



BEA WebLogic Integration™

Using Worklist Console

Copyright

Copyright © 1995-2006 BEA Systems, Inc. All Rights Reserved.

Restricted Rights Legend

This software is protected by copyright, and may be protected by patent laws. No copying or other use of this software is permitted unless you have entered into a license agreement with BEA authorizing such use. This document is protected by copyright and may not be copied photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form, in whole or in part, without prior consent, in writing, from BEA Systems, Inc.

Information in this document is subject to change without notice and does not represent a commitment on the part of BEA Systems. THE DOCUMENTATION IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. FURTHER, BEA SYSTEMS DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS REGARDING THE USE, OR THE RESULTS OF THE USE, OF THE DOCUMENT IN TERMS OF CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE.

Trademarks and Service Marks

Copyright © 1995-2006 BEA Systems, Inc. All Rights Reserved. BEA, BEA JRocket, BEA WebLogic Portal, BEA WebLogic Server, BEA WebLogic Workshop, Built on BEA, Jolt, JoltBeans, SteelThread, Top End, Tuxedo, and WebLogic are registered trademarks of BEA Systems, Inc. BEA AquaLogic, BEA AquaLogic Data Services Platform, BEA AquaLogic Enterprise Security, BEA AquaLogic Interaction, BEA AquaLogic Interaction Analytics, BEA AquaLogic Interaction Collaboration, BEA AquaLogic Interaction Content Services, BEA AquaLogic Interaction Data Services, BEA AquaLogic Interaction Integration Services, BEA AquaLogic Interaction Process, BEA AquaLogic Interaction Publisher, BEA AquaLogic Interaction Studio, BEA AquaLogic Service Bus, BEA AquaLogic Service Registry, BEA Builder, BEA Campaign Manager for WebLogic, BEA eLink, BEA Kodo, BEA Liquid Data for WebLogic, BEA Manager, BEA MessageQ, BEA SALT, BEA Service Architecture Leveraging Tuxedo, BEA WebLogic Commerce Server, BEA WebLogic Communications Platform, BEA WebLogic Enterprise, BEA WebLogic Enterprise Platform, BEA WebLogic Enterprise Security, BEA WebLogic Express, BEA WebLogic Integration, BEA WebLogic Java Adapter for Mainframe, BEA WebLogic JDriver, BEA WebLogic Log Central, BEA WebLogic Mobility Server, BEA WebLogic Network Gatekeeper, BEA WebLogic Personalization Server, BEA WebLogic Personal Messaging API, BEA WebLogic Platform, BEA WebLogic Portlets for Groupware Integration, BEA WebLogic Real Time, BEA WebLogic RFID Compliance Express, BEA WebLogic RFID Edge Server, BEA WebLogic RFID Enterprise Server, BEA WebLogic Server Process Edition, BEA WebLogic SIP Server, BEA WebLogic WorkGroup Edition, BEA Workshop for WebLogic Platform, BEA Workshop JSP, BEA Workshop JSP Editor, BEA Workshop Struts, BEA Workshop Studio, Dev2Dev, Liquid Computing, and Think Liquid are trademarks of BEA Systems, Inc. Accelerated Knowledge Transfer, AKT, BEA Mission Critical Support, BEA Mission Critical Support Continuum, and BEA SOA Self Assessment are service marks of BEA Systems, Inc.

All other names and marks are property of their respective owners.

Contents

1. Introducing Worklist Console

| | |
|---------------------------------|-----|
| Starting Worklist Console | 1-3 |
|---------------------------------|-----|

2. Worklist Administration

| | |
|--|------|
| Overview of the Worklist Module | 2-1 |
| Security Policies | 2-4 |
| Protected Resources | 2-5 |
| Explicit Security Policies | 2-5 |
| Implicit Security Policies | 2-8 |
| Operations and Policies | 2-9 |
| User-experience for Defining Policies | 2-14 |
| Defining Policies within WebLogic Server Default Security Provider | 2-15 |
| Defining Policies within Third-Party Security Providers | 2-20 |
| Out-of-box Security Policies | 2-21 |
| Default Security Policies | 2-23 |
| Listing and Locating Worklist System Instances | 2-25 |
| Managing Sessions | 2-27 |
| About Worklist Event Handlers and Event Types | 2-28 |
| Changing the Worklist System Instance Configuration | 2-30 |
| Setting the Global Worklist System Instance Policies | 2-32 |
| Setting the Worklist System Instance Policies | 2-34 |
| Setting the Global Task Plan Policies | 2-34 |

| | |
|--|------|
| Setting the Task Plan Policies | 2-36 |
| Purging Tasks | 2-37 |
| Listing and Locating Event Handlers | 2-37 |
| Changing the Event Handler Details | 2-39 |
| Listing and Locating Event Subscriptions | 2-41 |
| Adding Event Subscriptions | 2-42 |
| Changing Event Subscriptions | 2-45 |
| Deleting Event Subscriptions | 2-48 |
| Viewing Task Plan Details | 2-49 |
| Changing Task Plan Details | 2-50 |
| Listing and Locating Worklist Tasks | 2-54 |
| Constructing a Custom Query for Task Instances | 2-56 |
| Viewing and Changing Task Details | 2-60 |
| Updating Task State | 2-64 |
| Claiming a Task for a User | 2-67 |
| Assigning a Task to User or Group | 2-67 |
| Deleting Tasks | 2-69 |
| Managing User Profiles | 2-69 |
| Setting the E-mail Address of a User | 2-70 |
| Reassigning Work to a User | 2-71 |
| Listing and Locating Work Substitute Rules | 2-72 |
| Adding a Work Substitute Rule | 2-73 |
| Changing a Work Substitute Rule | 2-75 |
| Deleting a Work Substitute Rule | 2-77 |

3. User Management

| | |
|---|-----|
| Overview of the User Management Module | 3-2 |
| WebLogic Integration Users, Groups, and Roles | 3-3 |

| | |
|--|------|
| Default Roles and Groups | 3-4 |
| Security Provider Requirements for User Management | 3-7 |
| Listing and Locating Users | 3-7 |
| Adding a User | 3-8 |
| Viewing and Changing User Properties | 3-10 |
| Listing and Locating Groups | 3-12 |
| Adding a Group | 3-13 |
| Viewing and Changing Group Properties | 3-14 |
| Listing and Locating Roles | 3-16 |
| Adding a Role | 3-17 |
| Constructing a Role Statement | 3-18 |
| Adding Conditions to a Role Statement | 3-19 |
| Modifying the Role Statement | 3-26 |
| Viewing and Changing Role Conditions | 3-27 |
| Deleting Users, Groups, or Roles | 3-28 |

4. Business Calendar Configuration

| | |
|---|------|
| About Business Calendars and Business Time Calculations | 4-2 |
| Overview of the Business Calendar Module | 4-4 |
| Listing and Locating Business Calendars | 4-5 |
| Adding a Business Calendar | 4-6 |
| Viewing and Changing Business Calendars | 4-7 |
| Defining a Time Period Rule | 4-11 |
| Associating Business Calendars with Users | 4-14 |
| Exporting and Importing Business Calendars | 4-15 |
| Deleting Business Calendars | 4-17 |

Introducing Worklist Console

Worklist Console allows you to manage and monitor Worklist tasks, users, and the business calendar.

Worklist Console provides a navigation menu containing several modules for performing focused operations. The following table lists the modules available in Worklist Console and summarizes the tasks associated with each of those modules.

For information about task plans and tasks, creating and managing tasks, using Worklist controls, using the Worklist IDE, using the Worklist User Portal and so on, see [Using the Worklist](#).

| Module | Associated Tasks |
|---------------|---|
| Worklist | <ul style="list-style-type: none">Overview of the Worklist ModuleListing and Locating Worklist System InstancesManaging SessionsChanging the Worklist System Instance ConfigurationSetting the Global Worklist System Instance PoliciesSetting the Worklist System Instance PoliciesSetting the Global Task Plan PoliciesSetting the Task Plan PoliciesPurging TasksListing and Locating Event HandlersChanging the Event Handler DetailsListing and Locating Event SubscriptionsAdding Event SubscriptionsChanging Event SubscriptionsDeleting Event Subscriptions <hr/> <ul style="list-style-type: none">Viewing Task Plan DetailsChanging Task Plan DetailsListing and Locating Worklist TasksConstructing a Custom Query for Task InstancesViewing and Changing Task DetailsUpdating Task StateClaiming a Task for a UserAssigning a Task to User or GroupDeleting TasksManaging User ProfilesSetting the E-mail Address of a UserReassigning Work to a UserListing and Locating Work Substitute RulesAdding a Work Substitute RuleChanging a Work Substitute RuleDeleting a Work Substitute Rule |

| Module | Associated Tasks |
|-------------------|--|
| Worklist User | Overview of the User Management Module WebLogic Integration Users, Groups, and Roles Security Provider Requirements for User Management Listing and Locating Users Adding a User Viewing and Changing User Properties Listing and Locating Groups Adding a Group Viewing and Changing Group Properties Listing and Locating Roles Adding a Role Constructing a Role Statement Viewing and Changing Role Conditions Deleting Users, Groups, or Roles |
| Business Calendar | About Business Calendars and Business Time Calculations Overview of the Business Calendar Module Listing and Locating Business Calendars Adding a Business Calendar Viewing and Changing Business Calendars Defining a Time Period Rule Associating Business Calendars with Users Exporting and Importing Business Calendars Deleting Business Calendars |

Starting Worklist Console

Access to Worklist Console is password protected.

To start Worklist Console:

1. Open the following URL in your Web browser:

```
http://host name:port/worklistconsole
```

Here, *host name* is the host name or IP address of the WebLogic Server administrative server, and *port* is the server listening port.

2. Enter the username and password when prompted.

Note: To log into Worklist Console, you must be a valid WebLogic Server user. However, the actions that you can do and the information that you can see depends upon your security policy. For more information, see [“WebLogic Integration Users, Groups, and Roles” on page 3-3](#). For the sample integration domain, the default login details are:
username: weblogic
password: weblogic

The Worklist Console home page is displayed.

Worklist Administration

This section provides information you need to use the *Worklist* module in Worklist Console to:

- Understand security policies and the Worklist resources governed by those policies
- View and change Worklist system instances.
- Set global Worklist system and individual Worklist system; global task plan and individual task plan policies.
- Manage event handlers and event subscriptions.
- View and change task plans.
- View summary or detailed task status in order to monitor the progress of task completion against due dates.
- Perform queries to show individual workload.
- Reassign tasks in order to speed progress.
- Change task properties such as state or due date.
- Control task routing by creating or changing the work substitute rules.

Overview of the Worklist Module

The following table lists the pages you can access from the Worklist module. The tasks and help topics associated with each are provided:

| Page | Associated Tasks | Help Topics |
|---------------------------|---|---|
| Worklist System Instances | Viewing all the Worklist system instances. | “Listing and Locating Worklist System Instances” on page 2-25 |
| | Setting global worklist policy | “Setting the Global Worklist System Instance Policies” on page 2-32 |
| | Setting global task plan policy | “Setting the Global Task Plan Policies” on page 2-34 |
| | Manually purging tasks | “Purging Tasks” on page 2-37 |
| | Managing sessions | “Managing Sessions” on page 2-27 |
| | Viewing tasks | “Listing and Locating Worklist Tasks” on page 2-54 |
| Worklist System Instance | Changing the Worklist system instance details | “Changing the Worklist System Instance Configuration” on page 2-30 |
| | Viewing the tasks associated with the Worklist system instance. | “Listing and Locating Worklist Tasks” on page 2-54 |
| | Managing event handlers | “Listing and Locating Event Handlers” on page 2-37 |
| | Setting the policy of the selected Worklist system instance. | “Setting the Worklist System Instance Policies” on page 2-34 |
| | Managing sessions | “Managing Sessions” on page 2-27 |

| Page | Associated Tasks | Help Topics |
|------------------------|---|---|
| Worklist Tasks Summary | Viewing a list of task instances. Task plan ID, name, description, working and administrative state, name of current step, task completion due date, claimant, owner, and priority are displayed. | “Listing and Locating Worklist Tasks” on page 2-54 |
| | Updating the state of the task, or deleting the task. | “Updating Task State” on page 2-64 |
| | Constructing a custom query using properties such as task ID, description, due dates, and so on. | “Constructing a Custom Query for Task Instances” on page 2-56 |
| | Claiming the task for a user | “Claiming a Task for a User” on page 2-67 |
| | Assigning the task to selected users and / or group. | “Assigning a Task to User or Group” on page 2-67 |
| Worklist Task Details | Viewing and changing task instance properties. | “Viewing and Changing Task Details” on page 2-60 |
| | Updating the state of the task, or deleting the task. | “Updating Task State” on page 2-64 |
| | Claiming the task for a user. | “Claiming a Task for a User” on page 2-67 |
| | Assigning the task to selected users and / or group. | “Assigning a Task to User or Group” on page 2-67 |
| Worklist User Summary | Viewing a list of all users. | “Managing User Profiles” on page 2-69 |
| | Associating a business calendar with the selected user. | “Associating Business Calendars with Users” on page 4-14 |
| | Setting e-mail address of a user. | “Setting the E-mail Address of a User” on page 2-70 |
| | Reassigning work of the selected user to any other user either temporarily or permanently. | “Reassigning Work to a User” on page 2-71 |

| Page | Associated Tasks | Help Topics |
|-------------------------------|---|---|
| Work Substitute Routing Table | Viewing the list of work substitute rules. Rule name, effective date, expiration date, source, and target are displayed. | “Listing and Locating Work Substitute Rules” on page 2-72 |
| | Defining the name, effective date, expiration date, source, and target for a new work substitute rule. | “Adding a Work Substitute Rule” on page 2-73 |
| | Deleting a subscription rule. | “Deleting a Work Substitute Rule” on page 2-77 |
| | Changing the effective date, expiration date, source, or target for an existing work substitute rule. | “Changing a Work Substitute Rule” on page 2-75 |
| Task Plan Details | Setting task plan policy. You can view and edit the task plan details including the task plan summary details, task plan policies, user-defined properties, and task steps | “Changing Task Plan Details” on page 2-50 |

Security Policies

Worklist uses several types of policies to control access to certain global operations. You can define policies for the administration, creation, update, and retrieval of tasks. These policies can be defined for Worklist system instances and task plans (both global level and individual level).

You can provide authorization against tasks or Worklist system instances in a more granular way to allow access to the resource based on your business needs for security. For example, some types of tasks may require that a user be granted a specific role in order to create a task. Users granted this role may not be candidates for holding more global and powerful roles such as IntegrationAdmin. In such a scenario, you can set the per-task plan policy to grant appropriate privileges to work with a specific task plan without necessarily or inadvertently granting access to a wider range of resources.

In addition to the security policies that are explicitly defined for a role, there are certain implicit policies that are based on the user’s task affinity (for example, task owner, claimant, assignee, and so on).

Protected Resources

Worklist security protects access to the following resources:

- Worklist System Facilities - represented by `WorklistSystemResource`
- Tasks - represented by a `TaskPlanResource` for the type of the task.

For the types of operations that are protected for these resources, see [“Operations and Policies” on page 2-9](#).

Explicit Security Policies

Explicit policies explicitly define which roles a user must be granted in order to perform operations on the resource. The explicit policies are:

- **Admin** - Policy granting access to admin functions on a resource.
- **Create** - Policy granting access to create new instances of a resource.
- **Update** - Policy granting access to update or modify business-level properties of a resource.
- **Query** - Policy granting access to read properties of a resource or perform queries for instances of a resource.

In Worklist, security policies can be set for global and individual Worklist system instance; and global and individual task plans.

Note: When a specific resource (Worklist system instance or task plan) does not have a defined security policy it inherits the global policy for the resource. However, if the resource defines an explicit security policy, the global policy for the resource is ignored.

The following table lists the various security policies that can be explicitly set. When used with the default WebLogic Server authorization provider these policies are defined as a list of role names. Users granted any of the roles listed in the policy are authorized to perform the type of operation associated with the policy.

| Policy | Resource Type | Type of Operations |
|---------------|--------------------------|--|
| Admin | Task Plan | A user granted any one of these roles is authorized to perform any administrative action on tasks of this type. |
| | Task Plan (Global) | A user granted any one of these roles is authorized to perform any administrative action on any task. This includes tasks for which its associated task plan defines a specific administrative policy. |
| | Worklist System | A user granted any one of these roles is authorized to perform any administrative action on the given Worklist system instance. For example, the user can set purge intervals, report data stores, and so on. |
| | Worklist System (Global) | A user granted any one of these roles is authorized to perform any administrative action on any Worklist system instance. This includes Worklist system instances that do define a specific administrative policy. |
| Create | Task Plan | A user granted any one of these roles is authorized to create and perform any initial assignment for properties of tasks of this type. |
| | Task Plan (Global) | A user granted any one of these roles is authorized to create instances of any task plan that does not define a specific create policy. |
| | Worklist System | A user granted any one of these roles is authorized to create new configuration within this Worklist system instance. |
| | Worklist System (Global) | A user granted any one of these roles is authorized to create new configuration within any Worklist system instance that does not define a specific create policy. |

| Policy | Resource Type | Type of Operations |
|---------------|--------------------------|---|
| Update | Task Plan | A user granted any one of these roles is authorized to update the business-related, non-administrative information for the task. Examples of business-related information would be the task completion due date or task time estimates. Examples of administrative information would be the owner and task plan for the task. |
| | Task Plan (Global) | A user granted any one of these roles is authorized to update business-related information for any task for which its task plan does not define a specific update policy. |
| | Worklist System | A user granted any one of these roles is authorized to update business-related, non-administrative information for the Worklist System. For example, a user granted update privileges on a task plan could set the comment or properties for any task of that type. |
| | Worklist System (Global) | A user granted any one of these roles is authorized to update business related information within any Worklist system instance that does not define a specific update policy. |
| Query | Task Plan | A user granted any one of these roles is authorized to query for and view information about any task of this type. By contrast, a user not granted this privilege (or admin/update privileges either) must have a special affinity to a task in order to query information about it (i.e. the user must be the owner, creator, assignee or claimant for the task). Note that this policy does not authorize users to make changes to the information in a task. |
| | Task Plan (Global) | A user granted any one of these roles is authorized to query any task for which its task plan does not define a specific query policy. |
| | Worklist System | A user granted any one of these roles is authorized to query information for this Worklist system instance. |
| | Worklist System (Global) | A user granted any one of these roles is authorized to query information for any Worklist system instance that does not define a specific query policy. |

Implicit Security Policies

Tasks represent work items to be carried out by one or more human actors. Human actors may be associated with a task in the following ways. An actor's association with a task is called the actor's affinity to the task. The possible types of task affinity are:

- **Creator** – The actor who created the task.
- **Owner** – The actor responsible for the overall completion of the task. A task ordinarily is owned by the same owner throughout its lifetime.
- **Assignee** – One or more actors, or groups of actors who are candidates for claiming and eventually working on the task. To assign a task is like offering the task to its assignees to be claimed by a single claimant. Tasks often are assigned more than once during their lifetimes (though this is not required).
- **Claimant** – The single actor who is responsible for working on the task at its current step. Tasks often have many different claimants during their lifetimes.

The association between a task and human actors can be very dynamic. This makes it impossible to define an appropriate security policy that can take into account all the users that may eventually be associated with a task. To account for this, Worklist uses task affinity (current user associations with a task, for example Owner, Claimant, or Assignees) to make access control decisions. The following table lists the implicit security policies.

A given task affinity is granted a fixed set of privileges to perform operations on the tasks for which that affinity applies. So, each type of task affinity represents an implicit security policy. They are implicit because administrators do not need to define them explicitly in order for them to take effect.

The following table lists the implicit security policies.

| Policy | Description |
|----------|---|
| Claimant | Claimants are granted special privileges allowing them to perform user operations on tasks they claim. These operations include task update and query. |
| Owner | Owners are granted administrative privileges on the tasks they own. These privileges include the ability to perform administrative actions, task update, and query. |

| Policy | Description |
|---------------|---|
| Creator | Creators are granted query privileges on the tasks they created. |
| Assignee | Users on the assignee list for a task are authorized to query and claim tasks for which they are an assignee. |

Operations and Policies

The following table lists all the possible operations, as defined in the API, that can be performed on a given type of resource (via the Worklist API), and the policy that is consulted before allowing a user to perform the operation.

Notes: The operations listed for TaskPlan resources may exist on any one of the `WorklistTaskAdmin`, `WorklistTaskUser`, and `WorklistTaskQuery` interfaces.

