page. This page displays two options and a link to show more options.

- License E-Business Suite: Select this option to register the predefined E-Business Suite of products.
- License Component Application: Select this option to register products by component applications.
- Show More Options: Select this link to show a third product licensing option, License Applications Product.
- License Applications Products: This option becomes visible when Show More Options is selected. Select this option to register Oracle E-Business Suite products individually.

Select the desired option and click Continue.

License E-Business Suite

Selecting License E-Business Suite in the Product Licensing page opens the License E-Business Suite page. This page displays all products that will be registered when you choose to register the "E-Business Suite". Once the E-Business Suite is registered, individual products within the suite cannot be unregistered. This page displays all products that can be registered and contains three columns of information:

- Select: There is a check mark for each product that will be registered.
- Focus: Select the circle icon next to a component application to see just the products in the component application.
- Name: This is the name of the component applications or the products within a component application. Click the (+) or (-) icon to hide or show the individual products within a component application.

Click Next to move on to the License E-Business Suite Add-ons page.

License E-Business Suite Add-ons

The License E-Business Suite Add-ons page lists the products that are not included in the standard "E-Business Suite" list of products. Select the E-Business Suite Add-on products on this page. This page contains three columns of information:

- Select: Check the check box for the products that you want to register.
- Focus: Select the circle icon next to a component application to see just the products in the component application.
- Name: This is the name of the component applications or the products within a component application. Click the (+) or (-) icon to hide or show the individual products within a component application.

To register all E-Business Suite add-ons, click the Select All link. To deselect all selected E-Business Suite add-ons, click the Select None link. Once an E-Business Suite add-on is registered, it has a check box that is disabled and cannot be unregistered.

Click Next to advance to the License E-Business Suite Review page.

License E-Business Suite Review

Navigation: Site Map (Administration) > License Manager > Products > License E-Business Suite

The License E-Business Suite Review page lists the products that you selected to register in the License E-Business Suite and License E-Business Suite Add-ons pages. This page contains two columns of information:

- Focus: Select the circle icon next to a component application to see just the products in the component application.
- Name: This is the name of the product to register. Click the triangle icon to hide or show the individual products within a component application.

Click Submit to register the products.

License Component Application

Selecting License Component Application in the Product Licensing page opens the License Component Application page. This page displays all component applications that can be registered and contains three columns of information:

- Select: Check the check box for the component applications that you want to register.
- Focus: Select the circle icon next to a component application to see just the products in the component application.
- Name: This is the name of the component applications or the products within a component application. Click the (+) or (-) icon to hide or show the individual products within a component application.

To register all component applications, click the Select All link. To deselect all selected component applications, click the Select None link. Once a component application is registered, the individual products within the component application have check boxes that are greyed out and cannot be unregistered.

Click Next to advance to the License Component Application Review page.

License Component Application Review

The License Component Application Review page lists the products that you selected to register in the License Component Application page. This page contains two columns of information:

- Focus: Select the circle icon next to a component application to see just the products in the component application.

- Name: This is the name of the component application to register. Click the blue triangle to hide or show the individual products within a component application.

Click Submit to register the products.

License Applications Products

Selecting License Applications Product in the Product Licensing page opens the License Applications Products page. This page displays all products in the Oracle E-Business Suite system and allows you to register them individually.

To register all products, click the Select All link. To deselect all selected products, click the Select None link. Once a product is registered, it has a check box that is grayed out and cannot be unregistered.

Click the check box of the products that you want to register and click Next. This takes you to the License Applications Products Review page.

License Applications Product Review

The License Applications Products Review page lists the products that you selected to register in the License Applications Products page. This page contains two columns of information:

- Product Name: This is the name of the product to register.

- Product Abbreviation: This is the short name of the product to register, for example, AS or BIS.

Click Submit to register the products.

License Country-specific Functionalities

Selecting Country-specific Functionalities in the License section of the License Manager main page produces the License Country-specific Functionalities page. This page displays all country-specific functionalities in the Oracle E-Business Suite system and allows you to register them. This page contains three columns of information:

- Select: Check the check box for the country-specific functionality that you want to register. The already registered country-specific functionalities have check boxes that are greyed out. Once a country-specific functionality is registered, it cannot be unregistered.

- Country Name: This is the name of the country-specific functionality.

- Country Short Name: This is the short name of the country-specific functionality to register.

Once you select the country-specific functionalities that you want to register, click Next. This takes you to the License Country-specific Functionalities Review page.

License Country-specific Functionalities Review

The License Country-specific Functionalities Review page lists the country-specific functionalities that you selected to register in the License Country-specific Functionalities page. This page contains two columns of information:

- Country Name: This is the country name of the country-specific functionality to register.

- Country Short Name: This is the short name of the country-specific functionality to register, such as CO or JP.

Click Submit to register the country-specific functionality.

License Languages

Selecting Languages in the License section of the License Manager main page opens the License Languages page. This page displays all languages available for the Oracle E-Business Suite system and allows you to register them. This page contains these columns of information:

- Select: Check the check box for the languages that you want to register. The already registered languages have check boxes that are disabled.

- Language Name: This is the name of the language.

- Language Code: This is the language code, such as US or ESA.

Click the check box of the languages that you want to register and click Next. This takes you to the Base Language page.

Base Language

The Base Language page shows the current base language and list of languages that you can select as a base language for your Oracle E-Business Suite system.

The Current Base Language section contains one row and two columns of information:

- Name: This is the name of the current base language.

- Language Code: This is the base language code.

The Select New Base Language section contains a row for each registered language and three columns of information:

- Select: Select the language that you want to set as the base language.
- Language Name: This is the name of the language.
- Language Code: This is the language code.

Click Next to continue to the License Languages Review page.

License Languages Review

The License Languages Review page lists the languages that you selected to register in the License Languages page and the base language that you selected in the Base Language page. There are two sections in this page.

The Selected Languages section contains a row for each language you want to register and these columns of information:

- Name: This is the name of the language to register.
- Language Code: This is the language code of the language to register, such as CA or ESA.

The Base Language section contains one row and two columns of information:

- Name: This is the name of the selected base language.
- Language Code: This is the base language code, for example, US.

Click the Submit button to register the languages and set the base language and territory.

Reports Section

This section contains links to reports.

Licensed Products Report

Clicking the Licensed Products link in the Reports section of the License Manager main page produces the Licensed Products report. The report has two sections. The first section, Summary, shows the Status information. Status is the number of products installed and the number of products shared. Clicking on one of these status groups refreshes the second section of this report, List of Products according to the status selected.

Depending upon which group (Licensed or Shared) you clicked in the Summary section, the List of Products changes to show all licensed products or all shared products in the system. The List of Products section has four columns:

- Select: This option button determines which product's patch summary information is presented in the Patch Summary page.
- Product Abbreviation: This is the product short name, for example, FND or GL.
- Product Name: This is the name of the fully licensed product.
- Status: This is the license status of the product.

A filter at the top of the List of Products section allows you to narrow the contents of the report. You can filter by Product Abbreviation, Product Name, or (license) Status. For Status, you can choose from Licensed, Shared, or Not Licensed.

From this report you can access the Patch Information page for a specific product by selecting the product and clicking the Patch Information button, or by clicking the Product Name.

Shared Products Report

Clicking the Shared Products link in the Reports section of the License Manager main page produces the Shared Products report. The report has two sections. The first section, Summary, shows the Status information. Status is the number of products installed and the number of products shared. Clicking on one of these status groups refreshes the second section of this report, List of Products according to the status selected.

The List of Products section has four columns:

- Select: This option button determines which product's patch summary information is presented in the Patch Summary page.
- Product Abbreviation: The product short name, for example, FND or GL.
- Product Name: The name of the fully licensed product.
- Status: The license status of the product.

A filter at the top of the List of Products section allows you to narrow the contents of the report. You can filter by Product Abbreviation, Product Name, or (license) Status. For Status, you can choose from Licensed, Shared, or Not Licensed.

From this report you can access the Patch Information page for a specific product by selecting the product and clicking the Patch Information button, or by clicking the Product Name.

Country-specific Functionalities Report

Clicking the Country-specific Functionalities link in the Reports section of the License

Manager main page produces the Country-specific Functionalities report. This report displays all registered country-specific functionalities in the Oracle E-Business Suite system and contains two columns of information:

- Country Name: This is the country name of the country-specific functionality.
- Country Short Name: This is the country-specific functionality short name, such as CO or JP.

Clicking **OK** on the report returns you to the main License Manager page.

Clicking **Edit** takes you to the License Country-specific Functionalities page.

Languages Report

Clicking the Languages link in the Reports section of the License Manager main page produces the Languages report. This report displays the current database character set, the base language, and all registered languages.

The Licensed Languages section contains a row for each registered language and two columns of information:

- Language Name: This is the name of the registered language.
- Language Code: This is the short name of the registered language, such as CA or ESA.

The Base Language section contains one row and two columns of information:

- Language Name: This is the name of the base language.
- Short Name: This is the base language short name, for example, US.

Clicking OK on the report returns you to the main License Manager page.

Clicking Edit takes you to the License Languages page.

License Summary Report

Clicking the Summary link in the Reports section of the License Manager main page produces the License Summary report. This report displays a summary of all registered products, country-specific functionalities, languages, and base language. There are five sections in this report.

The Licensed Products section contains a row for each fully licensed product registered in the system and two columns of information:

- Product Name: This is the name of the registered product.
- Product Abbreviation: This is the product short name, for example, FND or GL.

The Shared Products section contains a row for each shared product registered in the system and two columns of information:

- Product Name: This is the name of the shared product.

- Product Abbreviation: This is the product short name, for example, AD or OE.

The Country-specific Functionalities section contains a row for each registered country-specific functionality and two columns of information:

- Country Name: This is the country name of the country-specific functionality.

- Country Short Name: This is the country-specific functionality short name, for example, CO or JP.

The Licensed Languages section contains a row for each registered language and two columns of information:

- Language Name: This is the name of the registered language.

- Language Code: This is the code of the registered language, for example, CA or ESA.

The Base Language section contains one row and two columns of information:

- Language Name: This is the name of the base language.

- Short Name: This is the base language short name, for example, US.

10

User Profiles

Overview of Setting User Profiles

A profile is a set of changeable options that affect the way your application looks and behaves. As System Administrator, you control how Oracle E-Business Suite applications operate by setting user profile options to the values you want. You can set user profile options at different levels: site, application, responsibility, user, server, and organization, depending on how the profile options are defined.

See: Defining Preferences with User Profile Options, *Oracle E-Business Suite User's Guide*.

Major Features

Profile Hierarchy

A profile option can be set at one or more levels, depending on its hierarchy type. Most profile options use the *Security* hierarchy type, meaning that they can potentially be set at the four levels: Site (lowest level) , Application, Responsibility, and User (highest level).

Note: A higher-level option value overrides a lower-level value.

Hierarchy Types

Hierarchy types enable system administrators to group and set profile options according to their business needs or the needs of the installation.

There are several hierarchy types: Security, Organization, Server, and Server+Responsibility.

Security

Security is the default hierarchy type. Profiles that use this hierarchy type follow the hierarchy: Site - Application - Responsibility - User.

> **Note:** Most profile options that existed before hierarchy type was introduced use Security.

Organization

Organization refers to operating unit. For example, clerks in different organizations may need to have different values for a given profile option, depending on their organization, but clerks in the same organization would use the same value. The Organization hierarchy type allows system administrators to set a profile option at the organization level, so that all users within that organization will use the profile option value set once at the organization level. Profiles using this hierarchy type follow the hierarchy Site - Organization - User.

