

K I N T A N A TM

Kintana Security Model

Version 5.0.0

Publication Number: KintanaSecurity-0603A

Kintana, Inc. and all its licensors retain all ownership rights to the software programs and related documentation offered by Kintana. Use of Kintana's software is governed by the license agreement accompanying such Kintana software. The Kintana software code is a confidential trade secret of Kintana and you may not attempt to decipher or decompile Kintana software or knowingly allow others to do so. Information necessary to achieve the interoperability of the Kintana software with other programs may be obtained from Kintana upon request. The Kintana software and its documentation may not be sublicensed and may not be transferred without the prior written consent of Kintana.

Your right to copy Kintana software and this documentation is limited by copyright law. Making unauthorized copies, adaptations, or compilation works (except for archival purposes or as an essential step in the utilization of the program in conjunction with certain equipment) is prohibited and constitutes a punishable violation of the law.

THIS DOCUMENTATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. IN NO EVENT SHALL KINTANA BE LIABLE FOR ANY LOSS OF PROFITS, LOSS OF BUSINESS, LOSS OF USE OR DATA, INTERRUPTION OF BUSINESS, OR FOR INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND, ARISING FROM ANY ERROR IN THIS DOCUMENTATION.

Kintana may revise this documentation from time to time without notice.

Copyright © 1997, 1998, 1999, 2000, 2001, 2002, 2003 Kintana, Incorporated. All rights reserved.

Kintana, Kintana Deliver, Kintana Create, Kintana Drive, Kintana Dashboard, Kintana Accelerator, Kintana Demand Management (DM), Kintana Portfolio Management (PFM), Kintana Program Management Office (PMO), Kintana Enterprise Change Management (ECM), Object*Migrator, GL*Migrator and the Kintana logo are trademarks of Kintana, Incorporated. All other products or brand names mentioned in this document are the property of their respective owners.

Kintana Version 5.0.0

© Kintana, Incorporated 1997 - 2003

All rights reserved.

Printed in USA

Kintana, Inc.

1314 Chesapeake Terrace, Sunnyvale, California 94089

Telephone: (408) 543-4400

Fax: (408) 752-8460

<http://www.kintana.com>

Contents

Chapter 1	
Introduction	1
Who should read this guide	2
Additional Resources	2
Kintana Documentation	2
<i>Kintana Business Application Guides</i>	3
<i>User Guides</i>	3
<i>Kintana Application Reference Guides</i>	4
<i>Kintana Instance Administration Guides</i>	4
<i>External System Integration Guides</i>	4
<i>Kintana Solution Guides</i>	5
<i>Kintana Accelerator Guides</i>	5
Kintana Services	5
Kintana Education	6
Kintana Support	6
.....	6
Chapter 2	
Key Concepts	7
Security Model Overview	7
License Key	9
Access Grants	10
Security Groups	10
Organization Unit	12
Entity-Level Restrictions	12
Participants	14
Request Participant	15
Package Participant	15
Project Participant	16
Field-Level Restrictions	16
Configuration-Level Restrictions	17

Chapter 3	
Users and Security Groups	19
Creating Users	19
Creating a User - Process Overview	20
Linking Users to Security Groups	24
Configure the User's Resource Information	26
Importing Users from a Database or LDAP Server	27
Creating Security Groups.....	27
Creating a Security Group by Specifying a List of Users	28
Using Kintana's Resource Management to Control User Security	31
Chapter 4	
Managing Your Kintana Licenses	33
Assigning Licenses in the User window.....	33
Assigning Licenses to Multiple Users in the License Workbench.....	35
Removing Licenses Using the Assign License Wizard	38
Assigning Licenses Using the Kintana Open Interface	39
Chapter 5	
Request Security	41
Viewing a Request	42
Restricting Request Viewing to Participants	43
Creating a Request.....	44
Enabling Users to Create Requests	44
Restricting Users from Selecting a Specific Workflow.....	45
Restricting Users from Selecting a Specific Request Type	46
Processing a Request.....	47
Providing Users with General Access to Update Requests	47
Enabling Users to Act on a Specific Workflow Step	49
Restricting Request Processing to Participants	49
Viewing and Editing Fields on a Request	49
Field-Level Data Security Overview	50
Field window: Attributes tab.....	51
Field window: Security tab	52
Request Type window: Status Dependencies tab.....	54
Deleting a Request	55
Overriding Request Security.....	55
Chapter 6	
Package Security	57
Viewing a Package	58

Restricting Package Viewing to Participants	59
Creating a Package	60
Enabling Users to Create Packages	60
Restricting Users from Selecting a Specific Workflow	61
Restricting Users from Selecting a Specific Object Type	62
Approving Package Lines	62
Enabling Users to Act on a Specific Workflow Step	63
Deleting a Package	63
Overriding Package Security.....	64
Chapter 7	
Project and Task Security	67
Viewing Projects and Tasks.....	68
Controlling Resources on the Project.....	69
Creating Projects	71
Editing Project and Task Information	71
Updating Tasks	72
Deleting Projects.....	73
Overriding Project Security	73
Chapter 8	
Resource Management Security	75
Working with Resources	76
Viewing Resource Information	76
Modifying Resource Information	76
Working with Resource Pools.....	77
Viewing Resource Pools	77
Creating Resource Pools	78
Modifying Resource Pools	78
Working with Skills	79
Viewing Skills	80
Creating, Modifying, and Deleting Skills	80
Working with the Organization Model	80
Viewing the Organization Model	80
Modifying Organization Definitions.....	81
Working with Staffing Profiles	81
Viewing Staffing Profiles	82
Creating Staffing Profiles	82
Modifying Staffing Profiles	83

Chapter 9	
Cost and Budget Data Security	85
Working with Cost Data	86
Viewing Cost Data	86
Enable Cost Data for a Project	86
Enable Cost Data for a Program	88
Modifying Cost Data	89
Working with Budgets	89
Viewing Budgets	90
Creating Budgets	90
Modifying Budgets	90
 Chapter 10	
Dashboard Security	93
Controlling User Access to Portlets.....	93
Disabling Portlets.....	93
Restricting User Access	94
Restricting Data to Participants.....	96
 Chapter 11	
Configuration Security.....	97
Setting Ownership for Kintana Configuration Entities	97
Removing Access Grants.....	99
 Appendix A	
Access Grants	103
 Appendix B	
Users and Licensing	115
Power and Standard Licenses	115
Kintana Drive Licenses and User Roles.....	116
Kintana Create Licenses and User Roles.....	118
Kintana Deliver Licenses and User Roles	120
Kintana Dashboard Licenses and User Roles	122
Kintana Solution Licenses.....	123
Demand Management	123
PMO	124
Time Management	124
Kintana Accelerator Licenses.....	124

Chapter 1 Introduction

The Kintana Security Model document details the features that can be used to control user access to certain data and functions in Kintana. Using a combination of license allocations, access grants and other security-related features, you can limit user access to screens, fields and functionality in Kintana. This document presents an overview of the data security model and provides instructions for controlling access to different Kintana entities.

This document discusses the following topics:

- *Key Concepts*
- *Users and Security Groups*
- *Managing Your Kintana Licenses*
- *Request Security*
- *Package Security*
- *Project and Task Security*
- *Resource Management Security*
- *Cost and Budget Data Security*
- *Dashboard Security*
- *Configuration Security*
- *Access Grants*
- *Users and Licensing*

Who should read this guide

This document provides details for the security that can be built into your Kintana processes and projects. This reference guide is used primarily by:

- Business users who are configuring a deployment system in Kintana (Kintana Deliver)
- Business users who are configuring a request resolution system in Kintana (Kintana Create)
- Project managers (Kintana Drive)
- Resource Managers
- Program Managers

Additional Resources

Kintana provides the following additional resources to help you successfully implement, configure, maintain and fully utilize your Kintana installation:

- [Kintana Documentation](#)
- [Kintana Services](#)
- [Kintana Education](#)
- [Kintana Support](#)

Kintana Documentation

Kintana product documentation is linked from the Kintana Library page. This page is accessed by:

- Selecting **HELP > KINTANA LIBRARY** from the Kintana Workbench menu.
- Selecting **HELP > CONTENTS AND INDEX** from the menu bar on the HTML interface. You can then click the **KINTANA LIBRARY** link to load the full list of product documents.

Kintana organizes their documents into a number of user-based categories. The following section defines the document categories and lists the documents currently available in each category.

- [*Kintana Business Application Guides*](#)
- [*User Guides*](#)
- [*Kintana Application Reference Guides*](#)
- [*Kintana Instance Administration Guides*](#)
- [*External System Integration Guides:*](#)
- [*Kintana Solution Guides*](#)
- [*Kintana Accelerator Guides*](#)

Kintana Business Application Guides

Provides instructions for modeling your business processes in Kintana. These documents contain process overviews, implementation instructions, and detailed examples.

- Configuring a Request Resolution System (Create)
- Configuring a Deployment and Distribution System (Deliver)
- Configuring a Release Management System
- Configuring the Kintana Dashboard
- Managing Your Resources with Kintana
- Kintana Reports

User Guides

Provides end-user instructions for using the Kintana products. These documents contain comprehensive processing instructions.

- Processing Packages (Deliver) User Guide
- Processing Requests (Create) User Guide
- Processing Projects (Drive) User Guide
- Navigating the Kintana Workbench:
Provides an overview of using the Kintana Workbench
- Navigating Kintana:
Provides an overview of using the Kintana (HTML) interface

Kintana Application Reference Guides

Provides detailed reference information on other screen groups in the Kintana Workbench. Also provides overviews of Kintana's command usage and security model.

- Reference: Using Commands in Kintana
- Reference: Kintana Security Model

- Workbench Reference: Deliver
- Workbench Reference: Configuration
- Workbench Reference: Create
- Workbench Reference: Dashboard
- Workbench Reference: Sys Admin
- Workbench Reference: Drive
- Workbench Reference: Environments

Kintana Instance Administration Guides

Provides instructions for administrating the Kintana instances at your site. These documents include information on user licensing and archiving your Kintana configuration data.

- Kintana Migration
- Kintana Licensing and Security Model

External System Integration Guides:

Provides information on how to use Kintana's open interface (API) to access data in other systems. Also discusses Kintana's Reporting meta-layer which can be used by third party reporting tools to access and report on Kintana data.

- Kintana Open Interface

Kintana Solution Guides

Provides information on how to configure and use functionality associated with the Kintana Solutions. Each Kintana Solution provides a User Guide for instructions on end-use and a Configuration Guide for instructions on installing and configuring the Solution.

Kintana Accelerator Guides

Provides information on how to configure and use the functionality associated with each Kintana Accelerator. Kintana Accelerator documents are only provided to customers who have purchased a site-license for that Accelerator.



Note

Kintana provides documentation updates in the Download Center section of the Kintana Web site (http://www.kintana.com/support/download/download_center.htm).

A username and password is required to access the Download Center. These were given to your Kintana administrator at the time of product purchase. Contact your administrator for information on Kintana documentation or software updates.

Kintana Services

Kintana is a strategic partner to its clients, assisting them in all aspects of implementing a Kintana technology chain - from pilot project to full implementation, education, project turnover, and ongoing support. Our Total Services Model tailors solution and service delivery to specific customer needs, while drawing on our own knowledgebank and best practices repository. Learn more about Kintana Services from our Web site:

<http://www.kintana.com/services/services.shtml>

Kintana Education

Kintana has created a complete product training curriculum to help you achieve optimal results from your Kintana applications. Learn more about our Education offering from our Web site:

<http://www.kintana.com/services/education/index.shtml>

Kintana Support

Kintana provides web-based interactive support for all products in the Kintana product suite via Contori.

<http://www.contori.com>

Login to Contori to enter and track your support issue through our quick and easy resolution system. To log in to Contori you will need a valid email address at your company and a password that will be set by you when you register at Contori.

Chapter 2 Key Concepts

The following key concepts and definitions are used when configuring security around your Kintana processes.

- *Security Model Overview*
- *License Key*
- *Security Groups*
- *Access Grants*
- *Organization Unit*
- *Entity-Level Restrictions*
- *Field-Level Restrictions*
- *Configuration-Level Restrictions*

Security Model Overview

Businesses often need to control access to certain information and business processes. This can be done to protect sensitive information, such as employee salaries, or to simplify business processes by hiding data that is irrelevant to the user. Kintana provides a set of features to help control data and process security on the following levels:

- Limiting who can access certain windows or pages.
- Limiting who can view or edit certain fields.
- Limiting the data displayed in sensitive fields or screens.

- Limiting which users can view, create, edit or process Kintana entities (Requests, Packages, Projects, etc.).
- Limiting which users can view, create or edit Kintana configuration entities (Workflow, Request Types, Object Types, Security Groups, etc.).
- Limiting which users can alter the security settings.

Kintana provides the following devices to control the data and process security. These features can be combined in a number of ways to provide a secure system:

- **Licenses:**
Each user is assigned a license that provides them with the option to be granted basic access to a set of Kintana product-related screens and functions. Licenses dictate available behavior but need to be used in conjunction with Access Grants to enable specific fields and functions. For example, a user with a Create Power License, but without any access grants, can log onto the system, but will not be able to view any screens or data.
- **Access Grants:**
Linked to users through security groups, access grants define which windows and functions users can view, edit or perform actions in. Access grants also provide varying levels of control over certain entities and fields. For example, a user with the Edit Requests grant can only delete Requests that he created, whereas a user with the Manage Requests grant can delete any Request in Kintana that he has access to.
- **Entity-level restrictions:**
Settings on the entity that specify who can create, edit, process and delete Kintana entities (such as Requests, Packages or Projects). You can also control which Request Types and Object Types can be used with certain Workflows. These restrictions are often configured in Kintana's configuration entities (Workflow, Request Type, Object Type, etc.).
- **Field-level restrictions:**
For each custom field that you define in Kintana, you can configure when it is visible or editable. For some fields, you can additionally specify which users can view or edit the field.
- **Configuration-level restrictions:**
You can specify, using Ownership Groups settings, which users can modify configuration entities in the system. For example, you can control

who is allowed to edit an existing Workflow. This allows you to guarantee that only appropriate users are altering your Kintana-controlled processes.

License Key

A Kintana license key is required for each site that is running the Kintana application. The license key stores such information as the number and types of licenses that you have purchased.

The Kintana license key is provided by Kintana when you purchase your Kintana licenses. When you purchase additional licenses, you need to contact Kintana to obtain a new license key that corresponds with the new number of users.

Kintana's license keys are delivered as a text strings that must be inserted into the `license.conf` file on the Kintana server. The `license.conf` file is located in the `<Kintana_Home>/conf` directory. A sample `license.conf` file is shown below.

```
com.kintana.core.server.LICENSE_KEY=40Fefa1555aeb28e115e0468f589222d03bba14b82c8f0...
com.kintana.core.server.PMO_LICENSE_KEY=c6c633e04ca765d4d88f97f1716cba66
com.kintana.core.server.DEM_LICENSE_KEY=f2f22cffc2da276a80f1c3af6eab7ddb
com.kintana.core.server.TIM_LICENSE_KEY=a8f3f4d1c7dfaca6487e5bdf1138efa8
```

Figure 2-1 Sample license.conf file contents

Kintana Solutions and Accelerators are licensed separately. When you purchase a Solution or Accelerator, Kintana will provide you with appropriate license information for those products. The license key information for Solutions will be appended to the `license.conf` file mentioned above. Kintana Accelerators are installed on a site-wide basis. For Accelerator installations, no modifications to the `license.conf` file are required.



Note

Kintana license keys are IP address dependent. If you plan on migrating your Kintana server to another machine or changing your Kintana server's IP address, you will need to obtain a new license key from Kintana support.

When you append the `license.conf` file, you need to stop and start the Kintana server for the new licenses to be recognized.

Access Grants

Access grants define which windows and functions users can view, edit or perform actions in. Access grants also provide varying levels of control over certain entities and fields. For example, a user with the `EDIT REQUESTS` grant can only delete Requests that he created, whereas a user with the `MANAGE REQUESTS` grant can delete any Request that he has access to.

Access grants also control which menu items are available in the Kintana Dashboard. For example, if you do not have the `EDIT REQUESTS` or `MANAGE REQUESTS` access grants, you will not see the **CREATE -> REQUEST** menu item.

Access grants are associated with Security Groups in the `SECURITY GROUPS WORKBENCH`. Security Groups are then associated with users. This provides each user in a Security Group with all of the access grants associated with that Security Group.

Kintana comes with a pre-defined list of Access Grants. Installing a Kintana Solution or Kintana Accelerator introduces additional Access Grants. See [“Access Grants”](#) on page 103 for a complete list of Kintana Access Grants. You can view which Access Grants a user has in the `USER` window in the Kintana Workbench.

Security Groups

Security Groups are constructed to provide a set of users with specific access to screens and functions within Kintana. Each Security Group is configured with a set of Access Grants that enable specific access. Users are then associated with one or more Security Groups.

A user's Security Group memberships determine which windows user can view or edit, which Workflows a user can use, and which Workflow Steps a user has authority to act on. Each Kintana user can be a member of multiple Security Groups. The collection of Security Groups to which a user belongs defines that user's role and access within Kintana.



Since users can be members of as many Security Groups as necessary, it is recommended that multiple Security Groups are created, each with a smaller range of responsibilities. Users can then be added to many different Security Groups to grant them their full range of access.

Security Groups can be used to control product access on the following levels:

- **Screen Security:**
Each Security Group contains a list of Access Grants that determine a user's screen security. Access Grants are used to grant access to view or edit a specific screen. By controlling the set of Access Grants for each user, specific functional roles for the user community can be defined.
- **Workflow Step Security:**
Each Workflow Step can be linked to a unique set of Security Groups. By adding or removing specific Security Groups from a Workflow Step in the Workflow window, you can control which Kintana users can act on that step. This security level provides an extremely detailed level of control over each Kintana user's actions.
- **Workflow Security:**
Security Groups can also control which Workflows users can select to deploy their objects (Packages) or resolve their Requests. When Kintana users generate a new Package or Request, they must choose a Workflow that the requested change or Request will follow. (Note: This is often defaulted for Requests through settings in the Request Type.) The list of Workflows from which the user can choose is determined by that user's Security Group membership.
- **Application Code Security:**
(This security level applies to Kintana Deliver only.) For complex Environments, information is often segmented in subsections called Application Codes. Application Code security can be defined to further restrict a user's ability to cross functional boundaries and apply unwanted changes to applications that are managed by other divisions.

Note

You should consider creating and maintaining two types of Security Groups:

- Security Groups to control who can act on a specific Workflow step (list of users without any special access grants)
- Security Groups to control who can access a particular screen or function (list of users and appropriate access grants)

This can greatly simplify your maintenance of a security model around Kintana processes. As new users are added to the system, they can be granted to appropriate screen and function access using one set of Security Groups and granted access to act on particular Workflow steps using another set.

Organization Unit

Kintana includes functionality for mapping all users into a company or department organization model. This ability helps you visualize roles within a department, enabling you to more effectively plan resource-dependent initiatives and communications in the future.

An Organization Unit is one group within the Organization Model. An Organization Unit typically consists of one or more Kintana users.

To help with configuring data and process security in Kintana, you can use the Organization Model to specify membership in a Security Group. The members listed in the specified Organization Unit are included in the Security Group definition and inherit all screen and function access defined for that group.

Organization units are configured in the standard (HTML) interface. Security Groups are configured in the SECURITY GROUPS WORKBENCH.

Entity-Level Restrictions

A number of Kintana entities include settings for controlling who can perform certain functions related to that entity. For example, using settings in the Request Type window, you can specify which users can use that Request Type when logging a Request. Some of the entity settings also provide a mechanism for how different Kintana entities work together. For example, using settings in the Workflow window, you can specify which Object Types can be used with that Workflow when creating a Package.

These settings are used in conjunction with the access grants to provide entity-based user restrictions and additional process logic. These settings are made within the Kintana Workbench.

Specific data-related security settings exist for the Kintana entities listed in [Table 2-1](#). A brief description of the available restrictions is provided.

Table 2-1. Data and Process Security Settings on Kintana Entities.

Kintana Entity	Setting Related to Data and Process Restrictions	Set in Workbench?
Budget	MODIFY BUDGET > CONFIGURE ACCESS FOR BUDGET page: Specify who can view and edit Budget information.	No

Table 2-1. Data and Process Security Settings on Kintana Entities.