Table 2-1 Operations and policies on a resource

| Resource | Operation | Policy |
|----------------|--|--|
| WorklistSystem | purgeTasks | Admin |
| | set<Configuration Property> (via WorklistSystemMBean) | WebLogic Server Admin Role (not Worklist policy based) |
| | get<Configuration Property> (via WorklistSystemMBean) | WebLogic Server Admin Role (not Worklist policy based) |
| | addWorkSubstituteRules removeWorkSubstituteRules updateWorkSubstituteRules | Global Admin, Global Update. See, “Out-of-box Security Policies” on page 2-21. |
| | getAllWorkSubstituteRules / getWorkSubstitute* | Global Admin, Global Update, Global Query. See, “Out-of-box Security Policies” on page 2-21. |
| | setGlobalWorklistSystemPolicy | Global Admin See, “Out-of-box Security Policies” on page 2-21. |
| | getGlobalWorklistSystemPolicy | Global Admin, Global Query, Global Update. See, “Out-of-box Security Policies” on page 2-21. |
| | setWorklistSystemPolicy | Admin |
| WorklistSystem | getWorklistSystemPolicy | Admin, Query, Update |

Table 2-1 Operations and policies on a resource

| Resource | Operation | Policy |
|----------------------|---|--|
| TaskPlanRegistry | registerTaskPlan, deregisterTaskPlan | WorklistSystem Admin, WorklistSystem Create |
| | getTaskPlan | Task Plan Admin, Task Plan Create, Task Plan Query, Task Plan Update |
| | getHostApplicationNames | <Everyone> |
| | getRootFolders | |
| | getSubFolders | |
| | getTaskPlanIds | Task Plan Admin, Task Plan Create, Task Plan Query, Task Plan Update (if no access is permitted for a task plan, it is omitted from the returned list of task plans) |
| getTaskPlansInFolder | Task Plan Admin, Task Plan Create, Task Plan Query, Task Plan Update (if no access is permitted for a task plan, it is omitted from the returned list of task plans for the folder) | |

Table 2-1 Operations and policies on a resource

| Resource | Operation | Policy |
|-----------------|--|--|
| TaskPlan | constructTask | Create |
| | setTaskProperties(<public property set>) | Admin, Update, Owner, Claimant |
| | takeActionOnTask | Admin, Owner, Claimant |
| | setTaskComment | Admin, Update, Owner, Claimant |
| | assignTask | Admin, Owner |
| | getCandidateUsers (with task instance) | Admin, Owner, Claimant |
| | getCandidateUsers (with task plan) | Admin, Create |
| | getUserWorkloadInfo (with task instance) | Admin, Owner, Claimant |
| | getUserWorkloadInfo (with task plan) | Admin, Create |
| | getUserAvailabilityInfoForPeriod | Subject to calendar access control (not task or TaskPlan specific) |
| | claimTask | Admin, Owner, Assignee |
| | returnTask | Admin, Owner, Claimant |
| | getTask | Admin, Query, Update, Owner, Creator, Claimant, Assignee |
| | getTaskAtDate | Admin, Query, Update, Owner, Creator, Claimant, Assignee |
| | getTaskEvents | Admin, Query, Update, Owner, Creator, Claimant, Assignee |
| | getTaskProperties(<public property set>) | Admin, Query, Update, Owner, Creator, Claimant, Assignee |
| | completeTask | Admin, Owner |
| | abortTask | Admin, Owner |
| | setErrorOnTask | Admin, Owner, Claimant |
| | clearErrorOnTask | Admin, Owner |

Table 2-1 Operations and policies on a resource

| Resource | Operation | Policy |
|--------------------|--|--|
| Task Plan (contd.) | suspendTask | Admin, Owner |
| | resumeTask | Admin, Owner |
| | reactivateTask | Admin, Owner |
| | deleteTask | Admin, Owner |
| | setTaskOwner | Admin, Owner |
| | setTaskCurrentStep | Admin, Owner |
| | setTaskPlanForTask | Admin, Owner |
| | setGlobalTaskPlanPolicy | Global Admin See, “Out-of-box Security Policies” on page 2-21. |
| | getGlobalTaskPlanPolicy | Global Admin, Global Query, Global Update. See, “Out-of-box Security Policies” on page 2-21. |
| | setTaskPlanPolicy | Admin |
| | getTaskPlanPolicy | Admin, Query, Update |
| | setTaskCreationDate | Admin, Owner |
| | setTaskPriority | Admin, Update, Owner |
| | setTaskCompletionDueDate, setTaskCurrentStepClaimDueDate setTaskCurrentStepCompletionDueDate | Admin, Update, Owner |
| | setTaskTimeEstimate, setTaskStepTimeEstimate | Admin, Update, Owner |
| | setTaskCurrentStepTimeEstimate | Admin, Update, Owner, Claimant |
| | addListener, removeListener, getListeners | Admin, Query |
| | addListener(isCritical=true), removeListener(isCritical=true) | Admin |

Table 2-1 Operations and policies on a resource

| Resource | Operation | Policy |
|--------------------|---|---|
| Task Plan (contd.) | getTaskIds, getTasks, getTaskDataCursor | Admin, Query Note: You must supply one or more task plans to call these |
| | getTaskIdsWithAffinity, getTasksWithAffinity, getTaskDataCursorWithAffinity | Admin, Query, Owner, Creator, Claimant, Assignee, Association |
| | Other Setters | Update, Owner |
| | Other Getters | Query, Owner, Creator, Claimant, Assignee, Association |

User-experience for Defining Policies

Security policies are defined in Worklist Console and associated with one of the protected resources described in the [“Protected Resources” on page 2-5](#). Security policies may also be set using the Worklist API, which is also used by Worklist Console.

Security policies are never stored directly in the metadata for a protected resource. Rather, these policies are stored in the active security provider for the WebLogic Server domain hosting Worklist. The security provider stores the policies and their association with a Worklist resource. At runtime, the Worklist runtime makes calls to the WebLogic Server security framework (specifically `isAccessAllowed` calls) using the current user identity to ensure that only authorized users gain access to protected resources. The `isAccessAllowed` call is made passing the `key` for a protected resource. The WebLogic Server security framework handles establishing the identity of the current user, and then calls into the authorization provider to make the actual decision for or against allowing access.

Note: The authorization provider stores the association of the policy expression with the resource for the policy. This mapping is one-to-one, and thus a given policy cannot apply to more than one resource. Also, the association treats the protected resource as an opaque resource key. Worklist defines resource keys for the protected resources it defines. These keys include the type and name or identifier for the resource, as well as the type of access being requested. For example, an attempt to get a property value from a task will result in the creation of a `PropertySet` resource describing the task plan ID, and property set name that contain the property, and the `Query` policy describing the type of access requested.

Different authorization providers use different expression languages for policies, and offer different capabilities in those expressions. The WebLogic Server default authorization provider allows a policy expression that is a list of role names. Worklist helps users work directly with the WebLogic Server default authorization provider and provides enough information to make manual integration with other providers possible.

Defining Policies within WebLogic Server Default Security Provider

Worklist provides API-level support for defining policies within the WebLogic Server default authorization provider. This API-level support defines a policy as a list of role names. No other type of policy expression is supported via the APIs. However, it is possible to define more detailed policies using the WebLogic Server default authorization provider policy expression language. For more information about this policy expression language, see “WebLogic Security Framework” in [WebLogic Security Service Architecture](#) in *Understanding WebLogic Security*. Custom policy expressions can be associated with the appropriate Worklist resource by constructing the appropriate instances of Worklist resource classes (see “[Defining Policies within WebLogic Server Default Security Provider](#)” on page 2-15), and then passing the resource instance and policy expression to methods in the WebLogic Server security framework API. For more information, see [Securing WebLogic Server](#) and [Securing WebLogic Resources Using Roles and Policies](#).

Worklist provides the following methods on the WorklistSystem interface to set the default administrative, creation, and query policies on a WorklistSystem resource:

```
public interface WorklistSystem {

    /**
     * Operations for which a Worklist system policy may be set
     */
    public static enum OPERATION { Admin, Create, Query, Update };
    ...
    /**
     * Set the global policy for *all* Worklist system instances that don't
     * specify their own explicit policy for the given operation type.
```

Worklist Administration

```
* Note, this method is provided for convenience only. BEA recommends you
* use WorklistAdminMBean instead.
* <p>
* Note, this method has the same effect regardless of what WorklistSystem
* instance is used, or what Worklist system instance it comes from.
* <p>
* To call this method, you must be granted one of the roles
* listed for the global Worklist System Admin policy (by default this is
* the Admin or IntegrationAdmin roles). If an unauthorized user attempts
* this call, a SecurityException will be thrown.
* <p>
* NOTE: This method will only work when you are using the WLS default
* authorization provider. If you are using a third-party provider, you
must
* use that provider's tools for assigning the policy to the task plan.
* @see
com.bea.wli.worklist.management.WorklistAdminMBean#setGlobalWorklistSystem
Policy(String, String[])
*/
public void setGlobalWorklistSystemPolicy(OPERATION operation,
                                           String[] roles)
    throws ManagementException, RemoteException;

/**
* Set a simple policy for this Worklist system instance and the given
* operation type. The policy is described in terms of the roles which are
* authorized to perform the given operation on this Worklist system
* instance.
```

```

* <p>
* To call this method, you must be granted one of the roles
* listed for this Worklist system instance's Admin policy, or you must be
* granted one of the roles listed for the global Worklist System Admin
* policy if this Worklist system instance has not had an explicit policy
* set for it. If an
* unauthorized user attempts this call, a SecurityException will be
thrown.
* <p>
* NOTE: This method will only work when you are using the WLS default
* authorization provider. If you are using a third-party provider, you
must
* use that provider's tools for assigning the policy to the Worklist
system
* instance.
* @param operation The type of operation for which the policy is being
set.
* @param roles The roles which are authorized to perform the given
* operation on tasks of the given type. If roles is empty or null,
* the policy will be reset to the default/global policy.
* @see #setGlobalWorklistSystemPolicy(OPERATION, String[])
*/
public void setWorklistSystemPolicy(OPERATION operation,
                                   String[] roles)
    throws ManagementException, RemoteException;
...
}

```

Note: The `setGlobalWorklistSystemPolicy` method sets the policy on the global `WorklistSystem` resource, regardless of the `Worklist` system instance that is being used. The `setWorklistSystemPolicy` method sets the policy on this instance of `WorklistSystem`.

Worklist provides the following methods on the `WorklistTaskAdmin` interface for setting policies on the global and specific task plans.

```
public interface WorklistTaskAdmin {
    ...
    /**
     * Operations for which a task plan policy may be set
     */
    public static enum OPERATION { Admin, Create, Query, Update };
    ...

    /**
     * Set the global policy for *all* task plans that don't specify their
     * own explicit policy for the given operation type. Note, this method is
     * provided for convenience only. BEA recommends you use
     WorklistAdminMBean
     * instead.
     * <p>
     * Note, this method has the same effect regardless of what
     WorklistTaskAdmin
     * instance is used, or what Worklist system instance it comes from.
     * <p>
     * To call this method, you must be granted one of the roles listed for
     * the global TaskPlan Admin policy (by default this is the Admin and
     * IntegrationAdmin roles).
```

```

* If an unauthorized user attempts this call, a SecurityException
* will be thrown.
* <p>
* NOTE: This method will only work when you are using the WLS default
* authorization provider. If you are using a third-party provider, you
must
* use that provider's tools for assigning the policy to the task plan.
* @see
com.bea.wli.worklist.management.WorklistAdminMBean#setGlobalTaskPlanPolicy
(String, String[])
*/
public void setGlobalTaskPlanPolicy(OPERATION operation, String[] roles)
    throws ManagementException, RemoteException;

/**
* Set a simple policy for the given task plan and operation type. The
* policy is described in terms of the roles which are authorized to
* perform the given operation on tasks of the given task plan.
* <p> To call this method, you must be granted one of the roles listed for
* the Admin policy for this task plan, or be granted one of the roles
* listed for the global TaskPlan Admin policy if this task plan has no
* explicit policy set for it.
* If an unauthorized user attempts this call, a ManagementException
* will be thrown.
* <p>
* NOTE: This method will only work when you are using the WLS default
* authorization provider. If you are using a third-party provider, you
must

```

```
* use that provider's tools for assigning the policy to the task plan.
* @param taskPlanId The ID of the TaskPlan for the tasks for which this
*     policy is being set.
* @param operation The type of operation for which the policy is being
set.
* @param roles The roles which are authorized to perform the given
operation
*     on tasks of the given type. If roles is empty or null, the policy
*     will be reset to the default/global policy.
* @see #setGlobalTaskPlanPolicy(OPERATION operation, String[] roles)
*/
public void setTaskPlanPolicy(TaskPlanId taskPlanId,
                               OPERATION operation,
                               String[] roles)
    throws ManagementException, RemoteException;

...
}
```

Defining Policies within Third-Party Security Providers

Worklist does not provide any direct support for defining policies within third-party authorization providers. However, a third-party provider that can plug into the WebLogic Server security framework should be able to make authorization decisions given the proper resource information.

This section describes the resources Worklist uses to enable authorization checks. It is these resources that are used to associate a policy in a third-party provider with the task plans you wish to control access to.

Worklist defines the following resources:

- **WorklistSystemResource** - Acts as an anchor point for defining global default admin, create, and query policies.

- **TaskPlanResource** - Acts as an anchor point for defining per-task plan admin, create, and query policies.

To define and store a policy for either of these resources in a third-party authorization provider, you must instantiate an instance of the appropriate resource implementation class and use it to obtain the proper resource identification information.

Given the proper identification for the resource, you can then use the tools of the third-party provider to associate a policy with the resource.

Documents related to security for WebLogic Server are located at the following URL:

<http://edocs/wls/docs92/security.html>

The implementation classes for these resources are in the `com.bea.wli.worklist.security` package. This package is not strictly public, but access to the resource implementation classes is supported for the purpose of obtaining resource identification for use with third-party providers.

Out-of-box Security Policies

The Worklist configuration extension template adds the following policies to the configuration of the WebLogic Server default authorizer. These policies are also the policies Worklist recommends when you are setting up a domain to host Worklist application modules. The following descriptions give detailed information about the resources Worklist considers protected resources, and the default policies recommended for those resources.

Each resource definition describes the resource in the following format:

```
resource type = "<type of resource to protect>"
    <key1 name> = "<key1 value>", ... , <keyN name> = "<keyN value>"
    Roles = { <Role 1>, ..., <Role N> }
```

where, the keys define parameters controlling the scope of the resource, and the Roles list defines the list of roles that are granted access to that resource. For Worklist, the Worklist system resource has type `WorklistSystem`, and task plan resources have type `TaskPlan`.

For `WorklistSystem` resources, the WebLogic Server security framework knows them by a type of `<wli-worklist-system>`. For `TaskPlan` resources the WebLogic Server security framework knows them by a type of `<wli-task-type>`. This type information along with the provided key/value pairs is enough to construct a low-level resource identifier for use with authorization providers other than the WebLogic Server default provider.

The policies described below are for the global WorklistSystem and TaskPlan resources. In other words, they do not apply to specific Worklist system instances or task plans. Rather, they exist as default policies for resources that do not define their own specific policies.

To set polices specific to a Worklist system instance or task plan you may either:

- Use the `WorklistSystem.setWorklistSystemPolicy()` or `WorklistTaskAdmin.setTaskPlanPolicy()` method to set policies using the WebLogic Server default authorization provider, or ...
- Use a third-party authorization provider's tool and giving it the low-level resource ID.

```
resource type = "WorklistSystem"
    operation key = "Admin"
    hostAppId key = null
    Roles = {Admin, IntegrationAdmin }

resource type = "WorklistSystem"
    operation key = "Create"
    hostAppId key = null
    Roles = {Admin, IntegrationAdmin }

resource type = "WorklistSystem"
    operation key = "Query"
    hostAppId key = null
    Roles = { Admin, IntegrationAdmin, IntegrationUser }

resource type = "WorklistSystem"
    operation key = "Update"
    hostAppId key = null
    Roles = {Admin, IntegrationAdmin }

resource type = "TaskPlan"
    operation key = "Admin"
    taskTypeId key = null
    Roles = {Admin, IntegrationAdmin }
```

```

resource type = "TaskPlan"
    operation key = "Create"
    taskTypeId key = null
    Roles = { Admin, IntegrationAdmin, TaskCreationRole,
Anonymous}
resource type = "TaskPlan"
    operation key = "Query"
    taskTypeId key = null
    Roles = {Admin, IntegrationAdmin, IntegrationUser }
resource type = "TaskPlan"
    operation key = "Update"
    taskTypeId key = null
    Roles = {Admin, IntegrationAdmin }

```

Default Security Policies

Worklist defines default policy expressions for the global Admin, Create, Query and Update policies for both Worklist system instances and task plans. These policies are automatically set when the BEA supplied authorization providers (for example, LDAP and SQL) are used. If you use a third-party authentication provider, these default policies should serve as a suggestion for BEA-recommended policies you should set within your provider (using their policy expression client tools).

The following table summarizes the actions the IntegrationMonitor, IntegrationOperator, and IntegrationAdmin, and IntegrationUser roles can execute by virtue of these default global policies.

Note: Administrators are free to modify the global policies. In that case, the values given in the table below may not necessarily apply.

Worklist Administration

| Resource | Action | IntegrationMonitor | IntegrationOperator | IntegrationAdmin | IntegrationUser |
|---|-----------|--------------------|---------------------|------------------|-----------------|
| Task Plans Configuration | Modify | | | ✓ | |
| | View | | | ✓ | ✓ |
| <p>This can be done via the TaskPlanRegistry only and not the WorklistSystem MBean.</p> | | | | | |
| Tasks | Modify | | | ✓ | |
| | Reassign | | | | |
| | Complete | | | | |
| | Cancel | | | | |
| | Claim | | | | |
| | Delete | | | | |
| | Purge | | | | |
| | Configure | | | | |
| | Security | | | ✓ | |
| | View | | | ✓ | |
| Worklist System Configuration | Modify | | | ✓ | |
| | View | | | ✓ | |
| Global Worklist System Policy | Create | | | ✓ | |
| | Delete | | | ✓ | |
| | Modify | | | ✓ | |
| | View | ✓ | ✓ | ✓ | ✓ |

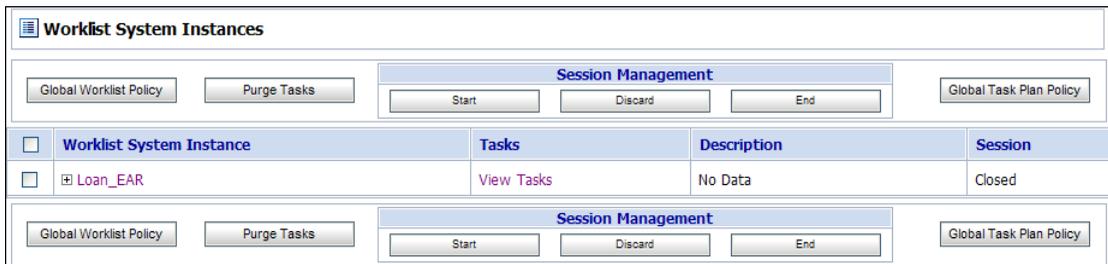
| Resource | Action | IntegrationMonitor | IntegrationOperator | IntegrationAdmin | IntegrationUser |
|--------------------------------|---|--------------------|---------------------|------------------|-----------------|
| Global Task Plan Policy | Create Delete Modify | | | ✓ | |
| | View | ✓ | ✓ | ✓ | ✓ |
| Users, Groups, and Roles | Create Delete Modify | | | ✓ | |
| | View | | | ✓ | |
| Business Calendars | Create Delete Modify | | | ✓ | |
| | Manage user and group mappings | | | ✓ | |
| | View | ✓ | ✓ | ✓ | ✓ |
| Work Substitutes | Create Delete Modify | | | ✓ | |
| | View | ✓ | ✓ | ✓ | ✓ |

Listing and Locating Worklist System Instances

A Worklist system instance is an instance of the Worklist API and its implementation. A user application can contain only one Worklist system instance, and that instance has the same name as the application that hosts it. A Worklist system instance provides access to the task plans deployed in an application, as well as the tasks that have been created based on that task plan. In

In addition, a Worklist system instance can be configured with its own security policies, runtime configuration, and so on.

The **Worklist System Instances** page displays the following information for each Worklist system instance.



| Property | Description |
|--------------------------|---|
| Worklist System Instance | Name assigned to the Worklist system instance. This value is the same as the name of the application hosting the Worklist system instance. Click this name to go to the Worklist System Instance page. |
| Tasks | Click View Tasks to view the Task Summary page. This page shows all tasks based on any task plan available to the Worklist System instance. |
| Description | Description of the Worklist System instance. |
| Session | The status of the current session is displayed. The status can be Started or Closed . |

You can do the following actions from the **Worklist System Instances** page:

| Click... | To... |
|-------------------------|--|
| Global Worklist Policy | Set the policy for all Worklist system instances that do not define their own explicit policy. For more information, see “Setting the Global Worklist System Instance Policies” on page 2-32 . |
| Purge Tasks | Manually purge all tasks that are eligible for purging. For more information, see “Purging Tasks” on page 2-37 . |
| Global Task Plan Policy | Set the global task plan policy. For more information, see “Setting the Global Task Plan Policies” on page 2-34 . |

| Click... | To... |
|--|--|
| View Tasks | View the Tasks Summary page. For more information, see “Listing and Locating Worklist Tasks” on page 2-54. |
|  next to the Worklist system instance | View and edit the task plan configuration. For more information, see “Viewing Task Plan Details” on page 2-49 and “Changing Task Plan Details” on page 2-50. |
| Start, Discard, or End | Manage the sessions. For more information, see “Managing Sessions” on page 2-27. |

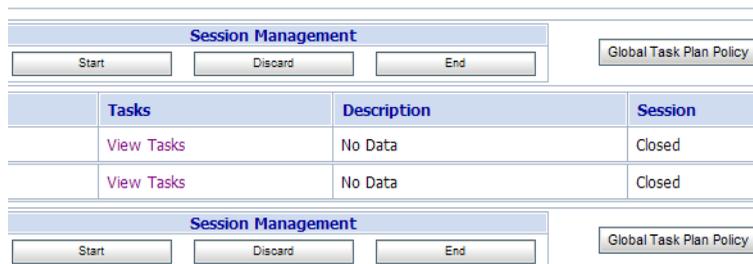
To list and locate the Worklist system instances:

1. In Worklist Console, select the **Worklist** module.
2. Select **Worklist System Instance(s)** in the left panel. The **Worklist System Instances** page appears.

All the existing Worklist system instances are displayed in this page.

Managing Sessions

Edit sessions allows you to edit Worklist system instance configuration and task plan configuration. Before you edit these configurations, you must start an edit session. You can view resources and configurations in the console without being in a session, but to edit these configurations, you must be in an active session. The **Session Management** section manages sessions in the console.