Server

The Server hierarchy type is used when the system needs to determine the middle-tier server on which the user's session is running. For example, the profile "Applications Web Agent" can be defined using the Server type. The setting of this profile option can differ for an internal server versus an external one. Cookie validation, can then be done against the value of this profile option. Profiles using this hierarchy type follow the hierarchy Site - Server - User.

Server+Responsibility

The Server+Responsibility hierarchy type allows you to set distinct profile values for specific combinations of server and responsibility. When evaluating profile values to use, the value found with the most specific match across all levels is chosen. At any level, a special default value can be chosen in case no other specific match at that level is found.

Either or both of the responsibility or server may have specific values, or may be the default value. For purposes of evaluating default matches, the server is considered to be at a lower level and less specific than the responsibility.

When evaluating profile values at this Server+Responsibility level, the system first looks for a specific match for both the responsibility and server level values. If no such match is found, it looks for a row matching responsibility and default for the server level. If no such match is found, it will next look for a row matching the server with default for the responsibility level. If no such match is found, it will continue up the hierarchy to the Site level.

The following table describes how the values of a profile using this hierarchy could be set up ("-" indicates default):

Level	Responsibility	Server	Profile Value
Site			A
Server+Responsibility	System Administrator	External	B
Server+Responsibility	-	External	C
Server+Responsibility	-	Internal	D
Server+Responsibility	System Administrator	-	E
Server+Responsibility	General Ledger Superuser	-	F
User	Joe Smith	-	G

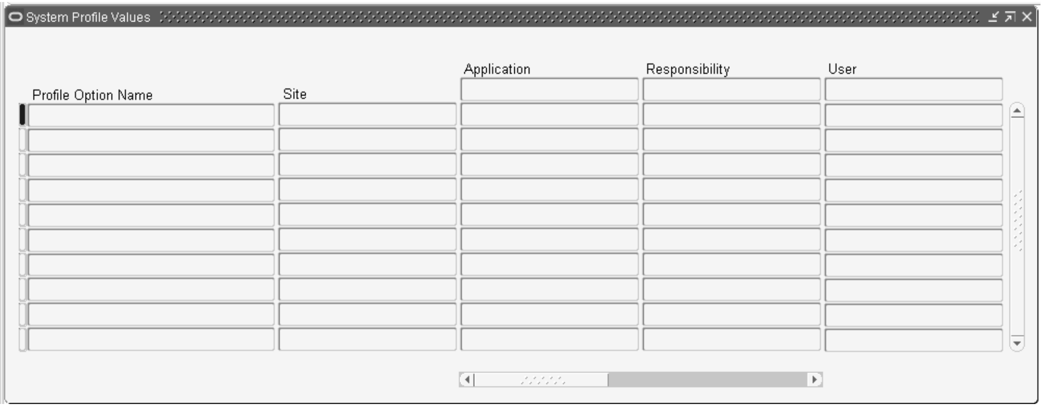
The following table lists the values of the profile that would be used in the given contexts:

Server	Responsibility	User	Profile Value	Explanation
External	System Administrator	Joe Smith	G	User matches.
External	System Administrator	Yali Xu	B	Responsibility plus Server match.
External	Human Resources Manager	Yali Xu	C	Server matches.
Internal	System Administrator	Yali Xu	E	Responsibility matches.
Custom	Human Resources Manager	Yali Xu	A	No match. Use Site level value.

Setting Profile Options

As System Administrator, you can use the Define Profile Values window to set profile options for your user community. If you change a user profile option value, your change takes effect as soon as your users log on again or changes responsibilities.

> **Note:** Profile option values are cached. Setting or unsetting a profile option value raises a cache invalidation business event. When this event is processed, the middle-tier profile cache is invalidated. If this business event takes an unusual amount of time to process, the invalidation might not occur as expected. In this case, the profile option cache can be cleared manually by navigating to Functional Administrator (seeded responsibility) > Core Services > Caching Framework, selecting the cache object 'PROFILE_OPTION_VALUE_CACHE' , and clicking the Clear Cache button.



You can also view how site-level profile options are set using Oracle Applications Manager (Site Map > Monitoring tab).

When you set a user profile, you provide Oracle E-Business Suite with standard information (such as printer) that describes a user, responsibility, application, or site. You can set values for user profile options at each profile level.

For the Security, Organization, and Server hierarchy types, the following describes how option settings are used:

Level	Option Settings
Site	All users at an installation site.

Application	All users of any responsibility associated with the application.
Responsibility	All users currently signed on under the responsibility.
User	An individual user, identified by their application username.
Server	An individual server.
Organization	A particular organization.

The values you set at each level provide runtime values for each user's profile options. An option's runtime value is the highest-level setting for that option.

When a profile option is set at more than one level, Site has the lowest priority, superseded by Application, then Responsibility, with User having the highest priority. A value entered at the Site level may be overridden by values entered at any other level. A value entered at the User level has the highest priority and overrides values entered at any other level.

Example

For example, assume the Printer option is set only at the Site and Responsibility levels. When the user logs on, the Printer option assumes the value set at the Responsibility level, since it is the highest-level setting for the option.

For the Server+Responsibility hierarchy type, option settings pertain to specific combinations of server and responsibility. The system first looks for a specific match for both server and responsibility values. If no such match is found, the system next looks for a profile option value matching responsibility, and with a default value for the server. If no such match is found, the system then looks for a profile option value matching the server, with default value for the responsibility. If no such match is found, the system will continue up the hierarchy to the Site level profile option value.

> **Tip:** As System Administrator, you should set site-level option values before specifying values at the other three levels after the installation of Oracle E-Business Suite. The option values specified at the site-level work as defaults until option values are specified at the other levels.

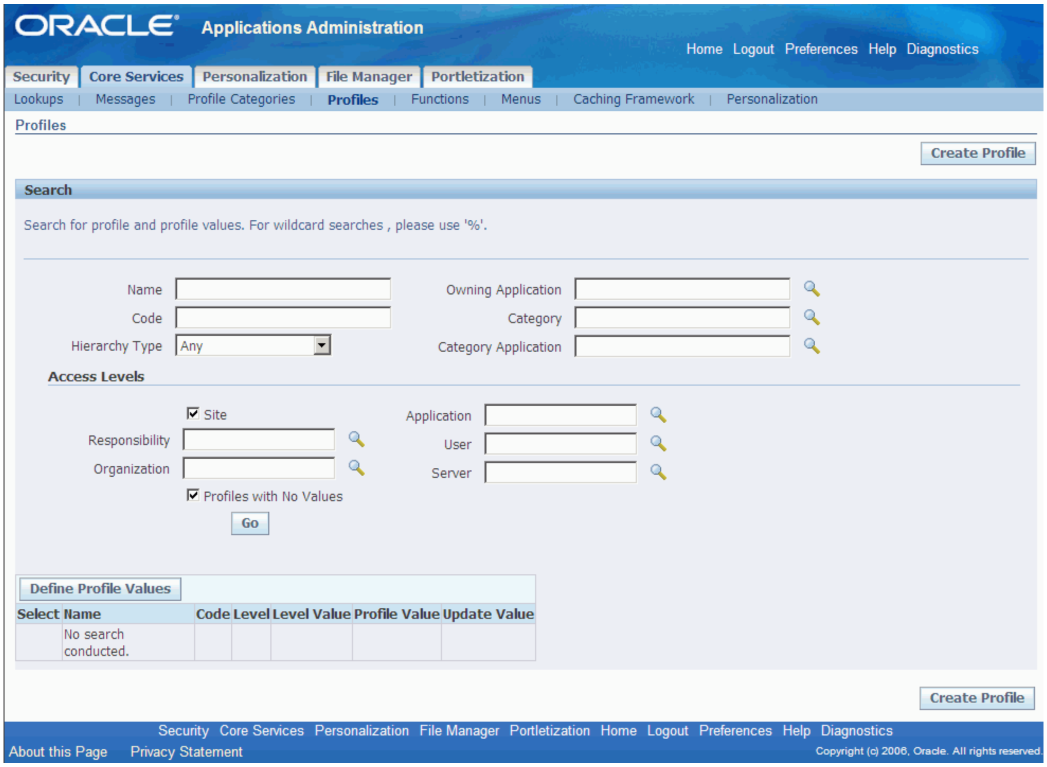
Oracle E-Business Suite users may use the Personal Profile Values window to set their own personal profile options at the user level. Not all profile options are visible to users, and some profile options, while visible, may not be updated by end users.

> **Note:** The display of NULL values has changed from that in previous

releases. In the Personal Profiles window, the default value column no longer displays a NULL value if a NULL value exists in the database. In the Examine window, NULL database values are not shown; the value set at a lower level is shown instead. If there are no non-NULL values set at a particular level, then a message appears stating that no values exist.

HTML-based Profile Pages

You can also use the HTML-based Profile pages to manage your profile values. These pages are available from the Functional Administrator responsibility under Core Services.


ORACLE Applications Administration
Home Logout Preferences Help Diagnostics
Security | Core Services | Personalization | File Manager | Portletization
Lookups | Messages | Profile Categories | Profiles | Functions | Menus | Caching Framework | Personalization
Create Profile
Go
Define Profile Values
Create Profile
Security Core Services Personalization File Manager Portletization Home Logout Preferences Help Diagnostics
About this Page Privacy Statement
Copyright (c) 2006, Oracle. All rights reserved.

Profiles

Search

Search for profile and profile values. For wildcard searches , please use '%'.

Name		Owning Application	
Code		Category	
Hierarchy Type	Any	Category Application	

Access Levels

☑ Site

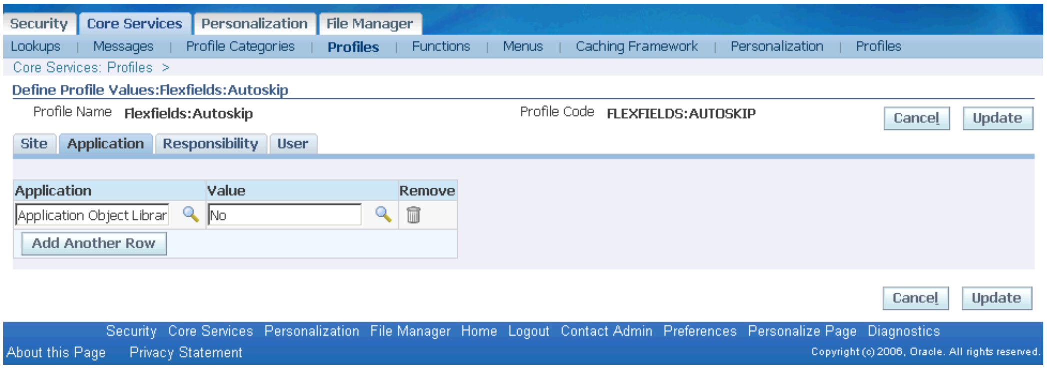
		Application	
Responsibility		User	
Organization		Server	

☑ Profiles with No Values

Select	Name	Code	Level	Level Value	Profile Value	Update Value
	No search conducted.					

The **Site** and **Profiles with No Values** check boxes on the Profiles page are selected by default. Therefore, when a search is performed and a profile option is selected, the system lists the values defined only at site level. To see the values defined at all the levels, uncheck these checkboxes before performing a search and selecting a profile option.

