KINTANA™

Installation Guide

Version 5.0

Installation Guide

Version 5.0

Kintana, Version 5.0

Kintana, Inc.
1314 Chesapeake Terrace, Sunnyvale, California 94089
Telephone: (408) 543-4400
Fax: (408) 752-8460
http://www.kintana.com

Contents

Chapter 1 Introduction

This document describes the requirements and procedures for installing and configuring the Kintana product suite.

A typical installation is guided by a Kintana Product Consultant. For any questions concerning the role of the Product Consultant during or following installation, go to the Kintana website at http://www.kintana.com.

Product Components

Besides the Kintana program software, there are several other necessary system components that must also be prepared in order to use the Kintana product suite. This section discusses what is required for a complete Kintana suite installation for the following:

- *Clients*
- *Server*
- *Database Objects*

All installed files will reside on a single server computer. Each Kintana client must have a supported Web browser installed. No additional application installation is required.

Windows NT/2000 computers that are sources or destinations for migration with the Kintana suite will require additional configuration, see *"Installing Kintana NetPack for Windows NT/2000"* on page 31.

Clients

All clients who are going to access the Kintana suite must have one of the following Web browsers installed:

- Netscape Communicator version 7.02 or higher
- Internet Explorer 5.0 or higher

Users who will be accessing the Kintana Workbench (Kintana's interface for configuration, administration, and advanced processing activities) require 30 MB of disk space in addition to normal browser install requirements. This space is used to store client side java files. To access the Kintana Workbench, the user must have the Java Plug In installed on their machine. This is automatically installed the first time the user accesses the Workbench. Java Plug In version 1.4.1_02 is required.

Refer to the "Kintana Compatibility Matrix," available on the Kintana Download Center, for a complete list of supported browsers.

Server

A full installation of the Kintana server requires a minimum of 425 MB of disk space on the server. The installation requires an additional 200MB of temporary space to extract the installation files.

Sites running Kintana servers vary widely in scope and complexity. Simply basing hardware sizing on the number of transactions entered into the system may not be sufficient. The amount of load on the server can vary depending on the complexity of system usage. Refer to *"Kintana System Administration Guide"* for additional information regarding server and database requirements.

The following filesystem objects are required:

- Version 1.3.1 or higher of the Java Developer's Kit (JDK). The JDK contains the Java Virtual Machine (JVM), which is the engine that runs the Kintana application server. The Kintana product suite requires a JDK of at least 1.3.1 to run correctly.

The Java Runtime Environment (JRE) is NOT supported by Kintana at this time. Refer to the "Kintana Compatibility Matrix," available on the Kintana Download Center, for the latest supported JVM versions.

- The Kintana program files.
- The Kintana product suite needs the System password (or a database user with system-level privileges) to the database instance where Kintana is installed. The Kintana product suite needs access to certain high level views, and the proper grants must be given to the KINTANA schema.
- **Windows NT only**: Kintana NetPack. The NetPack includes the Ataman Telnet server and a UNIX Bourne-again shell (BASH) emulator. This is necessary to run the server configuration scripts. (By default, this is automatically installed when installing the Kintana program files).

Preferred Platforms

The Kintana server may be installed on any UNIX or Windows machine with at least a supported 1.3.1 version of the Java Developer's Kit. Note that the Java Runtime Environment (JRE) is NOT supported. However, certain vendors have more robust implementations of the JDK, which result in improved performance for the Kintana server. The "preferred" platforms are:

1. Solaris 2.6 or higher
2. IBM AIX 4.3.x or higher
3. Windows 2000 Server
4. Windows NT 4.0 on Intel x86 architecture, with Service Pack 3 or later
5. HP UX 11 and 11i or higher

Windows 2000 Datacenter Server is NOT supported by Kintana at this time.

Web Server

The Kintana server ships with an embedded Web server. Integration with a stand alone web server is only required if you wish to run Kintana in cluster configuration or run the web server on a port less than 1024. External Web

servers supported are Apache, Microsoft IIS, and Netscape iPlanet on the supported Server platforms.

*SQL*Net*

The computer that hosts the Kintana server must also have SQL*Net v2 installed to communicate with the Kintana schema. SQL*Net must be configured to recognize the connection string of the Oracle database that contains the Kintana schema.

Email Server

Kintana can send email notifications to individuals, identifying pending actions or notifying users of status changes for various Packages, Requests, or Tasks. The Kintana product suite can integrate with any SMTP-compliant mail server, including Microsoft Exchange, UNIX sendmail, and others. The only required information is the IP address of the email server and the logon name of one or more valid users on the email server. The Kintana server uses these logon names as the "From" address for its notifications.

Database Objects

A set of tables and other database objects is maintained by Kintana in an Oracle database to store and process configuration and transaction data. Installation of these objects requires a schema on an Oracle 8.0.5 or higher database running SQL*Net v2. For more detailed information on compatible Oracle versions, consult the Kintana Compatibility Matrix, available on the Kintana Download Center.

The amount of tablespace required depends on the volume of Requests and Packages, and on the complexity of the anticipated Workflows. The following are required for a small installation:

- 200 MB of data space
- 100 MB of index space
- 200 MB for CLOB table space

Database requirements depend highly on the number of users, types of processes implemented, and type of activity performed. Please contact Kintana Support for details on how to size an installation.

Database Administration Tips

To ensure maximum performance and organization of a Kintana system, certain configurations need to be checked regarding the setup of the database on which the Kintana schema will be installed. The following list outlines the optimum Oracle database configuration. Please consult Oracle database administration documentation for more details. Refer to the *"Kintana System Administration Guide"* for a complete list of Kintana database and server configuration parameters.

If you are installing Kintana's Accelerator for Oracle Applications, refer to the Oracle Applications Accelerator configuration guide for an alternate set of database administration tips and requirements.

1. Generate three separate tablespaces:

   - Kintana data (at least 200 MB of space)
   - Kintana indexes (at least 100 MB of space)
   - CLOB (at least 200 MB of space)

   Be sure to specify the correct tablespaces when installing the Kintana schema.