The following table provides a list of actions you can take in the **Session Management** section.

| Click... | To... |
|----------|--|
| Start | Create a new session for the selected Worklist System instances. You must create a session to make changes to the task details. After you click Start, the status of the session is Started . |
| End | Save the configuration changes and close the session for the selected Worklist System instances. After you click End, the status of the session is Closed . |
| Discard | End the current session for the selected Worklist System instances without saving the changes. After you click Discard, the status of the session is Closed . |

About Worklist Event Handlers and Event Types

An event handler defines what Worklist-defined event listeners should do in response to events generated by changes in tasks that are managed by Worklist. Event handlers can define the behavior of event notification in response to task events. Event handlers can specify a response to various events that includes any or all of the following:

- Send an e-mail message
- Post an event to the pre-defined Worklist Message Broker channel
- Store the event into the default reporting store.

Any number of event handlers can be associated with a Worklist system instance. Each event handler specifies a number of task types for which it applies or it can indicate that it is a “global” event handler that applies to all task types.

For more information, see [“Changing the Event Handler Details” on page 2-39](#).

Event Handlers contain event subscriptions that define which events are of interest to the event handler, and what to do with those events. You can define event subscriptions to send notifications for various event types. An event subscription is associated with one or more event types and for each event subscription, the desired response to the event notification is also defined.

Each Worklist system instance contains three pre-defined event handlers. These are:

- **Worklist Global Email** - defines a set of common events for which e-mail should be sent, and a set of common recipients for e-mails when those events occur. This handler is disabled by default.
- **Worklist Global MessageBroker** - defines a set of common events for which MessageBroker events will be sent.
- **Worklist Global Reporting** - defines a set of common events which will be stored into the default reporting store.

Users can modify the configuration of any Worklist defined handler or subscription. In addition, users are free to enable or disable handlers and the subscriptions they contain at any time. However, handler and the subscriptions on the base Worklist handlers cannot be removed.

The various event types in Worklist are:

| Event Type | Description |
|------------------|--|
| ABORT | A task is aborted. |
| ASSIGN | Task is assigned, either directly or as a result of moving to a new step, or taking an assign action on the step. |
| CLAIM | Task is claimed, either directly or as a result of moving to a new step, or taking an assign action on the step. |
| CLEAR_ERROR | A task is reset from error set. |
| COMPLETE | A task is completed. |
| CREATE | Task is created. This event is followed by a STEP_CHANGE event and an ASSIGN or CLAIM event that arrives after the CREATE event. |
| DELETE | A task is deleted. |
| REACTIVATE | A completed or aborted task is reactivated. |
| RESUME | A suspended task is resumed. |
| RETURN | A claimed task is returned. The task status now changes to Assigned |
| SET_CURRENT_STEP | The current step of a task is forcibly set. This event is followed by a STEP_CHANGE event indicating the arrival of the task into the new step. This may be followed by ASSIGN, CLAIM, COMPLETE, or ABORT events, which depends on the new current step. |

| Event Type | Description |
|-------------------|---|
| SET_ERROR | A task is set to error state. |
| SET_USER_PROPERTY | Custom properties defined while creating the task plan are set. If the property is updated as part of taking an action, the old and new property values are represented by the TAKE_ACTION event. |
| STEP_CHANGE | The current step of the task changes. This can happen via a work action or set by an Administrator. |
| STEP_EXPIRE | A step of a task was not completed before its scheduled completion date. |
| SUSPEND | A task is suspended. |
| TAKE_ACTION | An action is taken. May be followed by a STEP_CHANGE event after a work action that targets a different step. May be followed by ASSIGN or CLAIM events if the task was assigned or claimed (after arriving at the new step after a work action, or after an assign action). May be followed by a RETURN event after a return action. May be followed by COMPLETE, or ABORT events after a work action if the new current step is a Complete or Abort step. |
| TASK_EXPIRE | A task was not completed before its scheduled completion date. |

Changing the Worklist System Instance Configuration

The **Worklist System Instance** page displays the Worklist system instance configuration details.

Worklist System Instance - Loan_EAR

Instance Name:

Purge Interval: Enter value in seconds. '0' value indicates that no automatic Purging will happen and user has to do Purging manually.

Default DataSource JNDI Name: Enter JNDI Name for default reporting. Datasources can be created in WLS Server Console

Default Reporting DataSource JNDI Name:

Enable Default Reporting Store: Select to enable default reporting store

MAIL SESSION INFORMATION

Mail Session Information: Enter the mail session name created on the WebLogic Server

You can start a session and change the Worklist system instance configuration. In addition, you can do the following actions from the **Worklist System Instance** page:

| Click... | To... |
|---------------------|--|
| View Task List | Locate and list Worklist tasks in the Task Summary page. For more information, see “Listing and Locating Worklist Tasks” on page 2-54. |
| Start Session | Start the session. For more information, see “Managing Sessions” on page 2-27. |
| View Event Handlers | View a list of existing event handlers. For more information, see “Listing and Locating Event Handlers” on page 2-37. |
| Set System Policy | Set the policy for the current Worklist system instance. For more information, see “Setting the Worklist System Instance Policies” on page 2-34. |

To change the Worklist System Instance configuration:

1. Locate the Worklist system instance. For more information, see [“Listing and Locating Worklist System Instances”](#) on page 2-25.
2. Click the name of the Worklist system instance. The **Worklist System Instance** page appears.
3. If you did not click **Start** in **Worklist System Instances** page, click **Start Session**. For more information, see [“Managing Sessions”](#) on page 2-27.

4. Do one of the following:
 - In the **Purge Interval** field, enter the duration, in seconds, after which this Worklist system instance should be purged. If you enter **0** as the purge interval, it implies that no automatic purging is done and you need to manually purge this Worklist system instance. For more information, see [“Purging Tasks” on page 2-37](#).
 - In the **Default Reporting Datasource JNDI Name** field, enter the JNDI name of the default reporting datasource. For more information, see [Create JDBC data sources in The WebLogic Server Administration Console help](#).
 - In the **Mail Session Information** field, enter the name of the mail session created on WebLogic Server. For more information, see [Create a Mail Session in The WebLogic Server Administration Console help](#).
 5. Click **Submit**. You are returned to the **Worklist System Instances** page.
 6. Click **End** to exit from the session.
- The configuration of the Worklist system instance is updated.

Setting the Global Worklist System Instance Policies

The **Set System Policy** page allows you to set the security policy for all Worklist system instances. When the policy is not set for a Worklist system instance, the global Worklist system instances policy is applied.

| Worklist Policy | Roles |
|-----------------|--|
| Admin: | Admin, IntegrationAdmin |
| Create: | Admin, IntegrationAdmin |
| Update: | Admin, IntegrationAdmin |
| Query: | Admin, IntegrationAdmin, IntegrationUser |

Buttons: Edit, Cancel

You can assign roles to any of the Worklist policy in the **Set Global Worklist Policy** page. Users belonging to the role can then do the operations associated with that role. For more information, see [“Security Policies” on page 2-4](#) and [“Security Provider Requirements for User Management” on page 3-7](#).

Note: For Admin, Create, and Query actions, any individual Worklist system instance policy takes precedence over the global Worklist policy. For more information, see [“Setting the Worklist System Instance Policies” on page 2-34.](#)

To set the global Worklist policy:

1. In Worklist Console, select the **Worklist** module.
2. Select **Worklist System Instance(s)** in the left panel. The **Worklist System Instances** page appears.
3. Click **Global Worklist Policy**. The **Set System Policy** page appears.
4. Click **Edit**. The **Set Global Worklist Policy** page appears.

| Action | Available Roles | Selected Roles | Description |
|---------|--|--|--|
| Admin: | Anonymous, AppTester, Deployer, IntegrationDeployer, IntegrationMonitor, IntegrationOperator | Admin, IntegrationAdmin | A user granted any one of these roles is authorized to perform any administrative action on any task for which its associated task plan does not define a specific administrative policy |
| Create: | Anonymous, AppTester, Deployer, IntegrationDeployer, IntegrationMonitor, IntegrationOperator | Admin, IntegrationAdmin | A user granted any one of these roles is authorized to create tasks of any task plan for which there is no specific creation policy. |
| Update: | Anonymous, AppTester, Deployer, IntegrationDeployer, IntegrationMonitor, IntegrationOperator | Admin, IntegrationAdmin | A user granted any one of these roles is authorized to update business-related non-administrative information for the Worklist System. |
| Query: | Anonymous, AppTester, Deployer, IntegrationDeployer, IntegrationMonitor, IntegrationOperator | Admin, IntegrationAdmin, IntegrationUser | A user granted any one of these roles is authorized to query for and view information about tasks of any type for which there is no specific creation policy. |

Buttons: Submit, Cancel

5. For each action, select one or more roles in the **Available Roles** list box and click (to select multiple options, press and hold the **Ctrl** key as you click each additional option). Make sure that at least one role is selected for each action. For more information, see [“Security Policies” on page 2-4](#) and [“Security Provider Requirements for User Management” on page 3-7.](#)

Note: Take care not to remove all roles from an admin policy for which you have access. Doing so will effectively lock you from making any further edits to that policy.

6. Click **Submit**.

The global Worklist system policy is updated. You are returned to the **Set System Policy** page. Click **Cancel** to return to the **Worklist System Instances** page.

Setting the Worklist System Instance Policies

In addition to setting the global policy for all Worklist system instances, you can set the policy of an individual Worklist system instance. For more information, see [“Setting the Global Worklist System Instance Policies” on page 2-32](#), [“Security Policies” on page 2-4](#), and [“Security Provider Requirements for User Management” on page 3-7](#).

To set the Worklist system instance policy:

1. In Worklist Console, select the **Worklist** module.
2. Select **Worklist System Instance(s)** in the left panel. The **Worklist System Instances** page appears.
3. Click the Worklist system instance name. The **Worklist System Instances** page appears.
4. Click **Set System Policy**. The **Set System Policy** page appears.
5. Click **Edit**. The **Set System Policy** page appears.
6. For each action, select one or more roles in the **Available Roles** list box and click  (to select multiple options, press and hold the **Ctrl** key as you click each additional option). For more information, see [“Security Policies” on page 2-4](#) and [“Security Provider Requirements for User Management” on page 3-7](#).

Note: Take care not to remove all roles from an admin policy for which you have access. Doing so will effectively lock you from making any further edits to that policy.

7. Click **Submit**.

The policy for the selected Worklist system instance is updated. You are returned to the **Set System Policy** page. Click **Cancel** to return to the **Worklist System Instances** page.

Setting the Global Task Plan Policies

The **View Global Task Plan Policies** page allows you to view and edit the global task plan policies. The global task plan policy takes precedence over the individual task plan policy.

| View Global Task Plan Policies | |
|--------------------------------|---|
| Worklist Policy | Roles |
| Admin: | Admin,IntegrationAdmin |
| Create: | Admin,Anonymous,IntegrationAdmin,TaskCreationRole |
| Update: | Admin,IntegrationAdmin |
| Query: | Admin,IntegrationAdmin,IntegrationUser |

You can assign roles to any of the Worklist policy in the **Set Global Worklist Policy** page. Users belonging to the role can then do the operations associated with that role. For more information, see [“Security Policies” on page 2-4](#) and [“Security Provider Requirements for User Management” on page 3-7](#).

Note: For Admin, Create, and Query actions, any individual task plan policy takes precedence over the global task plan policy. For more information, see [“Viewing and Changing Task Details” on page 2-60](#).

To set the global task plan policy:

1. In Worklist Console, select the **Worklist** module.
2. Select **Worklist System Instance(s)** from the left panel. The **Worklist System Instances** page appears.
3. Click **Global Task Plan Policy**. The **View Global Task Plan Policies** page appears.
4. Click **Edit**. The **Edit Global Task Plan Policy** page appears.

| Edit Global Task Plan Policy | | | |
|---|---|---|--|
| Admin: | Available Roles Anonymous AppTester Deployer IntegrationDeployer IntegrationMonitor IntegrationOperator | Selected Roles Admin IntegrationAdmin | A user granted any one of these roles is authorized to perform any administrative action on any task for which its associated task plan does not define a specific administrative policy |
| Create: | Available Roles Anonymous AppTester Deployer IntegrationDeployer IntegrationMonitor IntegrationOperator | Selected Roles Admin IntegrationAdmin TaskCreationRole | A user granted any one of these roles is authorized to create tasks of any task plan for which there is no specific creation policy. |
| Update: | Available Roles Anonymous AppTester Deployer IntegrationDeployer IntegrationMonitor IntegrationOperator | Selected Roles Admin IntegrationAdmin | A user granted any one of these roles is authorized to update business-related non-administrative information for the Worklist System. |
| Query: | Available Roles Anonymous AppTester Deployer IntegrationDeployer IntegrationMonitor IntegrationOperator | Selected Roles Admin IntegrationAdmin IntegrationUser | A user granted any one of these roles is authorized to query for and view information about tasks of any type for which there is no specific creation policy. |
| <input type="button" value="Submit"/> <input type="button" value="Cancel"/> | | | |

- For each action, select one or more roles in the **Available Roles** list box and click  (to select multiple options, press and hold the **Ctrl** key as you click each additional option). For more information, see [“Security Policies” on page 2-4](#), and [“Security Provider Requirements for User Management” on page 3-7](#).

Note: Take care not to remove all roles from an admin policy for which you have access. Doing so will effectively lock you from making any further edits to that policy.

- Click **Submit**.

The global task plan policy is updated. You are returned to the **View Global Task Plan Policies** page. Click **Cancel** to return to the **Worklist System Instances** page.

Setting the Task Plan Policies

You can set the individual task plan policy in the **Task Plan Details** page. The individual task plan policy takes precedence over the global task plan policy. For more information, see [“Setting the Global Task Plan Policies” on page 2-34](#).

You can assign roles to any of the Worklist policies in the **Task Plan Details** page. Users belonging to the role can then do the operations associated with that role. For more information,

see [“Security Policies” on page 2-4](#) and [“Security Provider Requirements for User Management” on page 3-7](#). For information about setting individual task plan policies, see the “To edit the task plan policies” procedure in [“Changing Task Plan Details” on page 2-50](#).

Purging Tasks

The runtime repository supports automatic purging of completed or aborted tasks (referred to as terminal tasks) based on a purge interval specified by you. The length of time to retain terminal task instances can be configured at both the system and task plan level.

When you change the Worklist system instance details, you can set the purge interval. For more information, see [“Changing the Worklist System Instance Configuration” on page 2-30](#). You can set the terminal tasks retention time when you set the task plan details. For more information, see [“Changing Task Plan Details” on page 2-50](#).

The purge process automatically runs at the purge interval and tasks that are terminal and are older than the configured system or task plan limits are permanently removed from the runtime repository.

If the purge interval is set to zero, you need to manually purge the tasks. You can manually purge tasks from the **Worklist System Instances** page.

To manually purge tasks:

1. In Worklist Console, select the **Worklist** module.
2. Select **Worklist System Instance(s)** from the left panel. The **Worklist System Instances** page appears.
3. Select the check box next to the Worklist system instance that contains the tasks that you want to purge.
4. Click **Purge Tasks**.

All the tasks in the selected Worklist system instance are purged.

Listing and Locating Event Handlers

The **Event Handlers** page displays a list of all existing event handlers. You can view the event handler name and the scope of the event handler. The scope of the event handler can be global and applicable to all tasks plans or specific to selected tasks plans associated with the event handler. For more information, see [“About Worklist Event Handlers and Event Types” on page 2-28](#).

| Event Handlers | |
|-------------------------------|----------------------|
| Items 1-3 of 3 | |
| Handler Name ▾ | Handled Task Plans ▲ |
| Worklist Global Email | Global |
| Worklist Global MessageBroker | Global |
| Worklist Global Reporting | Global |
| Items 1-3 of 3 | |
| Cancel | |

To locate an event handler:

1. In Worklist Console, select the **Worklist** module.
2. Select **Worklist System Instance(s)** in the left panel. The **Worklist System Instances** page appears.
3. Start a session. For more information, see [“Changing the Worklist System Instance Configuration” on page 2-30](#).
4. Click the Worklist system instance name. The **Worklist System Instance** page appears.
5. Click **View Event Handlers**. The **Event Handlers** page appears.

Note: The **View Event Handlers** button is enabled only when you are in a session.

6. To locate an event handler, do one of the following
 - Sort the list. Ascending ▲ and descending ▼ arrow buttons indicate sortable columns. Click the button to change the sort order.
 - Scroll through the pages. Use the controls in the lower left corner. Go to a page by selecting the page number or by using the arrow buttons to go to the next ►, previous ◀, first ◀◀, or last ▶▶ page.

Related Topics

- [“Changing the Event Handler Details” on page 2-39](#)
- [“Adding Event Subscriptions” on page 2-42](#)
- [“Changing Event Subscriptions” on page 2-45](#)

- [“Deleting Event Subscriptions” on page 2-48](#)

Changing the Event Handler Details

The **Event Handler Details** page displays the event handler details and a list of event subscriptions associated with the event. You can change the task plan details and the event subscriptions associated with the event handler. For more information, see [“About Worklist Event Handlers and Event Types” on page 2-28](#).

Note: Any changes to Event Handlers can be only be done in a session. Start a session before making any change. For more information, see [“Managing Sessions” on page 2-27](#).

The screenshot shows the 'Event Handler Details' page. It has a title bar with a menu icon and the text 'Event Handler Details'. Below the title bar is a section for 'TASK PLANS' with an 'Edit >>' link. The task plan details are: Handler Name: Worklist Global Email, Is Global Handler: Yes, Is Disabled: true. Below this is the 'EVENT SUBSCRIPTIONS' section, which includes a table with 5 items. The table has columns for 'Subscription Name', 'Event Types', and 'Is Removable'. At the bottom of the subscriptions section are three buttons: 'Add Subscription', 'Delete Subscription', and 'Cancel'.

| <input type="checkbox"/> | Subscription Name <small>△</small> | Event Types <small>△</small> | Is Removable <small>△</small> |
|--------------------------|------------------------------------|--|-------------------------------|
| <input type="checkbox"/> | ASSIGN Subs | ASSIGN | false |
| <input type="checkbox"/> | CLAIM Subs | CLAIM | false |
| <input type="checkbox"/> | CREATE Subs | CREATE | false |
| <input type="checkbox"/> | Other Events Subs | ABORT, SUSPEND, SET_CURRENT_STEP, TASK_EXPIRE, STEP_EXPIRE, RESUME, REACTIVATE, COMPLETE, CLEAR_ERROR, SET_ERROR | false |
| <input type="checkbox"/> | RETURN Subs | RETURN | false |

To edit the event handler details:

1. Locate the event handler that you want to change. For more information, see [“Listing and Locating Event Handlers” on page 2-37](#).
2. Click the event handler name. The **Event Handler Details** page appears.

Event Handler Details

TASK PLANS

Handler Name Worklist Global Email

Global Handler Selecting this checkbox will ignore 'Handled Taskplans' entered below

Disabled

| | | | |
|---------------------|--|---|--|
| Handled Task Plans: | Available Task Plans <input type="text" value="/Loan/loan_approval"/> | Selected Task Plans <input type="text"/> | Select Task Plans for this event handler |
|---------------------|--|---|--|

EVENT SUBSCRIPTIONS

Items 1-5 of 5

| <input type="checkbox"/> | Subscription Name △ | Event Types △ |
|--------------------------|--|--|
| <input type="checkbox"/> | ASSIGN Subs | ASSIGN |
| <input type="checkbox"/> | CLAIM Subs | CLAIM |
| <input type="checkbox"/> | CREATE Subs | CREATE |
| <input type="checkbox"/> | Other Events Subs | ABORT, SUSPEND, SET_CURRENT_STEP, TASK_EXPIRE, STEP_EXPIRE, RESUME, REACTIVATE, COMPLETE, CLEAR_ERROR, SET_ERROR |
| <input type="checkbox"/> | RETURN Subs | RETURN |

Items 1-5 of 5

3. Click **Edit** in the Task Plans section. The **Event Handler Details** page opens in the edit mode.

4. Do any of the following:

- Select the **Global Handler** check box to indicate that the current event handler is global and can be handled by all task plans.

If you clear this check box, you need to select the task plans that will be handled by this event handler.

- Select the **Disabled** check box to disable this event handler.

When you disable an event handler, all event subscriptions associated with the event handler are disabled. This implies that there will be no event notification sent from the event handler to the notification consumers.

- Select the task plans that will be associated with this event handler from the **Available Task Plans** list box and click (to select multiple options, press and hold the **Ctrl** key as you click each additional task plan)

This option is available only when the **Global Handler** check box is not selected.

5. Click **Submit**.

The event handler details are updated. You are returned to the **Event Handler Details** page.

You can also add, change or delete event subscriptions associated with the event handler. For more information, see [“Adding Event Subscriptions” on page 2-42](#), [“Changing Event Subscriptions” on page 2-45](#), and [“Deleting Event Subscriptions” on page 2-48](#). These changes to the event subscriptions associated with the event handler are reflected only after you end the current session.

Listing and Locating Event Subscriptions

The **Event Handler Details** page displays the event handler details and a list of event subscriptions associated with the event. You can change the task plan details and the event subscriptions associated with the event handler. You can also add, change, and delete event subscriptions from this page. For more information, see [“About Worklist Event Handlers and Event Types” on page 2-28](#).