To define a value for a profile option at some level, then select that profile option and click **Define Profile Values**. This will navigate you to the Define Profile Values page where you can add the value for all the relevant levels by navigating through the sub-tabs in that page.


Security
Core Services
Personalization
File Manager
Lookups | Messages | Profile Categories | Profiles | Functions | Menus | Caching Framework | Personalization | Profiles
Core Services: Profiles >
Cancel
Update
Site
Application
Responsibility
User
Add Another Row
Cancel
Update
Security Core Services Personalization File Manager Home Logout Contact Admin Preferences Personalize Page Diagnostics
About this Page Privacy Statement
Copyright (c) 2006, Oracle. All rights reserved.

Define Profile Values:Flexfields:Autoskip

Profile Name Flexfields:Autoskip

Profile Code FLEXFIELDS:AUTOSKIP

Application	Value	Remove
Application Object Librar	No	

Using Profile Options in Other Oracle E-Business Suite Features

Profile option settings may be used as a default value for a concurrent program's parameter or a flexfield's segment in the following forms:

- Concurrent Programs form, Parameters window, Parameter Detail region. See: Concurrent Programs Form, *Oracle E-Business Suite System Administrator's Guide - Configuration*.

- Request Set form, Report Parameters window. See: Defining Request Sets, *Oracle E-Business Suite System Administrator's Guide - Configuration*.

- Key Flexfield Segments form, Segment window, Validation Information region. See: Defaulting Segment Values, *Oracle E-Business Suite Flexfields Guide*.

- Descriptive Flexfield Segments form, Segment window, Validation Information region. See: Defaulting Segment Values, *Oracle E-Business Suite Flexfields Guide*.

To use a profile option's setting as a default value, navigate to the form's Default Type field and select *Profile*. Then, enter the profile option's internal name in the Default Value field.

Profile options can also be used in value set definitions. See: Overview of Values and Value Sets, *Oracle E-Business Suite Flexfields Guide*.

Examples of User Profile Options

Example

Your Accounts Payable department recently purchased a printer, and you want all the reports from that department to print on the new printer. Simply change the Printer profile option for Oracle Payables to reflect the purchase of the new printer.

> **Tip:** This example highlights the importance of default profile options.

If an application user of Oracle Payables or a responsibility associated with Oracle Payables already has a value specified for the printer profile option, that value will override the value you set at the application level. We suggest you first set user profile options at the site level, and then work your way up the hierarchy to other levels when appropriate.

Profile Categories

Profiles can be grouped into categories based on their functional area. Administrators can categorize profiles and then easily search on the profiles by category in the Profiles HTML-based page when they need to view or update them.

The Profiles and Profile Categories HTML-based pages can be accessed from the Functional Administrator and Functional Developer responsibilities. For more information on these, see: Overview of Functional Administrator and Functional Developer Responsibilities, *Oracle E-Business Suite System Administrator's Guide - Configuration*.

Profile Categories Search Page

From the Profiles Categories Search page, you can search based on the following criteria:

- Name
- Code (internal name)
- Application

The search results will list the profile categories that meet your criteria. You can click on a profile category name to view the profile options included in that category, and in turn, click on a profile option name to view and update its definition.

Creating a Profile Category

In creating a profile category, you specify a name, code, owning application, and description. You then add profiles to the category.

After creating a profile category, you can duplicate, update, or delete it.

Exportable Profiles for iSetup

Some profiles in the Applied Technology area are in a product-specific category called "Exportable" (internal name <application short name>_AZ_EXPORTABLE) for Oracle iSetup. To find out which profiles are in such a category, query for the profile category "Exportable" for the given application (for example, "Application Object Library").

User Profile Option Values Report

This report documents user profile option settings. Use this report when defining different profile option values for several responsibilities, or users, or for different applications.

Report Parameters

Profile Option Name

Choose the profile option name whose values you wish to report on. If you do not select a profile option name, then this report will document all profile options.

User Name

Choose the name of a user whose profile option values you wish to report on.

Application Short Name

Choose the name of an application whose profile option values you wish to report on.

Responsibility Name

Choose the name of a responsibility whose profile option values you wish to report on.

Report Headings

The report headings display the specified report parameters and provide you with general information about the contents of the report.

A

Profile Options in Oracle Application Object Library

Profile Options in Oracle Application Object Library

This section lists profile options in Oracle Application Object Library. These profile options are organized according to their functional area and are available to every product in Oracle E-Business Suite. For each profile option, we give a brief overview of how Oracle Application Object Library uses the profile's setting.

Unless otherwise noted, a profile option uses the Security hierarchy type.

A table is provided for most profile options that lists the access levels for the profile option (at which levels the system administrator can set the profile option). For Security profile options, there are four possible levels at which system administrators can view and update a profile option value: site, application, responsibility, and user. This table lists whether the profile option's value is visible at each of these levels, and whether it is updatable at each level.

> **Note:** For information on profile options related to Oracle Application Framework, see My Oracle Support Knowledge Document 1087332.1, *Oracle Application Framework Release Notes, Release 12.1.3*.

ADF Integration

The following profile is used for linking Application Development Framework (ADF) 11*g* applications deployed on an Oracle Application Server 11*g* container from the Oracle E-Business Suite home page. The ADF application should be run on a different middle tier than the Oracle E-Business Suite.

External ADF Application URL

Use this profile to specify the ADF application base URL.

Users can see but not update this profile option.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is FND_EXTERNAL_ADF_URL.

Calendar Support

These profile options are used in supporting non-Gregorian calendars in Oracle Forms-based products.

FND: Calendar Week Start Day

With the Hijrah calendar, users can choose the first day of week in a Date Picker by setting this profile option.

This profile option is visible and updatable on all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is FND_CALENDAR_WEEK_START_DAY.

FND: Forms User Calendar Profile Option

Users can set the FND: Forms User Calendar profile option to their preferred calendar. Valid values are: Arabic Hijrah. English Hijrah , Gregorian and Thai Buddha. By default, the user calendar displays the Gregorian calendar, but if this profile option is set to another value, that calendar is used.

Users can see and update this profile option.

This profile option is visible and updatable on all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is FND_FORMS_USER_CALENDAR.

FND: Tooltip Calendar

In Oracle Forms-based applications, users can set the FND: Tooltip Calendar to a calendar other than the preferred calendar. Within the Date Picker, a given date will be displayed in this calendar's format as a tooltip.

Users can see and update this profile option.

This profile option is visible and updatable on all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is FND_TOOLTIP_CALENDAR.

Concurrent Processing Execution

The internal name for this profile category is FND_CP_EXECUTION.

Concurrent:Active Request Limit

You can limit the number of requests that may be run simultaneously by each user. or for every user at a site. If you do not specify a limit, no limit is imposed.

Users cannot see or update this profile option.

Level	Visible	Allow Update
Site	Yes	Yes
Application	No	No
Responsibility	No	No
User	Yes	Yes

The internal name for this profile option is CONC_REQUEST_LIMIT.

Concurrent:Attach URL

Setting this option to "Yes" causes a URL to be attached to request completion notifications. When a user submits a request, and specifies people to be notified in the Defining Completion Options region, everyone specified is sent a notification when the request completes. If this profile option is set to Yes, a URL is appended to the notification that enables them to view the request results online.

Only the System Administrator can update this profile option.

Users can see but not update this profile option.

This profile options is visible at all levels but can only updated at the Site level.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is CONC_ATTACH_URL.

Concurrent:Conflicts Domain

Specify a conflict domain for your data. A conflict domain identifies the data where two incompatible programs cannot run simultaneously.

Users can see but not update this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is CONC_CD_ID.

Concurrent:Collect Request Statistics

Set this profile option to "Yes" to have statistics for your runtime concurrent processes collected.

To review the statistics you must run the Purge Concurrent Request and/or Manager Data program to process the raw data and have it write the computed statistics to the FND_CONC_STAT_SUMMARY table. You can then retrieve your data from this table using SQL*PLUS or on a report by report basis using the Diagnostics window from the Requests window.

Users cannot see nor change this profile option.

This profile option is visible at all levels but can only be updated at the Site level.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	No
User	Yes	No

The internal name for this profile option is CONC_REQUEST_STAT.

Concurrent:Date Parameter Increment Option

Use this profile to control how date parameters are automatically incremented for concurrent requests. In the Standard Request Submission window, the user can specify if to run a request periodically. The user can then specify that the interval be based on the start date of the requests, or specify the interval using a unit of time and number of units.

If this profile is set to "Start Date" then the date parameters for a given request will be incremented according to the difference between the requested start date of the request and the requested start date of the previous request. If this profile is set to "Resubmit" any date parameters are incremented according to the current request's date parameter and the amount of time represented by the number of units (RESUBMIT_INTERVAL) and the unit of time (RESUBMIT_INTERVAL_UNIT_CODE).

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	No
Responsibility	Yes	No
User	Yes	No

The internal name for this profile option is CONC_DATE_INCREMENT_OPTION.

Concurrent:Hold Requests

You can automatically place your concurrent requests on hold when you submit them.

The default is "No". The concurrent managers run your requests according to the priority and start time specified for each.

Changing this value does not affect requests you have already submitted.

"Yes" means your concurrent requests and reports are automatically placed on hold. To take requests off hold, you:

- Navigate to the Requests window to select a request
- Select the Request Control tabbed region
- Uncheck the Hold check box

Users can see and update this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is CONC_HOLD.

Concurrent:Multiple Time Zones

"Yes" sets the default value to 'Sysdate-1' for the 'Schedules Start Date' used by request submissions. Sysdate-1 ensures that you request is scheduled immediately regardless of which time zone your client session is running in. You should use this profile option when the client's session is running in a different time zone than the concurrent manager's session.

Users cannot see nor change this profile option.

This profile option is visible at all four levels and updatable at the Site level.

Level	Visible	Allow Update
Site	Yes	Yes
Application	No	No
Responsibility	No	No
User	No	No

The internal name for this profile option is CONC_MULTI_TZ.

Concurrent:Print on Warning

Set this profile option to "Yes" if you want concurrent request output to be printed if the requests completes with a status of Warning.

Users can see and update this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is CONC_PRINT_WARNING.

Concurrent:Report Copies

You can set the number of output copies that print for each concurrent request. The default is set to 1.

- Changing this value does not affect requests that you have already submitted.

Users can see and update this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is CONC_COPIES.

Concurrent:Request Priority

This displays the default priority number for your concurrent requests. Only a system administrator can change your request priority.

Requests normally run according to start time, on a "first-submitted, first-run" basis. Priority overrides request start time. A higher priority request starts before an earlier request.

Priorities range from 1 (highest) to 99 (lowest). The standard default is 50.

Users can see this profile option, but they cannot update it.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is CONC_PRIORITY.

Concurrent:Save Output

The Concurrent: Save Output profile is used to determine whether the default behavior of certain concurrent programs should be to save or delete their output files. This only affects concurrent programs that were created in the character mode versions of Oracle E-Business Suite (formerly Oracle Applications) and that have a null value for "Save Output".

- "Yes" saves request outputs.
- Some concurrent requests do not generate an output file.
- If your request output is saved, you can reprint a request. This is useful when requests complete with an Error status, for example, the request runs successfully but a printer malfunctions.
- Changing this value does not affect requests you have already submitted.

Users can see and update this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes

Level	Visible	Allow Update
User	Yes	Yes

The internal name for this profile option is CONC_SAVE_OUTPUT.

Concurrent:Sequential Requests

You can force your requests to run one at a time (sequentially) according to the requests' start dates and times, *or* allow them to run concurrently, when their programs are compatible.