Kintana Entity	Setting Related to Data and Process Restrictions	Set in Workbench?
Environment	ENVIRONMENT window: USER ACCESS tab: Specify who can use the Environment in Workflows or Environment Groups.	Yes
Environment Group	ENVIRONMENT GROUPS window: USER ACCESS tab: Specify who can use the Environment Group in a Workflow	Yes
Portlet	PORTLET window: USER ACCESS tab: Specify who can use a portlet on their Dashboard	Yes
Program	CONFIGURE ACCESS FOR PROGRAM page: Specify who can view the program; specify who can view the cost information related to the Program.	No
Project	PROJECT SETTINGS window: SECURITY tab: Specify who can view the project and tasks (participant); specify who can view cost information PROJECT SETTINGS window: PROJECT TEAM tab: Specify who can be used as a resource on the project	Yes
Project Template	PROJECT TEMPLATE window: SECURITY Tab: Specify who can view the project and tasks (participant); specify who can view cost information	Yes
Report Type	REPORT TYPE window: SECURITY tab: Specify who can view and submit reports of that Report Type	Yes
Request Header Type	REQUEST HEADER TYPE window: FILTER tab: Specify the behavior of the CONTACT NAME, ASSIGNED GROUP, and ASSIGNED TO fields	Yes
Request Type	REQUEST TYPE window: USER ACCESS tab: Specify which security groups can use this request type when logging requests REQUEST TYPE window: WORKFLOWS tab: Specify which Workflows can be used with this Request Type REQUEST TYPE window: RESTRICTION field: Specify if only participants can view and process Requests where they are a “participant”	Yes
Resource Pool	MODIFY RESOURCE POOLS > CONFIGURE ACCESS FOR RESOURCE POOL page: Specify who can view and edit Resource Pool information.	No

Table 2-1. Data and Process Security Settings on Kintana Entities.

Kintana Entity	Setting Related to Data and Process Restrictions	Set in Workbench?
Security Group	<p>SECURITY GROUP window: DELIVER WORKFLOWS tab: Specify which Workflows can be used by Security Group members when creating a Package</p> <p>SECURITY GROUP window: REQUEST TYPES tab: Specify which Request Types can be used by Security Group members when creating a Request.</p> <p>SECURITY GROUP window: DELIVER APP CODES tab: Specify which App Codes a user may specify when creating a Package Line.</p>	Yes
Staffing Profile	<p>MODIFY STAFFING PROFILES > CONFIGURE ACCESS FOR STAFFING PROFILE page: Specify who can view and edit Staffing Profile information.</p>	No
Workflow	<p>WORKFLOW window: DELIVER SETTINGS tab:</p> <ul style="list-style-type: none"> • (Package Line setting) Specify which Object Types can be used with the Workflow when creating a Package. • (Package Security setting) Specify if only users can view and process a Package where they are a “participant.” • (Filter settings) Specify the behavior of the ASSIGNED GROUP, and ASSIGNED USER fields. <p>WORKFLOW window: REQUEST TYPES tab: Specify which Request Types can be used to create another Request at a CREATE_REQUEST step in a Request Workflow.</p>	Yes



Note

As a general rule, these settings override the access grants. This means that if a user has an access grant to create Requests using the EDIT REQUESTS access grant, but is restricted from using certain Request Types in the Security Group definition, he will not be able to create the restricted Request Type.

Participants

You can configure Requests, Packages and Projects so that they are only visible to users who are directly involved with them. Kintana refers to these

users as “Participants.” A participant is defined uniquely for each supported Kintana entity.

Request Participant

Users who are involved in moving a Request through a Workflow are considered to be **Participants** in that Request. A Participant can be the:

- ASSIGNED TO user
- A member of the ASSIGNED GROUP
- The creator of the Request
- A member of a Security Group or a user associated with any of the Workflow Steps contained in the Workflow.

You can configure Kintana so that a Request is not visible to users who are not Participants. Additionally, users running standard Reports will only see information for Requests for which they are considered to be Participants.

The participant restriction is set for Requests in the RESTRICTION field on the REQUEST TYPE window.

Package Participant

Users who are involved in moving a Package through a Workflow are considered to be **Participants** in that Package. A Participant can be the:

- ASSIGNED TO user
- A member of the ASSIGNED GROUP
- The creator of the Package
- A member of a Security Group or a user associated with any of the Workflow Steps contained in the Workflow.

You can configure Kintana so that a Package is not visible to users who are not Participants. Additionally, users running standard Reports will only see information for Packages for which they are considered to be Participants.

The participant restriction is set for Packages in the **DELIVER SETTINGS** tab on the **WORKFLOW** window.

Project Participant

You can configure a Project such that only participants can view it or its Tasks. A Participant can be the:

- Users assigned as Project Managers
- Users assigned as a Resource on a Task
- Users in an assigned Resource Group

The participant restriction is set for Projects in the **SECURITY** tab on the **PROJECT SETTINGS** window.

Field-Level Restrictions

Kintana provides the ability to control which users can view or edit certain fields while processing Requests, Packages and Projects. You can configure this level of data security in the following places:

- **FIELD** definition window - **ATTRIBUTES** tab
Specify whether the field is generally displayed to the user. For Object Type fields, you can also specify whether the field is required or editable.
- **FIELD** definition window - **SECURITY** tab
Specify which users can view or edit the field. The Security tab is available for fields on Request Types, Request Header Types and Request User Data.
- **REQUEST TYPE** window - **STATUS DEPENDENCIES** tab (Request fields only)
Specify if the field is visible, editable, or required depending on the Request's status.

Configuration-Level Restrictions

Different groups of Kintana users have ownership and control over Kintana configuration entities. This allows you to guarantee that only appropriate users are altering your Kintana-controlled processes. These groups are referred to as Ownership Groups.

Unless a 'global' permission has been designated to all users for an entity, members of Ownership Groups are the only users who have the right to edit, delete or copy that entity. The Ownership Groups must also have the proper access grant for the entity in order to complete those tasks. For example, the EDIT WORKFLOWS Access Grant is needed to edit Workflows and Workflow Steps.

You can assign multiple Ownership Groups to the various entities. Ownership Groups are defined in the SECURITY GROUP window. Security Groups become Ownership Groups when used in the Ownership capacity.

You can select to specify Ownership Groups for the following entities involved in your deployment process:

- Environments
- Environment Groups
- Object Types
- Report Types
- Request Header Types
- Request Types
- Security Groups
- Special Commands
- User Definitions
- Validations
- Workflows
- Workflow Steps

The Ownership setting is accessed through the individual entity windows in the Kintana Workbench.

Chapter 3

Users and Security Groups

This chapter provides instructions for creating Kintana users and providing them with screen and function access in Kintana. The following topics are discussed:

- [Creating Users](#)
- [Creating Security Groups](#)

Related Topics:

- ["Sys Admin Workbench Reference"](#)
- ["Managing Resources in Kintana"](#)

Creating Users

Kintana users are created and defined in the USER WORKBENCH. For enterprises with a large number of users, Kintana provides additional methods of user creation. It is possible to import user information from other existing databases into Kintana interface tables, and then directly into Kintana. Similarly, users can be imported from a LDAP server, through the interface tables, into the application.

The following sections discuss topics related to creating a Kintana user:

- [Creating a User - Process Overview](#)
- [Linking Users to Security Groups](#)
- [Importing Users from a Database or LDAP Server](#)

Creating a User - Process Overview

To define a new Kintana user:

1. Click **NEW USER** on the USER WORKBENCH or select **FILE -> NEW -> USER**. The USER window opens.

The screenshot shows the 'User: Untitled1' dialog box with the following fields and values:

- User Information:** Username, First Name, Last Name, Company, Email Address, Phone Number.
- Authentication:** Authentication Mode: KINTANA; Password: [Redacted]; Start Date: April 24, 2003; End Date: [Redacted]; Last Login: [Redacted]; Password Exp. Days: [Redacted]; Password Exp. Date: April 24, 2003; Domain: [Redacted].
- Products:** Kintana Suite (Create, Drive, Deliver, Dashboard): No Access; Kintana Create: No Access; Kintana Drive: No Access; Kintana Deliver: No Access; Kintana Dashboard: No Access; Kintana Solution: [Redacted].
- Buttons:** Edit Resource, Time Management Settings, OK, Save, Cancel.

2. Enter the following required information: USERNAME, FIRST NAME, and LAST NAME. The username must be unique in Kintana.
3. Enter the general information the appropriate fields. Refer to [Table 3-1](#) for a detailed description of each field on the **USER INFORMATION** tab.
4. Create a Password for the user.
 - a. Click the button to the right of the required PASSWORD field. The ENTER OR CHANGE PASSWORD window opens.
 - b. Enter a password in the ENTER NEW PASSWORD field. Confirm in the CONFIRM NEW PASSWORD field. This password is encrypted both in the user interface and the database.
 - c. Click **OK** to close the window.

5. Specify when the Password will expire using either of the following methods:
 - o Select **YES** for NEW PASSWORD ON LOGIN to force the user to reset the password.
 - o Use the PASSWORD EXP. DAYS field to specify the number of days that a user has to change the password. When a value is entered in this field, the PASSWORD EXP. DATE field is automatically updated.
6. Select the a method for the user's authentication from the AUTHENTICATION MODE field. Possible values are **KINTANA**, **LDAP**, **NTLM**, and **SITEMINDER**. If **KINTANA** is chosen, then authentication is performed using Kintana's internal user database. If another authentication mode is chosen, authentication is performed using the enterprise directory database server. This field's behavior can be set in the server.conf by modifying the AUTHENTICATION_MODE parameter.
7. Select the products and license types to associate with the new user from the **PRODUCT** drop down lists. The text area to the right of the drop down lists will change to inform you of the number of licenses you have used. To assign identical access to all Kintana products with only one license, use the **SUITE** option. The **STANDARD LICENSE** provides access to the HTML interface. The **POWER LICENSE** provides access to all product functionality available through the Workbench and HTML interfaces. For more detailed information, see [“Managing Your Kintana Licenses”](#) on page 33. Users with **No ACCESS** to a Kintana product will not see that product's shortcut groups.

Tip: You can assign licenses to multiple users using the License Workbench. See [“Managing Your Kintana Licenses”](#) on page 33 for details.
8. Link the desired Security Groups to the user to specify the user's functional roles and Kintana access grants. See [“Linking Users to Security Groups”](#) on page 24 for instructions.
9. Select the Ownership Groups who will have the right to edit, copy or disable this user. See [“Setting Ownership for Kintana Configuration Entities”](#) on page 97.
10. Click **OK**.

The new user can now log onto Kintana using the username and password.

Table 3-1. User Window: User Information Tab Fields

Fields	Definition
USERNAME	Unique name for a user's Kintana account. The name entered to log onto Kintana.
COMPANY	The company the user works for. The values in this auto-complete list are set by the following Validation: CRT - COMPANY.
FIRST NAME	The first name of the specified user.
LAST NAME	The last name of the specified user.
EMAIL ADDRESS	The email address for a user. This address is referenced in other portions of the application and should be formatted as name@domain.com.
PHONE NUMBER	The phone number for the user.
AUTHENTICATION MODE	<p>A list of the methods available for authentication. Possible values are KINTANA, LDAP, NTLM, and SITEMINDER. If KINTANA is chosen, then authentication is performed using Kintana's internal user database. If another authentication mode is chosen, authentication is performed using the enterprise directory database server.</p> <p>See the "Kintana Open Interface" document for details.</p>
START DATE	The date when a user account becomes activated.
END DATE	The date on which a user account becomes disabled. You can leave this field blank to indicate no end date.
LAST LOGIN	<p>The date of a user's last system logon.</p> <p>This date is deleted based on a parameter in the server.conf file, DAYS_TO_KEEP_LOGON_ATTEMPT_ROWS. The default value for this parameter is 14 days. If there is no value in the LAST LOGIN field, the user has not logged in for at least 14 days (assuming the parameter has not been changed from the default to another value). See "Kintana System Administration Guide" for server.conf parameter details.</p>
DOMAIN	Used only when using NTLM authentication. This can be set in the KNTA_HOME/integration/ntlm/ntlm.conf file.
PASSWORD	The Kintana user's password. Kintana administrators can set restrictions on the password format: minimum length, required special characters, etc. These restrictions are specified in Kintana's server.conf file. See " Kintana System Administration Guide " for server.conf parameter details.

Table 3-1. User Window: User Information Tab Fields

Fields	Definition
NEW PASSWORD ON LOGON	Setting to determine whether to ask a user to enter a new password the next time they logon to Kintana.
PASSWORD EXP. DAYS	The number of days before a user's password expires. The first time a user logs on after the password expiration date, he will be prompted to enter a new password.
PASSWORD EXP. DATE	The date on which a user's password expires. The value in this non-updateable field is calculated by the PASSWORD EXPIRATION DAYS attribute or the ASK NEW PASSWORD ON LOGON attribute.
KINTANA SUITE	A list associating license types for all Kintana products with a user simultaneously. The STANDARD LICENSE provides access to HTML interface. The POWER LICENSE provides access to all product functionality available through the Workbench interface and additional access to advanced HTML interface functions. Users with No ACCESS to the suite will not see any screen groups.
KINTANA CREATE	A list associating a product license type with a user. The STANDARD LICENSE provides access to the HTML interface. The POWER LICENSE provides access to all product functionality available through the Workbench interface and additional access to advanced HTML interface functions. Users with No ACCESS to Create will not see the CREATE screen group.
KINTANA DRIVE	A list associating a product license type with a user. The STANDARD LICENSE provides access to HTML interface. The POWER LICENSE provides access to all product functionality available through the Workbench interface and additional access to advanced HTML interface functions. Users with No ACCESS to Drive will not see the DRIVE screen group.
KINTANA DELIVER	A list associating a product license type with a user. The STANDARD LICENSE provides access to HTML interface. The POWER LICENSE provides access to all product functionality available through the Workbench interface and additional access to advanced HTML interface functions. Users with No ACCESS to Deliver will not see the Deliver screen group.
KINTANA DASHBOARD	A list associating a product license type with a user. The Standard License provides access to the HTML Dashboard interface. The Power License provides access to the Dashboard Workbench screen used to configure custom portlets, the default Dashboard, and portlet security.
TIME MANAGEMENT	Kintana Solution license that only appears if you have purchased Kintana Time Management licenses from Kintana. Select STANDARD LICENSE to enable user access to Time Management functions in Kintana.

Table 3-1. User Window: User Information Tab Fields

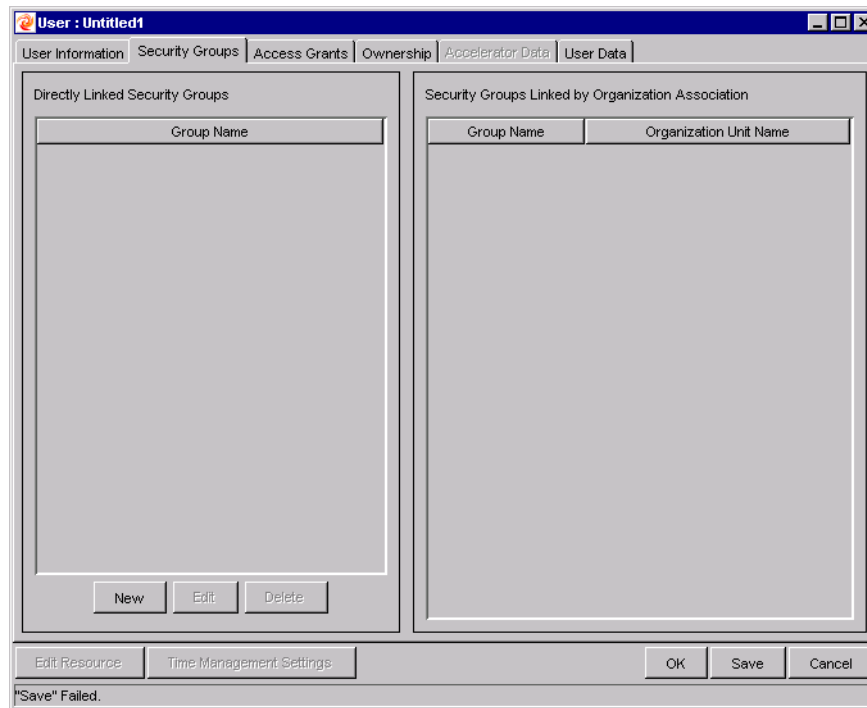
Fields	Definition
DEMAND MANAGEMENT	Kintana Solution license that only appears if you have purchased Kintana Demand Management licenses from Kintana. Select STANDARD LICENSE to enable user access to Demand Management functions in Kintana.
PMO	Kintana Solution license that only appears if you have purchased Kintana PMO licenses from Kintana. Select STANDARD LICENSE to enable user access to PMO functions in Kintana.
RESOURCE	Each Kintana user also has associated Resource settings such as Title, Direct Manager, Capacity, etc. Click this button to view or edit the Resource Settings associated with the user.

Linking Users to Security Groups

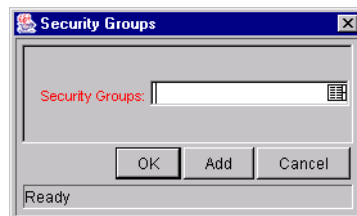
Users can be linked to Security Groups through the **SECURITY GROUPS** tab of the **USER** window. Users can also be linked to Security Groups through an Organization Model defined in Kintana.

To link a User to a Security Group using the **USER** window:

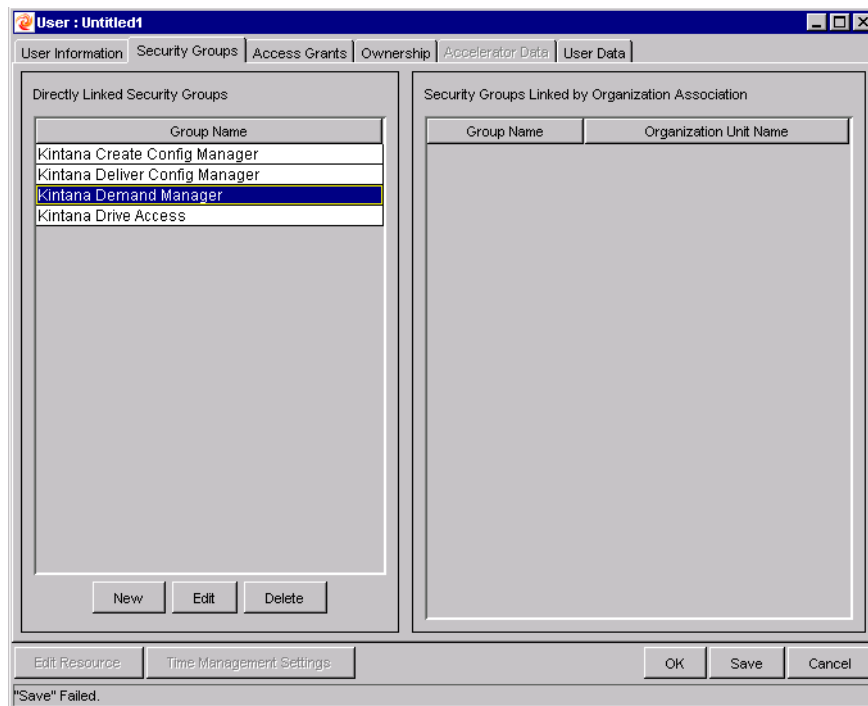
1. Open the **USER** window.
2. Click the **SECURITY GROUPS** tab.



3. Click **NEW**.



4. Click on the SECURITY GROUPS auto-complete list to view all of the Security Groups enabled in Kintana. Select the Security Groups that you would like to link to the user.
5. Click **OK** to add the list of Security Groups to the USER window.



6. Click **SAVE** to save the user information.



Note

If the user is associated with an Organization Unit (defined in Kintana's Resource Management product), he may inherit Security Group associations. These Security Groups will be listed in the **SECURITY GROUPS** tab in the SECURITY GROUPS LINKED BY ORGANIZATION ASSOCIATION list.

See "[Managing Resources in Kintana](#)" for details.

Configure the User's Resource Information

A Resource is a person who performs work tracked by Kintana. Resources in Kintana can include employees, contractors, managers, or any other category your organization may need. Each Kintana user is considered a Resource in Kintana. For each user, you can capture information specific to that Resource, such as:

- Skills — the main duties or abilities of the user (such as DBA or Programmer)

- **Cost Rate** — The hourly cost associated with a Resource or skill, which represents the charge-back or billed cost of their labor.
- **Workload Capacity** — A percentage that indicates what portion of a Resource’s working day is available for planned workload items. For instance, a particular DBA may have a lot of meetings every day, and therefore is set to devote 80% of her capacity to workload items.

Entering Resource information for each Kintana user is an optional activity. For instructions on configuring Resource information, see ["Managing Resources in Kintana"](#).