2. Generate at least one rollback segment for each of the new tablespaces mentioned above. These rollback segments should reside in a separate tablespace reserved for rollback segments. They should be generated with OPTIMAL size constraint to ensure that the rollback segments automatically deallocate space as it becomes free.

3. Generate an additional tablespace to be used as the temporary tablespace for the Kintana user. Be sure to specify this tablespace during the Kintana schema installation.

4. Unlimited quota on the data, index, and temporary tablespaces generated for the Kintana suite.

   - The following grants are also necessary:

     ```
     grant connect to &username;
     grant create session to &username;
     ```

```
grant create database link to &username;
grant create procedure to &username;
grant create sequence to &username;
```

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.

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

Installation and Configuration

This chapter describes the procedures for downloading, installing and configuring the Kintana Product Suite. The following topics are discussed:

A typical installation is guided by a Kintana Product Consultant. For any questions concerning the role of the Product Consultant during or following installation, contact Kintana.

The procedures in this chapter are required for proper installation and configuration. See *"Optional Configuration"* on page 53 for more information about available optional configurations for the system.

Downloading the Installation Package

The Kintana installation files are distributed from the Kintana Website (http://www.kintana.com/support/download/download_center.htm). A username and password is required for accessing Kintana software downloads.

Once you are logged into the Download Center, you will be provided with links to all the software you have purchased.

1. Kintana installation archive files are found in the Software Installs section of the Download Center. Use the file appropriate for the server operating system.

   UNIX: knta500en.tar

   Windows NT/2000: knta500en.zip

2. **Windows NT/2000 only**: If migrations between Windows NT/2000 computers are to be performed, it is necessary to download the Kintana NetPack. These tools can be found on the Download Center, from the Server Tools section. The NetPack installs the Ataman Telnet server on Windows Server and also a UNIX Bourne-again shell (BASH) emulator.

   knetpack20.exe

   Installation and configuration of the NetPack is discussed in *"Installing Kintana NetPack for Windows NT/2000"* on page 31. Download the appropriate installation file at this time and store it in a temporary area until the instructions in that section have been completed.

3. **Accelerators**: If one or more of the Kintana Accelerators are being installed, download the Accelerator installation archive from the Kintana Website for each Accelerator purchased.

   - Accelerators are available in the Software Installs section of the Download Center.

   - Download the installation archive for each Accelerator to be installed. For example, if the Oracle Applications Accelerator has been purchased, download the file oraapps_accel_v500.jar. There may be additional files to download depending on which Accelerators are installed.

     Please read the instructions on the Web page, and refer to the Accelerator-specific installation guides (also provided on the "Accelerators" Web page) for more details.

4. **Solutions**: If one or more of the Kintana Solutions are being installed, download the Solution installation archive from the Kintana Website for each Solution purchased.

   - Kintana Solutions are available in the Software Installs section of the Download Center.

- Download the installation archive for each Solution to be installed. For example, if the Demand Management Solution has been purchased, download the file kintana-500-DEM.jar.

  Please read the instructions on the Web page, and refer to the Solution-specific installation guides.

Once the installation files for the server's operating system have been obtained, follow the instructions in *"Application Installation"* on page 13 and *"Server Configuration"* on page 26 to install and configure the Kintana application server and database schema.

Application Installation

The installation archive described in the previous section contains all files and scripts necessary to generate the Kintana application server and database schema. Performing the Kintana installation will:

- Install the Kintana Server files
- Create and configure all database objects used by the server to store data.
- Configure the Kintana server (optionally)
- Generate security keys for password encryption within the Kintana server.

Kintana cannot be installed into a directory path whose name contains a space.

The process for installing Kintana is described below. Some of the installation steps depend on the platform onto which you are installing (Unix or Windows). Refer to the sections corresponding to your platform to obtain detailed instructions for that step. The installation steps must be performed in the order specified below.

1. *Installation Research and Considerations*
2. *Creating a Kintana User*
3. *Installing the Java Virtual Machine*
4. *Creating the Kintana Schemas Before Installing*

5. *Installing the Kintana Server*
6. *Generate the Database Links*
7. *Additional Database Configuration*

Installation Research and Considerations

Before proceeding with the Kintana installation, you need to gather certain system information and make a few other Kintana installation related decisions. These items are discussed in the following sections:

- *Options for Installing the Application Server*
- *Information Required for the Kintana Installation*

Options for Installing the Application Server

When installing the Kintana application server, the installation archive is unpacked, the Kintana server filesystem is generated, database schemas are created, and (on Windows only) the Windows service that runs the Kintana server as a background process is generated. You have options on how to perform certain tasks related to the Kintana installation. Refer to the below sections for a discussion of a few key installation options.

- *Use the Graphical or Console Installation? (Unix only)*
- *Automatically Create the Database Schema?*
- *Configure the Server During or After the Installation?*

Use the Graphical or Console Installation? (Unix only)

On Unix platforms, Kintana installations can be run in either graphical or console mode. When determining the mode in which to run the installation, there are several factors to consider.

- The graphical install is more user friendly. It allows you to go back and change parameters before starting the installation.
- In some cases, Console installations may be the only option. If you choose to install graphically and are accessing the target machine *remotely*, you may need additional software/configuration (for example, if you are accessing a Unix system from a Windows system you will need software that will allow the Unix application to redirect the display to Windows).

Automatically Create the Database Schema?

The Kintana server requires two distinct database schemas to store application data. A DBA may create these schemas prior to installation, or the installer will create them. If you would like to create the schemas prior to the installation, follow the instructions in *"Creating the Kintana Schemas Before Installing"* on page 21. The installation will then populate the schemas with the database objects and data required to run the server.

Configure the Server During or After the Installation?

The Kintana server requires configuration before it can be started. This can be done during the installation. If you choose to configure during the installation, you will be asked to input the values of the variables in *"Server Configuration"* on page 26. If you choose not to configure the server during installation, any information gathered will be inserted into the server configuration file, and complete configuration can be performed as a post-installation step. This is useful if you don't have all configuration information available at the time of installation.

Information Required for the Kintana Installation

The base Kintana installation will ask for several parameters to create and configure the Kintana server. All information must be entered, and will be validated before the installation can continue.