For each event subscription, you can view the name of the subscription, the event type and if this event subscription can be removed or not. When true is displayed in the **Is Removable** field, it implies that the event subscription can be deleted.

| EVENT SUBSCRIPTIONS | | | |
|--|---|--|--------------------------------------|
| | | | Items 1-5 of 5 |
| <input type="checkbox"/> | Subscription Name <small>△</small> | Event Types <small>△</small> | Is Removable <small>△</small> |
| <input type="checkbox"/> | ASSIGN Subs | ASSIGN | true |
| <input type="checkbox"/> | CLAIM Subs | CLAIM | true |
| <input type="checkbox"/> | CREATE Subs | CREATE | true |
| <input type="checkbox"/> | Other Events Subs | ABORT, SUSPEND, SET_CURRENT_STEP, TASK_EXPIRE, STEP_EXPIRE, RESUME, REACTIVATE, COMPLETE, CLEAR_ERROR, SET_ERROR | true |
| <input type="checkbox"/> | RETURN Subs | RETURN | true |
| | | | Items 1-5 of 5 |
| <input type="button" value="Add Subscription"/> <input type="button" value="Delete Subscription"/> <input type="button" value="Cancel"/> | | | |

To locate the event subscription:

1. In Worklist Console, select the **Worklist** module.
2. Select **Worklist System Instance(s)** in the left panel. The **Worklist System Instances** page appears.
3. Start a session. For more information, see [“Managing Sessions” on page 2-27](#).

4. Click the Worklist system instance name. The **Worklist System Instance** page appears.
5. Click **View Event Handlers**. The **Event Handlers** page appears.

Note: The **View Event Handlers** button is enabled only when you are in a session.

6. Click the event handler name. The **Event Handler Details** page appears.
A list of event subscriptions associated with the event handler are displayed on the page.
7. To locate an event subscription, do one of the following

- Sort the list. Ascending ▲ and descending ▼ arrow buttons indicate sortable columns. Click the button to change the sort order.
- Scroll through the pages. Use the controls in the lower left corner. Go to a page by selecting the page number or by using the arrow buttons to go to the next ►, previous ◀, first ◀◀, or last ▶▶ page.

The actions that you can do from the **Event Subscription** section of the **Event Handler Details** page are listed in the following table.

| Click... | To |
|---------------------|---|
| Add Subscription | Add a event subscription. For more information, see “Adding Event Subscriptions” on page 2-42. |
| Subscription Name | Edit an existing event subscription. For more information, see “Changing Event Subscriptions” on page 2-45. |
| Delete Subscription | Delete the selected event subscriptions. For more information, see “Deleting Event Subscriptions” on page 2-48. |

Adding Event Subscriptions

You can use the **Event Subscription Details** page to add event subscriptions that will be associated with event handlers. For more information, see [“About Worklist Event Handlers and Event Types” on page 2-28.](#)

Event Subscription Details

EVENT SUBSCRIPTION SUMMARY

Worklist System Instance: Loan_EAR

Event Handler: Worklist Global Email

Subscription Name: Enter subscription name

For All Event Types: Select to apply this subscription to all events

Event Types:

ABORT
 ASSIGN
 CLAIM
 CLAIM_EXPIRE_81X
 CLEAR_ERROR
 COMPLETE

Selected Event Types

Select Event Types for this event subscription

EMAIL NOTIFICATIONS

Subscription Disabled for Email: Click to disable/enable Email Notification

Locale: Enter the Locale for sending EMail Notifications

Encoding Character Set: Enter the Charset Name for sending EMail Notifications

Java Mail Session JNDI Name: Enter the JNDI Name specified in WLS Server

From Name: Enter From EMail address

ACTORS LIST:

Users:

Joe
 John
 Mark
 Mary
 weblogic

Selected Users

Select Users for this Event Subscription

Groups:

Administrators
 AppTesters
 Deployers
 IntegrationAdministrators
 IntegrationDeployers
 IntegrationMonitors

Selected Groups

Select Groups for this Event Subscription

Task Affinity:

Assignee
 Associate
 Claimant
 Creator
 Owner

Selected Task Actors

Select Task Actors for this Event Subscription

MESSAGEBROKER CONFIGURATION

Subscription Disabled for MessageBroker: Click to disable/enable MessageBroker events

REPORTING CONFIGURATION

Subscription Disabled for Reporting: Click to disable/enable Reporting events

To add a event subscription:

1. Locate the event handler to which you want to add the event subscription. For more information, see [“Listing and Locating Event Handlers”](#) on page 2-37.
2. Click the event handler name. The **Event Handler Details** page appears.
3. Click **Add Subscription**. The **Event Subscription Details** page appears.

4. Do the following:

- In the **Subscription Name** field, enter the name of the event subscription.
- Select the **For All Event Types** check box to apply this event subscription to all event types.
- Select one or more event types in the **Event Types** list box and click  (to select multiple options, press and hold the **Ctrl** key as you click each additional event type). For more information, see [“Listing and Locating Worklist System Instances” on page 2-25](#).

You need to select the event types only when the **For All Event Types** check box is not selected.

- Select the **Subscription Disabled for Email** check box to disable e-mail notification for this event subscription. Clear this check box if you want to enable e-mail notification.
- In the **Locale** field, select the locale to be used for sending e-mail notification.
- In the **Encoding Character Set** field, enter the name of the character set to be used for e-mail notification.
- In the **Java Mail Session JNDI Name** field, enter the name of the mail session created on WebLogic Server. For more information, see [Create a Mail Session](#) in *The WebLogic Server Administration Console* help.
- In the **From Name** field, enter the Internet Address from which the e-mail notification should sent to the user. Internet Address could be any valid e-mail address or valid name (without any space in the name).
- Select one or more users from the **Users** list box and click  (to select multiple options, press and hold the **Ctrl** key as you click each additional user name). The selected users will be associated with this event subscription.
- Select one or more groups from the **Groups** list box and click  (to select multiple options, press and hold the **Ctrl** key as you click each additional group name). The selected groups will be associated with this event subscription.
- Select one or more options from the **Task Actors** list and click  (to select multiple options, press and hold the **Ctrl** key as you click each additional option).

Task actors are specified in terms of their affinity to a task. Creator, Owner, Claimant, and Assignees are task actors who have a specify meaning and relation with respect to a task.

- Select the **Subscription Disabled for MessageBroker** check box to disable event notification using the Message Broker. When this check box is cleared, event notification using the Message Broker is enabled.
- Select the **Subscription Disabled for Reporting** check box to disable event notification to the default Reporting Store. When this check box is cleared, the default reporting store will receive event notification.

5. Click **Submit**.

The event subscription is added. The subscription details are displayed in the **Event Subscription Details** page in the view mode. If required, click **Edit** to modify the details or click **Back** to return to the **Event Handler Details** page.

Related Topics

- [“Changing Event Subscriptions” on page 2-45](#)
- [“Deleting Event Subscriptions” on page 2-48](#)

Changing Event Subscriptions

The **Event Subscription Details** page displays a summary of the event subscription, the event notification details, and the human actors associated with the event. You can change the event subscription details associated with the event handler. For more information, see [“About Worklist Event Handlers and Event Types” on page 2-28](#).

Event Subscription Details

Event Subscription Summary Edit >>

Worklist System Instance: Loan_EAR

Event Handler: Worklist Global Email

Subscription Name: testSub

For All Event Types: false

Handled Event Types: CLAIM

EMAIL NOTIFICATIONS Edit >>

Subscription Disabled for Email: true

Locale: en_US

Encoding Character Set: UTF-8

Java Mail Session JNDI Name:

From Name:

ACTORS LIST:

| Name ▲ | Type ▲ |
|---|---|
| Joe | User |
| IntegrationAdministrators | Group |

Task Affinity: Claimant

MessageBroker Configuration

Subscription Disabled for MessageBroker: true

Reporting Configuration

Subscription Disabled for Reporting: true

To change the event subscription details:

1. Locate the event handler to which you want to add the event subscription. For more information, see [“Listing and Locating Event Handlers” on page 2-37](#).
2. Click the event handler name. The **Event Handler Details** page appears.
3. Click the name of the event subscription. The **Event Subscription Details** page appears.
4. Click **Edit** in the **Event Subscription Summary** section. The Worklist system instance and the event handler name are displayed. You cannot modify these values.
5. Do any of the following:
 - Select the **For All Event Types** check box to apply this event subscription to all event types.

- Select one or more event types in the **Event Types** list box and click  (to select multiple options, press and hold the **Ctrl** key as you click each additional event type). For more information, see [“Listing and Locating Worklist System Instances” on page 2-25](#).
You need to select the event types only when the **For All Event Types** check box is not selected.
6. Click **Submit** or click **Edit** in the **Email Notification** section. If you click **Submit** now, only the event subscription summary details are modified and you return to the **Event Subscription Details** page.
 7. After you click **Edit** in the previous step, do any of the following:
 - Select the **Subscription Disabled for Email** check box to disable e-mail notification for this subscription. Clear this check box if you want to enable e-mail notification.
 - In the **Locale** field, select the locale to be used for sending e-mail notification.
 - In the **Encoding Character Set** field, enter the name of the character set to be used for e-mail notification.
 - In the **Java Mail Session JNDI Name** field, enter the name of the mail session created on WebLogic Server. For more information, see [Create a Mail Session](#) in *The WebLogic Server Administration Console* help.
 - In the **From Name** field, enter the Internet Address from which the e-mail notification should sent to the user. Internet Address could be any valid e-mail address or valid name (without any space in the name).
 - Select one or more users from the **Users** list box and click  (to select multiple options, press and hold the **Ctrl** key as you click each additional user name). The selected users will be associated with this event subscription.
 - Select one or more groups from the **Groups** list box and click  (to select multiple options, press and hold the **Ctrl** key as you click each additional group name). The selected groups will be associated with this event subscription.
 - Select one or more options from the **Task Actors** list and click  (to select multiple options, press and hold the **Ctrl** key as you click each additional option).
Task actors are specified in terms of their affinity to a task. Creator, Owner, Claimant, and Assignees are task actors who have a specify meaning and relation with respect to a task.

- Select the **Subscription Disabled for MessageBroker** check box to disable event notification using the Message Broker. When this check box is cleared, event notification using the Message Broker is enabled.
 - Select the **Subscription Disabled for Reporting** check box to disable event notification to the Reporting Store. When this check box is cleared, the default reporting store will receive event notification.
8. Do any one of the following:
- Click **Submit** to save the changes.
 - Click **Cancel** to discard the changes.
 - Click **Back** to discard the changes and return to the **Event Handler Details** page.

The event subscription is updated after you click **Submit**. The subscription details are displayed in the **Event Subscription Details** page in the view mode. If required, click **Edit** to modify the details or click **Back** to return to the **Event Handler Details** page.

Related Topics

- [“Adding Event Subscriptions” on page 2-42](#)
- [“Deleting Event Subscriptions” on page 2-48](#)

Deleting Event Subscriptions

You can delete an event subscription from the **Event Handler Details** page.

Note: You can delete an event subscription only when the **Is Removable** flag is set to `true` for that subscription. For event subscriptions that are deployed as part of the Worklist application (that is, not added after deployment in Worklist Console), this flag is set to `false`.

To delete an event subscription:

1. Locate the event handler from which you want to delete the event subscription. For more information, see [“Listing and Locating Event Handlers” on page 2-37](#).
2. Click the event handler name. The **Event Handler Details** page appears.
3. Select the check box next to the event subscriptions that you want to delete.
4. Click **Delete Subscription**. A confirmation message appears. Click **OK**.

The event subscription is deleted.

Viewing Task Plan Details

A task plan is a description of the steps, properties, task assignment rules, and so on that are common to a class of tasks defined for a given purpose. For more information about tasks and task plans, see [Creating and Managing Worklist Tasks](#) in *Using the Worklist*.

In the **Task Plan Details** page, you can view and edit the task plan details including the task plan summary details, task plan policies, user-defined properties, and task steps. For more information, see [“Changing Task Plan Details” on page 2-50](#).

To view the task plan details:

1. In Worklist Console, select the **Worklist** module.
2. Select **Worklist System Instance(s)** from the left panel. The **Worklist System Instances** page appears.
3. Click the  icon next to the Worklist system instance. All the task plans associated with the Worklist system instance are displayed.
4. Click the task plan that you want to view. The **Task Plan Details** page appears.

Task Plan Details - loan_approval

TASK PLAN SUMMARY: Edit >>

| | |
|-------------------------------|---------------------------|
| Task Plan Name: | loan_approval |
| Description: | |
| Version: | 1.0 |
| Time Estimate: | |
| Completion Due Date: | Interval, User, Calendar: |
| Task Owner: | |
| Terminal Task Retention Time: | |

TASK PLAN POLICIES Edit >>

| | |
|---------|--|
| Admin: | |
| Create: | |
| Update: | |
| Query: | |

PROPERTIES

User Defined Properties:

| Name | Description | Data Type | Default Value |
|-------------------|-------------|-----------|---------------|
| Collateral Assets | | String | |
| LoanAmt | | Integer | |
| Name | | String | |
| Notes | | String | |
| SSN | | String | |

CONSTRUCTORS

| Name | Description | Start Step | Required Properties | | |
|---------|-------------|----------------------|---------------------|----------------------|---------------|
| | | | Property Name | Property Description | Default Value |
| NewLoan | --- | OfficerReviewPending | SSN | LoanAmt | Name |

STEPS Edit >>

[View detailed information about steps](#)

| Step Name | Step Description | Action Properties | | |
|----------------------|------------------|------------------------|--------------------|----------------------|
| | | Action Name | Action Description | Next Step |
| LoanApproved | --- | | | |
| LoanRejected | --- | | | |
| ManagerReviewPending | --- | Approve | --- | LoanApproved |
| | | Reject | --- | LoanRejected |
| OfficerReviewPending | --- | Approve | --- | LoanApproved |
| | | Reject | --- | LoanRejected |
| | | Request Manager Review | --- | ManagerReviewPending |

[Return to Origin](#)

Changing Task Plan Details

In the **Task Plan Details** page, you can view and edit the task plan details including the task plan summary details, task plan policies, user-defined properties, and task steps.

To edit the task plan summary details:

1. Start the session. For more information, see [“Managing Sessions”](#) on page 2-27.

2. View the task plan details of the task plan that you want to change. For more information, see [“Viewing Task Plan Details” on page 2-49](#).
3. Click **Edit** next to the **Task Plan Summary** section.
4. Do one of the following:
 - In the **Time Estimate** field, enter the estimated time (specified as a business calendar interval, for example, 3min2hour1day or 10 years 5 hours 3 seconds) required to complete the task. This information is used by the default Worklist assignment handler for load balancing. If specified, this value is used as a default value for the time estimate setting on all the steps this task contains.
 - In the **Completion Due Date** field, specify the interval and specify the user or business calendar.

The interval may define a number of days, hours and/or minutes in the D days H hours M minutes format, where D is number of days, H is number of hours, and M is number of minutes.

The completion due date of the task is generated based on the interval, and the user or business calendar. For example, if the interval is specified as 10 days and the business calendar is selected. If current date is 1, and the next 5 days are busy based on selected business calendar, then the completed due date for the task would be 15.
 - In the **Task Owner** field, enter the default owner of the task instance associated with the task plan.
 - In the **Terminal Task Retention Time**, enter the duration (specified as a business calendar interval, for example, 3min2hour1day or 10 years 5 hours 3 seconds) for which Completed or Aborted tasks should be retained in the runtime store before becoming eligible for purging. For more information, see [“Purging Tasks” on page 2-37](#).
5. Click **Submit**.
6. End the session.

The task parameters have been updated. You are returned to the **Task Plan Details** page.

To edit the task plan policies:

Policies can be set at the individual task plan level or at the global task plan level. When set, individual task plan policy takes precedence over the global task plan. For more information, see [“Setting the Global Task Plan Policies” on page 2-34](#).

You can set the individual task plan policy in the **Task Plan Details** page. You can assign roles to any of the Worklist policies in the **Task Plan Details** page. Users belonging to the role can then do the operations associated with that role. For more information, see [“Security Policies” on page 2-4](#) and [“Security Provider Requirements for User Management” on page 3-7](#).

1. Start the session. For more information, see [“Managing Sessions” on page 2-27](#).
2. View the task plan details. For more information, see [“Viewing Task Plan Details” on page 2-49](#).
3. Click **Edit** next to the **Task Plan Policies** section.
4. For each action, select one or more roles in the **Available Roles** list and click  (to select multiple options, press and hold the **Ctrl** key as you click each additional role). For more information, see [“Security Policies” on page 2-4](#), and [“Security Provider Requirements for User Management” on page 3-7](#).

Note: Take care not to remove all roles from an admin policy for which you have access. Doing so will effectively lock you from making any further edits to that policy.

5. Click **Submit**.
6. End the session.

The policy for the selected task plan has been updated. You are returned to the **Task Plan Details** page.

To view and edit detailed information about the steps in a task:

1. Start the session. For more information, see [“Managing Sessions” on page 2-27](#).
2. View the task plan details. For more information, see [“Viewing Task Plan Details” on page 2-49](#).
3. Click **Edit** next to the **Steps** section. The **Complete Step Information** page appears.

Note: You can also click **View detailed information about the steps**. The **Complete Step Information** page appears. Click **Edit**.

You can configure the parameters for each step in the task and each action in a step.

4. For each step in the task, do the following:
 - In the **Time Estimate** field, enter the estimated time (specified as a business calendar interval, for example, 3min2hour1day or 10 years 5 hours 3 seconds) required

to complete the step. This information is used by the default Worklist assignment handler for load balancing.

- In the **Completion Due Date** field, specify the interval and specify the user or business calendar.

The interval may define a number of days, hours and/or minutes in the D days H hours M minutes format, where D is number of days, H is number of hours, and M is number of minutes.

The completion due date of the step is generated based on the interval, and the user or business calendar. For example, if the interval is specified as 10 days and the business calendar is selected. If current date is 1, and the next 5 days are busy based on selected business calendar, then the completed due date for the step would be 15.

- Select the one or more user names in the **Users** list box and click  (to select multiple options, press and hold the **Ctrl** key as you click each additional user name).
- Select the one or more column group names in the **Groups** list box and click  (to select multiple options, press and hold the **Ctrl** key as you click each additional group).
- In the **Candidate List Handling** field, select the type of handling to be applied while assigning the selected users or groups.
- If load balancing is applied while assigning the selected users or groups (you selected **Load_Balancing** in the **Candidate List Handling** list box in the previous step), in the **Load Balancing Check** field, select **Yes** or **No** to indicate if load balancing check is required or not.
- Repeat the above steps for each of the steps in the task.

5. For each action in a step, do the following:

- Select the one or more user names in the **Users** list box and click  (to select multiple options, press and hold the **Ctrl** key as you click each additional user name).
- Select the one or more column group names in the **Groups** list box and click  (to select multiple options, press and hold the **Ctrl** key as you click each additional group).
- In the **Candidate List Handling** field, select the type of handling to be applied while assigning the selected users or groups.
- If load balancing is applied while assigning the selected users or groups (you selected **Load_Balancing** in the **Candidate List Handling** list box in the previous step), in the **Load Balancing Check** field, select **Yes** or **No** to indicate if load balancing check is required or not.

- Repeat the above steps for each of the actions in the step.

6. Click **Submit**.

7. End the session.

The parameters associated with steps in a task and the actions in a step are updated. You are returned to the **Task Plan Details** page.

Listing and Locating Worklist Tasks

A task represents an activity that is assigned to a human user. The human user oversees the progress of the task and ensures that it is completed in a correct and timely fashion. For more information about tasks and task plans, see [Creating and Managing Worklist Tasks](#) in *Using the Worklist*.

The **Tasks Summary** page displays the following information for each task instance. For a more detailed description of the properties, see [“Viewing and Changing Task Details” on page 2-60](#).

| <input type="checkbox"/> | Task Name ▾ | Description ▲ | TaskPlanId ▲ | WorkingState ▲ | AdminState ▲ | CurrentStepName ▲ | CompletionDueDate ▲ | Owner ▲ | Claimant ▲ | Priority ▲ |
|--------------------------|-------------|---------------|-------------------------|----------------|--------------|----------------------|---------------------|----------|------------|------------|
| <input type="checkbox"/> | test | --- | /Loan/loan_approval:1.0 | CLAIMED | ACTIVE | ManagerReviewPending | --- | weblogic | Mary | 1 |

Apply this action on selected tasks: Suspend ▾ Submit Cancel

Claim the tasks for User: Joe ▾ Claim for User Select User and click 'Claim for User'

Click 'Assign' to assign selected tasks Assign->

| Property | Description |
|---------------|---|
| Task Name | Name assigned to the task. Click on the task name to view the Worklist Task Details page. For more information, see “Viewing and Changing Task Details” on page 2-60 . |
| Description | Description of the task. |
| Task Plan ID | The ID associated with the task plan. |
| Working State | Current Working State of the task. The Working State can be Assigned, Claimed, or Unassigned. |

| Property | Description |
|---------------------|--|
| Admin State | Current Administrative State of the task. This state can be Aborted, Active, Completed, Error, or Suspended. |
| Current Step Name | Name of the current step in the task. |
| Completion Due Date | Due date and time by which the task should be completed. |
| Assignees | One or more users or groups to which the task is assigned. |
| Claimant | If the task is claimed, the user who claimed the task. |
| Owner | The owner of the task. A user or group. |
| Priority | The priority assigned to the task. |

You can do the following actions from the **Tasks Summary** page:

| Action... | Description |
|------------------------------|---|
| Create custom query | Construct a custom query to locate specific task instances. For more information, see “Constructing a Custom Query for Task Instances” on page 2-56 . |
| Edit task details | Change the task instance details by clicking on the task name. For more information, see “Viewing and Changing Task Details” on page 2-60 . |
| Update task state | Depending on the current state of a task, you can suspend, resume, complete, abort, set error, clear error, claim, return, delete, or reactive the task. For more information, see “Updating Task State” on page 2-64 . |
| Claim task | Claim the selected tasks on behalf of another user. For more information, see “Claiming a Task for a User” on page 2-67 . |
| Assign task to user or group | Assign the selected tasks to the appropriate user or group. For more information, see “Assigning a Task to User or Group” on page 2-67 . |

To list and locate tasks:

1. Do any one of the following:

- In Worklist Console, select the **Worklist** module. The **Worklist System Instances** page appears. Click **View Tasks** against the required Worklist system instance.
- In the **Worklist System Instances** page, click on the Worklist system instance name. The **Worklist System Instance** page appears. Click **View Task List**.
- In the **Worklist System Instances** page, click  next to the Worklist system instance. The task plan associated with the Worklist system instance is displayed. Click **View Tasks**.