Importing Users from a Database or LDAP Server

For enterprises with a large number of users, Kintana includes an open interface for user creation. This API uses interface tables within the Kintana database instance. Data added to these interface tables is validated and eventually imported into standard Kintana tables, generating users that can be processed normally within Kintana. Kintana also supports importing users from an LDAP server.

Refer to the ["Kintana Open Interface"](#) document for full documentation on this feature. This document provides an overview of relevant Kintana data model points and provides detailed instructions for performing the user import.

Creating Security Groups

Security Groups are used in Kintana to control who can access certain screens and functionality in Kintana. See ["Key Concepts"](#) on page 7. The following sections provide instructions on defining Security Groups:

- [Creating a Security Group by Specifying a List of Users](#)
- [Using Kintana’s Resource Management to Control User Security](#)

The general process for creating a Security Group is as follows:

1. Specify Security Group membership on the **USERS** tab. This can be accomplished by providing a list of users or by associating the group with an organization unit defined in Kintana.

2. Specify the screen and feature access by linking the appropriate Access Grants. See “*Access Grants*” on page 103 for a full list of Kintana’s access grants.
3. For Security Groups to be used in a deployment process only -- Specify which Workflows users in this Security Group can use when deploying changes. This is set in the **DELIVER SETTINGS** tab.
4. For Security Groups to be used in a deployment process only -- Restrict the Security Group from using certain Application Codes when creating a Package Line. This restricts which applications each user can process objects through.



Note

You should consider creating and maintaining two types of Security Groups:

- Security Groups to control who can act on a specific Workflow steps (list of users without any special access grants)
- Security Groups to control who can access a particular screen or function (list of users and appropriate access grants)

This can greatly simplify your maintenance of a security model around Kintana processes. As new users are added to the system, they can be granted appropriate screen and function access and associated with specific Workflows.

Creating a Security Group by Specifying a List of Users

To generate and define a new Security Group:

1. Click **NEW SECURITY GROUP** in the SECURITY GROUP WORKBENCH or select **FILE > NEW > SECURITY GROUP** from the menu. The SECURITY GROUP window opens.

2. Enter the NAME and DESCRIPTION.
3. Select **YES** to enable this Security Group.

Only enabled Security Groups appear as a choice when generating or updating users or Workflows.

4. Select which Kintana entities (Requests, Projects or Packages) will use the Security Group by clicking their respective check boxes in the THIS SECURITY GROUP WILL BE USED BY field.
5. Link the desired Users to the Security Group.
 - a. Click **NEW** in the **USERS** tab. The **USERS** window opens.
 - b. Enter the desired username into the **USERS** field and click **ADD** or click on the **USERS** auto-complete list to display all available users. The **VALIDATE** window opens.
 - c. Select the desired **USER NAME**.
 - d. Click **OK**. The **Validate** window closes.
 - e. Click **OK** to add your selection to the **USERS** tab.
6. Link the desired Access Grants. Each Access Grant enables certain functions performed on a Kintana screen. See "[Access Grants](#)" on page 103 for a description of each available access grants.

- a. Select the desired Access Grants in the AVAILABLE ACCESS GRANTS list.
 - b. Click the right arrow button pointing to the LINKED ACCESS GRANTS list. The selected Access Grants are moved into the column.
7. Restrict the Security Group from using certain Workflows when processing Packages.
- a. Click the **DELIVER WORKFLOWS** tab.
 - b. Select the Workflows in the ALLOWED DELIVER WORKFLOWS list.
 - c. Click the left arrow button pointing to the RESTRICTED DELIVER WORKFLOWS list. The selected Workflows are moved into the column.
 - d. If all future Workflows should also be excluded, select the ALWAYS RESTRICT NEW WORKFLOWS check box.
8. Restrict the Security Group from using certain Application Codes when creating a Package Line. This restricts which applications each user can process objects through.
- a. Click the **DELIVER APP CODES** tab.
 - b. Select the App Codes in the ALLOWED DELIVER APP Codes list.
 - c. Click the left arrow button pointing to the RESTRICTED DELIVER APP CODES list. If all future App Codes are to be excluded, select the **ALWAYS RESTRICT NEW APP CODES** check box.
9. Restrict the Security Group from using certain Request Types.
- a. Click the **REQUEST TYPES** tab.
 - b. Select the Request Types in the ALLOWED REQUEST TYPES list.
 - c. Click the left arrow button pointing to the RESTRICTED REQUEST TYPES list. The selected Request Types are moved into the column.
10. Click the **OWNERSHIP** tab and select the Ownership Groups that have the right to edit, copy or delete the current Security Group. See [“Setting Ownership for Kintana Configuration Entities”](#) on page 97 for more information about setting Ownership for a new or existing Security Group.
11. (Optional) Enter any necessary information in the **USER DATA** tab’s fields.

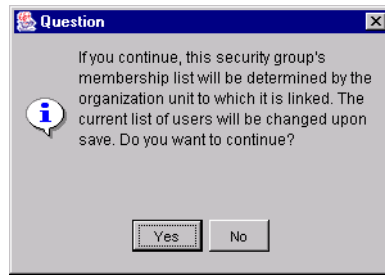
12. Click **OK** to register the current Security Group and close the SECURITY GROUP window. Click **SAVE** to save the information and leave the SECURITY GROUP window open.

Using Kintana's Resource Management to Control User Security

Users can also be associated to Security Groups through their inclusion in an organization model definition. Using Kintana's resource management capabilities, a user can be placed into a model that includes security and access information. See "[Managing Resources in Kintana](#)" for details.

To define a Security Group to use the members of an organization unit:

1. Open the SECURITY GROUP window.
2. Select DETERMINED BY ORGANIZATION UNIT in the MEMBERSHIP section of the **USERS** tab. The following question dialog opens.



3. Click **YES**.



Note

When you select an Organization Unit to control user access to the Security Group, any users specified in the Users list will be replaced with the members of the organization unit.

4. Select the ORGANIZATION UNIT.

5. Select whether you want to include:

- **Direct Members Only:**
Only direct members of the specified organization unit.
- **All Members (cascading)**
Members of this organization unit and its child units.

6. Click **OK**.

Refer to the "[Managing Resources in Kintana](#)" document for instructions on associating users with an Organization Model.

Chapter 4

Managing Your Kintana Licenses

Each user that is going to view or perform work in Kintana must be given an appropriate product license. Different licenses enable different parts of the application. For example, a Kintana Drive Power License grants a user access to Kintana's Project planning interface, whereas a Kintana Deliver Power Licence grants access to the interface for creating and processing Packages. See *"Users and Licensing"* on page 115 for a detailed discussion of each license in Kintana. The referenced appendix also includes a discussion of Standard versus Power licenses.

Licenses can be associated with users using three different methods:

- *Assigning Licenses in the User window*
- *Assigning Licenses to Multiple Users in the License Workbench*
- *Assigning Licenses Using the Kintana Open Interface*

Assigning Licenses in the User window

To assign a license to a single user in the User window:

1. Open the USER window for the user that you would like to assign a license to.
2. Select the desired licenses from the drop down lists on the lower half of the window. Selecting a **KINTANA SUITE** license will update the window to show that the user has either standard or power access to all Kintana core products (Create, Deliver, Drive and Dashboard).



Note

If your company has purchased Kintana Solutions, licensing options will appear below the product licenses. Kintana Accelerator licenses are issued on a site-wide basis and are therefore not included as an option in the USER window.

Select licences for the user.

The screenshot shows the 'User : jsmith' window with several tabs: 'User Information', 'Security Groups', 'Access Grants', 'Ownership', 'Accelerator Data', and 'User Data'. The 'User Information' tab is active, showing fields for Username (jsmith), First Name (John), Last Name (Smith), Email Address, and Phone Number. The 'Authentication' section includes 'Authentication Mode' (KINTANA), Password (*****), Start Date (April 15, 2003), End Date, Last Login (April 25, 2003 08:45:46 AM PDT), and Password Exp. Date (July 23, 2003). The 'Products' section is highlighted with a red box and contains the following items:

Product	License
Kintana Suite (Create, Drive, Deliver, Dashboard):	No Access
Kintana Create:	Power License
Kintana Drive:	Standard License
Kintana Deliver:	Power License
Kintana Dashboard:	Standard License
Kintana Solution Demand Management:	No Access

Below the 'Products' section, a list of 'Kintana Core Products License(s) Used' is shown:

- 1 Kintana Create, Power
- 1 Kintana Drive, Standard
- 1 Kintana Deliver, Power
- 1 Kintana Dashboard, Standard

At the bottom of the window, there are buttons for 'Edit Resource', 'Time Management Settings', 'OK', 'Save', and 'Cancel'. The status bar at the bottom indicates 'Ready'.

3. Click **SAVE** to save the new license settings for the user.



Note

You must have licenses available in the system in order to successfully apply them to a user. If you do not have enough licenses available, you will receive a message upon **SAVE**.

Assigning Licenses to Multiple Users in the License Workbench

You can use the LICENSE ADMINISTRATION window to assign licenses to a batch of Kintana users. This window provides a single access point from which to view current license usage and availability in the system. You can then launch the ASSIGN LICENSE wizard to lead you through the process.

To assign licenses using the ASSIGN LICENSE wizard:

1. Click the **LICENSE** icon in the **SYS ADMIN** screen group. The LICENSE ADMINISTRATION window opens. This window displays how many of each Kintana license is available (not used), and which Accelerators are installed at your site.
2. Click **ASSIGN LICENSES**. The ASSIGN LICENSE wizard opens.
3. FIND USERS step:
Locate the users that you would like to assign licenses to by entering search criteria in the fields and clicking **NEXT**. All users selected by the search will be assigned licenses later in the wizard process. You can specify users based on the fields defined in [Table 4-1](#).

The screenshot shows the 'Assign Licenses' wizard window. It features a sidebar on the left with three buttons: 'Find Users' (highlighted in red), 'Choose Licenses', and 'Confirm Changes'. The main area contains several search criteria fields, each with a list icon to its right. A red dashed box highlights the 'Find Users' section, which includes fields for Security Group, Username, Company, and Currently Assigned Licenses. Another red dashed box highlights the 'User data fields' section, which includes fields for Mentor, Location, Company, Publish STAR Data (with radio buttons for Yes and No), and Department. At the bottom right, there are three buttons: 'Cancel', '< Back', and 'Next >'.

Standard Find Users fields

User data fields defined for each Kintana User.

Table 4-1. License Administration Wizard - Find Users Step

Fields	Definition
SECURITY GROUP	Locates users that belong to a specific Security Group. You can select multiple Security Groups in this field. The search will return a list of all users that belong to any of the selected Security Groups.
USER NAME	Locates any users that are explicitly specified in this field.
COMPANY	Locates users that are associated with a specific company. Companies are associated with users in the CONTACTS screen on the CREATE WORKBENCH.
CURRENTLY ASSIGNED LICENSES	Locates all users that that currently have any of the licenses specified in this field.
USER DATA FIELDS	Search for users based on the custom 'User' User Data fields defined at your site.

4. CHOOSE LICENSES step.

Review the selected users and then specify which licenses to grant them by selecting the licenses from the license fields. Note that although all users may not be selected in the user list, the licenses specified will be applied to all of the users that meet the requirements from the FIND USERS step.

Review the selected users.

Select the licenses.

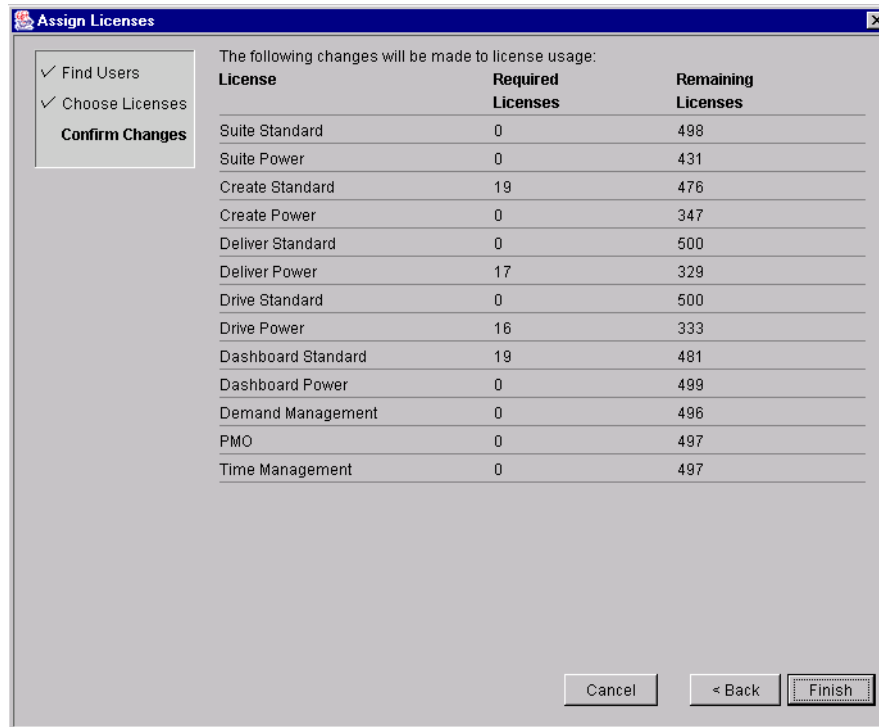
You have selected 19 users.

Username	First Name	Last Name	Enabled	Email Address
johnsmith	John	Smith	Y	johnsmith@kintana...
jsmith	John	Smith	Y	
matt2	admin	admin	Y	
rups admin	Rupali	Mayekar	Y	
ryan	ryan	evans	Y	

	Current Usage	Current Available	Required Licenses	Remaining Licenses
Suite:	No Access	0 Standard 15 Power	498 Standard 416 Power	0 Standard 431 Power
Create:	Standard License	0 Standard 2 Power	495 Standard 345 Power	19 Standard 347 Power
Deliver:	Power License	0 Standard 2 Power	500 Standard 346 Power	0 Standard 17 Power
Drive:	Power License	0 Standard 3 Power	500 Standard 349 Power	0 Standard 16 Power
Dashboard:	Standard License	0 Standard 2 Power	500 Standard 497 Power	19 Standard 0 Power
Solutions				
Demand Management:	No Access	6 Standard	490 Standard	0 Standard
PMO:	No Access	5 Standard	492 Standard	0 Standard
Time Management:	No Access	10 Standard	487 Standard	0 Standard

Cancel < Back Next >

5. Click **NEXT**.
6. **CONFIRM CHANGES**.
Review the license assignments. Ensure that the Remaining Licenses number is greater than or equal to zero. A negative number indicates that you do not have enough available licenses to apply to the set of users. If this is a negative number, you will not be able to complete the license assignment process.
7. Click **FINISH** to apply the licenses.



The following changes will be made to license usage:

License	Required Licenses	Remaining Licenses
Suite Standard	0	498
Suite Power	0	431
Create Standard	19	476
Create Power	0	347
Deliver Standard	0	500
Deliver Power	17	329
Drive Standard	0	500
Drive Power	16	333
Dashboard Standard	19	481
Dashboard Power	0	499
Demand Management	0	496
PMO	0	497
Time Management	0	497



Note

An available license will only be used if the selected user does not already have the license. Licenses will append, not overwrite, the license specifications for a user. (except when removing a license by specifying **No ACCESS**).

For example, John Smith meets the search requirements in the FIND USER step. In the CHOOSE LICENSE step, you specify that every user should be granted a Suite Power license. John Smith already has a Create Power license. When the licenses are applied, a Create Power license is not applied to John. Therefore, this is not counted in the Required Licenses or Remaining Licenses columns.

Removing Licenses Using the Assign License Wizard

The Assign License wizard can also be used to remove licenses from a set of users. To remove licenses:

1. Click the **LICENSE** icon in the **SYS ADMIN** screen group. The **LICENSE ADMINISTRATION** window opens.
2. Click **ASSIGN LICENSES**. The **ASSIGN LICENSE** wizard opens.
3. **FIND USERS** step:
Locate the users that you would like to remove licenses from by entering search criteria in the fields and clicking **NEXT**. All users selected by the search will be altered later in the wizard process.
4. **CHOOSE LICENSES** step:
Select **No ACCESS** from the license drop down list for whichever product licenses you wish to remove.
5. Click **NEXT**.
6. **CONFIRM CHANGES**.
Review the license changes.
7. Click **FINISH** to delete the specified licenses from the selected set of users.

Assigning Licenses Using the Kintana Open Interface

Licenses can also be applied to Kintana users using the Kintana Open Interface. This API uses interface tables within the Kintana database instance. Data added to these interface tables is validated and eventually imported into standard Kintana tables, generating or updating user account information.

Refer to the "[Kintana Open Interface](#)" document for full documentation on this feature. This document provides an overview of relevant Kintana data model points and provides detailed instructions for running the interface program.

Chapter 5 Request Security

Kintana allows you to exercise a great deal of control over your Request resolution system. You can restrict user actions around:

- **Request creation:**
 - o Who can create Requests.
 - o Who can use a specific Workflow.
 - o Who can use specific Request Types.
- **Request processing:**
 - o Who can approve / process each step in the Workflow.
 - o Who can view and edit fields in the Request.
 - o Who can delete a Request.
 - o Whether you only want “Participants” to process the Request. Participants are defined as the Assigned User, the creator of the Request, members of the Assigned Group, or any users who have access to the Workflow step(s).
- **Configuring your Request resolution process:**
 - o Who can edit the Workflow.
 - o Who can edit each Request Type.

Configuring this data and process security often involves a setting a number parameters: licenses, access grants, entity level settings and field level settings.

The following sections provide settings required for securing the specified actions or data:

- Viewing a Request
- Creating a Request
- Processing a Request
- Viewing and Editing Fields on a Request
- Deleting a Request
- Configuring Request Types
- Overriding Request Security



Note

Screen and function access provided through Access Grants are cumulative. If a user belongs to three different Security Groups, he will have all access provided to each of the groups. Therefore, to restrict certain screen and feature access, you need to remove the user from any Security Group that grants that access.

You can use the **ACCESS GRANTS** tabs in the **USER** window to see all Security Groups where specific access grants are included. You can then:

- Remove the user from the Security Group (using the **SECURITY GROUP** tab on the **USER** window)
- Remove the Access Grants from the Security Group (in the Security Group window). Note: you should only do this if no one in that Security Group needs the access provided in that Access Grant.



Note

This chapter discusses how to:

- Provide general view and edit access to a user
- Restrict viewing and editing privileges by using additional settings or removing certain access grants.

Viewing a Request

You can control which Kintana users can view a Request. To enable a user to view Requests in Kintana, set the following:

Table 5-1. Settings to enable Request viewing.

Setting	Value	Description
License	Kintana Create: Standard License	The Standard License provides a Kintana user with access to the Kintana interface. This is set in the USER window on the KINTANA WORKBENCH.
Access Grants linked to the Security Group	Create: View Requests	This Access Grant allows the user to view Requests. Note that the Edit Requests and Manage Requests also provide viewing privileges, but also enable more advanced editing and processing functions. Access Grants are set in the SECURITY GROUP window.

Restricting Request Viewing to Participants

The RESTRICTION drop down list in the REQUEST TYPE window lets you determine who can access a Request. Restricting access to Participants means that when non-Participant users search for Requests, they will not see a Request for which they are not a Participant. In this instance, Participants are defined as:

- The ASSIGNED TO User
- The creator of the Request
- Members of the ASSIGNED GROUP
- Any users who have access to the Workflow Step(s)

To let all Kintana users access Requests of the specific Request Type, select **UNRESTRICTED** in the REQUEST TYPE window.

To restrict the number of Kintana users who can access Requests to Participants of the Requests, select **PARTICIPANT**.

Creating a Request

You can control who can create certain Requests or use specific Request Types and Workflows. This provides a great deal of control over who can process changes of a certain type to specific environments. The following sections discuss how to control security related to Request creation:

- [Enabling Users to Create Requests](#)
- [Restricting Users from Selecting a Specific Workflow](#)
- [Restricting Users from Selecting a Specific Request Type](#)

Enabling Users to Create Requests

You can control which Kintana users have the ability to create and submit Requests. To enable a user to create and submit a Request, set the following:

Table 5-2. Settings to enable Request creation.

Setting	Value	Description
License	Kintana Create: Standard License	The Standard License provides a Kintana user with access to the Kintana interface, where the Request is created. This is set in the USER window on the KINTANA WORKBENCH.
Access Grants linked to the Security Group	Create: Edit Requests	This Access Grant allows the user to generate, edit and delete certain Requests. <ul style="list-style-type: none"> • User cannot delete a Request if user is not the owner. • To edit the Request, user must be its creator, the contact, or a member of the Workflow Steps security group. Access Grants are set in the SECURITY GROUP window.
	Create: Manage Requests	This Access Grant allows the user to edit or delete Requests at anytime. Access Grants are set in the SECURITY GROUP window.