Table 2-1. Required Installation Information

Prompt	Description
License Configuration File	The Kintana server is activated by license keys. The license keys are provided in a license.conf file, which needs to be obtained before installation. Contact Kintana Support if you do not have a valid license.conf file.
JAVA_HOME	The directory in which Java is installed.
Install Location	The directory in which the Kintana server will be installed and configured. If the directory does not exist it will be created. The directory path can not contain a space.
ORACLE_HOME	The directory in which the Oracle client tools are installed. The directory path can not contain a space.

Table 2-1. Required Installation Information

Prompt	Description
SQL*PLUS	The location of the SQL*PLUS utility. SQL*PLUS is not needed for the installation, but it required by the Kintana Server.
Database Access Information	In addition to installing the Kintana filesystem, the installation will create and populate database schemas needed to store application data. In order to access the database, the installation will ask for a username and password, and the valid components of a JDBC URL. If you choose to have the installation create the schemas, you will need to enter the system username and password. If you have chosen to create the schemas before installation, you must enter the Kintana schema username and password. The JDBC URL is used by the Kintana server to connect to the Oracle database. It is of the form: jdbc:oracle:thin:@<Hostname>:<Port>:<SID> You will be asked to the Hostname, Port, and SID of the database.
Kintana Schema	The username and password of the Kintana schema.
Reporting Meta-Layer Schema	The username and password of the Kintana Reporting Meta-Layer schema.
Tablespaces	The table, index, CLOB and temporary tablespaces of the Oracle database that should be used in the creation of schemas and database objects.
Windows Service Name	The name of the service for the Kintana server (*Windows only*). The installation will preface the service name with 'Kintana' to better identify the service. The service name is also used to create the Kintana Start Menu item.

Note

The JDBC URL is used by the Kintana server to locate its database schema. The value should be in the format: “jdbc:<subprotocol>:<subname>:<DB address>”

- <subprotocol> is “oracle”
- <subname> is “thin”
- <DB address> is in the format: “@<hostname>:<port>:<database SID>”. This is the address of the database on which the Kintana schema resides.
  i. <hostname> is the DNS name or IP address of the computer running the database.
  ii. <port> is the port used by SQL*Net to connect to this database. Its value is generally 1521, but the actual value can be obtained by looking at the corresponding entry in “tnsnames.ora”.
  iii. <database SID> is the SID of the database. This is usually identical to the database connect string. If it is different, an extra parameter is necessary. See the special instructions in *“Special Considerations”* on page 28.

Creating a Kintana User

The process for creating a Kintana user is different depending on which platform your Kintana Server is using (Unix or Windows). Refer the below section corresponding to your platform to obtain detailed instructions.

- *Creating a Kintana User for Windows*
- *Creating a Kintana User for Unix*

Creating a Kintana User for Windows

It is highly recommended that a new Windows user (‘kintana’, for example) is generated for the installation and all subsequent Kintana server maintenance. This user should be configured to be a member of at least the “Administrators” and “Domain Users” groups. Always logon to the Windows Server as

"kintana" when performing any Kintana server maintenance, such as stopping or restarting the Kintana server. This helps avoid filesystem permission issues, which can be difficult to track.

This user should have full access to the installation directory for Kintana and all of its subdirectories. The Administrators group must have at least read-only access to these directories.

Creating a Kintana User for Unix

The Kintana Product Suite may be installed under an existing UNIX account, or a custom account generated specifically for it, depending upon site preference. However, it is recommended that a custom account ("kintana", for example) is generated for installing and administering the Kintana Product Suite. Always logon to the UNIX server as "kintana" when performing any Kintana server maintenance, such as stopping or restarting the Kintana server. This helps avoid filesystem permission issues, which can sometimes be difficult to track.

Kintana does not require root access to be installed. You should not install the server as the root user.

Installing the Java Virtual Machine

Since the Kintana application server is Java-based, the server machine that hosts the Kintana application server must also host a JVM. JVMs native to each operating system are available either from Sun Microsystems or the operating system vendor, usually in the form of a Java Development Kit (JDK). Kintana application servers support multiple versions of JVM based on the operating system running on the server machine. For a list of supported JVMs, refer to the "Kintana Compatibility Matrix" document (available on the Kintana Download Center).

The process for installing the Java Virtual Machine (JVM) is different depending on which platform (Unix or Windows) your Kintana Server is being installed. Refer the below section corresponding to your platform to obtain the correct instructions.

- *Installing the JVM on Windows*

- *Installing the JVM on Unix*

Installing the JVM on Windows

The Kintana Server requires a Java Virtual Machine (JVM). The JVM is contained within the Java Developer's Kit (JDK). Kintana supports both versions 1.3.1 and 1.4.1 of the JDK. If the appropriate version of the JDK has not been installed on your computer, complete the following instructions. Otherwise, skip to *"Installing the Kintana Server on Windows"* on page 22.

1. Download the appropriate JDK for the operating system from the Javasoft Website.

   ```
   http://java.sun.com
   ```

2. Install the JDK according to the instructions provided. Hereafter, the directory where it is installed will be referred to as <JVM_Install_Dir>.

The JDK cannot be installed into a directory path whose name contains a space.

3. After the installation of the JVM, verify that the user that the Kintana Product Suite will be run under has the "java" executable in its path. The easiest method to verify this is to logon and run the command:

   ```
   java -version
   ```

   This should output text that tells you the version of java. If an error message is received, modify the PATH environment variable as appropriate.

4. Ensure that the JAVA_HOME environment variable has been set correctly. To check this run the following command:

   ```
   echo %JAVA_HOME%
   ```

   If this doesn't echo the correct path to Java, set it to the correct value.

To set the value of JAVA_HOME in DOS, use:

```
set JAVA_HOME="<JVM_Install_Dir>"
```

Installing the JVM on Unix

The Kintana server requires a Java Virtual Machine (JVM). The JVM is contained within the Java Developer's Kit (JDK). For the Solaris operating system we recommend using version 1.31. For more information about which versions of the JDK are supported by Kintana for other Unix operating systems, see the "Kintana Compatibility Matrix" document (located on the Kintana Download Center). If the appropriate JDK has not been installed on your computer, complete the following instructions. Otherwise, skip to *"Installing the Kintana Server on Unix"* on page 23.