The **Task Summary** page appears.

2. To locate a specific task, do one of the following:
 - Sort the list. Ascending  and descending  arrow buttons indicate sortable columns. Click the button to change the sort order.
 - Scroll through the pages. Use the controls in the lower left corner. Go to a page by selecting the page number or by using the arrow buttons to go to the next , previous , first , or last  page.
 - Select **Customize Table Header** and construct a custom query. All tasks that match the specified criteria are listed. For more information, see [“Constructing a Custom Query for Task Instances”](#) on page 2-56.

Constructing a Custom Query for Task Instances

The **Custom Query** page allows you to construct a complex task instance search.

Constructing a Custom Query for Task Instances

Construct a Custom Query

Task Name:

Task IDs: Enter comma separated values

Task Working State: Unassigned Assigned Claimed

Task Admin State: Active Suspended Completed Aborted Error

Comment (regexp):

Priority: **from:** **to:**

Assignee Contains: Enter comma separated values

Claimant Contains: Enter comma separated values

Owner Contains: Enter comma separated values

View

Column Display

| Available | Selected |
|-----------------|-------------------|
| AdminState | Description |
| Assignee | TaskPlanId |
| CanBeAborted | WorkingState |
| CanBeReassigned | AdminState |
| CanBeReturned | CurrentStepName |
| ClaimDueDate | CompletionDueDate |

Preserve Search Criteria: Select this checkbox and Apply to save this settings for this session. Just clicking Apply will be effective only once.

Preferences:

Maximum Results Returned: Choose maximum number when huge tasks are available, this may improve query performance.

Number of rows displayed per page: Choose number of rows to be displayed

The following table summarizes the available search criteria:

| Search Criteria | Description |
|-----------------|---|
| Task Name | Specify the task name. Use * to match zero or more characters. The search returns tasks that match the target name and also matches any other criteria specified by you. |
| Task IDs | Specify one or more task IDs (comma separated list). Do not use wildcards. The search returns task instances matching any of the specified task IDs. |

| Search Criteria | Description |
|----------------------|--|
| Task Working State | <p>Select the check box next to the working state of the task. The working state of the task could be:</p> <ul style="list-style-type: none"> • Unassigned • Assigned • Claimed <p>The search returns tasks in the specified states that also match any other criteria specified by you.</p> |
| Task Admin State | <p>Select the check box next to the administrative state of the task. The administrative state of the task could be:</p> <ul style="list-style-type: none"> • Active • Suspended • Completed • Aborted • Error <p>The search returns tasks in the specified states that also match any other criteria specified by you.</p> |
| Comment | <p>Specify a regular expression to match the target comment.</p> <p>The search returns tasks with matching comments that also match the other criteria specified by you.</p> |
| From and To Priority | <p>Specify the low and high ends of the priority range.</p> <p>The search returns tasks with an assigned priority that falls within the range (inclusive) that also match any other criteria specified.</p> |
| Assignee Contains | <p>Specify one or more users or groups (comma separated list). Do not use wildcards.</p> <p>The search returns tasks with an assignee that matches any of the users or groups and also matches any other criteria specified by you.</p> |
| Claimant Contains | <p>Specify one or more users (comma separated list).</p> <p>The search returns tasks with a claimant that matches any of the users and also matches any other criteria specified by you.</p> |

| Search Criteria | Description |
|-----------------------------------|--|
| Owner Contains | <p>Specify one or more users or groups (comma separated list). Do not use wildcards.</p> <p>The search returns tasks with an owner that matches any of the users or groups and also matches any other criteria specified by you.</p> |
| Column Display | <p>Specify the columns that you want to view in the Task Summary page. Select the one or more column options in the Available list box and click  (to select multiple options, press and hold the Ctrl key as you click each additional option).</p> <p>The results of the query are displayed in the Task Summary page with the selected columns.</p> |
| Preserve Search Criteria | <p>Select this check box and click Apply to save the specified search criteria during the current session. When you clear this option and click Apply, the specified search criteria is valid only for the current search.</p> |
| Maximum Results Returned | <p>Select the maximum number of search results that should be returned. To improve query performance when a large number of tasks are available, choose maximum number. The maximum number could be 10, 20, 30, 40, or 50.</p> |
| Number of rows displayed per page | <p>Select the number of rows that you want to view in the search results page. The number of rows could be 10, 20, 30, 40, or 50.</p> |

To execute a custom query:

1. In Worklist Console, select the **Worklist** module.
2. Click **Worklist System Instance(s)** in the left panel. The **Worklist System Instances** page appears.
3. Click **View Tasks** against the required worklist application. The **Task Summary** page appears.
4. Click **Customize Table Header**. The **Construct a Custom Query** form appears in the page.
5. Enter the search criteria. See the preceding table for the meaning of each search criteria.
6. Do one of the following:
 - Click **Apply** to view the tasks that match the specified search criteria in the **Task Summary** page.

- Click **Reset** to view the last saved search criteria.
- Click **Cancel** to hide the **Construct a Custom Query** form.

Viewing and Changing Task Details

The **Worklist Task Details** page allows you to view task properties. If the Administrative state of the task is **Active** (that is the task is not in Suspended, Aborted, Competed, or Error Administrative state), you can click **Edit** to update the task. For more information about Administrative state of tasks, see [Creating and Managing Worklist Tasks](#) in *Using the Worklist*.

Note: If an authenticator that implements the required MBeans is not configured, the options for updating the owner, or assigning or claiming the task are disabled. To learn more about the authenticator requirements, see “[Security Provider Requirements for User Management](#)” on page 3-7.

| Worklist Task Details - Loan_EAR | | | |
|---------------------------------------|--|-----------|--------------|
| Task Name: | test | | |
| Task ID: | 172.22.56.157--11a19654.10e2ccac4e.-7fe3 | | |
| Task Plan: | /Loan/loan_approval:1.0:Loan_EAR | | |
| Description: | | | |
| Comment: | | | |
| Priority: | 1 | | |
| TASK OWNERS, CLAIMANTS, AND ASSIGNEES | | | |
| Created date and Create by: | Mon Oct 09 17:53:37 IST 2006 weblogic | | |
| Last updated Date and User: | Tue Oct 10 16:16:21 IST 2006 weblogic | | |
| Owner: | weblogic | | |
| Claimant: | Mary | | |
| Assignees: | Users() and Groups(loanManager) | | |
| STATUS | | | |
| Step: | ManagerReviewPending | | |
| Admin State: | ACTIVE | | |
| Working State: | CLAIMED | | |
| DUE DATES | | | |
| Step Completion Due Date: | | | |
| Task Completion Due Date: | | | |
| CUSTOM TASK PROPERTIES | | | |
| Items 1-5 of 5 | | | |
| Name | Description | Data Type | Value |
| LoanAmt | | Integer | 20000 |
| Collateral Assets | | String | --- |
| SSN | | String | xyz |
| Name | | String | abc |
| Notes | | String | check it out |

The following table summarizes the properties displayed:

| Property | Description | Administrator Can Set (Yes/No) |
|----------------------------|---|---------------------------------------|
| Task Name | Name assigned to the task. You cannot edit this value. | No |
| Task ID | Unique task instance ID. You cannot edit this value. | No |
| Task Plan | The task plan associated with the current task. You cannot edit this value. | No |
| Description | Description of the task. You cannot edit this value. | No |
| Comment | Comment associated with the task. | Yes |
| Priority | Priority assigned to the task. This valid can be changed and must be a positive integer. | Yes |
| Created date and Create by | The date on which the task was created and the name of the user who created this task instance. | No |
| Last updated Date and User | The date on which the task was last updated and the name of the user who updated it. | No |
| Owner | User or group that owns the task. This is typically the stakeholder interested in getting the task completed. Use of the owner is application specific, but notification of task status (for example, task complete or overdue) is often sent to the owner. | Yes |
| Claimant | If the task has been claimed, the user that claimed the task. Claiming a task indicates a user's intent to complete the task. If the task has not yet been claimed, this field is empty. | No |
| Step | The name of the current step in the task. | Yes |

| Property | Description | Administrator Can Set (Yes/No) |
|--------------------------|---|--------------------------------|
| Admin State | Administrative state of the task. The task state represents the manner in which Worklist is currently treating the task instance. | No |
| | Aborted The task has been cancelled. An aborted task can be assigned, deleted, or reactivated. | |
| | Active The task is currently active and you can take any action on the task. | |
| | Completed The claimant has completed the task. | |
| | Error There was an error in the execution of the task. The task can return to previous state only after you fix the error. | |
| | Suspended The task is "on hold." An assigned, claimed, or started task can be placed in the suspended state. | |
| Working State | Working state of the task. The working state is the affinity of the task instance to the users who can work on the task. | No |
| | Assigned The assignees have be designated, but the task has not yet been claimed. | |
| | Claimed A user has claimed the task, thus indicating an intent to complete the task. | |
| | Unassigned The task assignees have not been designated. | |
| Step Completion Due Date | The date by which the current step in the task should be completed. | Yes |
| Task completion Due Date | The date by which the task should be completed. | Yes |
| Custom Task Properties | A list of all the custom properties that have been defined for the task is displayed. | Yes |

To view task properties:

1. Locate the task in the **Task Summary** page. See [“Listing and Locating Worklist Tasks” on page 2-54](#).
2. Click the task name. The **Worklist Task Details** page appears.

Actions that you can do in the **Worklist Task Details** page are listed in the following table:

| Action | Description |
|------------------------------------|---|
| Change the task properties | If the task is not Suspended, Aborted, or Completed, you can click Edit Task to change task properties as described in the following procedure. You can change task properties like comments, priority, owner, step, task completion due date, and step completion due date. In addition, you can also change any custom properties that were defined while creating the task plan. |
| Update the task status | Apply actions on the selected tasks and update the status of the task. For more information, see “Updating Task State” on page 2-64 . |
| Claim tasks | Claim the selected tasks for the selected user. For more information, see “Claiming a Task for a User” on page 2-67 . |
| Assign the task to a user or group | Assign the selected tasks to the selected users and / or groups. For more information, see “Assigning a Task to User or Group” on page 2-67 . |
| Delete tasks | Delete the selected tasks. For more information, see “Deleting Tasks” on page 2-69 . |

To change task properties:

1. On the **Worklist Task Details** page, click **Edit Task**.

Note: The **Edit Tasks** option is available only when the Administrative state of the task is **Active**.

The **Worklist System Instance - <Task Plan name> : <Task Name>** page is displayed.

2. Do one or more of the following as required:
 - In the **Comment** field, enter a new comment, or revise the existing comment.
 - In the **Priority** field, enter a new priority, or update an existing priority.
 - In the **Owner** field, specify the owner (user or group) for the task.

- In the **Step** field, select the current step associated with the task.
- In the **Task Completion Due Date** field, specify the month, date, year, hour, minute, and second (using the format indicated to the right of the field because this format is locale specific) when the task should be completed.
- In the **Step Completion Due Date** field, specify the month, date, year, hour, minute, and second (using the format indicated to the right of the field because this format is locale specific) when the current step should be completed.
- In the **Custom Task Properties** section, specify the appropriate values for the task property fields defined by you.

3. Click **Submit**.

The changes to the task are updated and you return to the **Worklist Task Details** page.

Updating Task State

Depending on the current state of a task instance, you can assign, claim, return, complete, suspend, abort, or delete the task. The following tables describes each available action. To learn more about task states and operations, see [Creating and Managing Worklist Tasks](#) in *Using the Worklist*.

Note: If an authenticator that implements the required MBeans is not configured, the options for updating tasks assignees or claimant are disabled. To learn more about the authenticator requirements, see [“Security Provider Requirements for User Management” on page 3-7](#).

| Action | Description |
|--------|---|
| Abort | Updates the task to the aborted state. If required, you can <code>reactivate</code> the task. |
| Assign | Designates who should perform the task and updates the task to the <code>Assigned</code> state. Tasks can be assigned to one or more users or groups. Once assigned, the task can be claimed by: <ul style="list-style-type: none"> • Any user to which it is assigned. • A member of any group to which it is assigned. For more information, see “Assigning a Task to User or Group” on page 2-67 . |
| Claim | Claims the task on behalf of the specified user and updates the task to the claimed state. Claiming a task indicates intent to complete the current step in the task. For more information, see “Claiming a Task for a User” on page 2-67 . |

| Action | Description |
|---------------|---|
| Clear Error | Clears the error state of the task. The Administrative state of the task becomes <code>Active</code> . |
| Complete | Updates a started task to the completed state. If required, you can <code>reactivate</code> the task. |
| Delete | Deletes the task from the system. For more information, see “Deleting Tasks” on page 2-69 . |
| Reactivate | Reactivates an aborted or completed task. The Administrative state of the task becomes <code>Active</code> . |
| Resume | Resumes a suspended task. The Administrative state of the task becomes <code>Active</code> . |
| Return | Reassigns a claimed task to the original assignees. The task returns to the <code>Assigned</code> state. |
| Set Error | Sets an error flag on the task. The Administrative state of the task becomes <code>Error</code> . You need to explicitly apply the <code>Clear Error</code> state to the task to make it <code>Active</code> again. |
| Suspend | Updates the task to the suspended state, indicating that the task is “on hold.” The Administrative state of the task becomes <code>Suspended</code> . |

The following table summarizes the actions available for the Administrative task state:

| Administrative State | Available Actions |
|-----------------------------|---|
| Aborted | Assign or Delete |
| Active | Complete, Suspend, Return, Abort, or Delete |
| Completed | Reactivate or Delete |
| Error | Clear error |
| Suspended | Resume or Delete |

The actions available in the Working state are:

| Working State | Available Actions |
|----------------------|--|
| Assigned | Assign, Claim, Suspend, Abort, or Delete |
| Claimed | Return, Suspend, Abort, or Delete |
| Unassigned | Assign, Suspend, Abort, or Delete |

You can update the state of a task in the following contexts:

- **Worklist Task Detail** page
- **Task Summary** page

To update the state from the Worklist Task Details page:

1. Locate the task. See [“Listing and Locating Worklist Tasks” on page 2-54](#).
2. Click the name of the task you want to update. The **Worklist Task Details** page appears.
3. Select the required action in the **Apply this action on selected tasks** list box.
4. A confirmation message appears. Click **OK**.
5. Click **Submit**.

The task state is updated to reflect the action. You can view the updated Administrative state of the task in the **Task Summary** page.

To update the state from the Task Summary page:

1. Locate the task or tasks to be updated. See [“Listing and Locating Worklist Tasks” on page 2-54](#).
2. Select the check box next to the tasks that you want to update.
3. Select the required action in the **Apply this action on selected tasks** list box.
4. A confirmation message appears. Click **OK**.
5. Click **Submit**.

The task state is updated to reflect the action. You can view the updated Administrative state of the task in the **Task Summary** page.

Related Topics

- [“Viewing and Changing Task Details” on page 2-60](#)
- [“Claiming a Task for a User” on page 2-67](#)
- [“Assigning a Task to User or Group” on page 2-67](#)
- [“Deleting Tasks” on page 2-69](#)

Claiming a Task for a User

You can claim a task for a user from the **Tasks Summary** page. For information about claiming a task from the Worklist User Portal, see [Using the Worklist](#).

To claim selected tasks for a user:

1. Locate the task. For more information, see [“Listing and Locating Worklist Tasks” on page 2-54](#).
2. Select the check box next to all the tasks that you want to claim for the user.
3. In the **Claim the tasks for User** field, select the user name.
4. Click **Claim for User**.

All selected tasks are claimed by the selected user.

Related Topics

- [“Viewing and Changing Task Details” on page 2-60](#)
- [“Updating Task State” on page 2-64](#)
- [“Assigning a Task to User or Group” on page 2-67](#)
- [“Deleting Tasks” on page 2-69](#)

Assigning a Task to User or Group

In the **Task Summary** page, you can assign selected tasks to selected users and / or groups. For information about assigning a task from the Worklist User Portal, see [Using the Worklist](#).

Worklist Applications Management

Tasks Summary - Loan_EAR

Note: Please enter Assignment Instructions for selected Tasks Types

Users:

Users: Joe, John, Mark, Mary, weblogic

Selected Users: [Empty]

Groups:

Groups: Administrators, AppTesters, Deployers, IntegrationAdministrators, IntegrationDeployers, IntegrationMonitors

Selected Groups: [Empty]

Candidate List Handling: NONE

Load Balancing Check: Yes

Assign-> Cancel

To assign selected tasks to users and / or groups:

1. Locate the task. For more information, see [“Listing and Locating Worklist Tasks” on page 2-54.](#)
2. Select the check box next to all the tasks that you want to assign to the users or group.
3. Click **Assign**. The **Tasks Summary** page appears.
4. Select the one or more user names in the **Users** list box and click (to select multiple options, press and hold the **Ctrl** key as you click each additional user name).
5. Select the one or more column group names in the **Groups** list box and click (to select multiple options, press and hold the **Ctrl** key as you click each additional group).
6. In the **Candidate List Handling** field, select the type of handling to be applied while assigning the selected users or groups.
7. If load balancing is applied while assigning the selected users or groups (you selected **Load_Balancing** in the **Candidate List Handling** list box in the previous step), in the **Load Balancing Check** field, select **Yes** or **No** to indicate if load balancing check is required or not.
8. Click **Assign**.

All selected tasks are assigned to the selected users and / or groups.

Related Topics

- [“Viewing and Changing Task Details” on page 2-60](#)
- [“Updating Task State” on page 2-64](#)
- [“Claiming a Task for a User” on page 2-67](#)
- [“Deleting Tasks” on page 2-69](#)

Deleting Tasks

To delete the selected tasks:

1. Locate the task or tasks to be deleted. See [“Listing and Locating Worklist Tasks” on page 2-54](#).
2. Select the check box next to the tasks that you want to delete.
3. Select the **Delete** action in the **Apply this action on selected tasks** list box.
4. A confirmation message appears. Click **OK**.
5. Click **Submit**.

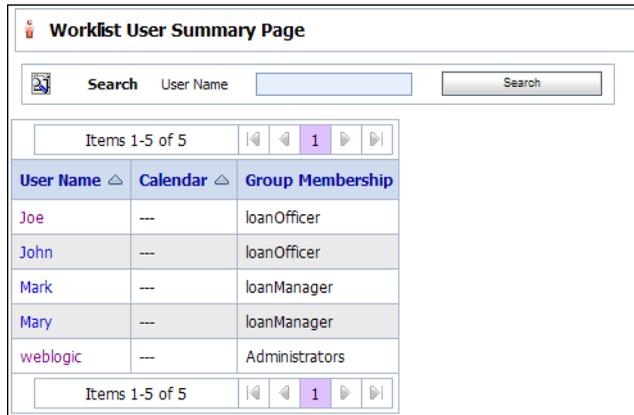
The selected tasks are deleted.

Related Topics

- [“Viewing and Changing Task Details” on page 2-60](#)
- [“Updating Task State” on page 2-64](#)
- [“Claiming a Task for a User” on page 2-67](#)
- [“Assigning a Task to User or Group” on page 2-67](#)

Managing User Profiles

The **Worklist User Summary** page lists all users and their associated group and business calendar names.



To locate a user:

1. In Worklist Console, select the **Worklist** module.
2. Select **User Profiles** in the left panel. The **Worklist User Summary** appears.
3. Do one of the following:
 - Filter by name. Enter the search target, then click **Search**. The rules matching the search criteria are displayed.
 - Sort the list. Ascending  and descending  arrow buttons indicate sortable columns. Click the button to change the sort order.
 - Scroll through the pages. Use the controls in the lower left corner. Go to a page by selecting the page number or by using the arrow buttons to go to the next , previous , first , or last  page.

Click on any user in this page and you can reassign work to another user or associate a business calendar to the user. For more information, see [“Reassigning Work to a User” on page 2-71](#) and [“Associating Business Calendars with Users” on page 4-14](#).

Setting the E-mail Address of a User

You can set the e-mail address of a user from the User Profiles link in the Worklist module. This e-mail address for any e-mail notification.

To set the e-mail address of a user:

1. In Worklist Console, select the **Worklist** module.
2. From the left panel, select **User Profiles**. The **Worklist Users Summary Page** appears.
3. Click the name of the user for whom you want to set the e-mail address. The **Associate User with Calendar** page appears.

4. Specify the e-mail address of the user.
5. If required, from the **Shared Calendar** drop-down list, select a named calendar, or select **System Calendar**.
6. Click **Submit** to set the e-mail address of the user and assign any selected calendar to the user.

Reassigning Work to a User

You can reassign existing tasks and task planks to users on a temporary basis or permanently reassign work (as in the case of employee leaving the company) to another user.

To reassign work:

1. Locate the user. For more information, see [“Managing User Profiles” on page 2-69](#).
2. Click the name of the user. The **Associate User with Calendar** page appears.

3. If user has left the company, select the check box next to the **Is Employee Leaving Permanently** field in the **Reassign Work** section. If this check box is not selected, only existing task plans and tasks are reassigned to the selected user.
4. In the **Target User** field, select the user to whom the work should be reassigned.
5. Click **Reassign Work**.

All deployed Worklist system instances are reassigned to the selected user.

Listing and Locating Work Substitute Rules

When users are not available (due to vacation or work assignment or other reasons) for handling tasks or when users leave the organization, tasks assigned to those users need to be assigned to other users or groups.