Table 5-2. Settings to enable Request creation.

Setting	Value	Description
Allowed Request Types in the SECURITY GROUP window	You must have at least one Request Type allowed.	<p>In order to process the intended Request correctly, you are required to select a Request Type when creating a Request. The Request Type you wish to use must be enabled in order for you to be able to create and submit a Request of that Type.</p> <p>This is set on the SECURITY GROUP window - REQUEST TYPES tab.</p>
Allowed Request Types in the WORKFLOW window.	You must allow at least one Request Type in each Workflow used to resolve Requests.	<p>You can associate Request Types with Workflows such that only certain Request Types can be processed through the Workflow. The Request Type you wish to use must be enabled so that the user can create a Request when using that Workflow.</p> <p>The default Request Type to be used with this Workflow can also be specified.</p> <p>This is set on the WORKFLOW window - REQUEST TYPES tab.</p>
Allowed Security Groups in the REQUEST TYPE window.	You must allow at least one Security Group to create Requests of this Type.	<p>You can associate Security Groups with Request Types such that only certain Security Groups are allowed to create Requests of a particular Type.</p> <p>You can also opt to allow all Security Groups enabled for Requests to create Requests of this Type.</p> <p>New Security Groups can automatically be added to this window if you so choose.</p> <p>This is set on the REQUEST TYPE window - USER ACCESS tab.</p>

Restricting Users from Selecting a Specific Workflow

You can restrict users from selecting specific Workflows when creating a new Request. To do this, set the following:

Table 5-3. Settings to restrict Workflow selection on a Request

Setting	Value	Description
Allowed Workflows in the REQUEST TYPE window	<p>Include the Workflows that you would like to allow.</p> <p>You can opt to allow all Workflows to be used with the Request Type.</p>	<p>When creating a Request, you are required to select a Workflow for the Request to proceed through. Users will not be able to select any Workflows not included in the WORKFLOWS tab of the REQUEST TYPE window.</p> <p>This is set on the REQUEST TYPE window - WORKFLOWS tab.</p>

Restricting Users from Selecting a Specific Request Type

You can restrict users from selecting specific Request Types when creating a new Request. To do this, set the following.

Table 5-4. Settings to restrict Request Type selection when creating a Request.

Setting	Value	Description
Allowed Security Groups in the REQUEST TYPE window.	You must allow at least one Security Group to create Requests of this Type.	<p>You can associate Security Groups with Request Types such that only certain Security Groups are allowed to create Requests of a particular Type.</p> <p>You can also opt to allow all Security Groups enabled for Requests to create Requests of this Type.</p> <p>This is set on the REQUEST TYPE window - USER ACCESS tab.</p>
Allowed Request Types in the WORKFLOW window.	You must allow at least one Request Type in each Workflow used to resolve Requests.	<p>You can configure a Workflow step to automatically spawn a Request. Use this setting to control which Request Types can be used at that step.</p> <p>This is set on the WORKFLOW window - REQUEST TYPES tab.</p>

Processing a Request

You can control who can process Requests following a Request submission. You can also control who can act on certain steps (decisions and executions) in your process. The following sections discuss how to control security related to Request processing:

- [Providing Users with General Access to Update Requests](#)
- [Enabling Users to Act on a Specific Workflow Step](#)
- [Restricting Request Processing to Participants](#)

Providing Users with General Access to Update Requests

All users who will be processing Requests must meet the following conditions:

Table 5-5. Settings required to process Requests in Kintana

Setting	Value	Description
License	Kintana Create: Standard	The Standard License provides a Kintana user with access to the Kintana interface. Users can act on all decision Workflow steps. This is set in the USER window on the KINTANA WORKBENCH.

Table 5-5. Settings required to process Requests in Kintana

Setting	Value	Description
Access Grants linked to the Security Group (not all are required)	Create: Edit Requests	<p>This Access Grant allows the user to generate, edit and delete certain Requests.</p> <ul style="list-style-type: none"> • User cannot delete a Request if it has been released or if user is not the owner. • To edit the Request, user must be its creator, the contact, or a member of the Workflow Steps security group. <p>Access Grants are set in the SECURITY GROUP window.</p>
	Create: Manage Requests	<p>This Access Grant allows the user to edit or delete Requests at anytime.</p> <p>Access Grants are set in the SECURITY GROUP window.</p>
	Create: Allow Request Field Updates	<p>This Access Grant allows the user to view and update any Request regardless of whether the user is its creator, the ASSIGNED TO user, a member of the ASSIGNED GROUP or a member of the Workflow Steps security group.</p> <p>Access Grants are set in the SECURITY GROUP window.</p>
	Create: Override Participant Restriction	<p>This Access Grant allows the user to view a Request regardless of whether the user is its creator, the ASSIGNED TO user, a member of the ASSIGNED GROUP or a member of the Workflow Steps security group.</p> <p>This grant should only be given to users who are permitted to view all Requests in the system.</p> <p>Access Grants are set in the SECURITY GROUP window.</p>

Enabling Users to Act on a Specific Workflow Step

You need to specify who can act on each step in the Workflow. Only users who are specified on the **SECURITY** tab in the **WORKFLOW STEP** window will be able to process that step.

Restricting Request Processing to Participants

The **RESTRICTION** drop down list in the **REQUEST TYPE** window lets you determine who can have access to Requests. Restricting access to Participants means that when non-Participant users search for Requests, they will not see the Requests for which they are not Participants. In this instance, Participants are defined as:

- The **ASSIGNED TO** User
- The creator of the Request
- Members of the **ASSIGNED GROUP**
- Any users who have access to the Workflow Step(s) -- this is specified in the Workflow Step **SECURITY** tab.

To restrict the number of Kintana users who can access Requests using the current Workflow to Participants of the Requests, select **PARTICIPANT**.

Viewing and Editing Fields on a Request

Kintana provides a number of features that can be used to restrict users from viewing or editing specific fields on a Request. This field-level data security is configured using the Request Type and Request Header Type windows in the Kintana Workbench. The following sections discuss the different methods for restricting users from viewing or editing fields on a Request.

- [Field-Level Data Security Overview](#)
- [Field window: Attributes tab](#)
- [Field window: Security tab](#)
- [Request Type window: Status Dependencies tab](#)



These sections assume that the user has been granted standard access to view and edit the Request, but does not have the CREATE: MANAGE REQUEST or CREATE: ALLOW REQUEST FIELD UPDATE Access Grants.

Field-Level Data Security Overview

Field editability and visibility can be set in the following places:

- FIELD window: **ATTRIBUTES** tab
Used to set general view and edit access for all users.
- FIELD window: **SECURITY** tab
Used to set view and edit access for a specific list of users.
- REQUEST TYPE window: **STATUS DEPENDENCIES** tab
Used to set view and edit access for a field depending on the Request's status.

Figure 5-1 illustrates the order that determines whether a field is visible to a particular user.

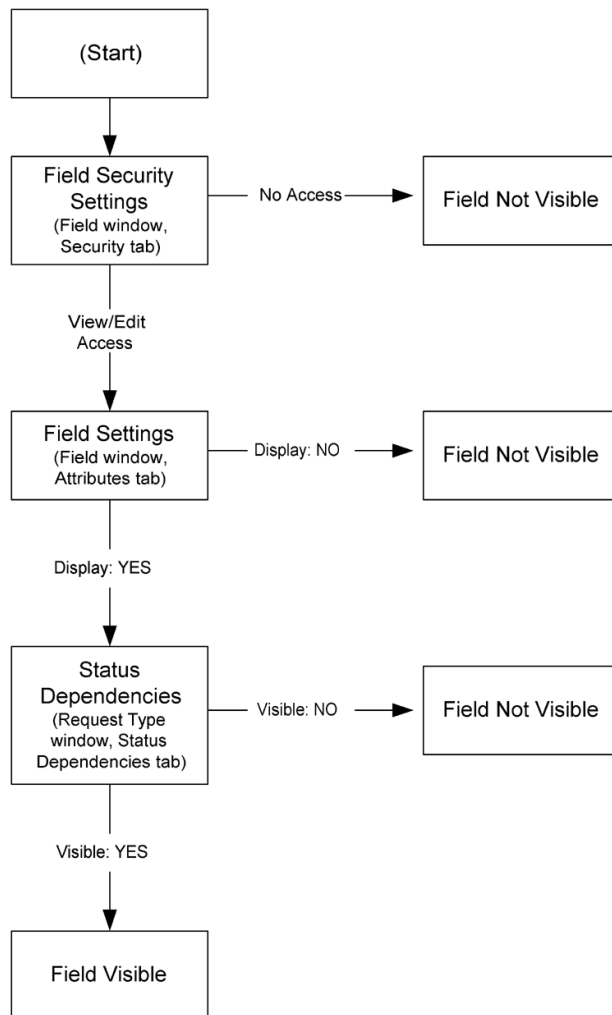


Figure 5-1 Field Visibility Interactions

Field window: Attributes tab

The **ATTRIBUTES** tab can be used to set general view and edit access for all users. The following settings are used to control visibility and editability of a field:

Table 5-6. Settings to control view and edit access in the Attributes tab.

Parameter	Description
Display	Controls whether the field is visible on the Request. If set to No , this field will not be visible to any user in Kintana.

Table 5-6. Settings to control view and edit access in the Attributes tab.

Parameter	Description
Display Only	Controls whether the field is editable on a Request. If set to YES , the field can not be updated.

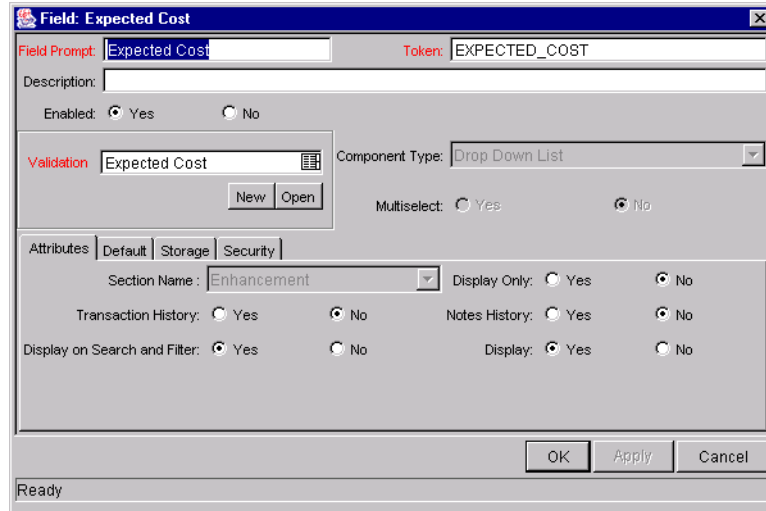


Figure 5-2 Field window: Attributes tab.

Field window: Security tab

The **SECURITY** tab can be used to set view and edit access for a specific list of users. To limit who can view and edit the field to a specific group of users:

1. Click Edit on the **SECURITY** tab. The EDIT FIELD SECURITY window opens.

Set default security for this field.
Note: Security may still be affected by Status Dependencies, Field Level Dependencies, etc.

This field is: Visible to all users
 Editable by all users

Select Users/Security Groups that can view this field:

Security Group:

Provide Editing Rights

Tokens Add: ➔

This field is visible to these Users/Security Groups:

Security Type	Security	Visible	Editable
---------------	----------	---------	----------

Remove

OK Cancel

Ready

2. Uncheck VISIBLE TO ALL USERS and EDITABLE BY ALL USERS.
3. Specify who can view or edit the field. You can select a **USER, SECURITY GROUP, STANDARD TOKEN, or USER DEFINED TOKEN.**
4. Add the selection to the right hand window.

Set default security for this field.
Note: Security may still be affected by Status Dependencies, Field Level Dependencies, etc.

This field is: Visible to all users
 Editable by all users

Select Users/Security Groups that can view this field:

Security Group:

Provide Editing Rights

Tokens Add: ➔

This field is visible to these Users/Security Groups:

Security Type	Security	Visible	Editable
Security Group Name	IT Consultants	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Security Group Name	IT Process Own...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Remove

OK Cancel

Ready

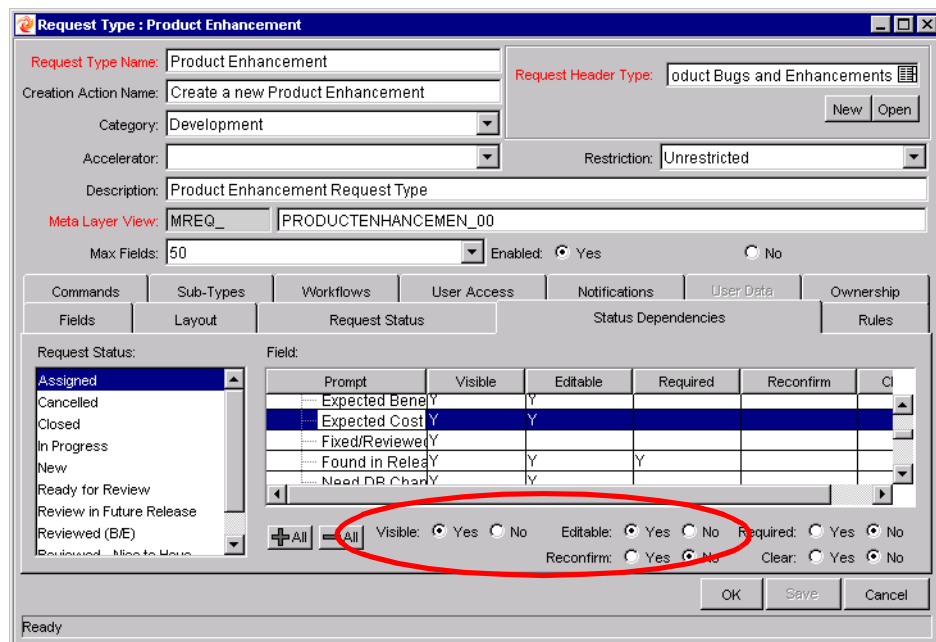
5. Click **OK** to save the settings.

Request Type window: Status Dependencies tab

Request field behavior can be linked directly to the Statuses of the Request. Select a field and a Request Status and assign that field's attributes under the given Request Status. This is done by toggling the radio buttons at the bottom of the screen. You can set view and edit access for a field depending on the Request's status using the following settings on the **STATUS DEPENDENCIES** tab:

Table 5-7. Settings for view and edit access in the Status Dependencies tab.

Parameter	Description
Visible	Determines whether or not a field is visible for a specific Request Status. If it is set to VISIBLE = No , then the field is not displayed.
Editable	If a field is set to EDITABLE = No for a specific Request Status, then it is not possible to edit the field at the given Request Status. If a field is set up as REQUIRED, RECONFIRM, or CLEAR, it must be set to EDITABLE = YES .



Deleting a Request

You can control which Kintana users can delete a Request. To enable a user to delete Requests in Kintana, set the following:

Table 5-8. Settings required to delete Requests in Kintana

Setting	Value	Description
License	Kintana Create: Power License	The Power License provides a Kintana user with access to the Kintana workbench and advanced Request processing options. This is set in the USER window on the KINTANA WORKBENCH.
Access Grants linked to the Security Group	Create: Edit Requests	Users with a Power License can delete the Request if they are the creator and the Request has not been submitted.
	Create: Manage Requests	Users with a Power License can delete or cancel any Request.
	Create: Override Participant Restriction	Access a Request regardless of whether the user is its creator, the ASSIGNED TO user, a member of the ASSIGNED GROUP or a member of the Workflow Steps security group. Access Grants are set in the SECURITY GROUP window.

Overriding Request Security

Users with the following settings can view, edit and delete any Request in Kintana:

Table 5-9. Settings required to override Request Security

Setting	Value	Description
License	Kintana Create: Power License	The Power License provides a Kintana user with access to the Kintana workbench and advanced Request processing options. This is set in the USER window on the KINTANA WORKBENCH.
Access Grants linked to the Security Group	Manage Requests	Perform advanced Request processing actions: creating, editing, deleting, changing the Request's workflow, and overriding references.
	Override Create Participant Restriction	View the detailed information on a restricted Request for which the user is not an active participant.

Users with the following access grant can edit Request Types, regardless of Ownership restrictions:

Table 5-10. Access Grant to override Request Type configuration security

Access Grant	Description
Ownership Override	Access and edit all configuration entities even if the user is not a member of one of the entity's Ownership Groups.

Chapter 6 Package Security

Kintana allows you to exercise a great deal of control over your deployment process. You can restrict users' actions around:

- **Package creation:**
 - o Who can create Packages.
 - o Who can use a specific Workflow.
 - o Who can use specific Object Types.
- **Package processing:**
 - o Who can approve / process each step in the Workflow.
 - o Whether you only want “Participants” to process the Packages. Participants are defined as the Assigned User, the creator of the Package, members of the Assigned Group, or any users who have access to the Workflow step(s).
- **Managing your deployment process:**
 - o Who can change the Workflow.
 - o Who can change each Object Type.
 - o Who can change the Environment and Environment Group definitions.
 - o Who can change the Security Group definitions.

Configuring this data and process security often involves a setting a number parameters: licenses, access grants, entity level settings and field level settings. Many Package-related security settings are configured in the Kintana Workflows used to process the Packages. This allows you to control which

processes are being used for deployments as well as which Environments are being impacted.

The following sections provide settings required for securing the specified actions or data:

- [Viewing a Package](#)
- [Creating a Package](#)
- [Approving Package Lines](#)
- [Deleting a Package](#)
- [Overriding Package Security](#)

Note

Screen and function access provided through Access Grants are cumulative. If a user belongs to three different Security Groups, he will have all access provided to each of the groups. Therefore, to restrict certain screen and feature access, you need to remove the user from any Security Group that grants that access.

You can use the **ACCESS GRANTS** tabs in the USER window to see all Security Groups where specific access grants are included. You can then:

- Remove the user from the Security Group (using the **SECURITY GROUP** tab on the USER window)
- Remove the Access Grants from the Security Group (in the Security Group window). Note: you should only do this if no one in that Security Group needs the access provided in that Access Grant.

Note

This chapter discusses how to enable a user to view or edit items in Kintana. You can restrict access by altering the specified settings or removing the specified access grants or licenses.

Viewing a Package

You can control which Kintana users can view a Package. To enable a user to view Packages in Kintana, set the following:

Table 6-1. Settings to view Packages in Kintana

Setting	Value	Description
License (only one is required)	Kintana Deliver: Standard License	The Standard License provides a Kintana user with access to the Kintana interface where they can view the Package approval page.
	Kintana Deliver: Power License	The Power License provides a Kintana user with access to the Kintana Workbench where he can view the Package.
Access Grants linked to the Security Group	Deliver: View Packages	<p>This Access Grant allows the user to view Packages.</p> <p>Note that the Edit Packages and Manage Packages also provide viewing privileges, but also enable more advanced editing and processing functions.</p> <p>Access Grants are set in the SECURITY GROUP window.</p>

Restricting Package Viewing to Participants

The **PACKAGE SECURITY** tab in the **WORKFLOW** window lets you determine who can have access to Packages that use the current Workflow. Restricting access to Participants means that when non-Participant users search for Packages, they will not see a Package that uses the current Workflow. In this instance, Participants are defined as:

- The Assigned User
- The creator of the Package
- Members of the Assigned Group
- Any users who have access to the Workflow Step(s)

To let all Kintana users access Packages using the current Workflow, select **ALL USERS**.

To restrict the number of Kintana users who can access Packages associated with this Workflow to Participants of the Packages, select **PARTICIPANTS ONLY**.

Creating a Package

You can control who can create Packages or use specific Object Types and Workflows. This provides a great deal of control over who can process changes of a certain type to specific environments. The following sections discuss how to control security related to Package creation:

- [Enabling Users to Create Packages](#)
- [Restricting Users from Selecting a Specific Workflow](#)
- [Restricting Users from Selecting a Specific Object Type](#)

Enabling Users to Create Packages

You can control which Kintana users have the ability to create and submit Packages. To enable a user to create and submit a Package, ensure that the following are set.

Table 6-2. Settings to enable Package creation.

Setting	Value	Description
License	Kintana Deliver: Power License	The Power License provides a Kintana user with access to the Kintana Workbench, where the Package is defined.
Access Grants linked to the Security Group (only one is required)	Deliver: Edit Packages	This Access Grant allows the user to generate, edit and delete certain Packages. <ul style="list-style-type: none"> • User cannot delete a Package if it has been released or if user is not the owner. • To edit the Package, user must be its creator, the 'assigned to' user, a member of the assigned group or a member of the Workflow Step security.
	Deliver: Manage Packages	This Access Grant allows the user to create, edit and delete Packages at anytime.