1. Download the appropriate JDK for the operating system. The appropriate JVM for the operating system should be publicly available on the server vendor's Web site.

2. Install the JVM according to the vendor's instructions. In some cases, a particular vendor provides custom installation packages that can be automatically installed with a command such as **`pkgadd`**. Other vendors provide a simple tar file that should be extracted. The directory where the JVM (regardless of the mechanism) is installed will be referred to as <JVM_Install_Dir>.

Many operating systems require that OS-specific patches be applied before the JVM is installed. Carefully follow all instructions provided by the server vendor while installing the JVM.

3. After the installation of the JVM, verify to the user that Kintana will be run under the "java" executable in its path. The easiest method to verify this is to logon and run the command:

   ```
   java -version
   ```

   This should output text such as "java version 1.3.1." If an error message is received, modify the PATH environment variable as appropriate

4. Ensure that the JAVA_HOME environment variable has been set correctly. To check this run the command:

   ```
   echo $JAVA_HOME
   ```

   If this doesn't echo the correct path to Java, set it to the correct value.

To set the value of JAVA_HOME:

In Bourne shell (SH, BASH, or KSH), use:

```
JAVA_HOME="<JVM_Install_Dir>"
export JAVA_HOME
```

In CSH, use:

```
setenv JAVA_HOME "<JVM_Install_Dir>"
```

Creating the Kintana Schemas Before Installing

The Kintana server requires two distinct database schemas to store application data. A DBA may create these schemas prior to the Kintana installation. Creating database schemas require privileges that a DBA might not want to grant to a Kintana administrator. To properly create the schemas and the permissions between them:

1. Unpack the Kintana installation bundle as outlined in *"Installing the Kintana Server"* on page 22. A directory named 'system' will be created. This directory contains the scripts that should be used to create the database schemas.

2. Run the script 'CreateKintanaUser.sql' against the database into which you are installing Kintana. The script will ask for a username and password, and the tablespaces that should be used by the Kintana schema.

```
sh> sqlplus system/<password>@<SID> \
    @CreateKintanaUser.sql \
     <username> \
     <password> \
     <data tablespace> \
     <index tablespace> \
     <temporary tablespace> \
     <CLOB tablespace>
```

3. Run the script CreateRMLUser.sql. The script will ask for a user name and password for the Reporting Meta-Layer schema, tablespace information, and the Kintana schema user name. The script will create the RML schema and establish the permissions between the RML and the Kintana schema.

```
sh> sqlplus system/<password>@<SID> \
     @CreateRMLUser.sql \
      <RML username> \
      <RML password> \
      <data tablespace> \
      <index tablespace> \
      <temporary tablespace> \
      <Kintana username>
```

If you choose to create the schemas prior to installation, you must specify 'Please use existing schemas' when prompted by the installation.

Installing the Kintana Server

The Kintana Application Server has been designed to connect to an Oracle 8.0.5 (or higher) database. The following steps are required to install the database objects and data used by the server. The steps in this section can be performed on any UNIX or Windows NT/2000 computer with SQL*Net connectivity to the database on which the Kintana database objects are to be installed.

The process for installing the Kintana server is different depending on which platform you are using (Unix or Windows). Refer the below section corresponding to your platform to obtain the correct instructions.

- *Installing the Kintana Server on Windows*
- *Installing the Kintana Server on Unix*

If the Kintana suite is to be used in conjunction with Object*Migrator or GL*Migrator, Kintana database objects must be installed on the same database as Object*Migrator and/or GL*Migrator. Furthermore, Kintana recommend that the existing Object*Migrator/GL*Migrator schema be used to house the Kintana database objects as well. This configuration simplifies some aspects of the integration between the Kintana suite and Object*Migrator/GL*Migrator.

Installing the Kintana Server on Windows

The installation utility for a Windows NT/2000 Server is an executable file that performs the steps required for a basic server installation. The executable and supporting files are contained in a zip file. The typical installation will automatically install the following components onto the server:

- Kintana Program Files
- Kintana Database Objects
- Start Menu item
- Windows service

To start the installation, extract all files from knta500en.zip anywhere on your file system. Locate the executable file knta500en.exe that was extracted and double-click it. You will be prompted for information as the installation proceeds (see *"Information Required for the Kintana Installation"* on page 15).

Once all information has been entered, the installation will install the Kintana files and configure the database. Status bars will keep you informed of the status of the installation. A summary of the installation will be displayed, alerting the user to any problems that were encountered.

Once the installation is complete, the Kintana suite is installed as a Windows service. The properties for this service may be viewed through the Services Control Panel item.

To complete the service setup, select the Kintana service in the Services Control Panel and click **Startup**. It is recommended that the startup type is set to **Automatic** so that the Kintana server restarts automatically when the computer is rebooted. Also, if a custom Kintana user is generated as recommended, set the 'Log On As' parameter to this username. Click **Save** to save the settings.

A Start menu item corresponding to the Windows service name entered during the installation will also be created. The menu provides links to Kintana documentation and an uninstall program.

If you chose not to configure the Kintana server during installation, please see *"Server Configuration"* on page 26.

Do not map the <KINTANA_HOME> directory to be accessible from an external Web server. This introduces a potential security risk. Using the Kintana Web server is recommended.

Installing the Kintana Server on Unix

To install Kintana on a Unix system, you must first extract the files into an empty directory from the download bundle by running:

```
tar xvf knta500en.tar
```

All the files and scripts necessary to install Kintana will be extracted. Where you choose to extract the files is inconsequential, as the installation will ask you where the software should be installed. After extracting the files, there should be a knta_install.sh shell script and several Jar files, and a system directory. Start the installation by running the installation script,

```
sh knta_install.sh [-awt|-console]
```

specifying the installation mode.

Table 2-2. Unix Installation Modes

Mode	Meaning
-awt	GUI mode. A window will appear which walks the user through the installation.
-console	Command line mode. The installation script will be run within the terminal session.