- Concurrent programs are incompatible if simultaneously accessing the same database tables incorrectly affects the values each program retrieves.
- When concurrent programs are defined as incompatible with one another, they cannot run at the same time.

"Yes" prevents your requests from running concurrently. Requests run sequentially in the order they are submitted.

"No" means your requests *can* run concurrently when their concurrent programs are compatible.

Changing this value does not affect requests you have already submitted.

Users can see and update this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is CONC_SINGLE_THREAD.

Concurrent:Wait for Available TM

You can specify the maximum number of seconds that the client will wait for a given transaction manager (TM) to become available before moving on to try a different TM.

Users can see and update this profile option.

This profile option is visible and updatable at the site and application levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	No	No
User	No	No

The internal name for this profile option is CONC_TOKEN_TIMEOUT.

Concurrent Processing File Server

The internal name for this profile category is FND_CP_FILE_SERVER.

RRA:Delete Temporary Files

When using a custom editor to view a concurrent output or log file, the Report Review Agent will make a temporary copy of the file on the client. Set this profile to "Yes" to automatically delete these files when the user exits Oracle E-Business Suite.

Only the System Administrator can update this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is FS_DELETE.

RRA:Enabled

Set this user profile to "Yes" to use the Report Review Agent to access files on concurrent processing nodes.

Only the System Administrator can update this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is FS_ENABLED.

RRA: Service Prefix

Using this new profile option allows you to override the default service name prefix (FNDFS_) assigned to the Report Review Agent. By assigning a new prefix to the Report Review Agent you can avoid having multiple instances of the Applications share executables.

Valid values for this option must be nine characters or less and use only alphanumeric characters or the underscore. We recommend using the underscore character as the last character of your value as in the default value "FNDFS_".

Users cannot see or update this profile option.

This profile option is visible and updatable at the site level only.

Level	Visible	Allow Update
Site	Yes	Yes
Application	No	No
Responsibility	No	No
User	No	No

The internal name for this profile option is FS_SVC_PREFIX.

RRA:Maximum Transfer Size

Specify, in bytes, the maximum allowable size of files transferred by the Report Review Agent, including those downloaded by a user with the "Copy File..." menu option in the Oracle E-Business Suite Report File Viewer and those "temporary" files which are automatically downloaded by custom editors. For example, to set the size to 64K you enter 65536. If this profile is null, there is no size limit.

Only the System Administrator can update this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is FS_MAX_TRANS.

Concurrent Processing Manager

The internal name for this profile category is FND_CP_MANAGER.

Concurrent:Debug Flags

Your Oracle support representative may access this profile option to debug Transaction Managers. Otherwise, it should be set to null.

Users cannot see nor change this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes

Level	Visible	Allow Update
User	Yes	Yes

The internal name for this profile option is CONC_DEBUG.

Concurrent:GSM Enabled

Use this profile option to enable Generic Service Management.

Level	Visible	Allow Update
Site	Yes	Yes
Application	No	No
Responsibility	No	No
User	No	No

The internal name for this profile option is CONC_GSM_ENABLED.

Concurrent:OPP Process Timeout

This profile option specifies the amount of time the manager waits for the OPP to actually process the request.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is CONC_PP_PROCESS_TIMEOUT.

Concurrent:OPP Response Timeout

This profile option specifies the amount of time a manager waits for the OPP to respond to its request for post processing.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is CONC_PP_RESPONSE_TIMEOUT.

Concurrent:PCP Instance Check

This profile option controls whether Parallel Concurrent Processing (PCP) will be sensitive to the state (up or down) of the database instance connected to on each middle-tier node.

When this profile option is set to "OFF", PCP will not provide database instance failover support; however, it will provide middle-tier node failover support when a node goes down.

Level	Visible	Allow Update
Site	Yes	Yes
Application	No	No
Responsibility	No	No
User	No	No

The internal name for this profile option is CP_INSTANCE_CHECK.

Concurrent Processing Submission

The internal name for this profile category is FND_CP_SUBMISSION.

Concurrent:Allow Debugging

This profile option allows debug options to be accessed by the user at submit time.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is FND_CONC_ALLOW_DEBUG.

Concurrent:Enable Request Submission in View Mode

Use this profile option to enable Request Submission in View Requests mode.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is CONC_FNDRSRUN_MODE.

Concurrent:Request Start Time

You can set the date and time that your requests are available to start running.

- If the start date and time is at or before the current date and time, requests are available to run immediately.
- If you want to start a request in the future, for example, at 3:45 pm on June 12, 2002, you enter 2002/06/12 15:45:00 as the profile option value.

> **Important:** You must ensure that this value is in canonical format (YYYY/MM/DD HH24:MI:SS) to use the Multilingual Concurrent Request feature.

- You must include both a date and a time.
- Changing this value does not affect requests that you have already submitted.
- Users can override the start time when they submit requests. Or, this profile option can be left blank and users will be prompted for a start time when they submit requests.

Users can see and update this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is CONC_REQ_START.

Concurrent: Show Requests Summary After Each Request Submission

Using this new profile option, you can choose to either have the Requests Summary displayed each time you submit a request, or retain the request submission screen.

The default is "Yes". "Yes" means the Requests Summary screen is displayed each time you submit a request.

If you choose "No", a decision window is opened asking you if you wish to submit another request. When you choose to submit another request you are returned to the submission window and the window is not cleared, allowing you to easily submit copies of the same request with minor changes.

Users can see and update this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes

Level	Visible	Allow Update
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is CONC_REQ_SUMMARY.

Concurrent:Validate Request Submission

This profile option prompts users in SRS form if no options or parameters have been changed from their defaults.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is CONC_VALIDATE_SUBMISSION.

Printer

You can select the printer which prints your reports. If a printer cannot be selected, contact your system administrator. Printers must be registered with Oracle E-Business Suite.

Users can see and update this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes

Level	Visible	Allow Update
User	Yes	Yes

The internal name for this profile option is PRINTER.

Concurrent Processing View Requests

The internal name for this profile category is FND_CP_VIEW_REQUESTS.

Concurrent:Show Request Set Stages

Set this profile option value to *Yes* to show request set stages in the concurrent request screens.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is CONC_SHOW_STAGES.

Concurrent:URL Lifetime

The numeric value you enter for this profile option determines the length of time in minutes a URL for a request ouput is maintained. After this time period the URL will be deleted from the system. This profile option only affects URLs created for requests where the user has entered values in the notify field of the Submit Request or Submit Request Set windows.

> **Important:** All request ouput URLs are deleted when the Purge Concurrent Requests and Manager... program is run even if the URL liftime has not expired.

Users can see and update this profile option.

This profile option is visible and updatable at the all levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	No
Responsibility	Yes	No
User	Yes	No

The internal name for this profile option is CONC_URL_LIFETIME.

FND: Default Request Days

This profile option specifies the default number of days to view requests.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is FND_DEFAULT_REQUEST_DAYS.

Maximum Page Length

Determines the maximum number of lines per page in a report.

Users can see and update this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes

Level	Visible	Allow Update
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is MAX_PAGE_LENGTH.

Viewer: Application for HTML, PCL, PDF, Postscript, Text, and XML

These profile options determine the applications a user will use to view reports in the given output formats. For example, you could set Viewer: Application for Text to 'application/word' to view a Text report in Microsoft Word.

Valid values are defined by the system administrator in the Viewer Options form.

Users can see and update these profile options.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal names for these profile options are FS_MIME_HTML, FS_MIME_PCL, FS_MIME_PDF, FS_MIME_PS, FS_MIME_TEXT, and FS_MIME_XML.

Viewer:Default Font Size

Using this new profile option, you can set the default font size used when you display report output in the Report Viewer.

The valid values for this option are 6, 8, 10, 12, and 14.

Users can see and update this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is FNDCPVWR_FONT_SIZE.

Viewer: Text

The Viewer: Text profile option allows you to send report output directly to a browser window rather than using the default Report Viewer. Enter "Browser" in this profile option to enable this feature.

Users can see and update the Viewer:Text profile option.

This profile option is both visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is EDITOR_CHAR.

Database

The internal name for this profile category is FND_DATABASE.

Database Instance

Entering a valid two_task connect string allows you to override the default two_task. This profile is specifically designed for use with Oracle Parallel Server, to allow different responsibilities and users to connect to different nodes of the server.

Users can see this profile option, but they cannot update it.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is INSTANCE_PATH.

FND: Resource Consumer Group

Resource consumer groups are used by the Oracle8i Database Resource Manager, which allocates CPU resources among database users and applications. Each form session is assigned to a resource consumer group. The system administrator can assign users to a resource consumer group for all of their forms sessions and transactions. If no resource consumer group is found for a process, the system uses the default group "Default_Consumer_Group".

Users can see this profile option, but they cannot update it.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is FND_RESOURCE_CONSUMER_GROUP.

Two Task

This profile option should be set by AutoConfig. only.

The TWO_TASK for the database. This profile is used in conjunction with the Gateway User ID profile to construct a connect string for use in creating dynamic URLs for the

Web Server. This should be set to the SQL*NET. alias for the database.

> **Note:** The TWO_TASK must be valid on the node upon which the WebServer is running

Users can see and but not update this profile option.

This profile option is visible at all levels but may only be updated at site level.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	No
Responsibility	Yes	No
User	Yes	No

The internal name for this profile option is TWO_TASK.

Debug

The internal name for this profile category is FND_DEBUG.

Account Generator:Debug Mode

This profile option controls Oracle Workflow process modes for the Account Generator feature in flexfields. This profile option should normally be set to "No" to improve performance. If you are testing your Account Generator implementation and using the Oracle Workflow Monitor to see your results, set this profile option to "Yes".

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is ACCOUNT_GENERATOR:DEBUG_MODE.

BIS/AOL:Debug Log Directory

The directory for BIS debugging log files.

Users can see and change this profile option.

System administrators can see and update this profile option at the site level only.

The internal name for this profile option is BIS_DEBUG_LOG_DIRECTORY.

FND: Override Directory

The FND:Override Directory profile option is used by the Work Directory feature. The value of FND: Override Directory should be the directory containing your alternate files. Typically, this profile option should be set at the User level only.

Using the Work Directory and this profile option should be done for debugging only, as they present a security risk.

Users can see but not update this profile option.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is APPLWRK.

Utilities: Diagnostics

Utilities: Diagnostics determines whether a user can automatically use the Diagnostics features. If Utilities:Diagnostics is set to Yes, then users can automatically use these features. Otherwise, certain Diagnostics features will be accessible only if the users have the necessary permissions granted to them. See: Controlling Access to the Oracle Forms-based Applications Diagnostics Menu, *Oracle E-Business Suite System Administrator's Guide - Configuration* for more information.

Users cannot see nor change this profile option.

This profile option is visible and updatable at the all levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is DIAGNOSTICS.

Utilities:SQL Trace

This profile option is used by concurrent processing only. SQL trace files can be generated for individual concurrent programs. The trace can be enabled at the user level by setting the profile "Utilities:SQL Trace" to "Yes". This profile can be enabled for a user only by System Administrator so that it is not accidentally turned on and disk usage can be monitored.

For more information on SQL trace, see the Oracle database documentation.

Users cannot see nor change this profile option.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is SQL_TRACE.

Deployment

The internal name for this profile category is FND_DEPLOYMENT.