Table 6-2. Settings to enable Package creation.

Setting	Value	Description
Allowed Deliver Workflows in the SECURITY GROUP window	You must have at least one Workflow allowed.	<p>When creating a Package, you are required to select a Workflow for the Package to proceed through. At least one Workflow must be enabled to be able to create and submit a Package. The user should select the Workflow intended to process the deploying objects.</p> <p>This is set on the SECURITY GROUP window - DELIVER WORKFLOWS tab.</p>
Allowed Deliver Object Types in the WORKFLOW window.	You must allow at least one Object Type in each Workflow used to deploy changes.	<p>You can associate Object Types with Workflows such that only certain Object Types can be processed through the Workflow. At least one Object Type must be enabled so that the user can create a Package Line when using that Workflow.</p> <p>This is set on the WORKFLOW window - DELIVER SETTINGS tab, under the PACKAGE LINE selection.</p>

Restricting Users from Selecting a Specific Workflow

You can restrict users from selecting specific Workflows when creating a new Package. To do this, ensure that the following conditions are met.

Table 6-3. Settings to restrict Workflow selection

Setting	Value	Description
Restricted Deliver Workflows in the Security Group window	Include the Workflows that you would like to restrict.	<p>When creating a Package, you are required to select a Workflow for the Package to proceed through. Users (in the Security Group) will not be able to select any Workflows included in the Restricted Deliver Workflows list.</p> <p>Note: If a user belongs to another Security Group that allows the use of that Workflow, the user will be able to select it.</p> <p>This is set on the SECURITY GROUP window - DELIVER WORKFLOWS tab.</p>



Restricting the Workflow selection also controls who can deploy changes to specific environments, because the source and destination Environments are defined in the Workflow step.

Restricting Users from Selecting a Specific Object Type

You can restrict users from selecting specific Object Types when creating a new Package. To do this, ensure that the following conditions are met.

Table 6-4. Settings to restrict Object Type selection

Setting	Value	Description
Restricted Deliver Object Types in the Workflow window.	Include the Object Type that you would like to restrict.	<p>You can associate Object Types with Workflows such that only certain Object Types can be processed through the Workflow. Users will not be able to select any Object Types included in the RESTRICTED DELIVER WORKFLOWS list.</p> <p>This is set on the WORKFLOW window - DELIVER SETTINGS tab, under the PACKAGE LINE selection.</p>

Approving Package Lines

All users who will be processing Package lines must meet the following conditions:

Table 6-5. Settings to enable Package processing.

Setting	Value	Description
License (at least one is required)	Kintana Deliver: Power License	The Power License provides a Kintana user with access to the Kintana Workbench. Users can act on all Workflow steps (decisions and executions) in the Workbench.
	Kintana Deliver: Standard	The Standard License provides a Kintana user with access to the Kintana standard interface. Users can act on all decision Workflow steps. Note: you must have a Power Licence to process execution steps.
Access Grants linked to the Security Group	Deliver: Edit Packages	This Access Grant allows the user to generate, edit and delete Packages. <ul style="list-style-type: none"> To edit the Package, user must be its creator, the 'assigned to' user, a member of the assigned group or a member of the Workflow Steps security group.
	Deliver: Manage Packages	This Access Grant allows the user to edit or delete Packages at anytime.

Enabling Users to Act on a Specific Workflow Step

You need to specify who can act on each step in the deployment Workflow. Only people who are specified on the **SECURITY** tab in the **WORKFLOW STEP** window will be able to process that step.

Deleting a Package

You can control which Kintana users can delete a Package. To enable a user to delete Package in Kintana, set the following:

Table 6-6. Settings required to enable a user to delete Requests in Kintana

Setting	Value	Description
License	Kintana Deliver: Power License	The Power License provides a Kintana user with access to the Kintana workbench and advanced Package processing options.
Access Grants linked to the Security Group	Deliver: Edit Packages	Users with a Power License can delete the Package if it has not been submitted and he is the owner.
	Deliver: Manage Requests	Users with a Power License can delete any Package they can access.

Overriding Package Security

Users with the following settings can view, edit and delete any Packages in Kintana:

Table 6-7. Settings to override Request Security

Setting	Value	Description
License	Kintana Deliver: Power License	The Power License provides a Kintana user with access to the Kintana workbench and advanced Package processing options.
Access Grants	Deliver: Manage Packages	View, edit and delete any Package in Kintana.
	Deliver: Override Deliver Participant Restriction	View the detailed information on a restricted Package for which the user is not an active participant.

Users with the following access grant can edit Kintana configuration entities, regardless of Ownership restrictions:

Table 6-8. Access Grant to override configuration security

Value	Description
Ownership Override	Access and edit all configuration entities even if the user is not a member of one of the entity's Ownership Groups.

Chapter 7

Project and Task Security

Kintana allows you to exercise control over your Project data. You can restrict user actions around:

- *Viewing Projects and Tasks*
- *Controlling Resources on the Project*
- *Creating Projects*
- *Editing Project and Task Information*
- *Updating Tasks*
- *Deleting Projects*
- *Overriding Project Security*

Configuring this data and process security often involves setting a number of parameters: licenses, access grants, entity level settings and field level settings. The following sections discuss the settings required for securing the specified actions or data.



Note

Screen and function access provided through Access Grants are cumulative. If a user belongs to three different Security Groups, he will have all access provided to each of the groups. Therefore, to restrict certain screen and feature access, you need to remove the user from any Security Group that grants that access.

You can use the **ACCESS GRANTS** tabs in the **USER** window to see all Security Groups where specific access grants are included. You can then:

- Remove the user from the Security Group (using the **SECURITY GROUP** tab on the **USER** window)
- Remove the Access Grants from the Security Group (in the Security Group window). Note: you should only do this if no one in that Security Group needs the access provided in that Access Grant.

Viewing Projects and Tasks

You can control which Kintana users can view Projects and Tasks. By default, any users with one of the following licenses and access grants can view Projects in Kintana.

Table 7-1. Settings to view Projects and Tasks in Kintana

Setting	Value	Description
License	Kintana Drive: Standard License	The Standard License provides a Kintana user with access to the Kintana interface where they can view the Project and Task information in the standard Kintana interface.
	Kintana Drive: Power License	The Power License provides a Kintana user with access to the Kintana Workbench where he can view Project and Task information using the Project Workbench.

Table 7-1. Settings to view Projects and Tasks in Kintana

Setting	Value	Description
Access Grants linked to the Security Group	Deliver: View Projects	View Project definitions in the Projects Workbench and standard Kintana interface. Note that the Edit Projects and Manage Projects also provide viewing privileges, but also enable more advanced editing and processing functions.

To restrict users from viewing Projects and Tasks, set the following:

Table 7-2. Settings to restrict a user from viewing Projects and Tasks

Setting	Value	Description
License	(REMOVE) Kintana Drive: Standard and Power licenses	Removing these licenses from the user keeps them from viewing any Project or Task related pages or windows in Kintana.
Access Grant	(REMOVE) Drive: View Projects ; Edit Projects ; Manage Projects	Removing these access grant from users keeps them from viewing Projects and Tasks.
Participant Restriction	Participant Restriction**	Restrict who can view Projects and Tasks to only "participants." Set in the SECURITY tab on the PROJECT SETTINGS window.

**A Participant can be the:

- Users assigned as Project Managers
- Users assigned as a Resource on a Task
- Users in an assigned Resource Group

Controlling Resources on the Project

Project Managers can specify who will be allowed to act as Resources for a Project. Resources can be users and groups of users. In the **PROJECT TEAM** tab, the Project Manager can choose to either:

- Allow all users with the Project option enabled in their Security Groups to be Resources for a Project.

Or

- Only allow those Resources who are specified in the **PROJECT TEAM** tab to be used as Resources for a Project. These Resources are listed in the tab's Resource table. For example, only the users shown in *Figure 7-1* can be added as Resources to the Project.

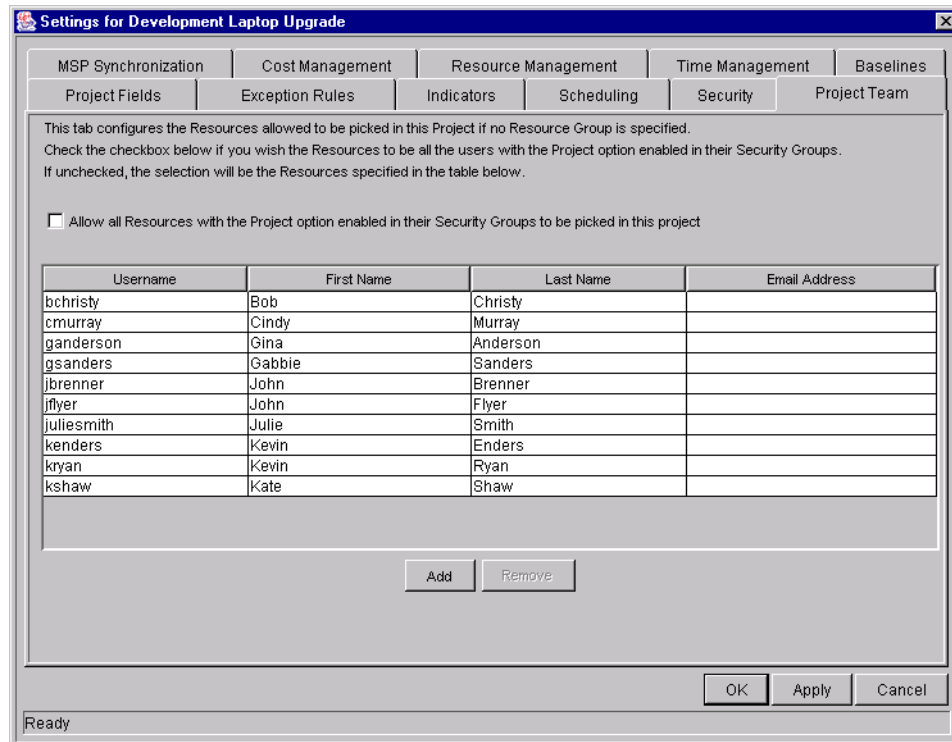


Figure 7-1 Project Team Tab on the Project Settings Window



Note

Exception: Users with the SYSADMIN: OVERRIDE KEY FIELDS SEGMENTATION can add any users as a Resource to the Project.

Creating Projects

You can control which Kintana users can create Projects and Tasks. By default, any users with one of the following licenses and access grants can view Projects in Kintana.

Table 7-3. Settings required to create a Project

Setting	Value	Description
License	Kintana Drive: Power License	The Power License provides a Kintana user with access to the Kintana Workbench where he can create Projects using the Project Workbench.
Access Grants (only one is required)	Edit Projects	Create Projects using the Projects Workbench. Update and delete Projects and Subprojects when specified as the Project Manager.
	Manage Projects	Create, edit and delete Projects. Override (or remove) References on Projects or Tasks.

Editing Project and Task Information

You can control which Kintana users can edit Project and Task information. This includes adding tasks to the Project and modifying Project settings. By default, users with the following licenses and access grants can edit Projects.

Table 7-4. Settings required to edit a Project

Setting	Value	Description
License	Kintana Drive: Power License	The Power License provides a Kintana user with access to the Kintana Workbench where he can edit Projects using the Project Workbench.

Table 7-4. Settings required to edit a Project

Setting	Value	Description
Access Grants (only one is required)	Edit Projects	Update and delete Projects and Subprojects when specified as the Project Manager.
	Manage Projects	Edit and delete any Projects. Override (or remove) References on Projects or Tasks.

Updating Tasks

You can control which Kintana users can update Tasks on Projects. Users with the following licenses and access grants can update Tasks.

Table 7-5. Settings required to update Tasks

Setting	Value	Description
License (only one is required)	Kintana Drive: Standard License	The Standard License provides a Kintana user with access to the Kintana interface where they can update Task status information in the standard Kintana interface.
	Kintana Drive: Power License	The Power License provides a Kintana user with access to the Kintana Workbench where he can update Task status information in the Kintana Workbench.
Access Grants	Update Tasks (Required)	Update Tasks when specified as a Resource on the Project.

To restrict users from updating Tasks, set the following:

Table 7-6. Settings to restrict a user from updating Tasks

Setting	Value	Description
License	(REMOVE) Kintana Drive: Standard License ; Power License	Removing these licenses from the user keeps him from access Projects and Tasks.

Table 7-6. Settings to restrict a user from updating Tasks

Setting	Value	Description
Access Grant	(REMOVE) Update Tasks	Removing these access grant from users keeps them from updating Tasks.
Participant Restriction in the SECURITY tab.	Participant Restriction	Restrict who can access Projects and Tasks to only "participants." Set in the SECURITY tab on the PROJECT SETTINGS window.

Deleting Projects

Only users with the following license and access grants can delete Projects.

Table 7-7. Settings to enable a user to delete a Project

Setting	Value	Description
License	Power License	The Power License provides a Kintana user with access to the Kintana Workbench where he can delete Projects.
Access Grants (Only one is required)	Edit Projects	Delete Projects when specified as the Project Manager for the Project or Subproject.
	Manage Projects	Delete any Project.

Overriding Project Security

Users with the following settings can view, edit and delete any Project in Kintana:

Table 7-8. Settings to override Request Security

Setting	Value	Description
Access Grants	Deliver: Manage Packages	View, edit and delete any Project in Kintana.
	Drive: Override Drive Participant Restriction	View the detailed information on a restricted Project for which the user is not an active participant.

Users with the following access grant can edit Kintana configuration entities, regardless of Ownership restrictions:

Table 7-9. Access Grant to override configuration security

Value	Description
Ownership Override	Access and edit all configuration entities even if the user is not a member of one of the entity's Ownership Groups.

Chapter 8

Resource Management Security

Kintana allows you to exercise control over data and process related to Resource Management functions in Kintana. You can restrict users' actions around:

- Working with Resources
- Working with Resource Pools
- Working with Skills
- Working with the Organization Model
- Working with Staffing Profiles

Configuring data and process security often involves setting a number of parameters: licenses, access grants, entity level settings and field level settings. The following sections discuss the settings required for securing the actions or data related to Kintana's Resource Management features.



Note

Screen and function access provided through Access Grants are cumulative. If a user belongs to three different Security Groups, he will have all access provided to each of the groups. Therefore, to restrict certain screen and feature access, you need to remove the user from any Security Group that grants that access.

You can use the **ACCESS GRANTS** tabs in the **USER** window to see all Security Groups where specific access grants are included. You can then:

- Remove the user from the Security Group (using the **SECURITY GROUP** tab on the **USER** window)
- Remove the Access Grants from the Security Group (in the Security Group window). Note: you should only do this if no one in that Security Group needs the access provided in that Access Grant.



Note

This chapter discusses how to enable certain functions within Kintana. By default, users are not expected to be given access to viewing or modifying information related to Budgets, Cost, Resource Pools, Staffing Profiles and Skills. The following chapters provide instructions for enabling the viewing and editing of these functions

Working with Resources

Each Kintana user has an associated Resource information page. This page is used to capture information on the individual user such as Title, Direct Manager, Capacity, etc. You can configure users to allow the following:

- [Viewing Resource Information](#)
- [Modifying Resource Information](#)

Viewing Resource Information

To allow a user to view resource information, set the following:

Table 8-1. Settings to allow users to view Resource information

Setting	Value	Description
Access Grant (only one is required)	Resource Mgmt: View my personal resource info only	Allows users to only view their own resource information.
	Resource Mgmt: View all resources	Allows users to view any resource information in the system.

Modifying Resource Information

To allow a user to modify resource information, set the following:

Table 8-2. Settings to allow users to modify Resource information

Setting	Value	Description
Access Grant (only one is required)	Resource Mgmt: Edit only resources that I manage	Edit Resource information for Resources that list the current user as the Direct Manager. A resource's Direct Manager is displayed on the VIEW RESOURCE page.
	Resource Mgmt: Edit all resources	Edit the Resource information for any Resource defined in Kintana.

Working with Resource Pools

You can configure users to allow the following actions:

- *Viewing Resource Pools*
- *Creating Resource Pools*
- *Modifying Resource Pools*

These actions are controlled by a combination of access grants and settings in the CONFIGURE ACCESS FOR RESOURCE POOL page. This page is shown in *Figure 8-1*.

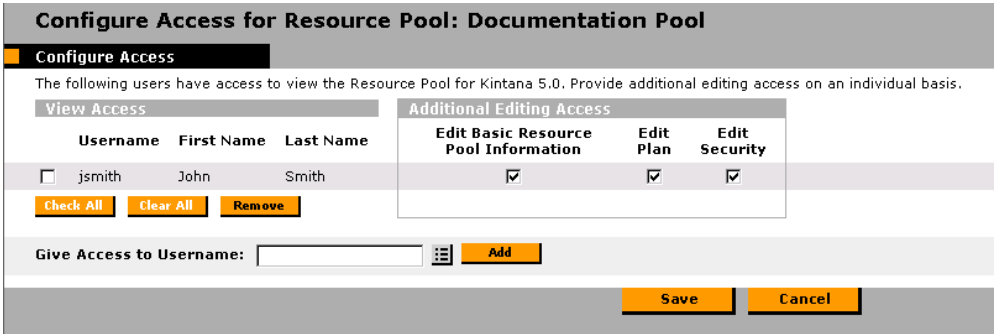


Figure 8-1 Configure Access for Resource Pool page

Viewing Resource Pools

To allow a user to modify Resource Pool information, set the following:

Table 8-3. Settings to allow users to view Resource Pool information

Setting	Value	Description
Access Grant (only one is required)	View Resource Pools	View Resource Pool information when the user has been granted view access in the CONFIGURE ACCESS FOR RESOURCE POOL page.
	View All Resource Pools	View Resource Pool information for all Resource Pools. Note: this grant provides unlimited access to view any resource pool in Kintana. Consider using View Resource Pool to provide more limited view access.
CONFIGURE ACCESS FOR RESOURCE POOL	VIEW ACCESS	Users included in the VIEW ACCESS list and have the View Resource Pools access grant can view the Resource Pool information.

Creating Resource Pools

To allow a user to create a Resource Pool, set the following:

Table 8-4. Settings to allow users to create Resource Pools

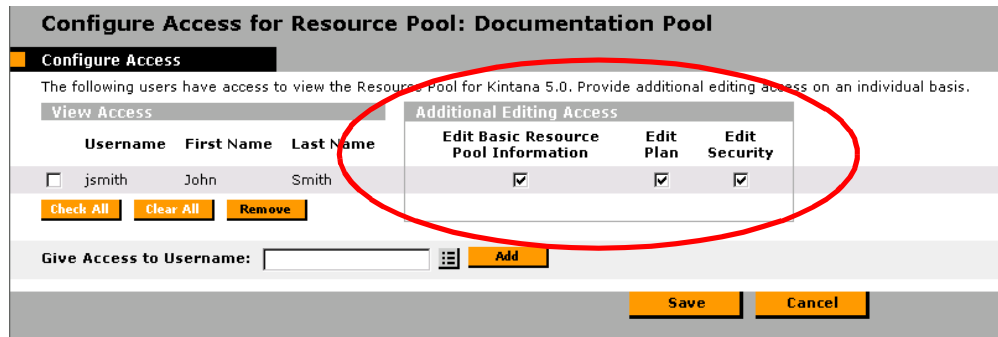
Setting	Value	Description
Access Grant	Edit Resource Pools	Create a new Resource Pool.
	Edit All Resource Pools	Create a new Resource Pool.
	Create Resource Pools (Required)	Create Resource Pools using the standard Kintana interface. The user must also have either the EDIT RESOURCE POOLS or EDIT ALL RESOURCE POOLS grant to perform this function.

Modifying Resource Pools

To allow a user to modify Resource Pool information, set the following:

Table 8-5. Settings to allow users to modify Resource Pools

Setting	Value	Description
Access Grant (only one is required)	Edit All Resource Pools	Edit and delete any Resource Pool.
	Edit Resource Pools	Edit Resource Pool information when the user has been granted edit access in the CONFIGURE ACCESS FOR RESOURCE POOL page. Delete these Resource Pools when given sufficient access in the CONFIGURE ACCESS FOR RESOURCE POOL page for that Resource Pool.
Additional Editing Access (see Description column)	Edit Basic Resource Pool Information	Used in conjunction with the Edit Resource Pools access grant. Allows the user to edit Resource Pool header fields and Notes. He will not be allowed to change the Periods or any information in the Resource Pool Breakdown section.
	Edit Plan	Allows the user to edit the Periods and the information in the Resource Pool Breakdown section.
	Edit Security	Allows the user to edit the list of users who can modify the Resource Pool using the CONFIGURE ACCESS FOR RESOURCE POOL page.