The script performs the following actions:

- Prompts the user for information required for installing the server. See *"Information Required for the Kintana Installation"* on page 15 for more information.
- Generates all database tables in the tablespace specified.
- If Oracle Applications is being used and plans exist to integrate with the Object*Migrator or GL*Migrator, the install script grants the Kintana schema access to some Oracle Applications database objects as needed.
- Creates all database objects (indexes, packages, views) and application data.
- Generates password security keys.
- Generates the server configuration file.

To improve the performance of your Kintana instance, the installation will rebuild statistics for the cost-based optimizer for versions 8.1.6 and higher. In order to do this, the following privileges must be granted to the Kintana schema as SYS (or on 9i, SYSTEM as sysdba).

```
grant select on v_$parameter to <KINTANA_SCHEMA>
```

```
grant execute on dbms_stats to <KINTANA_SCHEMA>
```

The installation will not finish until the privileges have been granted.

Generate the Database Links

If the Kintana suite is to be run with the Kintana Accelerator for Oracle Applications and the Object*Migrator or GL*Migrator, there may be an additional consideration to take prior to completing the database portion of the installation. If it has been decided to generate a new schema for the Kintana suite other than the schema in which Object*Migrator/GL*Migrator resides, then database links must be generated from the Kintana schema to all valid source and destination databases. This database link should connect to each apps Oracle schema that is part of a standard Oracle Applications installation.

The process for generating the database links is the same for both Unix and Windows.

It is not necessary to generate database links if the Kintana suite is installed into the existing Object*Migrator/GL*Migrator schema. In this case, the existing links generated during Object*Migrator/GL*Migrator installation can also be used by the Kintana suite.

From the Kintana schema, issue:

```
SQL> create database link DEV_LINK
SQL> connect to APPS identified by APPS
SQL> using 'DEV'
```

Repeat this for all databases that the Kintana suite is to access. A database link is required even for the database on which the Kintana schema resides to migrate Oracle Applications Objects to or from this database.

If all steps have been completed successfully, the database portion of the Kintana suite installation is complete.

Refer to the Kintana Accelerator for Oracle Applications installation doc for additional details.

Additional Database Configuration

For the Kintana suite to be able to keep track of the open database sessions it is using, ensure that a public grant exists on the V_$SESSION Dynamic Performance Table. To do this, connect as SYS to the database containing the Kintana schema and execute:

```
SQL> grant select on v_$session to public;
```

Server Configuration

The next step in installing the Kintana Product Suite is configuring the server to meet local network requirements. If you chose to configure the server during installation, you do not need to perform these steps.

Like the installation, the tool for configuring the Kintana server runs in both a graphical and console mode. As such, it has the same system configuration limitations and the installation, and requires an X-Windows session when running graphically.

This script reads the value of the JAVA_HOME environment variable to determine how to call “java”. To check if JAVA_HOME is set on a system, run:

In a UNIX shell (SH, BASH, KSH, CSH), use:

```
echo $JAVA_HOME
```

In DOS, use:

```
echo %JAVA_HOME%
```

If this doesn’t echo the correct path to Java, set it to the correct value.

To set the value of JAVA_HOME:

In Bourne shell (SH, BASH, or KSH), use:

```
JAVA_HOME="<JVM_Install_Dir>"
export JAVA_HOME
```

In CSH, use:

```
setenv JAVA_HOME "<JVM_Install_Dir>"
```

In DOS, use:

```
set JAVA_HOME="<JVM_Install_Dir>"
```

Standard Configuration Process

This section outlines the standard configuration process and describes all of the required settings for a typical installation. To configure the Kintana Server:

1. From the <KINTANA_HOME>/bin directory, execute kConfig.sh from a UNIX or DOS command line by running:

   ```
   sh kConfig.sh
   ```

You can also run the configuration tool in console mode. To do this, run the following from a UNIX or DOS command line:

```
sh kConfig.sh -console
```

2. The configuration wizard will walk you through the configuration of the Kintana server. Enter a value for each parameter as appropriate to the site. Use the Help button on the bottom of the screen for detailed descriptions of the configuration parameters. Some are defaulted and should not be changed except in special circumstances. Others are simply defaulted with typical values but may be overridden if desired.

   The parameters to be entered are shown in *Table 5-2 on page 51*, along with an example of each. All confidential information, such as passwords, remains hidden and is encrypted before it is stored.

Use forward slashes (/), NOT backslashes (\) for ALL file path separators, regardless of the operating system. The Kintana suite automatically uses the appropriate path separators when communicating with Windows, but expects to read only forward slashes from the configuration file.

3. The last section in the server configuration utility is "Custom Parameters." This is where necessary additional parameters are entered to account for non-standard configurations. Normally this folder is left blank.

4. After all parameter values have been entered, click **OK** or **Enter** (depending on the mode) to apply the configuration.

5. The configuration tool does a few additional things at this point:

   a. Writes the configuration parameters specified in the file named server.conf, which are read by the Kintana Server.

   b. Generates the files used to access the Kintana product (Workbench and Kintana interfaces). Also generates the access point for the customer's local Kintana Website, local_website.html.

   c. Generates other files needed internally by the Kintana server, such as resin.conf.

Special Considerations

In some special cases it may be necessary to add additional parameters to the server configuration. This can be done in the "Custom Parameters" section of the server configuration utility. To add a new parameter, type the parameter name in the "Parameter" field, its value in the "Value" field, and click **Add**. The parameter names must be preceeded by the prefix "com.kintana.core.server." For example, if a custom parameter named "NEW_PARAMETER" is being added, "com.kintana.core.server.NEW_PARAMETER" should be entered in the "Key" field.

Any parameters that are added to the "Custom Parameters" list are accessible from within the application as tokens of the form '[AS.<parameter name>].' (See the "Tokens" chapter in the System Administrator Guide for more information.)

In addition to any custom parameters that are added for specific configuration purposes, there are some standard parameters that may be needed in special situations. These are documented in *Table 2-3*. Normally these parameters are

defaulted correctly, but the defaults can be overridden by explicitly adding them to the “Custom Parameters” folder.