Non-availability of the user can be handled using any of the following methods:

- Set the business calendar of the user to **Busy**. For more information, see [“Defining a Time Period Rule” on page 4-11](#).
- Re-assign the work to another user. For more information, see [“Reassigning Work to a User” on page 2-71](#).
- Define substitution rules to dynamically re-route tasks or task status notifications to a substitute user or group.

The **Work Substitute Routing Table** page displays the following properties for each work substitute rule.

| Property | Description |
|-----------------|---|
| Name | Unique identifier for the substitution rule. |
| Effective date | The date the rule takes effect. If no date is specified, the rule takes effect immediately. |
| Expiration date | The date the rule expires. If no date is specified, the rule remains in effect indefinitely. |
| Source | The user or group that will be unavailable. |
| Target | The substitute user or group. (Only a group can substitute for a group; only a user can substitute for a user.) |

The screenshot shows the 'Work Substitute Management' window. At the top, there is a 'Work Substitute Routing Table' header with a search box and a 'Search' button. Below this is a table with the following data:

| <input type="checkbox"/> | Substitute Name | Effective Date | Expiry Date | Source | Target |
|--------------------------|-----------------|-----------------|-----------------|--------|--------|
| <input type="checkbox"/> | SubstituteRule | 10/6/06 5:30 PM | 10/6/06 5:30 PM | John | Joe |

Navigation controls for the table include 'Items 1-1 of 1' and arrow buttons. At the bottom, there are 'Add Substitute' and 'Delete Substitute' buttons.

To list and locate work substitute rules:

1. In Worklist Console, select the **Worklist** module.
2. From the left panel, select **Work Substitutes**.
3. To locate a specific work substitute rule, do one of the following:
 - Filter by name. Enter the search target (use ? to match any single character or * to match zero or more characters.), then click **Search**. The rules matching the search criteria are displayed.
 - Scroll through the pages. Use the controls in the lower left corner. Go to a page by selecting the page number or by using the arrow buttons to go to the next , previous , first , or last  page.

Related Topics

- [“Adding a Work Substitute Rule” on page 2-73](#)
- [“Changing a Work Substitute Rule” on page 2-75](#)
- [“Deleting a Work Substitute Rule” on page 2-77](#)

Adding a Work Substitute Rule

The **Add Substitute** page allows you to create a work substitute rule. These rules dynamically re-route tasks or task status notifications to a substitute user or group.

Work Substitute Management

Add Substitute

Substitute Rule Name: SubstituteRule

Effective Date:
 October 6 2006
 17 30

Expiration Date:
 October 6 2006
 17 30

***Source User or Group:** John

***Target User or Group:** Joel

Submit Cancel

To add a work substitute rule:

1. In Worklist Console, select the **Worklist** module.
2. From the left panel, select **Work Substitutes**. The **Work Substitute Routing Table** page appears.
3. Click **Add Substitute**. The **Add Substitute** page appears.
4. Enter a unique name for the substitute rule.
5. Select the **Effective Date** check box and specify the **Month, Date, Year** (using YYYY format), **Hour**, and **Minute**.
 This is the date and time the rule takes effect. If you do not check the **Effective Date** check box, the rule takes effect immediately
6. Select the **Expiration Date** check box and specify the **Month, Date, Year** (using YYYY format), **Hour**, and **Minute**.
 This is the date and time the rule expires. If you do not check the **Expiration Date** check box, the rule remains in effect indefinitely.
7. In the **Source User of Group** field, enter the user or group that will be unavailable.

8. In the **Target User of Group** field, enter the substitute user or group.

Note: In the target field, only a group can substitute for a group and only a user can substitute for a user.

9. Click **Submit**.

The **Work Substitute Routing Table** page is displayed. The new rule is included in the list. The tasks and task status notification of the source are now dynamically routed to the specified target during the effective and expiration dates (inclusive).

Related Topics

- [“Listing and Locating Work Substitute Rules” on page 2-72](#)
- [“Changing a Work Substitute Rule” on page 2-75](#)
- [“Deleting a Work Substitute Rule” on page 2-77](#)

Changing a Work Substitute Rule

The **Edit Substitute Rule** page allows you to change the properties of a work substitute rule.

The screenshot shows the 'Edit Substitute Rule' form within the 'Work Substitute Management' application. The form contains the following fields and controls:

- Substitute Rule Name:** A text field containing 'SubstituteRule'.
- Effective Date:** A date selection area with a checked checkbox, a month dropdown set to 'October', a day dropdown set to '6', and a year dropdown set to '2006'. Below this are two more dropdowns for the day of the month, set to '17' and '30'.
- Expiration Date:** A date selection area with a checked checkbox, a month dropdown set to 'October', a day dropdown set to '6', and a year dropdown set to '2006'. Below this are two more dropdowns for the day of the month, set to '17' and '30'.
- *Source User or Group:** A text field containing 'John'.
- *Target User or Group:** A text field containing 'Joe'.
- Buttons:** Three buttons at the bottom: 'Submit', 'Reset', and 'Cancel'.

To change a work substitute rule:

1. Locate the rule to be updated. See [“Listing and Locating Work Substitute Rules” on page 2-72](#).
2. Click the work substitute rule name. The **Edit Substitute Rule** page appears.
3. Do one or more of the following as required:
 - Select the **Effective Date** check box and specify the **Month, Date, Year** (using *YYYY* format), **Hour**, and **Minute**.

This is the date and time the rule takes effect. If you do not check the **Effective Date** check box, the rule takes effect immediately.
 - Select the **Expiration Date** check box and specify the **Month, Date, Year** (using *YYYY* format), **Hour**, and **Minute**.

This is the date and time the rule expires. If you do not check the **Expiration Date** check box, the rule remains in effect indefinitely.
 - In the **Source User of Group** field, specify a new user or group.
 - In the **Target User of Group** field, specify a new user or group.
4. Do one of the following:
 - To update the rule, click **Submit**.

The **Work Substitute Routing Table** page is displayed. The updated rule is included in the list.

Note: If there is an error, the **Edit Substitute Rule** page is redisplayed. A message indicating the problem is displayed above the input requiring correction.
 - To disregard changes and return to the **Work Substitute Routing Table** page, click **Cancel**.
 - To reset to the last saved values, click **Reset**.

Related Topics

- [“Adding a Work Substitute Rule” on page 2-73](#)
- [“Deleting a Work Substitute Rule” on page 2-77](#)

Deleting a Work Substitute Rule

You can delete work substitute rules from the **Work Substitute Routing Table** page.

To delete work substitute rules:

1. Locate the rules to be deleted. See [“Listing and Locating Work Substitute Rules” on page 2-72](#).
2. Click the check box next to each of the substitute rules that you want to delete.
3. Click **Delete Substitute**. A confirmation message appears. Click **OK**.

The selected substitute rules are deleted.

Related Topics

- [“Adding a Work Substitute Rule” on page 2-73](#)
- [“Changing a Work Substitute Rule” on page 2-75](#)

Worklist Administration

User Management

This section provides information you need to use the *Worklist Users* module of Worklist Console. This module allows you to manage users, groups, and roles defined in the default security realm. You can add, delete, and modify users, groups, and roles defined for the default security realm.

Note: You must be logged in as a member of the Administrators or IntegrationAdministrators group to add, delete, or modify a user, group, or role. See [“WebLogic Integration Users, Groups, and Roles”](#) on page 3-3.

The following topics are provided:

- [Overview of the User Management Module](#)
- [WebLogic Integration Users, Groups, and Roles](#)
- [Security Provider Requirements for User Management](#)
- [Listing and Locating Users](#)
- [Adding a User](#)
- [Viewing and Changing User Properties](#)
- [Listing and Locating Groups](#)
- [Adding a Group](#)
- [Viewing and Changing Group Properties](#)
- [Listing and Locating Roles](#)

- [Adding a Role](#)
- [Constructing a Role Statement](#)
- [Viewing and Changing Role Conditions](#)
- [Deleting Users, Groups, or Roles](#)

Overview of the User Management Module

The following table lists the pages you can access from the Worklist Users module. The tasks and help topics associated with each are provided:

| Page | Associated Tasks | Help Topics |
|----------------------|---|---|
| Users | | |
| View and Edit Users | View a list of users. For each user, the user name, group membership, and associated authentication provider are displayed. | “Listing and Locating Groups” on page 3-12 |
| | Delete one or more users. | “Deleting Users, Groups, or Roles” on page 3-28 |
| Add New User | Add a user by assigning a unique name and password. Optionally, assign a group membership to the user. | “Adding a User” on page 3-8 |
| View User Details | View user properties. | “Viewing and Changing User Properties” on page 3-10 |
| Edit User Details | Change user properties. Update the password or assign the user to one or more groups. | “Viewing and Changing User Properties” on page 3-10 |
| Groups | | |
| View and Edit Groups | View a list of groups. Group name, group membership, and authentication provider are displayed. | “Listing and Locating Groups” on page 3-12 |
| | Delete one or more groups. | “Deleting Users, Groups, or Roles” on page 3-28 |

| Page | Associated Tasks | Help Topics |
|------------------------------|--|--|
| Add New Group | Add a group by assigning a unique name. Optionally, assign the group to one or more existing groups. | “Adding a Group” on page 3-13 |
| View Group Details | View group properties. | “Viewing and Changing Group Properties” on page 3-14 |
| Edit Group Details | Change group properties. Update the group membership details. | “Viewing and Changing Group Properties” on page 3-14 |
| Roles | | |
| View and Edit Roles | View a list of roles. Role name and provider name are displayed. | “Listing and Locating Roles” on page 3-16 |
| | Delete one or more roles. | “Deleting Users, Groups, or Roles” on page 3-28 |
| Add New Role | Add a role by assigning a unique role name and defining the conditions that constitute the role statement. | “Adding a Role” on page 3-17 |
| View Role Conditions | View or change role conditions. Add, delete, or reorder conditions. | “Viewing and Changing Role Conditions” on page 3-27 |
| Add Role Conditions | Define a condition to be added. | “Constructing a Role Statement” on page 3-18 |
| Sort Role Conditions | Change the order of the conditions in the list. | “Constructing a Role Statement” on page 3-18 |
| Edit Role Conditions Command | Change the command that joins conditions. | “Constructing a Role Statement” on page 3-18 |

WebLogic Integration Users, Groups, and Roles

Users are entities that can be authenticated. Each user is assigned a unique identity within the realm. To make it easier to administer a large number of users, users can be organized into named groups. Groups can in turn be assigned membership in other groups.

Like other components of the platform, WebLogic Integration supports role-based authorization. Although the specific users that require access to the components that make up your WebLogic Integration application may change depending upon the deployment environment, the roles that require access are typically more stable. Authorization involves granting an entity permissions and rights to perform certain actions on a resource.

In role-based authorization, security policies define the roles that are authorized to access the resource. In addition to the built-in roles that are associated with certain administrative and monitoring privileges, security policies that control access to various resources can be configured from the Worklist Console.

Once the roles required for access are set, the administrator can map users or groups to the roles as required.

Unlike membership in a group, which is directly assigned, membership in a security role is dynamically calculated based on the set of conditions that define the role statement. Each condition specifies user names, group names, or time of day. Conditions are joined by conjunction (and) or disjunction (or) commands. When a principal (user) is “in” a role based on the evaluation of the role statement, the access permissions of the role are conferred on the principal. For more information, see [“Constructing a Role Statement” on page 3-18](#).

A set of default roles are defined for WebLogic Integration as a convenience for use in system management. Additional roles can be created to control access to implementation-specific resources. The roles created using the Worklist Console are created as WebLogic Server global roles.

Note: The following sections provide information specific to WebLogic Integration. To learn more about protecting resources in a platform-based application, see [Understanding WebLogic Security](#).

Default Roles and Groups

Any domain that supports WebLogic Integration includes a set of default WebLogic Integration roles and groups.

Note: Worklist does not build knowledge of these roles into its security enforcement. These roles are used in default policy settings installed with new domains via the configuration wizard. However, users can change these default policies to use other non WebLogic Integration-defined roles.

Default Roles

The following table lists the default WebLogic Integration roles. A brief description and initial role definition statement for each is provided. To learn more, see [“Default Security Policies” on page 2-23](#).

Although you can update the role statement associated with a default role, you cannot delete these roles.

Note: In addition to the default WebLogic Integration roles, there are also a number of default WebLogic Server roles. See [“Default Global Roles” in Users, Groups, And Security Roles](#) in *Securing WebLogic Resources Using Roles and Policies*.

| Default Role | Description | Initial Role Statement |
|---------------------|--|--|
| IntegrationAdmin | The WebLogic Integration administrator role. Typically, users granted this role are responsible for administrative activities across Worklist system instances and task plans. For more information, see “Default Security Policies” on page 2-23 . | Groups:(IntegrationAdministrators, Administrators) |
| IntegrationDeployer | The WebLogic Integration deployer role. Typically, users granted this role are responsible for deploying, configuring and maintaining WebLogic Integration applications. For more information, see “Default Security Policies” on page 2-23 . | Groups:(IntegrationDeployers) |
| IntegrationMonitor | The WebLogic Integration monitor role. Typically, users granted this role monitor the health of a WebLogic Integration application, but are not authorized to make any modifications to an application. For more information, see “Default Security Policies” on page 2-23 . | Groups:(IntegrationMonitors,Monitors) |

| Default Role | Description | Initial Role Statement |
|---------------------|--|---|
| IntegrationOperator | The WebLogic Integration operator role. Typically, users in this role make routine or scheduled changes to resources. They generally do not have full administrative permissions. For more information, see “Default Security Policies” on page 2-23 . | Groups:(IntegrationOperators,Operators) |
| IntegrationUser | The default WebLogic Integration user role. When first created, all users are assigned to the IntegrationUser role. | Groups:(IntegrationUsers) |

Default Groups

The following table lists the default groups:

| Default Role | Description |
|---------------------------|--|
| IntegrationAdministrators | The WebLogic Integration administrator group. This group is assigned to the IntegrationAdmin role and all members inherit that role. |
| IntegrationDeployers | The WebLogic Integration deployers group. This group is assigned to the IntegrationDeployer role and all members inherit that role. |
| IntegrationMonitors | The WebLogic Integration monitor group. This group is assigned to the IntegrationMonitor role and all members inherit that role. |
| IntegrationOperators | The WebLogic Integration operator group. This group is assigned to the IntegrationOperator role and all members inherit that role. |
| IntegrationUsers | The WebLogic Integration user group. This group is assigned to the IntegrationUser role and all members inherit that role. |

Note: In addition to the default WebLogic Integration groups, there are also a number of default WebLogic Server groups. See [“Default Groups” in Users, Groups, And Security Roles in *Securing WebLogic Resources Using Roles and Policies*](#).

Security Provider Requirements for User Management

The ability to define users and groups, and to configure security for Worklist resources is dependent on the availability of an authenticator that implements the following MBeans:

- `UserEditor`
- `GroupEditor`
- `GroupMemberLister`
- `MemberGroupLister`

If there is no authenticator that implements all the above MBeans, all functionality in the Worklist Console related to configuring users or groups, or to granting specific privileges to users or groups, is disabled.

As described in *Understanding WebLogic Security*, it is possible to run more than one security provider at a time. If multiple authenticators are running, the Worklist console allows you to specify in which provider to create a user or group. Worklist will query users and groups by name from any configured provider.

To learn more about WebLogic Server security realms and security providers, see “[Security Realms](#)” in *Understanding WebLogic Security*.

Listing and Locating Users

The **Summary of Users** page lists all the users defined in the default security realm.

The screenshot shows the 'Summary of Users' page in the Worklist Console. The page title is 'Worklist System Instance(s) > Users'. Below the title is a search bar with the label 'Search User Name' and a 'Search' button. The table below has the following data:

| <input type="checkbox"/> | User Name ▾ | Group Membership | Authentication Provider ▲ | Options |
|--------------------------|-------------|------------------|---------------------------|---------|
| <input type="checkbox"/> | weblogic | Administrators | SQLAuthenticator | |

At the bottom of the table, there are 'Add User' and 'Delete User' buttons. The page also shows pagination controls indicating 'Items 1-1 of 1'.

To list and locate users:

1. In Worklist Console, click the **Worklist Users** module and click **Users** in the left panel to view the **Summary of Users** page.

Note: You can also view the list of users in the **Worklist User Summary** page. From this page, you can assign business calendars to a user and also reassign work to a user. For more information, see [“Associating Business Calendars with Users” on page 4-14](#) and [“Reassigning Work to a User” on page 2-71](#)

2. To locate a specific user, do one of the following:
 - Filter by user name. Enter the search target (use * to match zero or more characters.), then click **Search**. The users matching the search criteria are displayed.
 - Resort the list. Ascending  and descending  arrow buttons indicate sortable columns. Click the button to change the sort order.
 - Scroll through the pages. Use the controls in the lower left corner. Go to a page by selecting the page number or by using the arrow buttons to go to the next , previous , first , or last  page.

Related Topics

- [“WebLogic Integration Users, Groups, and Roles” on page 3-3](#)
- [“Adding a User” on page 3-8](#)
- [“Viewing and Changing User Properties” on page 3-10](#)
- [“Deleting Users, Groups, or Roles” on page 3-28](#)

Adding a User

The **Add New User - General Configuration** page allows you to create a new user.

Worklist System Instance(s) > Users

Add New User - General Configuration

Save Cancel

| User Name | Jo | | | | |
|---|--|------------------|----------------|---|--|
| Password | •••••• | | | | |
| Confirm Password | •••••• | | | | |
| Authentication Provider | SQLAuthenticator | | | | |
| Group Membership | <table border="1"> <thead> <tr> <th>Available Groups</th> <th>Current Groups</th> </tr> </thead> <tbody> <tr> <td> <ul style="list-style-type: none"> AppTesters Deployers IntegrationAdministrators IntegrationDeployers IntegrationMonitors IntegrationOperators </td> <td> <ul style="list-style-type: none"> Administrators </td> </tr> </tbody> </table> | Available Groups | Current Groups | <ul style="list-style-type: none"> AppTesters Deployers IntegrationAdministrators IntegrationDeployers IntegrationMonitors IntegrationOperators | <ul style="list-style-type: none"> Administrators |
| Available Groups | Current Groups | | | | |
| <ul style="list-style-type: none"> AppTesters Deployers IntegrationAdministrators IntegrationDeployers IntegrationMonitors IntegrationOperators | <ul style="list-style-type: none"> Administrators | | | | |

Save Cancel

To add a user:

1. In Worklist Console, select the **Worklist Users** module.
2. From the left panel, select **Users**. You can view the **Summary of Users** page.
3. Click **Add User**. The **Add New User - General Configuration** page appears.
4. Enter a unique name for the user.

Note: The name must be unique across users and groups. That is, you cannot create a user that has the same name as a group.
5. Enter a password associated with the user.

Note: The password must be at least 8 characters long.
6. Re-enter the password for confirmation.
7. Select the authentication provider from the drop-down list.
8. If required, assign the user to one or more groups as follows:
 - a. From the **Available Groups** list, select the required groups. (To select multiple groups, press and hold the **Ctrl** key as you click each additional group.)
 - b. Click the  icon to move the selected groups to the **Current Groups** list.

If required, click the  icon to remove groups from the **Current Groups** list.

9. Click **Save**.

You can view the new user in the **Summary of Users** page.

Related Topics

- [“WebLogic Integration Users, Groups, and Roles” on page 3-3](#)
- [“Viewing and Changing User Properties” on page 3-10](#)
- [“Deleting Users, Groups, or Roles” on page 3-28](#)

Viewing and Changing User Properties

The **View User Details** page displays the user properties. If you are logged in with sufficient privileges, you can access the **Edit User Details** page to make changes to the user properties.

| View User weblogic Details | |
|--|------------------|
| User Name: | weblogic |
| Authentication Provider: | SQLAuthenticator |
| Groups: | Administrators |
| <input type="button" value="Reconfigure"/> <input type="button" value="Back"/> | |

To view user properties:

1. Locate the user. For more information, see [“Listing and Locating Users” on page 3-7](#).
2. Click the user name to display the **View User Details** page.

The user name, authentication provider, and group membership are displayed.

To change user properties:

1. On the **View User Details** page, click **Reconfigure**.

2. To update the password:

a. In the **New Password** field, enter the new password.

Note: The password must be at least 8 characters long.

b. In the **Confirm Password** field, enter the new password again.

3. Add or remove group assignments as follows:

To add groups:

a. From the **Available Groups** list, select the required groups. (To select multiple groups, press and hold the **Ctrl** key as you click each additional group.)

b. Click the  icon to move the selected groups to the **Current Groups** list.

To remove groups:

a. From the **Current Groups** list, select the required groups. (To select multiple groups, press and hold the **Ctrl** key as you click each additional group.)

b. Click the  icon to move the selected groups to the **Available Groups** list.

4. Do one of the following:

– To update the user, click **Save**.

The **View and Edit Users** page is displayed.

– To disregard the changes and return to the **View and Edit Users** page, click **Cancel**.

Related Topics

- “WebLogic Integration Users, Groups, and Roles” on page 3-3
- “Deleting Users, Groups, or Roles” on page 3-28

Listing and Locating Groups

The **Summary of Groups** page lists all the groups defined in the default security realm.

Summary of Groups

Search Group Name Search

Items 1-10 of 10

| <input type="checkbox"/> | Group Name ▾ | Group Membership | Authentication Provider ▲ | Options |
|--------------------------|---------------------------|------------------|---------------------------|---------|
| <input type="checkbox"/> | Administrators | | SQLAuthenticator | |
| <input type="checkbox"/> | App Testers | | SQLAuthenticator | |
| <input type="checkbox"/> | Deployers | | SQLAuthenticator | |
| <input type="checkbox"/> | IntegrationAdministrators | | SQLAuthenticator | |
| <input type="checkbox"/> | IntegrationDeployers | | SQLAuthenticator | |
| <input type="checkbox"/> | IntegrationMonitors | | SQLAuthenticator | |
| <input type="checkbox"/> | IntegrationOperators | | SQLAuthenticator | |
| <input type="checkbox"/> | IntegrationUsers | | SQLAuthenticator | |
| <input type="checkbox"/> | Monitors | | SQLAuthenticator | |
| <input type="checkbox"/> | Operators | | SQLAuthenticator | |

Items 1-10 of 10

Add Group Delete Group

To list and locate groups:

1. In Worklist Console, click the **Worklist Users** module and click **Groups** in the left panel to view the **Summary of Groups** page.
2. To locate a specific group, do one of the following:
 - Filter by group name. Enter the search target (use ? to match any single character or * to match zero or more characters.), then click **Search**. The groups matching the search criteria are displayed.