Working with Skills

You can configure users to allow the following:

- [Viewing Skills](#)
- [Creating, Modifying, and Deleting Skills](#)

Viewing Skills

To allow a user to view skill information, set the following:

Table 8-6. Settings to allow users to view Skill information

Setting	Value	Description
Access Grant	Resource Mgmt: View All Skills	Allows users to view Skills defined on Resources in Kintana.

Creating, Modifying, and Deleting Skills

To allow a user to modify the list of Skills set in Kintana, set the following:

Table 8-7. Settings to allow users to create, modify and delete Skills

Setting	Value	Description
Access Grant	Resource Mgmt: Edit All Skills	Edit any Skills defined in Kintana.

Working with the Organization Model

You can configure users to allow the following:

- [Viewing the Organization Model](#)
- [Modifying Organization Definitions](#)

Viewing the Organization Model

To allow a user to view Organization information in Kintana, set the following:

Table 8-8. Settings to view Organization information.

Setting	Value	Description
Access Grant	Resource Mgmt: View Organization	View the Organization Model and Organization Unit detail pages.

Modifying Organization Definitions

To allow a user to modify Organization information, set one of the following:

Table 8-9. Settings to modify Organization information.

Setting	Value	Description
Access Grant (only one is required)	Edit Entire Organization	Edit and delete any Organization Unit.
	Edit Only Organization Units That I Manage	Edit Organization Unit information for units that list the current user as the Manager in the VIEW ORGANIZATION UNIT page. Also delete any of these Organization Units.

Working with Staffing Profiles

You can configure users to allow the following actions:

- [Viewing Staffing Profiles](#)
- [Creating Staffing Profiles](#)
- [Modifying Staffing Profiles](#)

These actions are controlled by a combination of access grants and settings in the CONFIGURE ACCESS FOR STAFFING PROFILE page. This page is shown in [Figure 8-2](#).

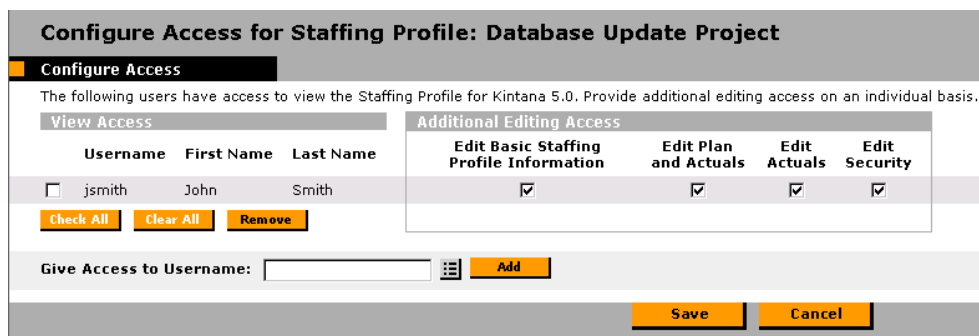


Figure 8-2 Configure Access for Resource Pool page

Viewing Staffing Profiles

To allow a user to view Staffing Profile information, set the following:

Table 8-10. Settings to allow users to view Resource Pool information

Setting	Value	Description
Access Grant (only one is required)	View Staffing Profiles	View Staffing Profile information when the user has been granted view access in the CONFIGURE ACCESS FOR STAFFING PROFILE page.
	View All Staffing Profiles	View Staffing Profiles information for all Staffing profiles. Note: this grant provides unlimited access to view any staffing profile in Kintana. Consider using the View Staffing Profiles grant to provide more limited view access.
CONFIGURE ACCESS FOR STAFFING PROFILE	VIEW ACCESS	Users included in the VIEW ACCESS list and have the View Staffing Profiles access grant can view the Staffing Profile information.

Creating Staffing Profiles

To allow a user to create a Staffing Profile, set the following:

Table 8-11. Settings to allow users to create Staffing Profiles

Setting	Value	Description
Access Grant	Edit Staffing Profiles	Create a new Staffing Profile.
	Edit All Staffing Profiles	Create a new Staffing Profile.
	Create Staffing Profiles (Required)	Create Staffing Profiles using the standard Kintana interface. The user must also have either the EDIT STAFFING PROFILES or EDIT ALL STAFFING PROFILES grant to perform this function.

Modifying Staffing Profiles

To allow a user to modify Staffing Profile information, set the following:

Table 8-12. Settings to allow users to modify Staffing Profiles

Setting	Value	Description
Access Grant	Edit All Staffing Profiles	Edit and delete any Staffing Profile.
	Edit Staffing Profiles	Edit Staffing Profile information when the user has been granted edit access in the CONFIGURE ACCESS FOR STAFFING PROFILE page. Delete these Staffing Profiles when given sufficient access in the CONFIGURE ACCESS FOR STAFFING PROFILE page for that Staffing Profile.

Table 8-12. Settings to allow users to modify Staffing Profiles

Setting	Value	Description
Additional Editing Access	Edit Basic Staffing Profile Information	Used in conjunction with the Edit Staffing Profiles access grant. Allows the user to edit Staffing Profile header fields and Notes. He will not be allowed to change the Periods or any information in the Staffing Profile Breakdown section.
	Edit Plan and Actuals	Allows the user to edit the Periods and the information in the Staffing Profile Breakdown section. Additionally, allows users to view and edit the planning and actuals data in the Profile Allocation table.
	Edit Actuals	Allows the user to edit the Periods and the information in the Staffing Profile Breakdown section. Additionally, allows users to view and edit the actuals data in the Profile Allocation table.
	Edit Security	Allows the user to edit the list of users who can modify the Staffing Profile using the CONFIGURE ACCESS FOR STAFFING PROFILE page.

Configure Access for Staffing Profile: Database Update Project

Configure Access

The following users have access to view the Staffing Profile for Kintana 5.0. Provide additional editing access on an individual basis.

View Access			Additional Editing Access			
Username	First Name	Last Name	Edit Basic Staffing Profile Information	Edit Plan and Actuals	Edit Actuals	Edit Security
<input type="checkbox"/>	jsmith	John	Smith	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Give Access to Username:

Chapter 9

Cost and Budget Data Security

Kintana allows you to exercise control over data and process related to financial functions (Cost and Budget) in Kintana. You can restrict users' actions around:

- *Working with Cost Data*
- *Working with Budgets*

Configuring data and process security often involves a setting a number parameters: licenses, access grants, entity level settings and field level settings. The following sections discuss the settings required for securing the actions or data related to Kintana's financial analysis features.



Note

Screen and function access provided through Access Grants are cumulative. If a user belongs to three different Security Groups, he will have all access provided to each of the groups. Therefore, to restrict certain screen and feature access, you need to remove the user from any Security Group that grants that access.

You can use the **ACCESS GRANTS** tabs in the **USER** window to see all Security Groups where specific access grants are included. You can then:

- Remove the user from the Security Group (using the **SECURITY GROUP** tab on the **USER** window)
- Remove the Access Grants from the Security Group (in the Security Group window). Note: you should only do this if no one in that Security Group needs the access provided in that Access Grant.



Note

This chapter discusses how to enable certain functions within Kintana. By default, users are not expected to be given access to viewing or modifying information related to Budgets or Cost. The following chapters provide instructions for enabling the viewing and editing of these functions

Working with Cost Data

Cost data can be associated with Tasks, Projects, Programs, Resources and Skills in Kintana. The following sections provide details for enabling users to view and edit cost-related data on these entities:

- [Viewing Cost Data](#)
- [Modifying Cost Data](#)

Viewing Cost Data

The following access grants are needed to view cost information in Kintana.

Table 9-1. Access Grants for viewing cost data

Access Grant	Description
Cost: View Cost Data	View Cost data related to Tasks, Projects, Programs, Resources and Skills. The user must also have access to view these entities.

Enable Cost Data for a Project

If Cost Management is enabled for a Project (set in the **COST MANAGEMENT** tab in the PROJECT SETTINGS window), you can specify who can view the related cost information. This is set in the **SECURITY** tab in the PROJECT SETTINGS window. You can make cost information on the Project and Tasks available to one of the following options:

- All users
- Project Managers for this Master Project only

- Project Managers for the Master Project and all of the Subprojects
- Participants for only the Tasks and Projects for which they are Participants
- Project Team only



Note

You must have the Edit Cost Security Access Grant to change these settings in the PROJECT SETTINGS window.

The screenshot shows a dialog box titled "Settings for IT Business Initiative" with a "Security" tab selected. The dialog has a tabbed interface with the following tabs: MSP Synchronization, Cost Management, Resource Management, Time Management, Baselines, Project Fields, Exception Rules, Indicators, Scheduling, Security, and Project Team. The "Security" tab contains two sections of radio button options:

- This Project and its Tasks can be viewed by:**
 - All users
 - Participant Restricted - Only users assigned as Project Managers, Resources, or in an assigned Resource Group
- Cost information on the Project and Tasks can be viewed by:**
 - All users
 - Project Managers for this Master Project only
 - Project Managers for Master Project IT Business Initiative and all of its subproject
 - Participants for only the Tasks and Projects for which they are Participants.
 - Project Team only.

At the bottom right of the dialog are buttons for "OK", "Apply", and "Cancel". The status bar at the bottom left shows "Ready".

Specified users will be able to access the **COST** and **EV ANALYSIS** tabs on the PROJECT window.



Tip

You can provide a granular level of cost-data view access by using a combination of Security settings and Access Grants. For example, you could provide All Users with cost data access, but only provide a limited set of users with the View Cost Data access grant.

Enable Cost Data for a Program

If Cost Management is enabled for a Program, you can specify who can view the related cost information. This is set in the CONFIGURE ACCESS FOR PROGRAM page. You can make cost information on the Program available to one of the following options:

- Only the Program Manager
- All Project Managers of Projects in this Program
- All other Program Managers
- All Program Managers; and Project managers in this Program
- Only specified Security Groups



Note

You must have the Edit Cost Security Access Grant to change these settings in the CONFIGURE ACCESS FOR PROGRAM page.

Create Program > Configure Access for Controlling IT Cost

Configure Access for Controlling IT Cost

Configure Access Done Cancel

Program Access

In addition to John Smith, the Program Manager(s) of this Program, give view access to:

- No One
- All Project Managers of Projects in this Program
- All other Program Managers
- All Program Managers; and Project managers in this Program
- Only these Security Groups:

Remove

Cost Access

In addition to John Smith, the Program Manager(s) of this Program, give view access to:

- No One
- All Project Managers of Projects in this Program
- All other Program Managers
- All Program Managers; and Project managers in this Program
- Only these Security Groups:

Remove

Done Cancel

Modifying Cost Data

Additional access grants are required to be able to modify cost data. See “[Viewing Cost Data](#)” on page 86 for information on enabling users to access (view) the cost information.

Table 9-2. Access Grants for modifying cost data

Access Grant	Description
Cost: Edit Cost Data	Edit Cost data related to Tasks, Projects, Programs, Resources and skills. The user must also have access to edit these entities.

Working with Budgets

You can configure users to allow the following actions:

- [Viewing Budgets](#)
- [Creating Budgets](#)
- [Modifying Budgets](#)

These actions are controlled by a combination of access grants and settings in the CONFIGURE ACCESS FOR BUDGET page. This page is shown in [Figure 9-1](#).

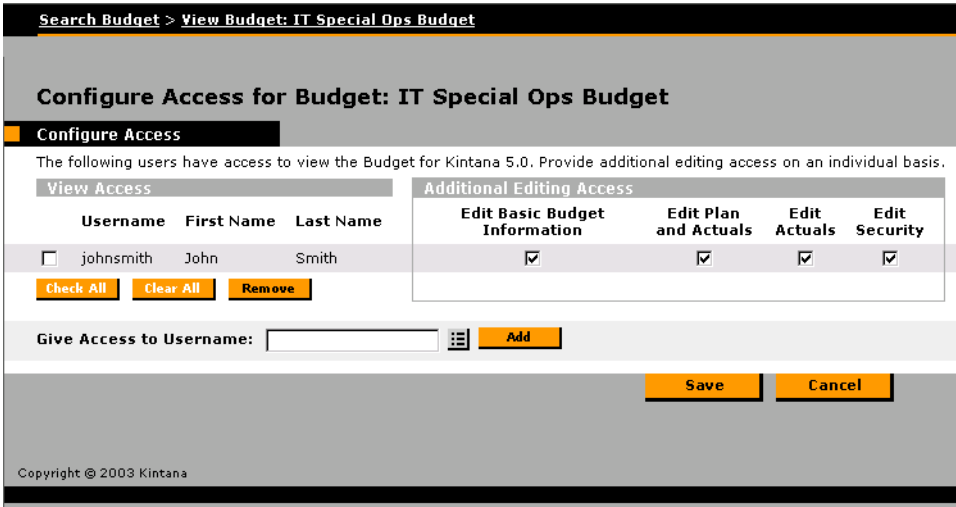


Figure 9-1 Configure Access for Budget page

Viewing Budgets

To allow a user to view a Budget, set the following:

Table 9-3. Settings to view Budget information

Setting	Value	Description
Access Grant (only one is required)	View Budgets	View Budget information when the user has been granted view access in the CONFIGURE ACCESS FOR BUDGET page.
	View All Budgets	View Budget information for all Budgets. Note: this grant provides unlimited access to view any Budget in Kintana. Consider using View Budgets to provide more limited view access.
CONFIGURE ACCESS FOR BUDGETS	VIEW ACCESS	Users included in the VIEW ACCESS list and have the View Budgets access grant can view the Budget information.

Creating Budgets

To allow a user to create a Budget, set the following:

Table 9-4. Settings to create Budgets

Setting	Value	Description
Access Grant	Edit Budgets	Create a new Budget.
	Edit All Budgets	Create a new Budget.
	Create Budgets (Required)	Create Budgets using the standard Kintana interface. The user must also have either the EDIT BUDGETS or EDIT ALL BUDGETS grant to perform this function.

Modifying Budgets

To allow a user to modify Budget information, set the following:

Table 9-5. Settings to allow users to modify Budgets.

Setting	Value	Description
Access Grant (only one is required)	Edit All Budgets	Edit and delete any Budget.
	Edit Budgets	Edit Budget information when the user has been granted edit access in the CONFIGURE ACCESS FOR BUDGET page. Delete these Budgets when given sufficient access in the CONFIGURE ACCESS FOR BUDGET page for that Budget.
Additional Editing Access	Edit Basic Budget Information	Used in conjunction with the Edit Budgets access grant. Allows the user to edit Budget header fields, user data, and notes. He will not be allowed to change the Periods or any information in the Budget Breakdown section.
	Edit Plan and Actuals	Allows the user to edit the Periods and the information in the Budget Breakdown section. Additionally, allows users to view and edit the planning and actuals data in the Budget Breakdown table.
	Edit Actuals	Allows the user to edit the Periods and the information in the Budget Breakdown section. Additionally, allows users to view and edit the actuals data in the Budget Breakdown table.
	Edit Security	Allows the user to edit the list of users who can modify the Budgets using the CONFIGURE ACCESS FOR BUDGET page.

Search Budget > View Budget: IT Special Ops Budget

Configure Access for Budget: IT Special Ops Budget

Configure Access

The following users have access to view the Budget for Kintana 5.0. Provide additional editing access on an individual basis.

View Access			Additional Editing Access			
Username	First Name	Last Name	Edit Basic Budget Information	Edit Plan and Actuals	Edit Actuals	Edit Security
<input type="checkbox"/>	johnsmith	John Smith	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Give Access to Username:

Copyright © 2003 Kintana

Chapter 10 Dashboard Security

The Kintana Dashboard provides users with quick access to Kintana data through the inclusion of a number of system and custom portlets on their Dashboards. To secure this data, Kintana allows you to:

- Allow only certain users to use a specific portlet
- View only data for items (Requests, Packages, or Projects) for which they are a “participant”

Controlling User Access to Portlets

You can control portlet user access at two levels:

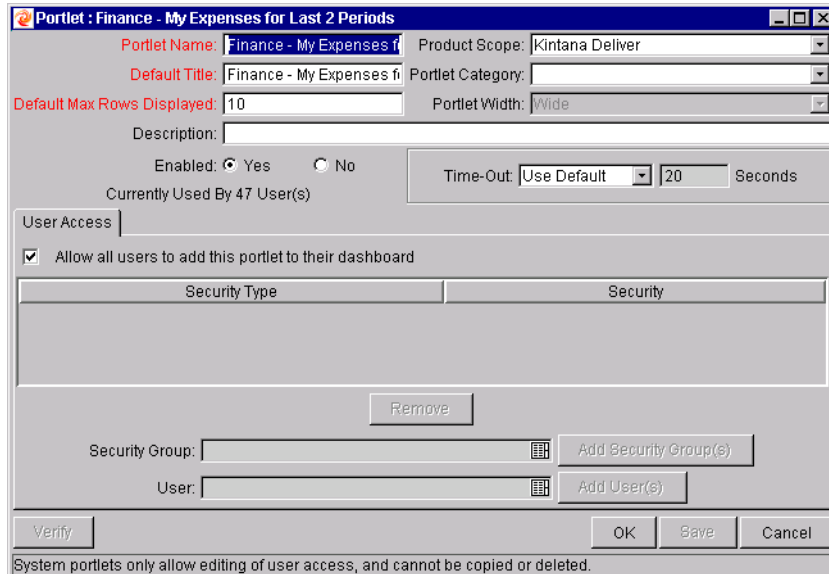
- [Disabling Portlets](#)
- [Restricting User Access](#)

Disabling Portlets

You can disable custom-built portlets at your site. To disable a portlet:

1. Click the **DASHBOARD** screen group and click the **PORTLETS** icon.
2. Search for and open the custom Portlet that you would like to disable.

Note that you can not disable Kintana system portlets. To control access to these portlets, you can restrict user access. See [Restricting User Access](#) for details.



3. Click **ENABLED = No**.



Note

If there are any users currently using the portlet on their Dashboard, disabling the portlet will delete it from their Dashboards.

4. Click **SAVE**.

Related Topics:

- ["Using the Kintana Dashboard"](#)
- ["Configuring the Kintana Dashboard"](#)

Restricting User Access

You can control which users can add a portlet to their Dashboard. For example, you may want to restrict the Package-related portlets to only members involved in the deployments. Enabling only the portlets that a specific user needs will make it easier for that user to personalize their Dashboard, because there are fewer (non-relevant) portlets to choose from.

To specify which users can use the portlet on their Dashboard:

1. Click the **DASHBOARD** screen group and click the **PORTLETS** icon.
2. Search for and open the Portlet that you would like to configure.
3. Click the **USER ACCESS** tab. For system portlets (such as My Packages), the **USER ACCESS** tab is the only displayed tab.

Portlet: My Packages

Portlet Name: My Packages Product Scope: Kintana Deliver

Default Title: My Packages Portlet Category: Packages

Default Max Rows Displayed: 5 Portlet Width: Wide

Description: Displays all Packages created by or assigned to the current user. Users can drill down

Enabled: Yes No

Currently Used By 32 User(s)

Time-Out: Use Default 20 Seconds

User Access

Allow all users to add this portlet to their dashboard

Security Type	Security

Remove

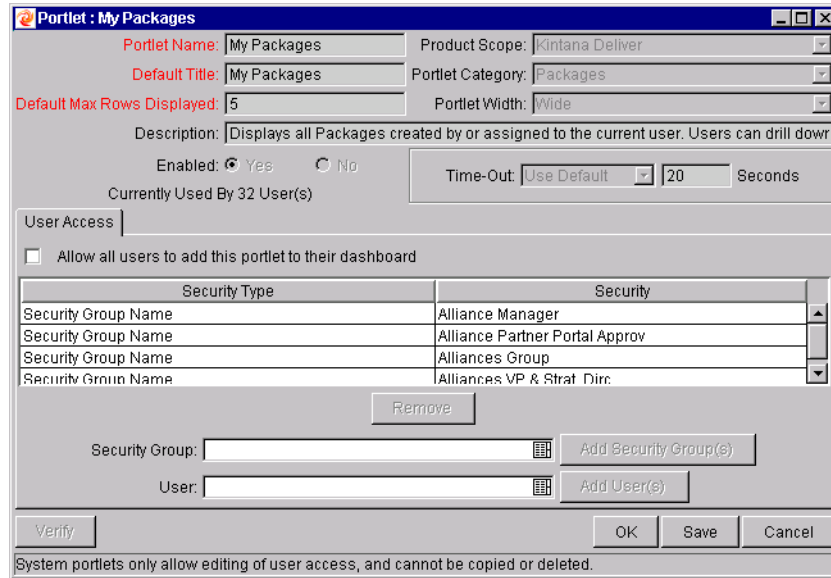
Security Group: Add Security Group(s)

User: Add User(s)

Verify OK Save Cancel

System portlets only allow editing of user access, and cannot be copied or deleted.