Forms Runtime Parameters

Use this profile to specify certain forms runtime parameters. The profile value must be entered in as parameter=value. Each parameter-value pair must be separated by a single space. For example:

record=collect log=/tmp/frd.log debug_messages=yes

In order for the parameters updated in this profile option to go into effect, you must exit and log back in to Oracle E-Business Suite.

Users can see but not update this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is FND_MORE_FORM_PARAMS.

Gateway User ID

Oracle login for gateway account. This should be the same as the environment variable GWYUID. For example, *applsyspub/pub*.

Users cannot see or update this profile option.

This profile option is visible at all levels but can only be updated at the site level.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	No
Responsibility	Yes	No
User	Yes	No

The internal name for this profile option is GWYUID.

Site Name

Site Name identifies an installation of Oracle E-Business Suite. The value of this profile should be set via AutoConfig.

The Site Name appears in the title of the MDI window. If you want additional information on your installation to appear in the title, for example, "Test" or "Production", you can add that information here.

Users cannot see nor change this profile option.

This profile option is visible and updatable at the site level.

Level	Visible	Allow Update
Site	Yes	Yes
Application	No	No
Responsibility	No	No
User	No	No

The internal name for this profile option is SITENAME.

Socket Listener Port

This profile option defines the port number used by the Forms Client Controller.

The default value for this profile option is '6945'.

The E-Business Suite Home page uses the Socket Listener Port profile for launching forms from Framework HTML sessions. With this architecture, a user navigating through different forms/responsibilities in a Framework session will reuse the same Oracle Forms session instead of opening multiple ones. So a user will never have more than one Forms session open on his/her PC at any given time, for a given database.

It is possible to have multiple Oracle Forms sessions open where each is connected to a different database, but the Socket Listener Port profile must be set to a different value beforehand on each database. For example, set it to 6945 on database A, 6946 on database B, and 6947 on database C. This profile option must be set at the site level in advance of any users attempting to use this functionality, as it cannot be set on a per-user basis.

Users can see but not update this profile option.

Level	Visible	Allow Update
Site	Yes	Yes

Level	Visible	Allow Update
Application	No	No
Responsibility	No	No
User	No	No

The internal name for this profile option is SOCKET_LISTENER_PORT.

TCF: HOST

Set this to the name of the host running the TCF Socket Server.

This profile option is visible at all levels and updatable at the site and application level only.

Users can see but not update this profile option.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	No
User	Yes	No

The internal name for this profile option is TCF:HOST.

TCF: PORT

Set this profile option to the port number at which TCF Socket Server accepts connections.

Users can see and but not update this profile option.

This profile option is visible at all levels and updatable at the site and application level only.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	No
User	Yes	No

The internal name for this profile option is TCF:PORT.

Discoverer

The internal name for this profile category is FND_DISCOVERER.

ICX: Discoverer Launcher, Forms Launcher, and Report Launcher

These profile options are used by the Oracle E-Business Suite Personal Homepage.

Set the site level value of each of these profile options to the base URL for launching each application. The profile option value should be sufficient to launch the application, but should not include any additional parameters which may be supplied by the Personal Homepage.

Users can see these profile options, but they cannot update them.

These profile options are visible and updatable at all levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for these profile options are ICX_DISCOVERER_LAUNCHER, ICX_FORMS_LAUNCHER, and ICX_REPORT_LAUNCHER.

Document Sequencing

The internal name for this profile category is FND_DOC_SEQ.

Sequential Numbering

Sequential Numbering assigns numbers to documents created by forms in Oracle financial products. For example, when you are in a form that creates invoices, each invoice document can be numbered sequentially.

Sequential numbering provides a method of checking whether documents have been posted or lost. Not all forms within an application may be selected to support sequential numbering.

Sequential Numbering has the following profile option settings:

Always Used You may not enter a document if no sequence exists for it.

Not Used You may always enter a document.

Partially Used You will be warned, but not prevented from entering a document, when no sequence exists.

Users can see this profile option, but they cannot update it.

This profile option is visible and updatable at the site, application, and responsibility levels.

> **Note:** If you need to control Sequential Numbering for each of your set of books, use the 'Responsibility' level. Otherwise, we recommend that you use either the 'Site' or 'Application' level to set this option.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	No	No

The internal name for this profile option is UNIQUE:SEQ_NUMBERS.

Flexfields

The internal name for this profile category is FND_FLEXFIELDS.

Flexfields:AutoSkip

You can save keystrokes when entering data in your flexfields by automatically skipping to the next segment as soon as you enter a complete valid value into a segment.

- "Yes" means after entering a valid value in a segment, you automatically move to the next segment.
- "No" means after entering a valid value in a segment, you must press [Tab] to go to the next segment.

> **Note:** You may still be required to use tab to leave some segments if the valid value for the segment does not have the same number of characters as the segment. For example, if a segment in the flexfield holds values up to 5 characters and a valid value for the segment is 4 characters, AutoSkip will not move you to the next segment.

Users can see and update this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is FLEXFIELDS:AUTOSKIP.

Flexfields:BiDi Direction

This profile option controls the appearance of the flexfields window in Applications running in Semitic languages. Possible values are "Left To Right" and "Right To Left".

Users can see and update this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is FLEXFIELDS:BIDI_DIRECTION.

Flexfields:Open Descr Window

You can control whether a descriptive flexfield window automatically opens when you navigate to a customized descriptive flexfield.

- "Yes" means that the descriptive flexfield window automatically opens when you navigate to a customized descriptive flexfield.
- "No" means that when you navigate to a customized descriptive flexfield, you must choose **Edit Field** from the Edit menu or use the List of Values to open the descriptive flexfield window.

Users can see and update this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is FLEXFIELDS:OPEN_DESCR_WINDOW.

> **Note:** This profile option does not apply to descriptive flexfields in folders.

Flexfields:Open Key Window

You can control whether a key flexfield window automatically opens when you navigate to a key flexfield.

- "Yes" means that the key flexfield window automatically opens when you navigate to a key flexfield.
- "No" means that when you navigate to a key flexfield, you must choose **Edit Field** from the Edit menu or use the List of Values to open the key flexfield window.

Users can see and update this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is FLEXFIELDS:OPEN_KEY_WINDOW.

Flexfields:Shorthand Entry

If shorthand flexfield entry is defined for your flexfield, you can use a shorthand alias to automatically fill in values for some or all of the segments in a flexfield.

Not Enabled Shorthand Entry is not available for any flexfields for this user, regardless of whether shorthand aliases are defined.

New Entries Only Shorthand Entry is available for entering new records in most foreign key forms. It is not available for combinations forms, updating existing records, or entering queries.

Query and New Entry Shorthand Entry is available for entering new records or for entering queries. It is not available for updating existing records.

All Entries Shorthand Entry is available for entering new records or updating old records. It is not available for entering queries.

Always	Shorthand Entry is available for inserting, updating, or querying flexfields for which shorthand aliases are defined.

Users can see and update this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is FLEXFIELDS:SHORTHAND_ENTRY.

Flexfields:Show Full Value

If an alias defines valid values for *all* of the segments in a flexfield, and Flexfields: Shorthand Entry is enabled, when you enter the alias the flexfield window does not appear.

"Yes" displays the full flexfield window with the cursor resting on the last segment.

Users can see and update this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is FLEXFIELDS:SHOW_FULL_VALUE.

Flexfields:Validate On Server

This profile option is set to "Yes" to enable server side, PL/SQL flexfields validation for

Key Flexfields. This improves performance when using Key Flexfields over a wide area network by reducing the number of network round trips needed to validate the entered segment combinations.

You may find, however, that your validation's performance is better with client side validation. In this case, set this profile option to "No".

Users can see and update this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is FLEXFIELDS:VALIDATE_ON_SERVER.

Folders

The internal name for this profile category is FND_FOLDERS.

Folders:Allow Customization

Your system administrator controls whether you can create or customize a folder definition layout in folder block.

- "Yes" means that you can create or customize a folder definition, that is, the entire Folder menu is enabled in the folder block.
- "No" means that you can only open an existing folder definition in a folder block, that is, only the Open option is enabled in the Folder menu.

Users can see this profile option, but they cannot update it.

Level	Visible	Allow Update
Site	No	No
Application	No	No

Level	Visible	Allow Update
Responsibility	No	No
User	Yes	Yes

The internal name for this profile option is FLEXVIEW:CUSTOMIZATION.

Forms UI

The internal name for this profile category is FND_FORMS_UI.

Flexfields:LOV Warning Limit

Use Flexfields:LOV Warning Limit to improve efficiency when retrieving a list of values.

Sometimes, particularly when no reduction criteria has been specified, an LOV can take a very long time to run if there is a very significant amount of data in it. Set this profile option to the number of rows to be returned before the user is asked whether to continue retrieving the entire list.

Users can see and update this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is QUICKPICK_ROWS_BEFORE_WARN.

FND: Enable Cancel Query

Oracle E-Business Suite allows end users to cancel certain long-running queries, such as retrieving data in a block. When these operations exceed a threshold of time, approximately ten seconds, a dialog will display that allows the user to cancel the query.

Set the FND: Enable Cancel Query profile option to Yes if you wish to enable the ability to cancel a form query. This profile option may be set at the site, application, responsibility or the user level.

Users can see but not update this profile option.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is FND_ENABLE_CANCEL_QUERY.

FND: Indicator Colors

The default for this profile option is null, which means "Yes." When this profile option is set to Yes:

- Required fields are displayed in yellow.
- Queryable fields are displayed in a different color while in enter-query mode.
- Fields that cannot be entered (read-only) are rendered in dark gray.

Users can see and update this profile option.

Level	Visible	Allow Update
Site	No	No
Application	No	No
Responsibility	No	No
User	Yes	Yes

The internal name for this profile option is FND_INDICATOR_COLORS.

Forms Keyboard Mapping File

Use this profile option to define the path of the Keyboard Mapping File.

The "Keys" window displays the keystrokes to perform standard Forms operations, such as "Next Block" and "Clear Record." This window can be viewed at anytime by pressing Ctrl+k. The keyboard mappings can be customized as follows:

- The System Administrator must locate the Oracle Forms resource file on the middle tier, typically called fmrweb.res.
- Make a copy of the file, name it as desired, and locate it in the same directory as the original
- Open the new file in any text editor and make the desired keystroke mapping changes. Comments at the top of the file explain how the mappings are performed.
- To run the new mapping file, specify the complete path and file name in this profile option.

Users can see and update this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is FND_FORMS_TERM.

Indicate Attachments

This profile option allows you to turn off indication of attachments when querying records (for performance reasons).

Users can see and update this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is ATCHMT_SET_INDICATOR.

Java Color Scheme

If the Java Look and Feel profile option is set to Oracle, the Java Color Scheme can be specified as follows:

- Swan (default)
- Teal
- Titanium
- Red
- Khaki
- Blue
- Olive
- Purple

The Java Color Scheme profile has no effect if the Java Look and Feel is set to Generic.

> **Important:** Setting the Java Color Scheme profile option to a value other than 'swan' (the default value) can have a considerable impact on forms user response time performance.
>
> For some users, setting this profile option to a value other than 'swan' may be desirable for accessibility reasons. See: Oracle E-Business Suite Accessibility Features, *Oracle E-Business Suite User's Guide* and "Accessibility in Oracle Forms Applications" at http://www.oracle.com/accessibility/apps02.html.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is FND_COLOR_SCHEME.

Java Look and Feel

Oracle E-Business Suite Professional User Interface (Forms-based applications) can be run with either the Oracle Look and Feel or the Generic Look and Feel. The Oracle Look and Feel consists of a new look and feel for each item, and a predefined set of color schemes. The Generic Look and Feel adheres to the native interface and color scheme of the current operating system.