- Resort the list. Ascending ▲ and descending ▼ arrow buttons indicate sortable columns. Click the button to change the sort order.
- Scroll through the pages. Use the controls in the lower left corner. Go to a page by selecting the page number or by using the arrow buttons to go to the next ►, previous ◀, first ◀◀, or last ▶▶ page.

Related Topics

- [“WebLogic Integration Users, Groups, and Roles”](#) on page 3-3
- [“Adding a Group”](#) on page 3-13
- [“Viewing and Changing Group Properties”](#) on page 3-14
- [“Deleting Users, Groups, or Roles”](#) on page 3-28

Adding a Group

The **Add New Group** page allows you to add a new group.

To add a group:

1. In Worklist Console, select the **Worklist Users** module.
2. From the left panel, select **Groups**. You can view the **Summary of Groups** page.
3. Click **Add Group**. The **Add New Group** page appears.

4. Enter a unique name for the group.

Note: The name must be unique across users and groups. That is, you cannot create a group that has the same name as a user.

5. Select the authentication provider from the drop-down list.

6. To make this group a member of one or more other groups, do the following:

a. From the **Available Groups** list, select the required groups. (To select multiple groups, press and hold the **Ctrl** key as you click each additional group.)

b. Click the  icon to move the selected groups to the **Current Groups** list.

If required, click the  icon to remove groups from the **Current Groups** list.

Note: To make another group a member of this new group, you must update the membership assignments for that group. For more information, see [“Viewing and Changing Group Properties”](#) on page 3-14.

7. Click **Save**.

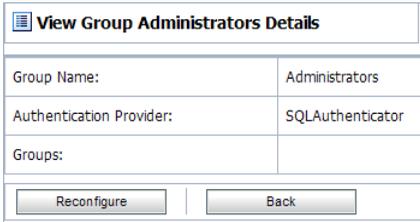
You can view the new user in the **Summary of Groups** page.

Related Topics

- [“WebLogic Integration Users, Groups, and Roles”](#) on page 3-3
- [“Viewing and Changing Group Properties”](#) on page 3-14
- [“Deleting Users, Groups, or Roles”](#) on page 3-28

Viewing and Changing Group Properties

The **View Group Details** page displays group properties. If you are logged in with sufficient privileges, you can access the **Edit Group Details** page to make changes.



| View Group Administrators Details | |
|--|------------------|
| Group Name: | Administrators |
| Authentication Provider: | SQLAuthenticator |
| Groups: | |
| <input type="button" value="Reconfigure"/> <input type="button" value="Back"/> | |

To view group properties:

1. Locate the group. See [“Listing and Locating Groups”](#) on page 3-12.
2. Click the group name to display the **View Group Details** page.

The name assigned to the group, authentication provider, and all the groups in which the current group is a member are displayed.

To change group properties:

1. On the **View Group Details** page, click **Reconfigure**. The Edit Group

2. Add or remove group membership assignments as follows:

To add groups:

- a. From the **Available Groups** list, select the required groups. (To select multiple groups, press and hold the **Ctrl** key as you click each additional group.)
- b. Click the  icon to move the selected groups to the **Current Groups** list.

To remove groups:

- a. From the **Current Groups** list, select the required groups. (To select multiple groups, press and hold the **Ctrl** key as you click each additional group.)
 - b. Click the  icon to move the selected groups to the **Available Groups** list.
3. Do one of the following:
 - To update the group, click **Save Changes**.

The **View and Edit Groups** page is displayed.

- To disregard the changes and return to the **View and Edit Groups** page, click **Cancel**.

Related Topics

- [“WebLogic Integration Users, Groups, and Roles” on page 3-3](#)
- [“Deleting Users, Groups, or Roles” on page 3-28](#)

Listing and Locating Roles

The **Global Roles** page lists the roles defined in the default security realm.

| <input type="checkbox"/> | Role Name ↕ | Provider Name |
|--------------------------|---------------------|-----------------|
| <input type="checkbox"/> | Admin | XACMLRoleMapper |
| <input type="checkbox"/> | Anonymous | XACMLRoleMapper |
| <input type="checkbox"/> | AppTester | XACMLRoleMapper |
| <input type="checkbox"/> | Deployer | XACMLRoleMapper |
| <input type="checkbox"/> | IntegrationAdmin | XACMLRoleMapper |
| <input type="checkbox"/> | IntegrationDeployer | XACMLRoleMapper |
| <input type="checkbox"/> | IntegrationMonitor | XACMLRoleMapper |
| <input type="checkbox"/> | IntegrationOperator | XACMLRoleMapper |
| <input type="checkbox"/> | IntegrationUser | XACMLRoleMapper |
| <input type="checkbox"/> | Monitor | XACMLRoleMapper |

To list and locate roles:

1. In Worklist Console, click the **Worklist Users** module and click **Roles** in the left panel. The **Global Roles** page appears.
2. To locate a specific role, do one of the following:
 - Resort the list. Ascending ▲ and descending ▼ arrow buttons indicate sortable columns. Click the button to change the sort order.
 - Scroll through the pages. Use the controls in the lower left corner. Go to a page by selecting the Next and Previous links.

Related Topics

- [“WebLogic Integration Users, Groups, and Roles” on page 3-3](#)

- “Adding a Role” on page 3-17
- “Constructing a Role Statement” on page 3-18
- “Viewing and Changing Role Conditions” on page 3-27
- “Deleting Users, Groups, or Roles” on page 3-28

Adding a Role

The **Add New Role** page allows you to create a new role.

To add a role:

1. In Worklist Console, select the **Worklist Users** module.
2. From the left panel, select **Roles**. You can view a list of existing global roles.
3. Click **New**. The **Create New Group** page appears.
4. Enter a unique name for the new role.
5. Select the provider name for the role from the drop-down list.
6. Click **OK**.

The role is created and is listed in the Roles page. You may need to click Next to view the new role.

Related Topics

- [“WebLogic Integration Users, Groups, and Roles” on page 3-3](#)
- [“Listing and Locating Roles” on page 3-16](#)
- [“Constructing a Role Statement” on page 3-18](#)
- [“Viewing and Changing Role Conditions” on page 3-27](#)
- [“Deleting Users, Groups, or Roles” on page 3-28](#)

Constructing a Role Statement

To determine who is in a security role at runtime, a role contains one or more conditions. For example, a basic role might simply name the Administrator group. At runtime, the WebLogic Security Service interprets this policy as "place the Administrator group in this role." For more information, see [“Adding Conditions to a Role Statement” on page 3-19](#).

You can create more complex conditions and combine them using the logical operators AND and OR (which is an inclusive OR). You can also negate any condition, which would make sure that a user is not in the role. The entire collection of conditions must be true for a user or group to be granted the security role.

Role Conditions

Combination

- NOT** Group : Deployer
 - Or
- User : John

Or

Group : Administrators

After you have added conditions to the statement, you can update the joining commands, move the position of a condition, combine conditions, delete conditions, or negate a condition. For more information, see [“Modifying the Role Statement” on page 3-26](#).

Adding Conditions to a Role Statement

If you are logged in with sufficient privileges, you can add conditions from the **Global Role Conditions** page. The **Global Role Conditions** page is displayed when you select a role from the Global Roles list. See [“Listing and Locating Roles” on page 3-16](#).

When you add a condition to a role statement, you can use any of the existing predicates or policy conditions. Each predicate is a predefined role statement that can be used to define the security policy statement. For each predicate, you need to edit the arguments that are associated with that predicate.

These predicates include:

- Basic role conditions that include adding specified users or groups to the role, allowing or denying access to everyone, and so on.
- Date and time based role conditions, which are used to grant access to the principals based on the date or time you specify.
- Context element role conditions, which are used to create security roles based on the value of HTTP Servlet Request attributes, HTTP Session attributes, and EJB method parameters.

For more information, see [“Security Role Conditions” in Users, Groups, And Security Roles in Securing WebLogic Resources Using Roles and Policies](#).

To add a group to the role:

1. On the **Global Role Conditions** page, click **Add Condition**. The **Choose a Predicate** page appears.

2. Select **Group** from the **Predicate List** drop-down list.
3. Click **Next**. The **Edit Arguments** page appears.
4. Specify the group name and click **Add**.

You can add one or more groups to this role. If you add multiple groups, the condition evaluates as true if the user is a member of ANY of the groups associated with this role.

Note: To remove any group, select the group in the Remove list and click **Remove**.

5. Click **Finish**.

The condition is added to the role statement and displayed on the **Global Role Conditions** page.

To add a users to the role:

1. On the **Global Role Conditions** page, click **Add Condition**. The **Choose a Predicate** page appears.
2. Select **User** from the **Predicate List** drop-down list.
3. Click **Next**. The **Edit Arguments** page appears.
4. Specify the user name and click **Add**.

You can add one or more users to this role.

Note: To remove any user, select the user in the Remove list and click **Remove**.

5. Click **Finish**.

The condition is added to the role statement and displayed on the **Global Role Conditions** page.

To add principals to this role only on specified days of the week:

1. On the **Global Role Conditions** page, click **Add Condition**. The **Choose a Predicate** page appears.
2. Select **Access occurs on specified days of the week** from the **Predicate List** drop-down list.
3. Click **Next**. The **Edit Arguments** page appears.
4. Enter the day of the week on which principals will be assigned to this role.
5. Enter the GMT offset. If the time zone in your location is ahead of GMT, enter **GMT + hh:mm** and if time zone in your location is behind GMT, enter **GMT -hh:mm**.
6. Click **Finish**.

The condition is added to the role statement and displayed on the **Global Role Conditions** page.

To add principals to this role only between a specified time:

1. On the **Global Role Conditions** page, click **Add Condition**. The **Choose a Predicate** page appears.
2. Select **Access occurs between specified hours** from the **Predicate List** drop-down list.
3. Click **Next**. The **Edit Arguments** page appears.
4. Enter the start time and the end time between which principals will be assigned to this role. Enter time in **hh:mm AM|PM** format.
5. Enter the GMT offset. If the time zone in your location is ahead of GMT, enter **GMT + hh:mm** and if time zone in your location is behind GMT, enter **GMT -hh:mm**.
6. Click **Finish**.

The condition is added to the role statement and displayed on the **Global Role Conditions** page.

To add principals to this role only when the context element's value is greater than a numeric constant:

1. On the **Global Role Conditions** page, click **Add Condition**. The **Choose a Predicate** page appears.
2. Select **Context element's value is greater than a numeric constant** from the **Predicate List** drop-down list.
3. Click **Next**. The **Edit Arguments** page appears.
4. Enter the name of the context element.
5. Enter a numeric value. Principals are assigned to this role based on the specified context element's value being greater than this number.
6. Click **Finish**.

The condition is added to the role statement and displayed on the **Global Role Conditions** page.

To deny access to everyone:

1. On the **Global Role Conditions** page, click **Add Condition**. The **Choose a Predicate** page appears.
2. Select **Deny Access to everyone** from the **Predicate List** drop-down list.

3. Click **Finish**.

All users and groups are denied access to this role.

To add principals to this role only when the context element's value is equal to a numeric constant:

1. On the **Global Role Conditions** page, click **Add Condition**. The **Choose a Predicate** page appears.
2. Select **Context element's value equals a numeric constant** from the **Predicate List** drop-down list.
3. Click **Next**. The **Edit Arguments** page appears.
4. Enter the name of the context element.
5. Enter a numeric value. Principals are assigned to this role based on the specified context element's value being equal to this number.
6. Click **Finish**.

The condition is added to the role statement and displayed on the **Global Role Conditions** page.

To add principals to this role only before a specified date:

1. On the **Global Role Conditions** page, click **Add Condition**. The **Choose a Predicate** page appears.
2. Select **Access occurs before** from the **Predicate List** drop-down list.
3. Click **Next**. The **Edit Arguments** page appears.
4. Enter the date before which principals will be assigned to this role. Enter date in **m/d/yy** or **m/d/yy hh:mm:ss AM|PM** format.
5. Enter the GMT offset. If the time zone in your location is ahead of GMT, enter **GMT + hh:mm** and if time zone in your location is behind GMT, enter **GMT -hh:mm**.
6. Click **Finish**.

The condition is added to the role statement and displayed on the **Global Role Conditions** page.

To add principals to this role only on the specified day of the month:

1. On the **Global Role Conditions** page, click **Add Condition**. The **Choose a Predicate** page appears.

2. Select **Access occurs on the specified day of the month** from the **Predicate List** drop-down list.
3. Click **Next**. The **Edit Arguments** page appears.
4. Enter the day of the month on which principals will be assigned to this role.
Principals will be assigned to this role only after an ordinal day in the month. Enter the ordinal number of the day within the current month with values in the range from -31 to 31. Negative values count back from the end of the month, so the last day of the month is specified as -1. 0 indicates the day before the first day of the month.
5. Enter the GMT offset. If the time zone in your location is ahead of GMT, enter **GMT + hh:mm** and if time zone in your location is behind GMT, enter **GMT -hh:mm**.
6. Click **Finish**.

The condition is added to the role statement and displayed on the **Global Role Conditions** page.

To add principals to this role only when the context element's value is equal to a string constant:

1. On the **Global Role Conditions** page, click **Add Condition**. The **Choose a Predicate** page appears.
2. Select **Context element's value equals a string constant** from the **Predicate List** drop-down list.
3. Click **Next**. The **Edit Arguments** page appears.
4. Enter the name of the context element.
5. Enter a string value. Principals are assigned to this role based on the specified context element's value being equal to this string value.
6. Click **Finish**.

The condition is added to the role statement and displayed on the **Global Role Conditions** page.

To add principals only when the defined context element is available:

1. On the **Global Role Conditions** page, click **Add Condition**. The **Choose a Predicate** page appears.
2. Select **Context element defined** from the **Predicate List** drop-down list.
3. Click **Finish**.

Principals are assigned to this role only when the specified context element exists.

To allow access to everyone:

1. On the **Global Role Conditions** page, click **Add Condition**. The **Choose a Predicate** page appears.
2. Select **Allow Access to everyone** from the **Predicate List** drop-down list.
3. Click **Finish**.

All users and groups are assigned to this role.

To add principals only after a specified date:

1. On the **Global Role Conditions** page, click **Add Condition**. The **Choose a Predicate** page appears.
2. Select **Allow access after** from the **Predicate List** drop-down list.
3. Click **Next**. The **Edit Arguments** page appears.
4. Enter the date after which principals will be assigned to this role. Enter date in **m/d/yy** or **m/d/yy hh:mm:ss AM|PM** format.
5. Enter the GMT offset. If the time zone in your location is ahead of GMT, enter **GMT + hh:mm** and if time zone in your location is behind GMT, enter **GMT -hh:mm**.
6. Click **Finish**.

The condition is added to the role statement and displayed on the **Global Role Conditions** page.

To add principals only before the specified day of the month:

1. On the **Global Role Conditions** page, click **Add Condition**. The **Choose a Predicate** page appears.
2. Select **Access occurs before the specified day of the month** from the **Predicate List** drop-down list.
3. Click **Next**. The **Edit Arguments** page appears.
4. Enter the day of the month before which principals will be assigned to this role.

Principals will be assigned this role only before an ordinal day in the month. Enter the ordinal number of the day within the current month with values in the range from -31 to

31. Negative values count back from the end of the month, so the last day of the month is specified as -1. 0 indicates the day before the first day of the month.
5. Enter the GMT offset. If the time zone in your location is ahead of GMT, enter **GMT + hh:mm** and if time zone in your location is behind GMT, enter **GMT -hh:mm**.
 6. Click **Finish**.

The condition is added to the role statement and displayed on the **Global Role Conditions** page.

To add principals to this role only when the context element's value is less than a numeric constant:

1. On the **Global Role Conditions** page, click **Add Condition**. The **Choose a Predicate** page appears.
2. Select **Context element's value is less than a numeric constant** from the **Predicate List** drop-down list.
3. Click **Next**. The **Edit Arguments** page appears.
4. Enter the name of the context element.
5. Enter a numeric value. Principals are assigned to this role based on the specified context element's value being less than this number.
6. Click **Finish**.

The condition is added to the role statement and displayed on the **Global Role Conditions** page.

To add principals only after the specified day of the month:

1. On the **Global Role Conditions** page, click **Add Condition**. The **Choose a Predicate** page appears.
2. Select **Access occurs after the specified day of the month** from the **Predicate List** drop-down list.
3. Click **Next**. The **Edit Arguments** page appears.
4. Enter the day of the month after which principals will be assigned to this role.

Principals will be assigned this role only after an ordinal day in the month. Enter the ordinal number of the day within the current month with values in the range from -31 to 31. Negative values count back from the end of the month, so the last day of the month is specified as -1. 0 indicates the day before the first day of the month.

5. Enter the GMT offset. If the time zone in your location is ahead of GMT, enter **GMT + hh:mm** and if time zone in your location is behind GMT, enter **GMT -hh:mm**.
6. Click **Finish**.

The condition is added to the role statement and displayed on the **Global Role Conditions** page.

To add principals only when Server is running in development mode:

1. On the **Global Role Conditions** page, click **Add Condition**. The **Choose a Predicate** page appears.
2. Select **Server is in development mode** from the **Predicate List** drop-down list.
3. Click **Finish**.

Users and groups will be assigned to this role only when the server is running in development mode.

Modifying the Role Statement

If you are logged in with sufficient privileges, you can update the conditions in the role statement, move the position of the conditions, or delete conditions from the **Global Role Conditions** page.

To update a condition:

1. On the **Global Role Conditions** page, click the value associated with the role condition. The **Edit Arguments** page appears.
2. Make required changes and click **Finish**. You return to the **Global Role Conditions** page.
3. Click **Save**.

The condition is updated.

In addition to updating a condition, you can use the following action buttons to modify the role statement:

| Action button | Click this button to |
|----------------------|---|
| Add Condition | Add a condition to the role statement |
| Combine | Combine two or more conditions in the role statement. Select the check box next to the conditions that you want to combine. Conditions in the combination are first validated before moving to the next condition in the role statement. |
| Uncombine | Remove the combine relation between conditions in a combination. Select the check box next to Combination before you click this action button. |
| Move Up | Move up the validation order of the selected condition. |
| Move Down | Move down the validation order of the selected condition. |
| Remove | Delete a selected condition from the role statement. Click the check box next to the condition to select it for deletion. |
| Negate | Negate a selected condition. That is, apply the NOT binary operation on the condition. For example, if the condition is NOT Group: Deployer, it means that all groups except the Deployer group are associated with the role. |

Related Topics

- [“WebLogic Integration Users, Groups, and Roles” on page 3-3](#)
- [“Listing and Locating Roles” on page 3-16](#)
- [“Adding a Role” on page 3-17](#)
- [“Viewing and Changing Role Conditions” on page 3-27](#)
- [“Deleting Users, Groups, or Roles” on page 3-28](#)

Viewing and Changing Role Conditions

The **View Role Conditions** page displays the role statement. If you are logged in with sufficient privileges, you can access the **Edit Role Details** page to make changes.

Save

Global Role Conditions

This page is used to edit the conditions for a global role on an application.

This is the name of the global role.

Name Admin

These conditions determine membership in the role.

Role Conditions

Add Conditions Combine Uncombine Move Up Move Down Remove Negate

Group : Administrators

Add Conditions Combine Uncombine Move Up Move Down Remove Negate

Save

To view and edit role conditions:

1. Locate the role. For more information, see [“Listing and Locating Roles”](#) on page 3-16.
2. Click the role name to display the **Global Role Conditions** page.
The role name and role statement are displayed.
3. To edit the role statement, see [“Constructing a Role Statement”](#) on page 3-18.

Related Topics

- [“WebLogic Integration Users, Groups, and Roles”](#) on page 3-3
- [“Listing and Locating Roles”](#) on page 3-16
- [“Adding a Role”](#) on page 3-17
- [“Deleting Users, Groups, or Roles”](#) on page 3-28

Deleting Users, Groups, or Roles

You can delete users, groups, or roles from the respective View and Edit page.

To delete users:

1. Locate the users to be deleted. For more information, see [“Listing and Locating Groups”](#) on page 3-12.
2. Click the check box to the left of all the users you want to delete.

3. Click **Delete** or the  icon. A confirmation message appears. Click **OK**.

To delete groups:

1. Locate the groups to be deleted. For more information, see [“Listing and Locating Groups” on page 3-12](#).
2. Click the check box to the left of all the groups you want to delete.
3. Click **Delete** or the  icon. A confirmation message appears. Click **OK**.

To delete roles:

1. Locate the roles to be deleted. For more information, see [“Listing and Locating Roles” on page 3-16](#).
2. Click the check box to the left of all the roles you want to delete.
3. Click **Delete**. A confirmation message appears. Click **Yes**.

User Management

Business Calendar Configuration

This section provides the information you need to use the *Business Calendar* module of Worklist Console.

Note: You must be logged in as a member of the Administrators, IntegrationAdministrators, or IntegrationOperators group to map, import, or otherwise modify a business calendar. See [“WebLogic Integration Users, Groups, and Roles”](#) on page 3-3.