4. Un-check the **ALLOW ALL USERS TO ADD THIS PORTLET TO THEIR DASHBOARD** field. The **SECURITY GROUP** and **USER** fields are enabled.
5. Select the desired **Security Groups** or **Users** and click the respective **ADD** button. They are added to the **USER ACCESS** tab.



6. Click **SAVE**.

You can restrict access by specifying multiple Security Groups and Users for each portlet. Only members of the specified Security Group or the specified users can add this portlet to their Dashboard.



You can restrict user access for both custom and system portlets.

Restricting Data to Participants

The Kintana Dashboard respects any participant-restrictions configured for Requests, Packages or Projects. When these items are restricted, only users who are directly involved with them can view their data on the Dashboard. Restricted items will not be displayed in portlets or returned in searches.



The participant-restriction model is supported by all of Kintana's system portlets. Custom portlets are not supported. They will display whatever information is specified in the SQL query that defines the portlet.

Chapter 11 Configuration Security

Kintana allows you to set security around the Kintana configuration. You can establish configuration security around all of the Kintana configuration entities. This includes such activities as controlling:

- Who can change a Workflow.
- Who can change each Object Type.
- Who can change Request Types
- Who can change User and Security Group definitions.

The following sections discuss some options for securing your Kintana configurations:

- [*Setting Ownership for Kintana Configuration Entities*](#)
- [*Removing Access Grants*](#)

Setting Ownership for Kintana Configuration Entities

Different groups of Kintana users have ownership and control over Kintana entities. These groups are referred to as Ownership Groups. Unless a 'global' permission has been designated to all users for an entity, members of Ownership Groups are the only users who have the right to edit, delete or copy that entity. The Ownership Groups must also have the proper access grant for the entity in order to complete those tasks. For example, the `EDIT WORKFLOWS` Access Grant is needed to edit Workflows and Workflow Steps.

You can assign multiple Ownership Groups to the various entities. Ownership Groups are defined in the SECURITY GROUP window. Security Groups become Ownership Groups when used in the Ownership capacity.

You can select to specify Ownership Groups for the following entities involved in your process:

- Environments
- Environment Groups
- Object Types
- Report Types
- Request Header Types
- Request Types
- Security Groups
- Special Commands
- User Definitions
- Validations
- Workflows
- Workflow Steps

The Ownership setting is accessed through the individual entity windows in the Kintana Workbench. For example, to set the Ownership for Workflows:

1. Open the Workflow.
2. Click the **OWNERSHIP** tab.
3. Click the **ONLY GROUPS LISTED BELOW THAT HAVE THE EDIT WORKFLOWS ACCESS GRANT** radio button.
4. Click **ADD**. The **ADD SECURITY GROUP** window opens.
5. Select the **SECURITY GROUP**.
6. Click **ADD** to add the current Security Group and continue adding more Security Groups. Click **OK** to add the current Security Group and close the **ADD SECURITY GROUP** window.

The Security Group(s) you selected displays in the **OWNERSHIP** tab under the SECURITY GROUP column.

Workflow : Untitled5

Workflow | Layout | Step Sequence | Deliver Settings

Package Workflows | Request Types | Ownership | Used By | User Data

Give ability to edit this Workflow to:

All users with the Edit Workflows Access Grant

Only groups listed below that have the Edit Workflows Access Grant

Security Group	Description
Kintana Deliver Config Manager	Configuration Manager for Kintana Deliver

Add Remove

Verify OK Save Cancel

Ready

7. Click **OK** to save the selection and close the WORKFLOW window. Click **SAVE** to save the selection and leave the Workflow window open.

Note

The SYS ADMIN: OWNERSHIP OVERRIDE access grant allows the user to access and edit configuration entities even if he is not a member of one of the entity's Ownership Groups. This access grant should be given only to super-users who may need to configure Kintana processes for multiple groups.

Removing Access Grants

You can also restrict the ability to modify Kintana configuration entities by removing the user from any Security Group that grants that access.

You can use the **ACCESS GRANTS** tabs in the USER window to see all Security Groups where specific access grants are included. You can then either:

- Remove the user from the Security Group (using the **SECURITY GROUP** tab on the USER window)

- Remove the Access Grants from the Security Group (in the SECURITY GROUP window). Note: You should only do this if no one in that Security Group needs the access provided in that Access Grant.

The following table lists the access grants that provide edit access to different Kintana configuration entities.

Table 11-1. Access Grants for editing Kintana configuration entities

Category	Access Grant Name	Description
Config	Edit Notification Templates	Create, edit and delete Notification Templates in the NOTIFICATION TEMPLATES WORKBENCH.
Config	Edit Report Types	Create, edit and delete Report Types in the REPORT TYPES WORKBENCH.
Config	Edit Special Commands	Create, edit and delete Special Commands in the SPECIAL COMMANDS WORKBENCH.
Config	Edit User Data	Create, edit and delete User Data definitions in the USER DATA WORKBENCH.
Config	Edit Validation Values	Create, edit and delete Validation values in the VALIDATIONS WORKBENCH.
Config	Edit Validations	Create, edit and delete Validations in the VALIDATION WORKBENCH.
Config	Edit Workflows	Create, edit and delete Workflows in the WORKFLOWS WORKBENCH.
Create	Edit Request Header Types	Create, edit and delete Request Header Types in the REQUEST HEADER TYPES WORKBENCH.
Create	Edit Request Types	Create, edit and delete Request Types in the REQUEST TYPES WORKBENCH.
Dashboard	Edit Default User Homepage	View and edit the default User Homepage for all Kintana Dashboard users.
Dashboard	Edit Portlet Definition	Create, edit and delete Portlets in the PORTLETS WORKBENCH.
Deliver	Edit Object Types	Create, edit and delete Object Types in the OBJECT TYPES WORKBENCH.
Drive	Edit Calendars	Create, edit and delete Project Calendars in the PROJECTS WORKBENCH.
Drive	Edit Project Templates	Create, edit and delete Project Templates in the PROJECT TEMPLATES WORKBENCH.

Table 11-1. Access Grants for editing Kintana configuration entities

Category	Access Grant Name	Description
Drive	Edit Projects	Create Projects using the Projects Workbench. Update and delete Projects and Subprojects when specified as the Project Manager.
Environments	Edit Environments	Create, edit and delete Environments in the ENVIRONMENTS WORKBENCH.
Sys Admin	Edit Security Groups	Create, edit and delete Security Groups in the SECURITY GROUPS WORKBENCH.
Sys Admin	Edit Users	Create, edit and delete Users in the USERS WORKBENCH.
Time Mgmt	Edit Activities	Create, edit and delete Activities in the ACTIVITIES WORKBENCH.
Time Mgmt	Edit Charge Codes	Create, edit and delete Charge Codes in the CHARGE CODES WORKBENCH.
Time Mgmt	Edit Override Rules	Create, edit and delete Override Rules in the OVERRIDE RULES WORKBENCH.
Time Mgmt	Edit Time Mgmt Settings	Edit Time Management settings for a user in the TIME MGMT SETTINGS WORKBENCH. Also enables the TIME MANAGEMENT SETTINGS button in the USER window.

Appendix

A

Access Grants

Access Grants enable certain activities within Kintana. Kintana comes with a pre-defined list of Access Grants. Installing a Kintana Solution or Kintana Accelerator introduces additional Access Grants. [Table A-1](#) lists the available Access Grants and provides a description of each grant.

Note

View access grants provide read-only access to screens and entities. Users without the **VIEW** Access Grant will be unable to see certain workbenches or windows.

Edit access grants typically enable a user to view, create, modify and delete entities in certain circumstances. For example, if you have the Edit Requests access grant, you can delete Requests that you have created.

Manage access grants typically enable the same functions as the Edit access grants (create, modifying, and deleting), but are less restricted. For example, if you have the Manage Requests access grant, you can delete any Request in the system that you can access, even if you did not create the Request.

Refer to [Table A-1](#) for the details on the specific access grant.

Table A-1. Kintana Access Grants

Category	Access Grant Name	Description
Config	Edit Notification Templates	Create, update and delete Notification Templates in the NOTIFICATION TEMPLATES WORKBENCH.
Config	Edit Report Types	Create, update and delete Report Types in the REPORT TYPES WORKBENCH.

Table A-1. Kintana Access Grants

Category	Access Grant Name	Description
Config	Edit Special Commands	Create, update and delete Special Commands in the SPECIAL COMMANDS WORKBENCH.
Config	Edit User Data	Create, update and delete User Data definitions in the USER DATA WORKBENCH.
Config	Edit Validation Values	Create, update and delete Validation values in the VALIDATIONS WORKBENCH.
Config	Edit Validations	Create, update and delete Validations in the VALIDATION WORKBENCH.
Config	Edit Workflows	Generate, update and delete Workflows in the WORKFLOWS WORKBENCH.
Config	View Notification Templates	View Notification Template definitions in the NOTIFICATION TEMPLATES WORKBENCH.
Config	View Report Types	View Report Type definitions in the the REPORT TYPES WORKBENCH.
Config	View Special Commands	View Special Command definitions in the SPECIAL COMMANDS WORKBENCH.
Config	View User Data	View User Data definitions in the USER DATA WORKBENCH.
Config	View Validations	View Validations in the VALIDATIONS WORKBENCH.
Config	View Workflows	View Workflow definitions in the WORKFLOWS WORKBENCH.
Cost	Approve Budgets	<p>Change the BUDGET STATUS value on the MODIFY BUDGET page to "APPROVED." The user must also have the UPDATE BUDGETS STATUS grant and either the EDIT BUDGET or EDIT ALL BUDGETS grant to perform this function.</p> <p>Note that "APPROVED" only appears in the BUDGET STATUS list if you have this grant.</p>
Cost	Create Budgets	Create Budgets using the standard Kintana interface. The user must also have either the EDIT BUDGETS or EDIT ALL BUDGETS grant to perform this function.
Cost	Edit All Budgets	Edit Budget information for all Budgets in Kintana.
Cost	Edit Budgets	Edit Budget information when the user has been granted edit access in the CONFIGURE ACCESS FOR BUDGET page.
Cost	Edit Cost Data	Edit Cost data related to Tasks, Projects, Programs, Resources and skills. The user must also have access to edit these entities.

Table A-1. Kintana Access Grants

Category	Access Grant Name	Description
Cost	Edit Cost Security	Edit Cost security settings for a Project in the PROJECT SETTINGS window. Edit Cost security settings for a Program in the PROGRAM SECURITY CONFIGURATION page. Note: The user must also be able to edit the Project Settings and Program Security in order for this grant to be relevant.
Cost	Update Budget Status	Change the BUDGET STATUS value on the MODIFY BUDGET page. The user must also have either the EDIT BUDGETS or EDIT ALL BUDGETS grant to perform this function.
Cost	View All Budgets	View Budget information for all Budgets in Kintana.
Cost	View Budgets	View Budget information when the user has been granted view access in the CONFIGURE ACCESS FOR BUDGET page.
Cost	View Cost Data	View Cost data related to Tasks, Projects, Programs, Resources and skills. The user must also have access to view these entities.
Create	Allow Request Field Updates	View and update any Request, regardless of whether or not the user is the creator or Contact.
Create	Edit Contacts	Create and update Contacts in the CONTACTS WORKBENCH.
Create	Edit Request Header Types	Create, update and delete Request Header Types in the REQUEST HEADER TYPES WORKBENCH.
Create	Edit Request Types	Create, update and delete Request Types in the REQUEST TYPES WORKBENCH.

Table A-1. Kintana Access Grants

Category	Access Grant Name	Description
Create	Edit Requests	<p>Perform basic Request processing actions: create Requests, edit certain Requests, and delete your un-submitted Requests depending on your license (standard versus power).</p> <p>Standard License:</p> <ul style="list-style-type: none"> • Allows the user to generate Requests. • User cannot change the Workflow when creating or editing a Request. • To edit the Request, user must be its creator, a member of the Workflow Steps security group or associated with the current contacts. Otherwise, user can only view the Request. <p>Power License:</p> <ul style="list-style-type: none"> • Has the same permissions as those listed for Standard License. • Allows user to delete the Request if the user is the creator and the Request has not been submitted.
Create	Manage Contacts	Edit and delete Contacts using the CONTACTS WORKBENCH.
Create	Manage Requests	<p>Perform advanced Request processing actions: creating, editing, deleting, changing the Request's workflow, and overriding references. This access enables different functions depending on your license (standard versus power).</p> <p>Standard License:</p> <ul style="list-style-type: none"> • User can change the Workflow when creating and editing a Request. • User always has permission to edit the Request. • Override and/or remove any References on any Request. <p>Power License:</p> <ul style="list-style-type: none"> • Has the same permissions as those listed for Standard License. • User always has permission to delete or cancel a Request.
Create	Override Create Participant Restriction	View the detailed information on a restricted Request for which the user is not an active participant.
Create	Submit Create DSS Reports	Create, submit and cancel Kintana DSS reports using either the standard interface or the Workbench.

Table A-1. Kintana Access Grants

Category	Access Grant Name	Description
Create	Submit Create Reports	Create, submit and cancel standard Kintana reports using either the standard interface or the Workbench.
Create	View All Contacts in Request	View all Contacts in a Request even if a company is associated with the Request.
Create	View Contacts	View the Contact definition in the CONTACTS WORKBENCH.
Create	View Request Header Types	View Request Header Type definitions in the REQUEST HEADER TYPES WORKBENCH.
Create	View Request Types	View the Request Type definition in the REQUEST TYPES WORKBENCH.
Create	View Requests	View Request Type definitions in the REQUEST TYPES WORKBENCH.
Dashboard	Edit Default User Homepage	View and edit the default User Homepage for all Kintana Dashboard users.
Dashboard	Edit Portlet Definition	Create, edit and delete Portlets in the PORTLETS WORKBENCH.
Dashboard	View Portlet Definition	View Portlet definitions in the PORTLETS WORKBENCH.
Deliver	Edit Object Types	Create, edit and delete Object Types in the OBJECT TYPES WORKBENCH.
Deliver	Edit Packages	<p>Perform basic Package processing actions: create, edit certain related Packages, and delete certain un-submitted Packages.</p> <ul style="list-style-type: none"> • To edit the Package, user must be its creator, the 'assigned to' user, a member of the assigned group or a member of the Workflow Steps security group. • User cannot delete a Package if it has been released or if user is not the owner. <<dev check -- what is the "owner">>

Table A-1. Kintana Access Grants

Category	Access Grant Name	Description
Deliver	Edit Releases	<p>Perform basic Release processing actions in the RELEASES WORKBENCH: create, edit, process, and delete certain related Releases.</p> <p>Users with this grant can:</p> <ul style="list-style-type: none"> • View any Release • Be designated as the Release Manager in the Release window • Create Releases • Edit or delete any Release that they created • Act on any Distribution Workflow steps where they are included in the step's security. • Edit or delete a Release that they did not create (only when they are designated as the Release Manager in the RELEASE MANAGEMENT window).
Deliver	Manage Packages	Edit or delete any Packages.
Deliver	Manage Releases	<p>Create, edit and delete any Release using the RELEASES WORKBENCH.</p> <p>Users with this grant can:</p> <ul style="list-style-type: none"> • Create a Release • Be designated as the Release Manager in the Release window • Edit or delete any Release in Kintana (regardless of whether they are specified as the Release Manager in the RELEASE MANAGEMENT window).
Deliver	Override Deliver Participant Restriction	View the detailed information on a restricted Package for which the user is not an active participant.
Deliver	Submit Deliver DSS Reports	Create, submit and cancel Kintana DSS reports using either the Workbench or standard interface.
Deliver	Submit Deliver Reports	Create, submit and cancel standard Kintana reports using either the standard Kintana interface or the Workbench.
Deliver	Submit Environment Refreshes	Create and submit an Environment Refresh in the ENV REFRESH WORKBENCH.
Deliver	View Environment Refreshes	View Environment Refresh definitions in the ENV REFRESH WORKBENCH.
Deliver	View Object Types	View Object Type definitions in the OBJECT TYPES WORKBENCH.

Table A-1. Kintana Access Grants

Category	Access Grant Name	Description
Deliver	View Packages	View Packages in the standard Kintana interface or the Kintana Workbench.
Deliver	View Releases	View Release definitions in the Releases Workbench. Act on any Distribution Workflow steps where the user is included in the step's security.
Demand Mgmt	Manage Demands	Access the Demand Management scheduling functions, the consolidated picture of demand, and all other Demand Management menu items related to scheduling or managing demand.
Drive	Edit Calendars	Create, update and delete Project Calendars in the PROJECTS WORKBENCH.
Drive	Edit Project Templates	Create, update and delete Project Templates in the PROJECT TEMPLATES WORKBENCH.
Drive	Edit Projects	Create Projects using the Projects Workbench. Update and delete Projects and Subprojects when specified as the Project Manager.
Drive	Manage Projects	Create, edit and delete Projects. Override (or remove) References on Projects or Tasks.
Drive	Override Drive Participant Restriction	View the detailed information on a restricted Project for which the user is not an active participant.
Drive	Submit Drive DSS Reports	Create, submit and cancel Kintana DSS reports using either the standard Kintana interface or the Workbench.
Drive	Submit Drive Reports	Create, submit and cancel standard Kintana reports using either the standard Kintana interface or the Workbench.
Drive	Update Tasks	Update Project Tasks using the Projects Workbench or Kintana Dashboard.
Drive	View Calendars	View Project Calendars in the PROJECTS WORKBENCH.
Drive	View Project Templates	View Project Templates in the PROJECT TEMPLATES WORKBENCH.
Drive	View Projects	View Project definitions in the Projects Workbench and standard Kintana interface.
Environments	Edit Environments	Create, update and delete Environments in the ENVIRONMENTS WORKBENCH.
Environments	View Environments	View Environment definitions in the ENVIRONMENTS WORKBENCH.

Table A-1. Kintana Access Grants

Category	Access Grant Name	Description
PMO	Edit Programs	Update Programs where the user is specified as the Program Manager.
PMO	Manage Programs	Create and update any Program.
PMO	View Programs	View Program definitions.
Resource Mgmt	Approve Resource Pools	Change the RESOURCE POOL STATUS value on the MODIFY RESOURCE POOL page to " APPROVED ." The user must also have the UPDATE RESOURCE POOL STATUS grant and either the EDIT RESOURCE POOLS or EDIT ALL RESOURCE POOLS grant to perform this function. Note that " APPROVED " only appears in the RESOURCE POOL STATUS list if you have this grant.
Resource Mgmt	Approve Staffing Profiles	Change the STAFFING PROFILE STATUS value on the MODIFY STAFFING PROFILE page to " APPROVED ." The user must also have the UPDATE STAFFING PROFILE STATUS grant and either the EDIT STAFFING PROFILES or EDIT ALL STAFFING PROFILES grant to perform this function. Note that " APPROVED " only appears in the STAFFING PROFILE STATUS list if you have this grant.
Resource Mgmt	Create Resource Pools	Create Resource Pools using the standard Kintana interface. The user must also have either the EDIT RESOURCE POOLS or EDIT ALL RESOURCE POOLS grant to perform this function.
Resource Mgmt	Create Staffing Profiles	Create Staffing Profiles using the standard Kintana interface. The user must also have either the EDIT STAFFING PROFILES or EDIT ALL STAFFING PROFILES grant to perform this function.
Resource Mgmt	Edit All Resource Pools	Edit and delete any Resource Pool.
Resource Mgmt	Edit All Resources	Edit the Resource information for any Resource defined in Kintana.
Resource Mgmt	Edit All Skills	Create, edit, and delete all Skills defined in Kintana.
Resource Mgmt	Edit All Staffing Profiles	Edit and delete any Staffing Profile.
Resource Mgmt	Edit Entire Organization	Edit and delete any Organization Unit.
Resource Mgmt	Edit Only Organization Units That I Manage	Edit Organization Unit information for units that list the current user as the Manager in the VIEW ORGANIZATION UNIT page. Also delete any of these Organization Units.