To specify the look and feel set this profile to "generic" or "oracle".

If the Oracle Look and Feel is used, the profile Java Color Scheme can be set. The Java Color Scheme profile has no effect if the Java Look and Feel is set to Generic.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is FND_LOOK_AND_FEEL.

Framework Logging and Alerting

The internal name for this profile category is FND_FWK_LOGGING_ALERTING.

FND: Log Filename for Middle-Tier

The file name for the file to hold debugging messages used in the Logging Service. If the value of this profile option is null, then the Logging Service is turned off.

Users can see but not update this profile option.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is AFLOG_FILENAME.

FND: Log Level

The Logging Service can filter out debugging messages depending on their priority level.. There are five levels of the Debug/Trace Service:. In order from highest priority to lowest priority, they are: Errors, Exceptions, Events, Procedures, and Statements. The Debug Log Level is the lowest level that the user wants to see messages for.. The possible profile option values are Null (which means off), and the five priority levels above. For instance, if the "FND: Debug Log Level" profile is set to "EVENT", then the file will get the messages that the programmer had marked as "EVENT", "EXCEPTION", or "ERROR".

Users can see but not update this profile option.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is AFLOG_LEVEL.

FND: Log Module

The Logging Service can filter out debugging messages depending on their module.

Module names are unique across applications and coding languages. If a module is specified for this profile option, then only messages for that module will be written to the log file. If this profile option is left blank then messages for all modules will be written to the log file.

Users can see but not update this profile option.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is AFLOG_MODULE.

Help System

The internal name for this profile category is FND_IHELP.

Applications Help Web Agent

Applications Help Web Agent is optional and should only be used if you want to launch online help on a web server different from the one specified by the Applications Servlet Agent.

> **Important:** For most installations, this profile should be set to NULL. Only specify a value if you want to use a different web server than that for the Applications Servlet Agent.

Specify the entire online help URL for this profile's value.

If this profile option is not set, the online help tree navigator will default to starting up at the host name and port number that is specified by the Applications Servlet Agent profile option. The DBC file used will be that of the database where online help was invoked.

Users can see this profile option, but they cannot update it.

This profile option is visible and updatable at all levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is HELP_WEB_AGENT.

Help Localization Code

This code determines which localized context-sensitive help files a user accesses.

Users can see this profile option, but they cannot update it.

This profile option is visible and updatable at the responsibility and user levels.

Level	Visible	Allow Update
Site	No	No
Application	No	No
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is HELP_LOCALIZATION_CODE.

Help Tree Root

This profile option determines which tree is shown in the navigation frame when context-sensitive help is launched.

If Help Tree Root is set to "null" or "NULL" (case insensitive), then the online help is launched in a single frame, without the navigation and search features.

Users can see this profile option, but they cannot update it.

This profile option is visible and updatable at all levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is HELP_TREE_ROOT.

Help Utility Download Path

Use this profile option to define the directory into which the Help Utility downloads help files from the Oracle E-Business Suite Help System.

Users can see this profile option, but they cannot update it.

This profile option is visible and updatable at all levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is HELP_UTIL_DL_PATH.

Help Utility Upload Path

Use this profile option to define the directory from which the Help Utility uploads help files to the Oracle E-Business Suite Help System.

Users can see this profile option, but they cannot update it.

This profile option is visible and updatable at all levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is HELP_UTIL_UL_PATH.

Multi Organization Setup

The internal name for this profile category is FND_MULTI_ORG.

MO:Operating Unit

In Multiple Organization installations, Oracle E-Business Suite uses the profile option MO: Operating Unit to link an operating unit to a responsibility. You must set this profile option for each responsibility. For more information on setting this profile option, see: *Multiple Organizations in Oracle E-Business Suite*.

Users can see but not update this profile option.

This profile option is visible and updatable at the responsibility level only.

Level	Visible	Allow Update
Site	No	No
Application	No	No
Responsibility	Yes	Yes
User	No	No

The internal name for this profile option is ORG_ID.

NLS

The internal name for this profile category is FND_NLS.

Currency:Mixed Precision

Use Mixed Currency Precision to specify how many spaces are available to the right of the decimal point when displaying numbers representing different currencies.

- Normally, currency numbers are right-justified.
- Each currency has its own precision value that is the number of digits displayed to the right of a decimal point. For U.S. dollars the precision default is 2, so an example display is 345.*70*.
- Set Mixed Currency Precision to be equal to or greater than the *maximum* precision value of the currencies you are displaying.

  For example, if you are reporting on rows displaying U.S. dollars (precision=2), Japanese yen (precision=0), and Bahraini dinar (precision=3), set Mixed Currency Precision=3.

> **Note:** The Currency profile options pertain to currency only, not to other numeric fields.

Users can see and update this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is CURRENCY:MIXED_PRECISION.

Currency:Negative Format

You can use different formats to identify negative currency. The default identifier is a hyphen (-) preceding the currency amount, as in "-xxx". You can also select:

Angle brackets < > < xxx >

Trailing hyphen - xxx -

Parentheses ( ) (xxx)

Square Brackets [ ] [xxx]

> **Note:** The Currency profile options pertain to currency only, not to other numeric fields.

Users can see and update this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is CURRENCY:NEGATIVE_FORMAT.

> **Note:** Currency:Negative Format only affects the display of currency values . Non-currency negative numbers appear with a preceding hyphen regardless of the option selected here.

Currency:Positive Format

You can use different formats to identify positive currency values. The default condition is no special identifier.

> **Note:** The Currency profile options pertain to currency only, not to other numeric fields.

Users can see and update this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes

Level	Visible	Allow Update
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is CURRENCY:POSITIVE_FORMAT.

Currency:Thousands Separator

You can separate your currency amounts in thousands by placing a thousands separator. For example, one million appears as 1,000,000.

Users can see and update this profile option.

> **Note:** The Currency profile options pertain to currency only, not to other numeric fields.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is CURRENCY:THOUSANDS_SEPARATOR.

Default Country

This is the default source for the Country field for all address zones and is used by the Flexible Address Formats feature, the Flexible Bank Structures feature and the Tax Registration Number and Taxpayer ID validation routines.

The profile can be set to any valid country listed in the Maintain Countries and Territories form and can be set to a different value for each user.

Users can see and update this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is DEFAULT_COUNTRY.

FND: Native Client Encoding

FND: Native Client Encoding indicates the character set that a client machine uses as its native character set. The value must be one of the Oracle character sets and should correspond to the client native character set. The character set used in a client machine varies depending on language and platform. For example, if a user uses a Windows machine with Japanese, the value should be JA16SJIS. But if a user uses a Solaris machine with Japanese, the value should be JA16EUC. The value is normally set in the user level since each user uses different machine, but it can be set in every level for a default value.

This profile option is used when storing text data. When a user uploads text files as attachments, the current value of FND: Native Client Encoding is stored along with the text data. With the value of this profile option, the server can then convert the text data to another character set as necessary when the text data is downloaded.

Users can see and update this profile option.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is FND_NATIVE_CLIENT_ENCODING.

ICX: HTML directory

This profile is used by some applications to construct URLs for certain pages. It is usually set to 'OA_HTML'.

Users can see but not update the profile value.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is ICX_OA_HTML.

ICX: Preferred Currency

This profile determines in which currency a user will see the currency number in the UI.

For example, the source currency number might be stored in database such as 10.00 as US Dollar (USD), but the displayed currency number is based on the currency set in this profile option such as 1,200 as Japanese Yen (JPY). In this multi-currency conversion, USD is source currency and JPY is the profile option value.

This profile option is for currency display purpose especially for self-service type applications.

This profile option is a generic preference that a user can set through the Oracle Application Framework Preferences page. The profile option value is used across Oracle E-Business Suite so that the user sees currency numbers in all applications based on the currency chosen.

The currencies must be set up through the Oracle General Ledger application properly (the following must be set properly: Enabled/Disabled, Active Date and Exchange ratio between currencies). Proper setup ensures that the currency chosen is available in the system, and the currency number can be converted from the source (functional) currency to the target currency (the currency chosen by a user as this profile option value) with the specified exchange ratio. This profile option is tightly linked to GL currency setup. For more information, see: Defining Currencies, *Oracle General Ledger User's Guide*.

Users can see and update this profile option.

Level	Visible	Allow Update
Site	Yes	Yes
Application	No	No
Responsibility	No	No
User	Yes	Yes

The internal name for this profile option is ICX_PREFERRED_CURRENCY.

Server Timezone

The time zone of the database server.

Users can see this profile option, but they cannot update it.

Level	Visible	Allow Update
Site	Yes	Yes
Application	No	No
Responsibility	No	No
User	No	No

The internal name for this profile option is SERVER_TIMEZONE_ID.

Personalization

The internal name for this profile category is FND_PERSONALIZATION.

Initialization SQL Statement - Custom

This profile option allows you to add site-specific initialization code (such as optimizer settings) that will be executed at database session initialization. The value of this profile option must be a valid SQL statement.

The system administrator may set this profile option at any level.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is FND_INIT_SQL.

Security

The internal name for this profile category is FND_SECURITY.

AuditTrail:Activate

You can turn AuditTrail on or off (Yes or No). The default setting is No (Off).

When you enter or update data in your forms, you change the database tables underlying the forms you see and use.

AuditTrail tracks which rows in a database table(s) were updated at what time and which user was logged in using the form(s).

- Several updates can be tracked, establishing a trail of audit data that documents the database table changes.
- AuditTrail is a feature enabled on a form-by-form basis by a developer using Oracle's Application Object Library.
- All the forms that support AuditTrail are referred to as an *audit set*.
- Not all forms may be enabled to support AuditTrail.
- To enable or disable AuditTrail for a particular form, you need access to Oracle Application Object Library's Application Developer responsibility.

Users cannot see nor change this profile option.

This profile option is visible and updatable at the site and application levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	No	No
User	No	No

The internal name for this profile option is AUDITTRAIL:ACTIVATE.

Enable Security Groups

This profile option is used by the Security Groups feature, which is used by HRMS security only. For more information on Security Groups, see the Oracle HRMS documentation.

The possible values are 'None' (N), and 'Service Bureau' (Y).

Only the System Administrator can update this profile option.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	No	No
User	No	No

The internal name for this profile option is ENABLE_SECURITY_GROUPS.

Hide Diagnostics Menu Entry

This profile option determines whether users can access the Diagnostics menu entry from the Help menu. The default value is Yes, with the Diagnostics menu entry is hidden. If it is set to No, the Diagnostics menu entry is visible.

Users cannot see nor change this profile option.

This profile option is visible and updatable at the all levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is FND_HIDE_DIAGNOSTICS.

ICX: Limit time

This profile option determines the absolute maximum duration (in hours) of a user's session, regardless of activity.

Users cannot see or update this profile option.

Level	Visible	Allow Update
Site	Yes	Yes
Application	No	No
Responsibility	No	No
User	Yes	Yes

The internal name for this profile option is ICX_LIMIT_TIME.

ICX: Session Timeout

This profile option determines the length of time (in minutes) of inactivity in a user's session before the session is disabled. If the user does not perform any operation in Oracle E-Business Suite for longer than this value, the session is disabled. The user is provided the opportunity to re-authenticate and re-enable a timed-out session. If re-authentication is successful, the session is re-enabled and no work is lost. Otherwise, Oracle E-Business Suite ends the session without saving pending work.