The following topics are provided:

- [About Business Calendars and Business Time Calculations](#)
- [Overview of the Business Calendar Module](#)
- [Viewing and Changing Business Calendars](#)
- [Adding a Business Calendar](#)
- [Viewing and Changing Business Calendars](#)
- [Defining a Time Period Rule](#)
- [Associating Business Calendars with Users](#)
- [Exporting and Importing Business Calendars](#)
- [Deleting Business Calendars](#)

About Business Calendars and Business Time Calculations

Business calendars represent the operating hours of a business. A business calendar specifies a time zone and a set of time period rules. The time period rules determine the days, dates, and hours that are free (available for business activities) and busy (unavailable for business activities). Time period rules are evaluated in sequence as follows:

- Rules that appear later in the list supersede rules that appear earlier in the list.
- Intervals for which there are no rules are busy intervals.

A business calendar can be used for business calendar calculation and for checking user availability for a task.

The following examples illustrate how to a business calendar is constructed.

Example 1

The following is an example of a business calendar for the year 2003:

| Time Periods | Free or Busy |
|----------------------|--------------|
| Mon, 9:00AM - 5:00PM | Free |
| Wed, 9:00AM - 5:00PM | Free |
| Fri, 9:00AM - 5:00PM | Free |
| Jan 1, 2003 | Busy |
| Oct 13, 2003 | Busy |
| Feb 17, 2003 | Busy |
| May 26, 2003 | Busy |
| Jul 4, 2003 | Busy |
| Sep 1, 2003 | Busy |

In the above, the first three rules define Mondays and Wednesdays from 9 to 5 as free. By default, all other time is busy. The remaining rules designate the American business holidays that fall on Mondays, Wednesdays, or Fridays as busy, selectively overriding the regular free intervals.

Example 2

The following is an example of a business calendar for a night-shift worker whose regular hours are from 10 PM to 6 AM three nights a week.

| <input type="checkbox"/> | Time Periods | Free or Busy |
|--------------------------|------------------------|--------------|
| <input type="checkbox"/> | Sun, 10:00PM - 11:59PM | Free |
| <input type="checkbox"/> | Mon, 0:00AM - 6:00AM | Free |
| <input type="checkbox"/> | Tue, 10:00PM - 11:59PM | Free |
| <input type="checkbox"/> | Wed, 0:00AM - 6:00AM | Free |
| <input type="checkbox"/> | Thu, 10:00PM - 11:59PM | Free |
| <input type="checkbox"/> | Fri, 0:00AM - 6:00AM | Free |

Of the calendars defined within WebLogic Integration, one must be designated as the system calendar. Initially, the system calendar is a default calendar named **System Calendar**, but you can switch the system calendar designation to a custom calendar at any time.

When allocating worklist tasks to users, the business calendar assigned to a user can be referenced to determine whether or not the user is available. Each user is associated with one of the following:

- *A named calendar*

In this case, the specified calendar is used to determine busy and free time.

- *No calendar*

In this case, the calendar currently designated as the system calendar is used to determine busy or free time.

In addition to being mapped to users in order to determine user availability, business calendars are used in the calculation of *business time*. When specifying the times that business events are to take place (such as a message being sent or a particular task instance becoming overdue), you may wish to express time intervals in business time by associating the interval with a business calendar. For example, suppose the following:

- A Timer event generator is configured to send a message every 24 hours from January 1 to January 31, 2003.
- The business calendar shown in [Example 1](#) is associated with the 24 hour interval. Therefore, the 24 hour interval represents business time calculated against the calendar.

When calculating business time, free time periods are counted to determine when a business time interval has elapsed. Based on the business calendar shown at the beginning of this section, the free days in January fall on the following dates: 3, 6, 8, 10, 13, 15, 17, 22, 24, 27, 29, 31. Since each free day has 8 free hours, a Timer event generator configured to send a message every 24 business hours would send messages at 5 PM on the 8th, 15th, 24th, and 31st.

For more information, see “Defining Channel Rules for a Timer Event Generator” in [Event Generators](#) in *Using the WebLogic Integration Administration Console*.

When calculating business time against a business calendar, if the interval is specified by a mixture of days, hours, and minutes (for example, 3 days, 4 hours, and 5 minutes), the days are accounted for first, then the hours, and finally the minutes. The passage of a day in a business calendar is the passage of any day or date that has any free time defined for it.

If the calculation lands on a time that is busy, the calendar is rolled in the direction of the operation in one minute intervals until the next free time is reached. For example, if the calculation adds time (`addBusinessTime` method) and the addition lands on a busy time, the result rolls forward in one minute intervals until next available free minute. Alternately, if the calculation subtracts time (`subtractBusinessTime` method) and the subtraction lands on a busy time, the result rolls backward in one minute intervals until next available free minute. For instance, if the free time is 9:00 AM. to 5:00 PM, the subtraction rolls back to 4:59 PM.

For additional information about the methods available for business calendar operations (for example, determining whether or not a user is free or determining a due date based on the passage of a business time interval), see the com.bea.wli.calendar.api Javadoc.

Overview of the Business Calendar Module

The following table lists the pages you can access from the Business Calendar module. The tasks and help topics associated with each are provided.

| Page | Associated Tasks | Help Topics |
|---|---|---|
| Business Calendar Management | View a list of business calendars. Calendar name, status (in use: true or false), and type (system calendar: true or false) are displayed. | “Viewing and Changing Business Calendars” on page 4-7 |
| | Add a business calendar. | “Adding a Business Calendar” on page 4-6 |
| | Export or import business calendar time period rules and time zone. | “Exporting and Importing Business Calendars” on page 4-15 |
| | Delete a business calendar. | “Deleting Business Calendars” on page 4-17 |
| View Business Calendar Details | View business calendar properties. Business calendar name, time zone, time period rules, and type (indication of whether or not the calendar is the system calendar) are displayed. | “Viewing and Changing Business Calendars” on page 4-7 |
| | Update time period rules by adding, changing, deleting or reordering (sorting) rules | |
| Add Business Calendar Time Period Rule | Define a time period rule to be added. | “Defining a Time Period Rule” on page 4-11 |
| Update Business Calendar Time Period Rule | Change an existing time period rule. | |
| Associate Users to a Business Calendar | Select a business calendar and assign the calendar to selected users. | “Deleting Business Calendars” on page 4-17 |
| | Remove the business calendar assignment from selected users. | |

Listing and Locating Business Calendars

The **Business Calendar Management** page lists the defined business calendars. For each business calendar, the **In Use** and **Is System Calendar** status (true or false) are also displayed.

The screenshot shows the 'Business Calendar Management' interface. At the top, there is a search bar and a 'Search' button. Below that are buttons for 'Add Calendar', 'Export', 'Import', and 'Delete'. A table displays two items, with 'Items 1-2 of 2' and a page indicator '1'. The table has columns for 'Calendar Name', 'In Use', and 'Is System Calendar'. Below the table is another set of 'Add Calendar', 'Export', 'Import', and 'Delete' buttons.

| <input type="checkbox"/> | Calendar Name ▾ | In Use ▲ | Is System Calendar ▲ |
|--------------------------|--------------------------------|----------|----------------------|
| <input type="checkbox"/> | Acme Financial System Calendar | false | false |
| <input type="checkbox"/> | System Calendar | false | true |

To list and locate roles:

1. In Worklist Console, select the **Business Calendar** module.
2. To locate a specific business calendar, do one of the following:
 - Filter by business calendar name. Enter the search target, then click **Search**. The business calendars matching the search criteria are displayed.
 - Resort the list. Ascending ▲ and descending ▼ arrow buttons indicate sortable columns. Click the button to change the sort order.
 - Scroll through the pages. Use the controls in the lower left corner. Go to a page by selecting the page number or by using the arrow buttons to go to the next ►, previous ◀, first ◀◀, or last ▶▶ page.

Related Topics

- [“Viewing and Changing Business Calendars” on page 4-7](#)
- [“Adding a Business Calendar” on page 4-6](#)
- [“Exporting and Importing Business Calendars” on page 4-15](#)
- [“Deleting Business Calendars” on page 4-17](#)

Adding a Business Calendar

The **Create Business Calendar** page allows you to add a new calendar.

The screenshot shows a web-based dialog box for creating a business calendar. At the top, it indicates the current location: 'Worklist System Instance(s) > Business Calendar'. Below this is a header for the 'Calendar Portlet'. The main content area features a 'Create Business Calendar' button. Underneath, there is a text input field labeled '*Name of Calendar:' containing the text 'TestCalendar'. At the bottom of the dialog, there are two buttons: 'Create' and 'Cancel'.

To add a business calendar:

1. In Worklist Console, select the **Business Calendar** module. The **Business Calendar Management** page appears.
2. Click **Add Calendar**. The **Create Business Calendar** page appears.
3. In the **Business Calendar Name** field, enter a unique name.
4. Click **Create**.

The business calendar is created with a default set of time period rules.

5. Update the time period rules as required. For more information, see [“Viewing and Changing Business Calendars”](#) on page 4-7.

Related Topics

- [“About Business Calendars and Business Time Calculations”](#) on page 4-2
- [“Viewing and Changing Business Calendars”](#) on page 4-7
- [“Defining a Time Period Rule”](#) on page 4-11
- [“Associating Business Calendars with Users”](#) on page 4-14

Viewing and Changing Business Calendars

The **View Business Calendar Details** page allows you to view the business calendar properties.

Business Calendar Configuration

 **View Business Calendar Details**

Business Calendar Name: System Calendar
Time Zone: Asia/Calcutta
Is a system calendar: true
[Edit Calendar Details...](#)

Time Period Rules:

Items 1-5 of 5

| <input type="checkbox"/> | Time Periods | Free or Busy |
|--------------------------|----------------------|--------------|
| <input type="checkbox"/> | Mon, 9:00AM - 5:00PM | Free |
| <input type="checkbox"/> | Tue, 9:00AM - 5:00PM | Free |
| <input type="checkbox"/> | Wed, 9:00AM - 5:00PM | Free |
| <input type="checkbox"/> | Thu, 9:00AM - 5:00PM | Free |
| <input type="checkbox"/> | Fri, 9:00AM - 5:00PM | Free |

Items 1-5 of 5

[Add a New Rule...](#)
[Sort Calendar Rules...](#)

If you are logged in with sufficient privileges, you can:

- Update the time zone or designate a calendar as the system calendar.
- Add a time period rule.
- Change a time period rule.
- Delete one or more time period rules.
- Sort the time period rules.

To view business calendar properties:

1. Locate the business calendar. For more information, see [“Viewing and Changing Business Calendars” on page 4-7](#).
2. Click the calendar name to display the **View Business Calendar Details** page.

The calendar name, time zone, type (system calendar true or false), and time period rules are displayed.

To update the time zone or designate a calendar as the system calendar:

1. On the **View Business Calendar Details** page, click **Edit Calendar Details**.

The **Edit Business Calendar** page is displayed.

2. Do one or both of the following:

- To update the time zone, select a new time zone for the **Time Zone** drop-down list.
- To designate this calendar as the system calendar, check the **Set as system calendar** check box.

Note: If the current calendar has already been designated as the system calendar, this check box is not available in the **Edit Business Calendar** page.

3. Click **Submit**.

To add a time period rule:

1. On the **View Business Calendar Details** page, click **Add a New Rule**.

The **Add Business Calendar Time Period Rule** page is displayed.

Add Business Calendar Time Period Rule

Business Calendar Name: Acme Financial System Calendar

Time Period Type: Day of Week

Day of Week: Thu

Start Hour and Minute: 10 : 00 Optional

End Hour and Minute: 17 : 00 Optional

Free or Busy: Busy

Submit Reset Cancel

2. Define the time period as required. For more information, see [“Defining a Time Period Rule” on page 4-11.](#)
3. Click **Submit** to add the rule and return to the **View Business Calendar Details** page.

To change a time period rule:

1. From the Time Period Rules table, select the rule that you want to change.
The **Update Business Calendar Time Period Rule** page is displayed.

Update Business Calendar Time Period Rule

Business Calendar Name: Acme Financial System Calendar

Time Period Type: Day of Week

Day Of Month: Sat

Start Hour and Minute: 08 : 00 Optional

End Hour and Minute: 12 : 00 Optional

Free or Busy: Busy

Submit Reset Cancel

2. Define the time period as required. For more information, see [“Defining a Time Period Rule” on page 4-11.](#)
3. Click **Submit** to update the rule and return to the **View Business Calendar Details** page.

To sort the time period rules:

1. On the **View Business Calendar Details** page, click **Sort Calendar Rules**.
The **Sort Calendar Rules** page is displayed.

Sort Calendar Rules

Business Calendar Name: Acme Financial System Calendar

Time Period Rules:

| Time Periods | Free or Busy | |
|-----------------------|--------------|---|
| Mon, 8:00AM - 6:00PM | Free | ▼ |
| Tue, 8:00AM - 6:00PM | Free | ↕ |
| Wed, 8:00AM - 6:00PM | Free | ↕ |
| Thu, 8:00AM - 6:00PM | Free | ↕ |
| Fri, 8:00AM - 6:00PM | Free | ↕ |
| Sat, 8:00AM - 12:00PM | Free | ▲ |

Items 1-6 of 6

2. Move the position of a rule by clicking the up or down arrow to the right of the rule.
3. Click **Submit** to update the list and return to the **View Business Calendar Details** page.

To delete a time period rule:

1. In the Time Period Rules table, click the check box to the left of the rule or rules that you want to delete.
2. Click **Delete Rule**. A confirmation message appears. Click **OK**.

Defining a Time Period Rule

The **Add Business Calendar Time Period Rule** and **Update Business Calendar Time Period Rule** pages allow you to define the properties of a time period rule. There are three types of rules:

- Day of the Week
- Calendar Date
- Date Range

To define a Day of the Week rule:

1. From the **Time Period Type** drop-down list, select **Day of Week**.

Time Period Type: Day of Week
Day of Week: Sun
Start Hour and Minute: 00 : 00 Optional
End Hour and Minute: 00 : 00 Optional
Free or Busy: Free

- From the **Day of Month** drop-down list, select **Sun, Mon, Tues, Wed, Thu, Fri, or Sat**.
- Specify the time period interval in 24 hour time format (also known as military time) as follows:
 - From the **Start hour and minute** drop-down lists, select the time period start hour and minute.
 - From the **End hour and minute** drop-down lists, select the time period end hour and minute.

Note: If you do not specify start and end times (that is, if **00:00** is specified for both) the **Free or Busy** status specified in the following step applies to the entire day.

- From the **Free or Busy** drop-down list, select **Free or Busy**.

To define a Calendar Date rule:

- From the **Time Period Type** drop-down list, select **Calendar Date**.

Time Period Type: Calendar Date
Year: 2006 Optional Format: YYYY
Month: Nov Optional
Day Of Month: 16
Start Hour and Minute: 08 : 00 Optional
End Hour and Minute: 12 : 00 Optional
Free or Busy: Free
Submit Reset Cancel

- In the **Year** field, specify the year in **YYYY** format.
- From the **Month** drop-down list, select the month.
- From the **Day of the Month** drop-down list, select the date.

5. Specify the time period interval in 24 hour time format (also known as military time) as follows:
 - From the **Start hour and minute** drop-down lists, select the time period start hour and minute.
 - From the **End hour and minute** drop-down lists, select the time period end hour and minute.

Note: If you do not specify start and end times (that is, if **00:00** is specified for both) the **Free or Busy** status specified in the following step applies to the entire day.

6. From the **Free or Busy** drop-down list, select **Free** or **Busy**.

To define a Date Range rule:

1. From the **Time Period Type** drop-down list, select **Date Range**.

The screenshot shows a configuration window for a Time Period Rule. The 'Time Period Type' is set to 'Date Range'. The 'Year' field is '2006'. The 'Start Month' is 'Mar', 'End Month' is 'Nov', 'Start Day Of Month' is '1', and 'End Day Of Month' is '1'. The 'Free or Busy' status is set to 'Busy'. There are 'Submit', 'Reset', and 'Cancel' buttons at the bottom. A note 'Optional Format: YYYY' is visible next to the Year field.

2. In the **Year** field, specify the year in *YYYY* format.
3. Select the time period start date as follows:
 - From the **Start Month** drop-down list, select the month.
 - From the **Start Day of the Month** drop-down list, select the date.
4. Select the time period end date as follows:
 - From the **End Month** drop-down list, select the month.
 - From the **End Day of the Month** drop-down list, select the date.
5. From the **Free or Busy** drop-down list, select **Free** or **Busy**.

Related Topics

- [“Viewing and Changing Business Calendars” on page 4-7](#)

Associating Business Calendars with Users

The **Associate Users with Calendar** page allows you to:

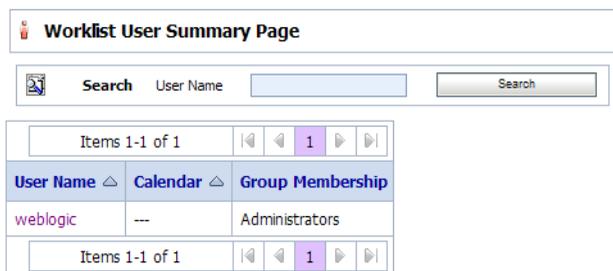
- Assign a business calendar to a user.
- Remove the business calendar assignment from a user.

Notes:

- If a user is not mapped to a calendar, the system calendar is used. To learn how a calendar mapped to a user can be used in determining worklist task dates, see “Task Due Dates” in [Creating and Managing Worklist Tasks](#) in *Using the Worklist*.
- If an authenticator that implements the required MBeans is not configured, the calendar mapping options are disabled. To learn more about the authenticator requirements, see [“Security Provider Requirements for User Management” on page 3-7](#).

To assign a business calendar to one or more users:

1. In Worklist Console, select the **Worklist** module.
2. From the left panel, select **User Profiles**. The **Worklist Users Summary Page** appears.



3. Click the name of the user to whom you want to associate a business calendar. The **Associate User with Calendar** page appears.

4. Specify the e-mail address of the user.
5. From the **Shared Calendar** drop-down list, select a named calendar, or select **System Calendar**.
6. Click **Submit** to assign the selected calendar to the user.

To remove the business calendar assignment from one or more users:

1. In Worklist Console, select the **Worklist** module.
2. From the left panel, select **User Profiles**. The **Worklist Users Summary Page** appears.
3. Click the name of the required user. The **Associate User with Calendar** page appears.
4. From the **Shared Calendar** drop-down list, select **None**.
5. Click **Submit** to remove the business calendar association.

Related Topics

- [“Viewing and Changing Business Calendars” on page 4-7](#)

Exporting and Importing Business Calendars

You can export and import business calendars. When you export a business calendar, the calendar name, time zone, and business rules are exported in XML format. When you import a calendar, if the name specified by the `<sch:name>` element in the XML file matches an existing calendar, the rules and time zone defined in the existing calendar are overwritten by the rules defined in the XML file. If the name specified by the `<sch:name>` element does not match any existing calendar, a new calendar is created.

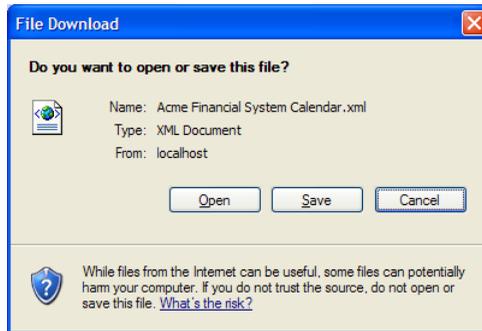
If the calendar you are importing has the same name as the calendar currently designated as the system calendar, the system flag element `<sch:systemFlag>` must be set to `Y` in the XML file.

If you are importing a new calendar, or updating a calendar that is not currently designated as the system calendar, the system flag is reset to **F** on import, regardless of the setting in the XML file.

To export a business calendar:

1. Locate the calendar to be exported. For more information, see “[Viewing and Changing Business Calendars](#)” on page 4-7.
2. Click the check box to the left of the calendar to select it.
3. Click **Export**.

The **File Download** page dialog is displayed and you are prompted to open the file or save it to a local directory.

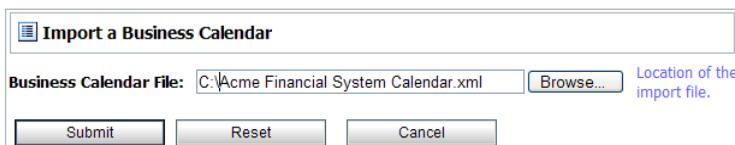


4. Click **Save** to download the calendar. The **Save As** dialog appears.
5. Navigate to the target directory, specify an appropriate file name, and then click **Save**. The calendar is now saved in you target directory.

To import a business calendar:

1. In Worklist Console, select the **Business Calendar** module. The **Business Calendar Management** page appears.
2. Click **Import**.

The **Import a Business Calendar** page is displayed.



3. Specify the name and location of the XML file in the **Business Calendar File** field. Click **Browse** to navigate to the file. The **Choose file** dialog appears.
4. Navigate to the source directory, select the appropriate file, and then click **Open**.
The name and location of the selected file appears in the **Business Calendar File** field.
5. Click **Submit** to import the specified calendar file.

The calendar is imported and listed in the **Business Calendar Management** page.

Deleting Business Calendars

The **Business Calendar Management** page allows you to delete selected calendars.

Note: You cannot delete a calendar if it is in use (mapped to a user) or is designated as the system calendar. See [“Deleting Business Calendars” on page 4-17](#) to update the **In Use** status.

To delete calendars:

1. Locate the calendars to be deleted. For more information, see [“Viewing and Changing Business Calendars” on page 4-7](#).
2. Click the check box to the left of the calendars that you want to delete.
3. Click **Delete**.

Note: If any of the selected calendars are currently being referenced by a Timer event generator, a warning is displayed. Click **Cancel** to cancel the delete operation, or **OK** to anyway delete the selected calendars.

Business Calendar Configuration