Table 2-3. Special Configuration Parameters and Examples

Parameter	Description	Sample Value
com.kintana.core.server.DB_CONNECTION_STRING	When specifying the JDBC_URL parameter, the SID of the database on which the Kintana schema resides is requested. It is assumed that the connection string for this database is the same as the SID. However, this is not always the case. If the connect string (for connecting to the database via SQL*Plus from the Kintana server computer) is different than the database SID, please add this parameter and supply the correct connect string.	PROD
com.kintana.core.server.NON_DOMAIN_FTP_SERVICES	**Windows NT only!** FTP servers on Windows NT typically require the entry of the NT domain along with the username (in the form “Domain\Username”) when opening an FTP session. By default, Kintana includes the domain name when entering the username in an FTP session to a Windows NT computer. If an FTP server that does not require the domain name is used, this parameter can be used to override the default functionality. Contact Kintana support (support@kintana.com) for more information.	WAR-FTPD
com.kintana.core.server.TEMP_DIR	General Kintana temp directory. This currently defaults to a /temp/ subdirectory of the /logs/ directory, but might be moved due to system constraints. Include the full path when using this parameter.	

Generating Password Security

To ensure password security, the Kintana products utilize a client/server encryption model utilizing the ElGamal Algorithym that generates a public/private key pair. All client/server encryption is done using the server’s public key and only the server is able to decrypt the data using the private key. This means that the client application does not have access to decrypted data.

Generating the Private and Public keys

Public and private keys are generated during the installation of Kintana, residing in `KINTANA_HOME/security`. All passwords are encrypted using these keys. The key pair only needs to be generated once. If you feel that the security of your server has been breached, follow the steps below to regenerate the key pair and regenerate the key pair and re-encrypt all passwords.

To create the private and public key pair, the kKeygen.sh script (located in <KINTANA_HOME>/bin directory) must be run. This script generates the new key pair which is used to encrypt passwords during server configuration. Any new passwords generated later are also encrypted using this key pair.

- From the <KINTANA_HOME>/bin directory, execute kKeygen.sh from a UNIX or DOS prompt by running:

```
sh kKeygen.sh
```

This script prompts for the following information (if server.conf does not exist):

a. The JDBC_URL (e.g. jdbc:oracle:thin:@DBhost.domain.com:1521:SID) is needed for the server to communicate to the database

b. The username for the Kintana database schema.

c. The password for the Kintana database schema.

On completion of the script, the two keys are placed in the <KINTANA_HOME>/security directory. These files are public_key.txt and private_key.txt.

On UNIX, the kKeygen.sh script sets the files to be read-only permission for the user running the script. If this user differs from the user starting the server, the server may not be able to read the keys and will be unable to start.

After the script has been run on Windows, the files remain readable by anyone. It is up to the System Administrator to make sure non-trusted users do not have read privilege to those files.

Additional Configuration & System Considerations for Windows

If configured correctly, the Kintana Product Suite will be able to execute commands on remote computers as well as move files. While the UNIX operating system was designed with this in mind, Windows needs additional components. Two of these components are provided in the Kintana NetPack (namely a Telnet server and a UNIX shell emulator). Others (such as an FTP server) are standard components of Windows that must be installed.

Installing Kintana NetPack for Windows NT/2000

The Kintana NetPack installs Ataman TCP Remote Logon Services (Telnet) and the UNIX Bourne-again shell (BASH) command processor. If the Kintana suite will be accessing Windows NT/2000 computers in the network for command execution, the Kintana NetPack must be installed on each of those computers.

If the Ataman Telnet server is to be installed on a server running Microsoft's IIS Web Server, then NT's \Winnt\System32\Telnet.exe must be disabled.

For each Windows NT/2000 computer that the Kintana suite accesses, perform the following steps:

- *Creating a Kintana User*
- *Running the Installer*
- *Configuring Ataman TCP Remote Logon Services*

Creating a Kintana User

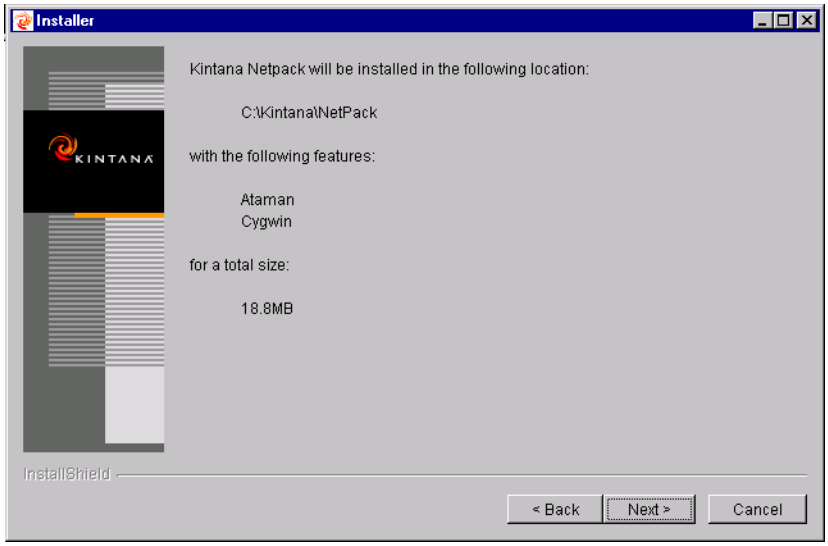
For the Kintana suite to execute commands on a remote computer, it must logon to that computer with a valid username and password. Any existing user will function, but Kintana recommends that a new user is created specifically for this purpose on each remote computer that the Kintana suite will access. For the remainder of this discussion it is assumed that a user named "Kintana" has been generated and given user full user privileges to its Home directory (i.e. 'D:\Users\Kintana').

Note

Ensure the Administrators group has read access (at least) to Kintana's Home directory. If not, Telnet will not allow kintana to access its Home directory, even though it has read and write permissions in that directory.

Running the Installer

The Kintana NetPack uses the familiar InstallShield software to install Telnet and BASH. The installation is a simple two-step process. The install screen is shown below.