Table A-1. Kintana Access Grants

Category	Access Grant Name	Description
Resource Mgmt	Edit only resources that I manage	Edit Resource information for Resources that list the current user as the Direct Manager. A resource's Direct Manager is displayed on the VIEW RESOURCE page.
Resource Mgmt	Edit Resource Pools	Edit Resource Pool information when the user has been granted edit access in the CONFIGURE ACCESS FOR RESOURCE POOL page. Delete these Resource Pools when given sufficient access in the CONFIGURE ACCESS FOR RESOURCE POOL page for that Resource Pool.
Resource Mgmt	Edit Staffing Profiles	Edit Staffing Profile information when the user has been granted edit access in the CONFIGURE ACCESS FOR STAFFING PROFILE page. Delete these Staffing Profiles when given sufficient access in the CONFIGURE ACCESS FOR STAFFING PROFILE page for that Staffing Profile.
Resource Mgmt	Update Resource Pool Status	Change the RESOURCE POOL STATUS value on the MODIFY RESOURCE POOL page. The user must also have either the EDIT RESOURCE POOLS or EDIT ALL RESOURCE POOLS grant to utilize this grant.
Resource Mgmt	Update Staffing Profile Status	Change the STAFFING PROFILE STATUS value on the MODIFY STAFFING PROFILE page. The user must also have either the EDIT STAFFING PROFILES or EDIT ALL STAFFING PROFILES grant to utilize this grant.
Resource Mgmt	View All Resource Pools	View Resource Pool information for all Resource Pools.
Resource Mgmt	View all resources	View the Resource information page for any Resource defined in Kintana.
Resource Mgmt	View All Skills	View all Skills defined in Kintana.
Resource Mgmt	View All Staffing Profiles	View Staffing Profile information for all Staffing Profiles.
Resource Mgmt	View my personal resource info only	View only the user's own Resource information page.
Resource Mgmt	View Organization	View the Organization Model and Organization Unit detail pages.
Resource Mgmt	View Resource Pools	View Resource Pool information when the user has been granted view access in the CONFIGURE ACCESS FOR RESOURCE POOL page.
Resource Mgmt	View Staffing Profiles	View Staffing Profile information when the user has been granted view access in the CONFIGURE ACCESS FOR STAFFING PROFILE page.

Table A-1. Kintana Access Grants

Category	Access Grant Name	Description
Sys Admin	Edit Dependent References	Create and edit dependency relationships between Kintana entities and their References.
Sys Admin	Edit Security Groups	Create, update and delete Security Groups in the SECURITY GROUPS WORKBENCH.
Sys Admin	Edit Users	Create, update and delete Users in the USERS WORKBENCH.
Sys Admin	Manage Reports	Delete any Report submitted in Kintana using the REPORTS WORKBENCH.
Sys Admin	Migrate Kintana Objects	Migrate Kintana Objects using the Kintana Migrators.
Sys Admin	Override Key Fields Segmentation	View all information contained in restricted key fields. Key fields include: <ul style="list-style-type: none"> • RESOURCE and RESOURCE GROUP fields in Drive Tasks • ASSIGNED USER, ASSIGNED GROUP and CONTACTS fields in Create Requests • ASSIGNED USER and ASSIGNED GROUP fields in Deliver Packages
Sys Admin	Ownership Override	Access and edit all configuration entities even if the user is not a member of one of the entity's Ownership Groups.
Sys Admin	Server Administrator	Stop the Kintana server, logon to the Application when the server is started in Restricted Mode, and send messages via kWall.sh.
Sys Admin	Server Tools: Execute Admin Tools	Execute administration reports in the ADMIN TOOLS window and view the SQL RUNNER window in the SERVER TOOLS WORKBENCH.
Sys Admin	Server Tools: Execute SQL Runner	Execute SQL statements in the SQL RUNNER window and view the ADMIN TOOLS window in the SERVER TOOLS WORKBENCH.
Sys Admin	Synchronize Meta Layer	Perform Reporting Meta Layer synchronizations using the REPORT TYPES WORKBENCH.
Sys Admin	View Security Groups	View Security Group definitions in the SECURITY GROUPS WORKBENCH.
Sys Admin	View Server Tools	View the SQL RUNNER and ADMIN TOOLS screens in the SERVER TOOLS WORKBENCH.
Sys Admin	View Users	View User definitions in the USERS WORKBENCH.
Time Mgmt	Approve Time Sheets	Approve or reject time Sheets when the resource is a direct report or when the Time Sheet has been " DELEGATED TO " the user.

Table A-1. Kintana Access Grants

Category	Access Grant Name	Description
Time Mgmt	Close Time Sheets	Close or freeze Time Sheets when the resource is a direct report or when the Time Sheet has been "DELEGATED TO" the user.
Time Mgmt	Edit Activities	Create, modify and delete Activities in the ACTIVITIES WORKBENCH.
Time Mgmt	Edit Charge Codes	Create, modify and delete Charge Codes in the CHARGE CODES WORKBENCH.
Time Mgmt	Edit Override Rules	Create, modify and delete Override Rules in the OVERRIDE RULES WORKBENCH.
Time Mgmt	Edit Time Mgmt Settings	Edit Time Management settings for a user in the TIME MGMT SETTINGS WORKBENCH. Also enables the TIME MANAGEMENT SETTINGS button in the USER window.
Time Mgmt	Edit Time Sheets	Edit Time Sheets when the resource is a direct report or when the Time Sheet has been "DELEGATED TO" the user.
Time Mgmt	Edit Work Allocations	View and edit Work Allocations. The user can also close or delete allocations he created.
Time Mgmt	Manage Work Allocations	View, edit, delete and close any Work Allocation.
Time Mgmt	View Activities	View Activities in the ACTIVITIES WORKBENCH.
Time Mgmt	View Charge Codes	View Charge Code definitions in the CHARGE CODE WORKBENCH.
Time Mgmt	View Override Rules	View Override Rules in the OVERRIDE RULES WORKBENCH.
Time Mgmt	View Time Mgmt Settings	View Time Management settings for a user in the TIME MGMT SETTINGS WORKBENCH. Also enables the TIME MANAGEMENT SETTINGS button in the USER window.
Time Mgmt	View Time Sheets	View a user's Time Sheet information.
Time Mgmt	View Work Allocations	View Work Allocations in Kintana.

Appendix B

Users and Licensing

The following sections explain the different License types for each Kintana product. Also discussed are the user roles and responsibilities each License is meant to suit, and the functionality they grant.

- [*Power and Standard Licenses*](#)
- [*Kintana Drive Licenses and User Roles*](#)
- [*Kintana Create Licenses and User Roles*](#)
- [*Kintana Deliver Licenses and User Roles*](#)
- [*Kintana Dashboard Licenses and User Roles*](#)
- [*Kintana Solution Licenses*](#)
- [*Kintana Accelerator Licenses*](#)

Power and Standard Licenses

Each user must have a Kintana license to log onto Kintana. Kintana features two License types: Standard and Power. Each License type is meant to suit different business needs and responsibilities, and therefore grants a different set of functionality.

The Power License provides access to all product features through both the Kintana Workbench and the standard Kintana HTML interface, accessible through any Web browser. The Standard License provides access to product features only through Kintana's HTML interface and the Kintana Dashboard.

Power Licenses implicitly provide a user with access to all product features available to a Standard License user, as well as the use of the Kintana Workbench. For example, a user with a Drive Power License does not require

an additional Standard License to perform the tasks associated with Standard Licenses; for example, updating Tasks in the HTML interface.



Note

Kintana users' access to screens and functions in Kintana are controlled by a combination of License and Access Grants. The following sections discuss only the licenses required to perform specific actions. For additional details on Access Grants which are also required, refer to the Access Grant documentation in the "[Kintana Security Model](#)".

Kintana Drive Licenses and User Roles

A Drive Power License provides advanced product features for:

- Project Managers who creates, plans, and monitors Projects.
- Project Managers who create and configure Project Templates.
- Kintana Administrators who configure and administer the Kintana application -- setting up users, assigning security, and configuring Report Types.

A Drive Standard License provides access to routine product features for:

- Project Participants who execute Project Tasks -- updating Tasks as Completed, adding Notes, attaching documents, etc.
- Project Managers who only select and run reports.
- Project Managers who monitor Project status without editing Projects.

The following tables detail the business roles best suited to each Drive License, along with their associated tasks and functionality.

Table B-1. Kintana Drive Power License - Roles and Functionality

Business Role	Tasks Associated with Role	Product Capabilities
Project Managers Project Leads Program Managers	Creating, planning, and monitoring projects. Updating tasks. Assigning resources Setting start and end dates. Setting task dependencies. Running project reports. Configuring Project Templates.	Access to Workbench and HTML interface including Dashboard. Configuring report types and validations. Setting up users and security. Configuring Project Templates. Creating/Updating Projects -- adding/removing Tasks, dependencies, Subprojects. Deleting/Canceling Projects.
Kintana Administrators	Setting up users. Assigning security groups. Configuring report types.	Modifying all standard and custom Project/Task information -- Resource assignments, Effort, Confidence, etc. Adding/removing References including Packages, Requests, other Projects, attachments. Advanced querying. Running, scheduling, and configuring reports. All capabilities listed for Standard license. Create a Budget Create a Staffing Profiles/Resource Pools

Table B-2. Kintana Drive Standard License - Roles and Functionality

Business Role	Tasks Associated with Role	Product Capabilities
Task Owners Project Participants	Updating Tasks as complete. Attaching References. Completing Project-Manager-requested fields for Tasks. Updating Notes. Running reports.	Access to Kintana HTML interface and Dashboard. Querying and viewing existing Projects and Tasks. Adding Notes. Updating Project-Manager-requested fields for Tasks.
Upper-Level Managers Other Stakeholders	Viewing Project status. Running reports.	Adding/Updating/Deleting Action Items. Adding References -- documents, URLs, Requests, other Projects. Running reports.

Kintana Create Licenses and User Roles

A Create Power License provides advanced product features for:

- Users who are assigned Requests and are actively involved in resolving them.
- Users who manage the prioritization, assignment, and resolution of Requests.
- Kintana configuration experts who configure and administer the Kintana application -- setting up users, assigning security, and creating Request Types, Workflow and Report Types.

A Create Standard License provides access to routine product features for a user who

- Requestors who submit, monitor, and sign off on their own Requests.
- Upper-Level Managers who run reports and provide approvals.



Note

An additional access grant (CREATE: ALLOW REQUEST FIELD UPDATES) can be assigned to the user. This access grant allows users to view and update any Request, regardless of whether or not they are its creator or Contact.

The following table details the business roles best suited to each Create License, along with their associated tasks and functionality.

Table B-3. Kintana Create Power License - Roles and Functionality

Business Role	Tasks Associated with Role	Product Capabilities
Analysts Help Desk Staff Managers Project Leaders Project Team	Assigning and prioritizing Requests. Updating Request information. Moving Requests through the workflow. Running reports.	Access to Workbench and HTML interface including Dashboard. Direct updating of Request fields when not creator or contact of Request. Configuring workflows, report types, and validations. Setting up users and security.
Kintana Administrators	Configuring workflows and Request Types. Setting up users. Assigning security groups. Configuring report types.	Configuring Request Types and Request Header Types. Re-opening, deleting, and canceling Requests. Scheduling and acting on eligible "execution" workflow steps. Adding/Removing References including Projects, Requests, and Packages. Running, scheduling, and configuring reports. Advanced querying. All capabilities listed for Standard license. Perform Batch Request Updates

Table B-4. Kintana Create Standard License - Roles and Functionality

Business Role	Tasks Associated with Role	Product Capabilities
Requestors Request Contacts	Submitting Requests. Monitoring the status of their own Requests. Providing user sign-off. ** Monitoring and updating all Requests	Access to HTML interface and Dashboard. Creating new Requests. Searching for existing Requests. Adding Notes and References including documents and URLs. Acting on eligible “decision” workflow steps.
Upper-Level Managers	Running reports. Providing approvals. ** Monitoring and updating all Requests	Updating Request Header and Detail fields through workflow step transactions. Direct updating of Request Header and Detail fields provided user is either Request creator or contact, or is in the “Assigned to” group. Running reports. ** Direct updating of fields in any Request regardless of whether user is Request creator or contact.

Kintana Deliver Licenses and User Roles

A Deliver Power License provides advanced product features for:

- Developers who create Packages for deployment.
- Technical Managers or other staff who are actively involved in managing or executing deployments and releases.
- Kintana configuration experts who configure and administer the Kintana application -- setting up users, assigning security, and creating Object Types, Workflows and Environments.

A Deliver Standard License provides access to routine product features for:

- IT Managers who only need to make deployment approvals.
- QA or Business Analysts who need to make approvals in the deployment process.

The following table details the business roles best suited to each Deliver License, along with their associated tasks and functionality.

Table B-5. Kintana Deliver Power License - Roles and Functionality

Business Role	Tasks Associated with Role	Product Capabilities
Developers	Creating and updating Packages for deployment. Monitoring Package status. Running reports.	Access to Workbench and HTML interface including Dashboard. Configuring workflows, report types, and validations.
DBAs System Administrators Config Managers Technical Project Leads Release Managers	Creating Packages. Updating Package information. Making approvals. Scheduling and executing migrations. Creating and managing deployment releases. Assigning Packages to developers. Configuring Object Types, workflows, and environments. Running reports.	Setting up users and security. Configuring and maintaining environments and Object Types. Creating, updating, deleting, and canceling Packages. Acting on and schedule eligible “execution” workflow steps. Adding/Removing Package References including Projects and Requests. Advanced querying. Scheduling, running, and configuring reports. Refreshing environments.
Kintana Administrators	Configuring Object Types, workflows, and environments. Setting up users. Assigning security groups. Configuring report types.	Creating and managing Releases. Creating and executing Release distributions. All capabilities listed for Standard license.

Table B-6. Kintana Deliver Standard License - Roles and Functionality

Business Role	Tasks Associated with Role	Product Capabilities
IT Managers QA Analysts Business Analysts	Viewing Package status. Making approvals for cases (QA Completed, Stakeholder Analysis Complete, etc.) when modeled in Kintana Deliver workflows. Running reports.	Access to HTML interface and Dashboard. Querying and viewing existing Packages. Adding Notes and Package References including document attachments and URLs. Acting on eligible “decision” workflow steps. Running reports.

Kintana Dashboard Licenses and User Roles

A Kintana Dashboard Power License provides advanced product features for:

- Configuring the Default Kintana Dashboard.
- Setting Portlet access in the Portlet Workbench.
- Creating custom portlets using the Portlet Workbench.
- Kintana Administrators who configure and administer the Kintana application -- setting up users, assigning security, etc.

A Kintana Dashboard Standard License provides access to routine product features for:

- Adding portlets to the Dashboard.
- Personalizing Dashboard pages and Portlets.



Note

The Kintana Dashboard provides convenient visibility into your Kintana data. Other licenses (Kintana Create, Kintana Deliver, Kintana Drive) are required for capturing and processing critical business data. Use the Dashboard licenses in conjunction with other licenses to get the most flexible Kintana experience.

The following table details the business roles best suited to each Kintana Dashboard License, along with their associated tasks and functionality.

Table B-7. Kintana Dashboard Power License - Roles and Functionality

Business Roles	Product Capabilities
Kintana Application Configuration Experts	Access to Workbench and HTML interface. Setting up users and security. Building custom Portlets. Configuring the Default Dashboard. Running, scheduling, and configuring reports. All capabilities listed for Standard license.

Table B-8. Kintana Dashboard Standard License - Roles and Functionality

Business Roles	Product Capabilities
Kintana Standard Users	Access to HTML interface and Dashboard. View Kintana data by adding and personalizing portlets to the Kintana Dashboard.

Kintana Solution Licenses

If you have purchased licenses for a Kintana Solution, you can assign licenses to users. The following sections discuss the licenses available for each Kintana Solution:

- *Demand Management*
- *PMO*
- *Time Management*

Demand Management

The Kintana Solution for Demand Management provides a single application and repository to capture all demand placed on IT. Kintana consolidates information from the many different sources so you can both view aggregate demand in real time and report against it. In addition, Kintana streamlines the end-to-end process (from demand through deployment) of fulfilling demand.

Table B-9. Demand Management Standard License - Roles and Functionality

Business Roles	Product Capabilities
CIO	Viewing Demand captured in Kintana
Demand Manager	Creating / Capturing Demand
Team / Group Manager	Analyzing Demand Scheduling, assigning and rejecting Demand

PMO

The Kintana Program Management Office Solution provides organizations with a single location from which Program Managers can initiate, operate, and manage their portfolio of programs and projects.

Table B-10. PMO Standard License - Roles and Functionality

Business Roles	Product Capabilities
Program Manager	Creating, editing and deleting Business Objectives.
Program Resource	Creating, defining and editing Programs. Submitting and managing Program Issues. Requesting Resources and managing resource requests. Submitting and managing Risks. Submitting and managing Scope Changes.

Time Management

The Kintana Time Management Solution allows you to budget time against bodies of work within the rest of Kintana, enter actual time worked for these bodies of work, and then review, approve, and report on these actuals.

Table B-11. Time Management Standard License - Roles and Functionality

Business Roles	Product Capabilities
Time Sheet Approvers	Creating, editing, deleting, and closing Work Allocations.
Resources Managers	Entering, releasing, reviewing and approving Time Sheets.

Kintana Accelerator Licenses

Kintana Accelerators are provided on a site-license basis (i.e. they do not have to be associated with individual users). Accelerator licenses enable additional

screens and fields in Kintana. See the documentation for the Accelerators installed at your site for details.

Index

A

Accelerator Licenses 124
 Access Grants 8, 10
 list 103
 removing 99
 Additional Resources
 Kintana documentation 2
 Kintana education 6
 Kintana services 5
 Kintana support 6
 Advanced Configuration
 Guides 2
 Application Code Security 11
 Authentication Mode 22

B

Budget Security 85
 Budgets
 creating 90
 modifying 90
 viewing 90

C

Configuration Security 97
 Configuration-Level Restrictions 17
 Configuration-level restrictions 8
 Cost Data
 enabling on a program 88
 enabling on a project 86

 modifying 89
 viewing 86
 Cost Security 85

D

Dashboard
 restricting data to participants 96
 Dashboard Security 93
 Data Security 1
 Documentation 2

E

Entity-Level Restrictions 12
 Entity-level restrictions 8

F

Field-Level Restrictions 16
 Field-level restrictions 8
 Financial Information Security 85

K

Kintana Create
 licenses and user roles 118
 Kintana Dashboard
 licenses and user roles 122
 Kintana Deliver

 licenses and user roles 120
 Kintana Drive
 licenses and user roles 116

L

License
 Accelerators 124
 Kintana Create 118
 Kintana Dashboard 122
 Kintana Deliver 120
 Kintana Drive 116
 Kintana Solutions 123
 License Key 9
 License Overview 115
 Licenses 8
 assigning in batch 35
 assigning in the User window 33
 assigning using the open interface 39
 managing 33
 removing using the wizard 38
 using the wizard 35

O

Organization Model 80
 changing 81
 viewing 80
 Organization Unit 12
 Ownership 97

P

- Package
 - acting on workflow step 63
 - creating 60
 - deleting 63
 - participant restriction 59
 - selecting a specific Object Type 62
 - selecting a specific workflow 61
 - viewing 58
- Package Lines
 - approving 62
- Package Security 57
 - overriding 64
- Participants 14
 - Package 15
 - Project 16
 - Requests 15
- Portlets
 - controlling access 93
 - disabling 93
 - restricting user access 94
- Power License 115
- Project
 - editing 71
- Project Security 67
 - overriding 73
- Projects
 - controlling resources 69
 - creating 71
 - deleting 73
 - viewing 68

R

- Request
 - creating 44
 - participant restrictions 43
 - processing 47
 - viewing 42
- Request Security 41
- Requests
 - acting on workflow step 49
 - deleting 55
 - enabling users to create 44
 - field attributes 51
 - field level security 50, 52
 - overriding security 55
 - selecting a specific Request Type 46
 - selecting a specific workflow 45
 - status dependencies 54
 - updating 47
 - viewing and editing fields 49
- Resource
 - viewing 76
- Resource Management Security 75
- Resource Pools 77
 - creating 78
 - modifying 78
 - viewing 77
- Resources 69, 76
 - modifying 76

S

- Screen Security 11
- Security Groups 10, 19
 - creating 27
 - membership controlled by Resource Management 31
 - specifying list of users 28
- Security Model 1
- Security Model Overview 7
- Security Overview 1
- Skills 79
 - creating 80
 - deleting 80
 - editing 80
 - viewing 80
- Solution Licenses 123
- Staffing Profiles 81
 - creating 82
 - modifying 83
 - viewing 82
- Standard License 115

T

- Task
 - editing 71
- Task Security 67
- Tasks
 - updating 72
 - viewing 68

U

User Roles

- Kintana Create 118

- Kintana Deliver 120

- Kintana Drive 116

Users 19

- creating 19

- importing from a database
or LDAP 27

- linking to security groups
24

- resource information 26

W

Workflow Security 11

Workflow Step Security 11