If this profile option to 0 or NULL, then user sessions will never time out due to inactivity.

Users can see this profile option, but they cannot update it.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is ICX_SESSION_TIMEOUT.

Node Trust Level

Determines the level of trust assigned to a Web server. This profile option uses the Server hierarchy type. This profile option is used in conjunction with the profile option Responsibility Trust Level. For more information on using these profile options, see: Restricting Access to Responsibilities Based on User's Web Server, *Oracle E-Business Suite System Administrator's Guide - Configuration*.

Users can see but not update this profile option.

This profile option is visible and updatable at the site and server level only.

Level	Visible	Allow Update
Site	Yes	Yes
Server	Yes	Yes
User	No	No

The internal name for this profile option is NODE_TRUST_LEVEL.

Responsibility Trust Level

Responsibilities or applications with the specified level of trust can only be accessed by an application server with at least the same level of trust.

This profile option is used in conjunction with the profile option Node Trust Level. For more information on using these profile options, see: Restricting Access to Responsibilities Based on User's Web Server, *Oracle E-Business Suite System Administrator's Guide - Configuration*.

Users can see this profile option, but they cannot update it.

The system administrator access is described in the following table:

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	No	No

The internal name for this profile option is APPL_SERVER_TRUST_LEVEL.

Sign-On:Audit Level

Sign-On:Audit Level allows you to select a level at which to audit users who log in to Oracle E-Business Suite. Four audit levels increase in functionality: None, User, Responsibility, and Form.

None is the default value, and means do not audit any users who log in to Oracle E-Business Suite.

Auditing at the User level tracks:

- who signs on to your system
- the times users log on and off

Auditing at the Responsibility level performs the User level audit functions and tracks:

- the responsibilities users choose
- how much time users spend using each responsibility

Auditing at the Form level performs the Responsibility level audit functions and tracks:

- the forms users choose
- how long users spend using each form
- System Administrator visible, updatable at all levels.

Users cannot see nor change this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is SIGNONAUDIT:LEVEL.

Sign-On:Notification

"Yes" displays a message at login that indicates:

- If any concurrent requests failed since your last session,
- How many times someone tried to log in to Oracle E-Business Suite with your username but an incorrect password, and
- When the default printer identified in your user profile is unregistered or not specified.

Users can see and update this profile option.

This profile option is visible and updatable at all four levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is SIGNONAUDIT:NOTIFY.

Signon Password Case

Oracle E-Business Suite gives you the ability to control case sensitivity in user passwords through this profile option. This profile has two possible settings:

- Sensitive - Passwords are stored and compared as they are, with the password case preserved. During validation, the entered password must match the decrypted version otherwise an error message is displayed. With Release 12, this option is the default behavior. All newly created or changed passwords are treated as case sensitive.

  > **Note:** Users who have not changed their passwords since the installation of Release 12 are not affected until they do change their passwords.

  A password expiration utility is available if the System Administrator requires that all users convert to case sensitive passwords upon the next login. This utility expires all passwords in FND_USER, including that of SYSADMIN and default Vision accounts, and can be run as a SQL Script ($FND_TOP/sql/AFCPEXPIRE.sql) or as a Concurrent Program (FNDCPEXPIRE_SQLPLUS).

- Insensitive (or unset) - Passwords are treated as case insensitive. In Insensitive mode, passwords are stored and compared in uppercase, similar to that in earlier releases. During validation, the entered password and the decrypted password are compared in uppercase. If the passwords do not match, an error is displayed.

Users can see but not update this profile option.

Level	Visible	Allow Update
Site	Yes	Yes
Application	No	No
Responsibility	No	No
User	No	No

The internal name for this profile option is SIGNON_PASSWORD_CASE.

Signon Password Custom

This profile specifies the full name of the class containing custom password validation logic.

Users can see but not update this profile option.

Level	Visible	Allow Update
Site	Yes	Yes
Application	No	No
Responsibility	No	No
User	Yes	Yes

The internal name for this profile option is SIGNON_PASSWORD_CUSTOM.

Signon Password Failure Limit

The Signon Password Failure Limit profile option determines the maximum number of login attempts before the user's account is disabled.

Users cannot see or update this profile option.

Level	Visible	Allow Update
Site	Yes	Yes
Application	No	No
Responsibility	No	No
User	Yes	Yes

The internal name for this profile option is SIGNON_PASSWORD_FAILURE_LIMIT.

Signon Password Hard to Guess

The Signon Password Hard to Guess profile option sets rules for choosing passwords to ensure that they will be "hard to guess." A password is considered hard-to-guess if it follows these rules:

- The password contains at least one letter and at least one number.
- The password does not contain the username.
- The password does not contain repeating characters.

Users can see but not update this profile option.

Level	Visible	Allow Update
Site	Yes	Yes
Application	No	No
Responsibility	No	No
User	Yes	Yes

The internal name for this profile option is SIGNON_PASSWORD_HARD_TO_GUESS.

Signon Password Length

Signon Password Length sets the minimum length of an Applications signon password. If no value is entered the minimum length defaults to 5.

Users can see but not update this profile option.

Level	Visible	Allow Update
Site	Yes	Yes
Application	No	No
Responsibility	No	No
User	Yes	Yes

The internal name for this profile option is SIGNON_PASSWORD_LENGTH.

Signon Password No Reuse

This profile option specifies the number of days that a user must wait before being allowed to reuse a password.

Users can see but not update this profile option.

Level	Visible	Allow Update
Site	Yes	Yes

Level	Visible	Allow Update
Application	No	No
Responsibility	No	No
User	Yes	Yes

The internal name for this profile option is SIGNON_PASSWORD_NO_REUSE.

Single Sign-On Account Settings

The internal name for this profile category is FND_SSO_ACCOUNT_SETTINGS.

ICX: Client IANA Encoding

This profile option is used to determine the character set of text displayed by Java Server pages. The value is the code set of the middle tier. It is used to allow the online help system to support languages other than American English. The default setting is the Western European character set (ISO-8859-1).

This profile option should be set only at the site level.

> **Important:** This profile option must not be set to NULL at the site level.

Users can see this profile option, but they cannot update it.

This profile option is visible and updatable at the all levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is ICX_CLIENT_IANA_ENCODING.

Web Server Deployment

The internal name for this profile category is FND_WS_DEPLOYMENT.

Applications Servlet Agent

This profile option must be set to the URL base for the servlet execution engine on Apache. Oracle E-Business Suite uses the value of this profile option to construct URLs for JSP and SERVLET type functions. The syntax is:

```
https://<hostname>:<port>/<servlet_zone>
```

Example:

```
https://ap523sun.us.oracle.com:8888/oa_servlets
```

Users can see this profile option, but they cannot update it.

This profile option is visible and updatable at all levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	Yes	Yes
Responsibility	Yes	Yes
User	Yes	Yes

The internal name for this profile option is APPS_SERVLET_AGENT.

Applications Web Agent

Provides the base URL for the Applications Schema's WebServer DAD. You set this profile option during the install process.

This profile option is visible and updatable at all levels.

Level	Visible	Allow Update
Site	Yes	Yes
Application	No	No

Level	Visible	Allow Update
Responsibility	No	No
User	Yes	Yes

The internal name for this profile option is APPS_WEB_AGENT.

B

Using Predefined Alerts

Overview of Oracle Alert

Oracle Alert is your complete exception control solution.

Oracle Alert gives you an immediate view of the critical activity in your database. It helps you keep on top of important or unusual business events you need to know about, as they happen. Oracle Alert gives you real-time measurements of staff and organization performance, so you can zero in on potential trouble spots immediately. You can automate routine transactions with Oracle Alert, saving your valuable time for more essential tasks. And, Oracle Alert does all this online, so you do not have to contend with a pile of paperwork.

Oracle Alert gives you the flexibility you need to monitor your business information the way you want.

For more information on Oracle Alert, see the *Oracle Alert User's Guide.*

Basic Business Needs

Oracle Alert meets the following basic business needs:

- Informs you of exception conditions as they occur
- Lets you specify the exception conditions you want to know about, as often as you want to know about them
- Informs you of exception conditions by sending alert messages through a single application -- your electronic mail
- Takes actions you specify, based upon your response to an alert message
- Automatically performs routine database tasks, according to a schedule you define
- Integrates fully with your electronic mail system

Oracle Alert Runtime Features

If you do not have a licensed copy of the full Oracle Alert product, you may still derive benefit from major Oracle Alert features by using the predefined alerts that are packaged with your Oracle E-Business Suite product.

All Oracle E-Business Suite products are packaged with a runtime version of Oracle Alert. Although all the Oracle Alert windows are available in this runtime version, not all the features in those windows are enabled. With the runtime version of Oracle Alert, you can run only the predefined alerts that are packaged with your product; you cannot create new alerts.

Alert Definitions

Alert

A mechanism that checks your database for a specific exception condition. An alert is characterized by the *SQL SELECT statement* it contains. A SQL SELECT statement tells your application what database exception to identify, as well as what output to produce for that exception.

For example, you can define an alert to flag purchase orders exceeding $10,000, and have that alert output the name of the individual who requested the purchase order, as well as the name of the individual's manager. All predefined alerts are listed in the Alerts window of Oracle Alert.

Event Alert

An event alert monitors the occurrence of a specific exception or change in your database. An exception in your database results if you add or update information using your Oracle E-Business Suite windows. The event alert monitors the database for exceptions based on its SQL SELECT statement.

Periodic Alert

A periodic alert periodically reports key information according to a schedule that you define. Rather than notify you of immediate exceptions in the database like an event alert, a periodic alert scans for specific database information specified by its SQL SELECT statement at scheduled intervals.

Alert Action

An alert action is an action you want your alert to perform. An alert action can be dependent on the output from the alert. An alert action can fall under one of three categories:

- Detail action-an action that represents one exception found in the database

- Summary action-an action that represents multiple exceptions found in the database

- No exception action-an action that represents no exceptions found in the database

An action can include sending an electronic mail message to a mail ID, running an Oracle E-Business Suite program, running a program or script from your operating system, or running a SQL script to modify information in your database.

You can have more than one action for an alert and an action can incorporate the output of the alert. For example, you may want a particular alert to send a message to a manager, as well as run an Oracle E-Business Suite program when an exception occurs.

Action Sets

An action set is a sequence of alert actions that are enabled for a particular alert. Each action that you include in an action set can be assigned a sequence number so that you can specify the order in which the actions are performed. Some predefined alerts may also have more than one action set. You can also assign a sequence number to each action set to specify the order in which each action set is performed.

Predefined Alerts

There are two types of predefined alerts:

- **Event alerts**-for example, the Receiving Notification alert for Oracle Purchasing notifies the requestor with a mail message when an item is received and entered in the Receipts window.

- **Periodic alerts**-for example, the Forecast Over-Consumption alert for Oracle Material Planning checks every day for over-consumption of the forecast and sends you a mail message if the current forecast quantity listed in the Forecast Entries window goes below zero.

> **Tip:** See your product's reference guide for a list of the predefined alerts that are packaged with your Oracle E-Business Suite product.

Using Predefined Alerts

All predefined alerts are initially disabled. You must enable the alerts you want to use. Select the Oracle Alert Manager responsibility when you start Oracle E-Business Suite to view or use a predefined alert. The Alert Manager responsibility gives you access to the Oracle Alert menu.

Navigate to the Alerts window to enable or edit predefined alerts. To display the predefined alert(s) for your Oracle E-Business Suite product, execute a query with your Oracle E-Business Suite product name in the Application field.