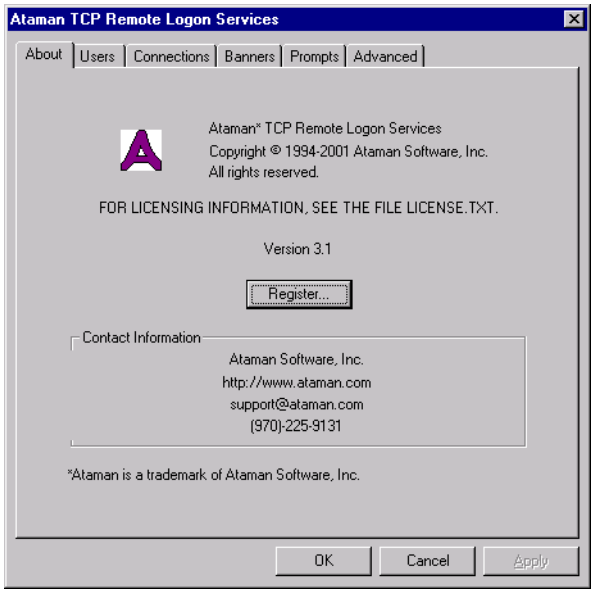
1. Copy the file knetpack20.exe to the Windows NT/2000 computer on which the Kintana NetPack is to be installed.

2. Execute knetpack20.exe and follow the instructions provided as the installation proceeds.

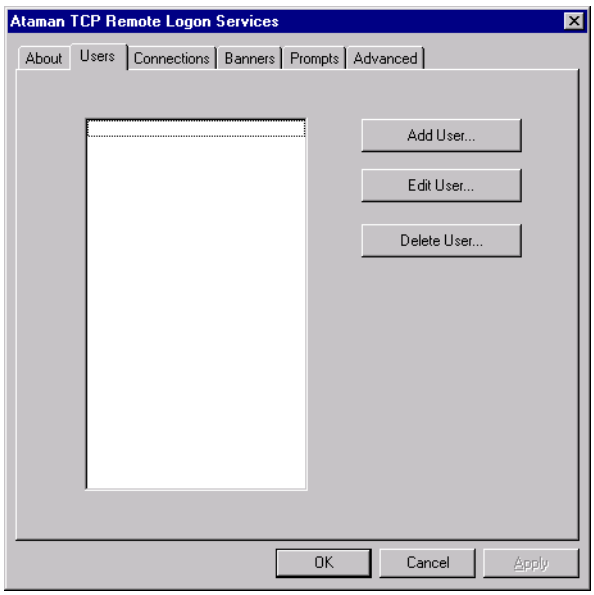
Configuring Ataman TCP Remote Logon Services

Once installed, Telnet must be configured to work correctly with the Kintana Product Suite. This is done through a new "Ataman TCP R. L. Services" Control Panel (which is generated during NetPack install) as follows:

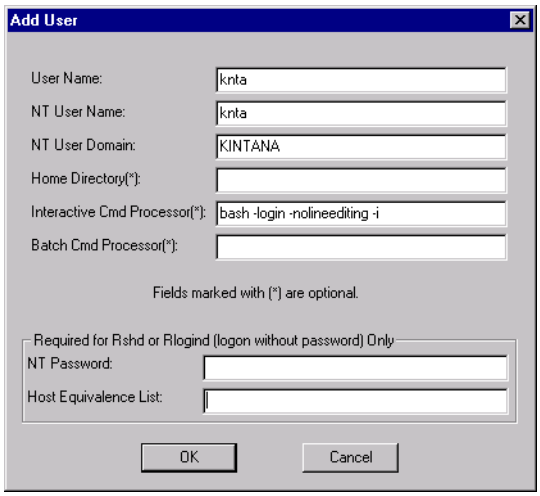
1. Logon to the Windows NT/2000 computer as Administrator. Open **Settings -> Control Panel -> Ataman TCP R. L. Services**. This opens the Ataman Control Panel:



2. Go to the Users screen by clicking the **Users** tab



3. Add the custom user by clicking **Add User**, which brings up the following window.



4. Enter the appropriate information in the text fields for User Name (“knta”), NT User Name (“knta”), NT User Domain, and Home Directory. In the field labeled Interactive Cmd Processor, enter the following:

   a. For a BASH version 2 or greater, enter:

      ```
      bash -login -noediting -i
      ```

   b. For a version less than version 2 of BASH, enter:

      ```
      bash -login -nolineediting -i
      ```

   (This tells Telnet to use the bash command processor in interactive logon mode.)

   Find the version of BASH by typing the following at a DOS prompt:

   ```
   bash -version
   ```

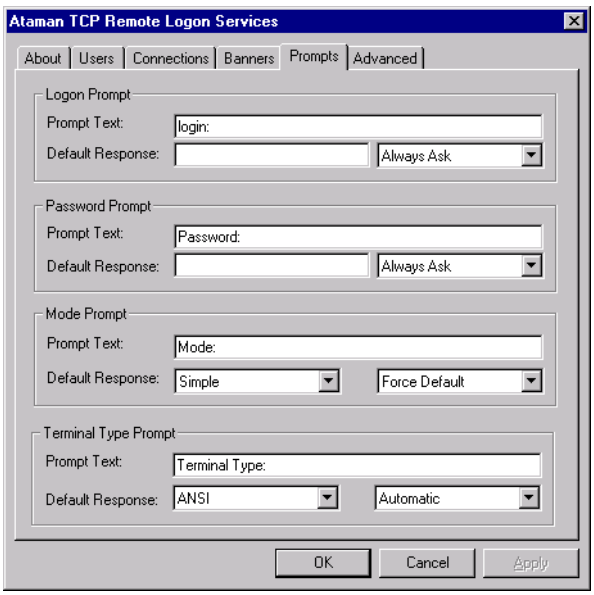
   c. Leave every other text field blank. Click **OK** when done.

Note

If user “knta” is in a Workgroup, then the NT User Domain entry should be the server DNS name.

5. Go to the Banners screen by clicking the **Banners** tab and enter any banners that are to be displayed upon logon (i.e. “Welcome to <machine name> (NT 4.0)”).