The Name field displays the name of the predefined alert. The Type field indicates if the alert is an event or a periodic alert.

You can enable an alert to run by checking the Enabled check box. You can also enter an End Date to specify the date until you want this alert run.

Choose the Alert Details button to open the Alert Details window. Choose the Alert Installations tabbed region to display the available Installations.

Enter the Oracle ID of the application installation you want your alert to run against. You can select only the Oracle IDs that are associated with the application that owns your alert. You can disable an Oracle ID for the alert temporarily by unchecking the Enabled check box.

Choose the Actions button to open the Actions window. Oracle Alert automatically displays the actions that are defined for the alert.

In the Actions window, if the Action Type is Detail, choose the Action Details button to display details for that action.

The alert action sends an alert action message to the mail ID listed in the To field of the Message Detail zone. If the mail ID is in the format ***&NAME***, where ***Name*** is an output defined by your alert, you need not modify this field. If, however, the mail ID in the To field is not in the above format or if there is no value entered in the field, you must enter the mail ID(s) of the person(s) you wish to receive the alert action message. After modifying the contents of this window, save your work.

Navigate to the Oracle Alert Options window. Use this window to define the options Oracle Alert uses when checking your alerts.

In the Alerts window, choose the Actions Sets button to navigate to the Action Sets window. Oracle Alert automatically displays the action sets defined for the alert.

Check the Enabled check box for each action set you wish to use. You may also enter an End Date field to specify the date until you want this alert action set to be enabled.

In addition, in the Action Set Members block, check the Enabled check box for each action set member you want to use in that action set.

You may also enter an End Date to specify the date until you want this alert action set member to be enabled. When you finish, save your work.

Your predefined alert is now ready to use.

Customizing Predefined Alerts

You can customize predefined alerts in the following ways to suit your business needs:

Electronic Mail Integration

Oracle Alert leverages the Workflow Notification Mailer to send alert e-mail messages to your users. Ensure that you set up mail servers and configure the Workflow Notification Mailer to send e-mail messages according to your alert requirements. See:

Setting Up Notification Mailers, *Oracle Workflow Administrator's Guide*.

Standard Alert Message Text

You can customize the message header and footer text that appears in all your alert message actions. Navigate to the Message Elements tabbed region of the Oracle Alert Options window, and four message elements appear automatically. Each element represents a specific type of message text that appears in all your alert mail messages.

In the runtime version of Oracle Alert, you need to edit only the Message Action Header and Message Action Footer elements. Simply customize the text that appears to alter the text at the beginning and end of every alert message. You may also leave the text blank if you do not want to display any standard text in your alert messages. Save your work when you are done making changes in this window.

Alert Frequency

You can schedule the frequency you wish to run each predefined periodic alert. You may want to check some alerts every day, some only once a month, still others only when you explicitly request them. You have the flexibility to monitor critical exceptions every day, or even multiple times during a 24-hour period. And, you can set less significant exceptions to a more infrequent schedule; for example, a monthly schedule.

To change the frequency of a predefined alert, navigate to the Alerts window. Perform a query to display the predefined periodic alert you wish to modify, then alter the Frequency of the periodic alert.

Alert History

Oracle Alert can keep a history of exceptions and actions for a particular alert. Use the Alerts window to alter the number of days of history you wish to keep for an alert. Simply change the Keep N Days field to the number of days of history you wish to keep.

Suppressing Duplicates

If you do not want Oracle Alert to send repeated messages for the same alert exception, you can choose to suppress duplicate messages. If Oracle Alert finds a duplicate exception condition for the alert, it simply does not execute the action set members for that alert again.

Use the Suppress Duplicates check box in the Action Sets block of the Alerts window to specify this option. The default for the Suppress Duplicates check box is unchecked. If you check the Suppress Duplicates check box, you must also make sure you keep history for the alert at least one day longer than the number of days between alert checks. Oracle Alert uses the history information to determine if an exception is a duplicate.

Message Actions

If a predefined alert involves a message action, you can customize certain aspects of that message action. Navigate to the Actions block in the Alerts window by choosing the Actions button. In this block, move your cursor to the row representing the message action you want to customize, then choose the Action Details button to open the Action Detail window for that message action. You can modify the following features of the message action:

- Recipient list-you can add or delete mail IDs in the List, To, Cc, Bcc, or Print For User fields. You should not modify any mail IDs listed with the format ***&Name***, as they represent mail ID's defined by the alert output.

- Printer-you can modify the name of the printer to which you want Oracle Alert to direct the message.

- Text-you can modify the boilerplate text that you want your alert message to send. Do not edit any of the alert outputs (in the format ***&Name***) used in the body of the text. For summary messages, edit only the opening and closing text within the summary message. Save your work when you finish making modifications.

Summary Threshold

Predefined alerts use one of three action types: detail action, summary action, and no exception action. A no exception action is straightforward in that Oracle Alert performs the defined action when no exceptions are found for the alert.

But how does Oracle Alert know when to perform a detail or a summary action? Oracle Alert can perform a detail action for every exception it finds, regardless of the number of exceptions, or Oracle Alert can perform a summary action for a unique set of exceptions. For example, you can receive individual mail messages for each exception found by an alert, or you can receive a single mail message summarizing all the exceptions found by the alert.

In the Members tabbed region of the Action Sets block of the Alerts window, you can set a Summary Threshold to specify how many exceptions Oracle Alert can find before it should change the action from a detail action to a summary action.

Oracle Alert Precoded Alerts

Your Oracle Alert installation contains custom alerts that are designed to help you manage your database and the data you generate when you use Oracle Alert. Oracle Alert provides eight alerts that systematically monitor your system for potential tablespace, disk space, and allocation problems, making your Database Administrators more efficient, and increasing database performance.

Occasionally, you will want to purge your database of obsolete concurrent requests, alert checks, and action set checks. Oracle Alert provides two alerts that let you periodically remove old files, freeing up valuable tablespace and increasing database performance.

This section gives you an overview of these alerts, and suggestions on how to use them to enhance your system performance.

Terms

Before reading this discussion of precoded alerts, you may want to familiarize yourself with the following Glossary terms:

- Periodic Alert
- Exception
- Action
- Detail Action
- Summary Action
- No Exception Action
- Input

Oracle Alert DBA Alerts

Oracle Alert DBA alerts help you manage your database by notifying you regularly of:

- Tables and indexes unable to allocate another extent
- Users who are nearing their tablespace quota
- Tablespaces without adequate free space
- Tables and indexes that are too large or are fragmented
- Tables and indexes that are near their maximum extents

Customizable Alert Frequencies

Oracle Alert DBA alerts are periodic alerts, so you determine how often they check your database. Set them to run daily, weekly, or monthly, according to your database needs.

Summary and No Exception Messages

If Oracle Alert finds the database exceptions specified in a DBA alert, it sends you a message summarizing all exceptions found. If Oracle Alert finds no exceptions, it sends you a message reporting that no exceptions were found. Oracle Alert keeps you notified of the status of your database, even if it is unchanging.

Customizable Alert Inputs

Inputs let you customize your DBA alerts. You can specify the ORACLE username, table, or index you want your alerts to target, and you can specify the threshold number of extents, maximum extents, or blocks Oracle Alert should look for. You can also define your input values at the action set level, so you can create multiple action sets that target different usernames, tables, and indexes. You can create as many action sets as you need.

Support for Multiple Database Instances

The Applications DBA application owns the Oracle Alert DBA alerts. This lets Oracle Alert perform the DBA alerts for every database instance you create, even those that reside outside Oracle Alert's database.

Applications DBA Alerts Descriptions

The following descriptions list the customizable frequency and inputs of each DBA alert.

Tables Unable to Allocate Another Extent

This alert looks for tables where the next extent is larger than the largest free extent.

Frequency	Every N Calendar Days
Inputs	Table Name, ORACLE Username

Indexes Unable to Allocate Another Extent

This alert looks for indexes where the next extent is larger than the largest free extent.

Frequency	Every N Calendar Days
Inputs	Index Name, ORACLE Username

Users Near Their Tablespace Quota

This alert detects users that are near their tablespace quota.

Frequency	Every N Calendar Days
Inputs	ORACLE Username Tablespace Name Check minimum percent free space remaining

Check maximum percent space use

Minimum total free space remaining (in bytes)

Maximum percent space used

Tablespaces Without Adequate Free Space

This alert looks for tablespaces without a specified minimum amount of free space.

Frequency	Every N Calendar Days
Inputs	Tablespace Name Check total free space remaining Check maximum size of free extents available Maximum size of free extents available (in bytes) Minimum total free space remaining (in bytes)

Indexes Too Large or Fragmented

This alert detects indexes that exceed a specified number of blocks or extents.

Frequency	Every N Calendar Days
Inputs	Index Name ORACLE Username Check maximum number of blocks Check maximum number of extents Maximum number of blocks Maximum number of extents

Tables Too Large or Fragmented

This alert detects tables that exceed a specified number of blocks or extents.

Frequency	Every N Calendar Days
Inputs	Table Name ORACLE Username Check maximum number of blocks Check maximum number of extents Maximum number of blocks

	Maximum number of extents

Tables Near Maximum Extents

This alert searches for tables and indexes that are within a specified number of extents of their maximum extents.

Frequency	Every N Calendar Days
Inputs	Table Name ORACLE Username Minimum number of extents remaining

Indexes Near Maximum Extents

This alert searches for tables and indexes that are within a specified number of extents of their maximum extents.

Frequency	Every N Calendar Days
Inputs	Index Name ORACLE Username Minimum number of extents remaining

Oracle Alert Purging Alerts

Two of the Oracle Alert precoded alerts are designed to help you manage the data you generate when you use Oracle Alert. While using Oracle Alert you should be able to:

- Automatically delete concurrent requests older than a specified number of days
- Automatically clean out alert checks and action set checks that are older than a specified number of days

Customizable Alert Frequencies

You determine the schedule for running your purge alerts. On the schedule you define, Oracle Alert submits the purge alerts to the Concurrent Manager, and deletes all old concurrent requests.

Customizable Alert Inputs

Inputs let you customize your alerts. You specify which application and which concurrent program you want your purge alerts to target, and you decide when your data becomes unnecessary or "old." You define your input values at the action set level, so you can create multiple action sets that target different applications and different concurrent programs. You can create as many action sets as you need, so you can keep your system free from unnecessary files.

Oracle Alert Purging Alerts Descriptions

The following descriptions list the customizable frequency and inputs of each purging alert.

Purge Alert and Action Set Checks

This alert looks for alert and action set checks older than the number of days you specify, and runs a SQL statement script that deletes them.

Alert Type	Periodic
Periodicity	Every N Calendar Days
Inputs	Application Name, Number of days since alert check

> **Note:** Oracle Alert will not delete alert checks and/or action set checks for a response processing alert that has open responses.

Purge Concurrent Requests

This alert looks for concurrent requests and their log and out files that are older than the number of days you specify, and runs a concurrent program that deletes them. If you enter a concurrent program name input, you should use the program name (located in the column USER_CONCURRENT_PROGRAM_NAME in the table FND_CONCURRENT_REQUESTS), and not the optional description that may accompany the concurrent program name in the Requests window.

Alert Type	Periodic
Periodicity	Every N Calendar Days
Inputs	Application Name Concurrent Program Name Number of days since concurrent request was submitted to the Concurrent Manager
Operating System Program	Deletes log file, out file, and corresponding record of each concurrent request
Arguments	Concurrent request ID

Index