6. Go to the Prompts screen by clicking the **Prompts** tab.



7. Edit the fields so they match the following:

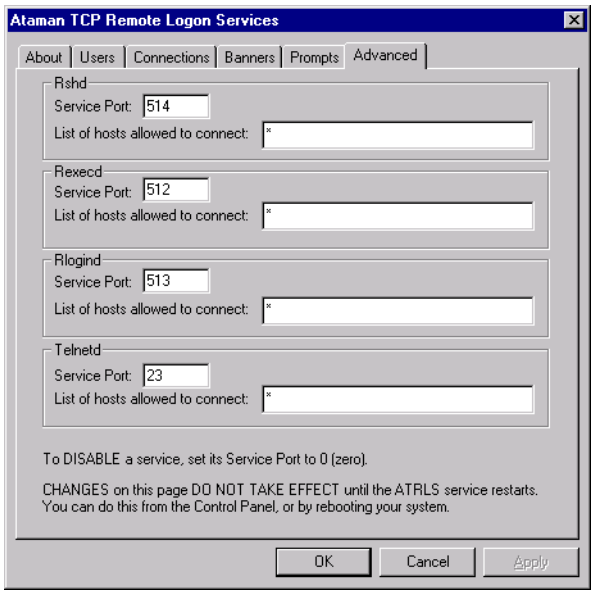
   a. In the Logon Prompt region:

      `Prompt text: login:` (Leave a space after 'login:')

   b. In the Mode Prompt region:

      `Default Response:  simple / Force Default`

8. Go to the Advanced screen by clicking the **Advanced** tab.

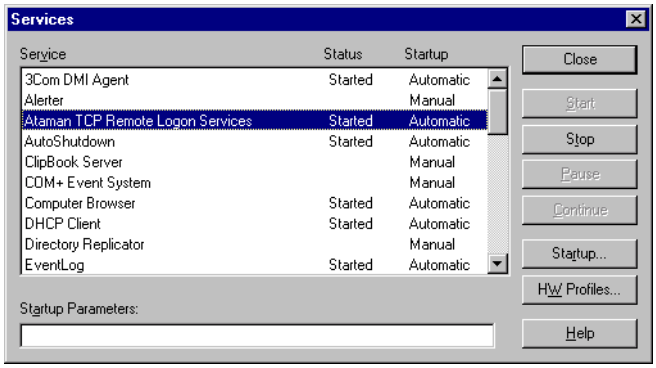


9. Edit the fields and click **OK.**

For more information about the Telnet server, the Ataman TCP Remote Logon Services User's Manual is provided with the Kintana NetPack. It is called userman.doc and resides in the Ataman install directory.

Once configuration is complete, the Ataman Service must be started. This is done through the standard Services Control Panel. To do this:

1. Open **Settings -> Control Panel -> Services**. This opens the Services Control Panel.



2. Select the line containing the “Ataman TCP Remote Logon Services” Service and click **Start**. (If the Service is already started, stop it by clicking **Stop** and restart it for the new settings to take effect.)

Configuring the FTP Server

The Kintana Product Suite uses FTP to perform file migrations from one computer to another. To transfer files between computers on a network, each source and destination computer must be running an FTP server. On UNIX platforms this is very straightforward, but Windows NT computers usually require some additional FTP server configuration to function with the Kintana suite. Any standard FTP server for Windows NT/2000 will work. The Microsoft Internet Information Server for Windows NT (IIS) contains a FTP server as one of its components. IIS is a standard component of Windows NT/2000 4.0 Server, and is available for Windows NT 3.51 for free from Microsoft's Web site.

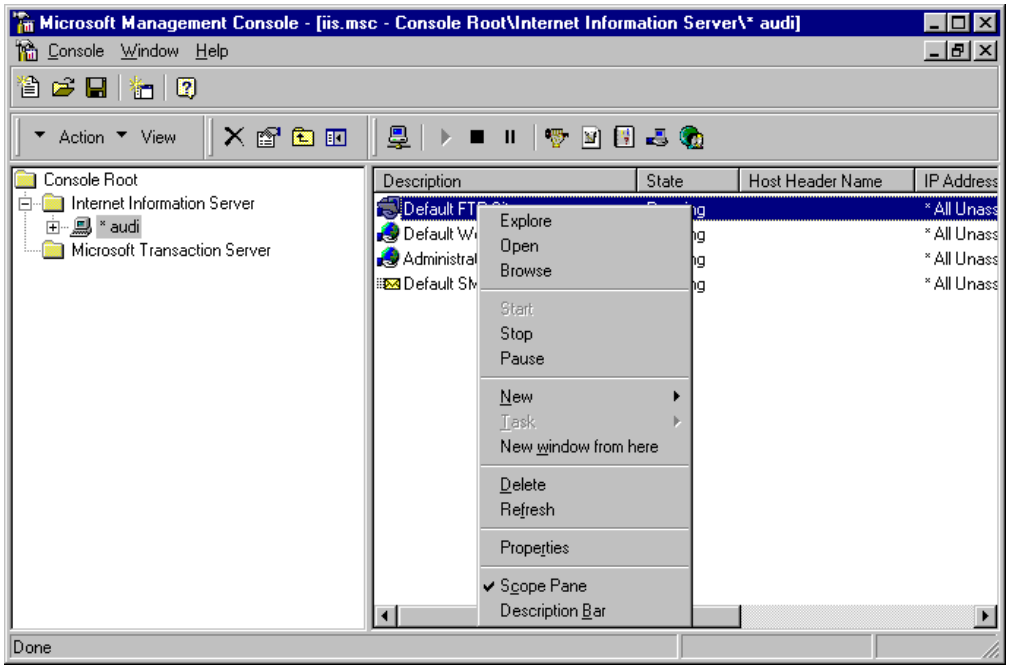
To configure the FTP server for each computer, ensure that the NT user account, with which the Kintana suite uses to open a connection, has access to the directories that the files are to be moved to. Some FTP servers require mapping such directories to FTP aliases, and a configuration utility is provided to do this. (For IIS this is called the Internet Service Manager.) Configuration steps vary depending on the type of FTP server used. The best way to test whether or not the Kintana suite is able to transfer files to a particular Windows NT Server is to manually test it first. If it is possible to open a FTP session and then “cd” to different directories, the Kintana suite should be able to do the same.

For the File and Directory Chooser components to work properly, the FTP server Directory Listing Style must be set to **UNIX** and not **MS-DOS**.

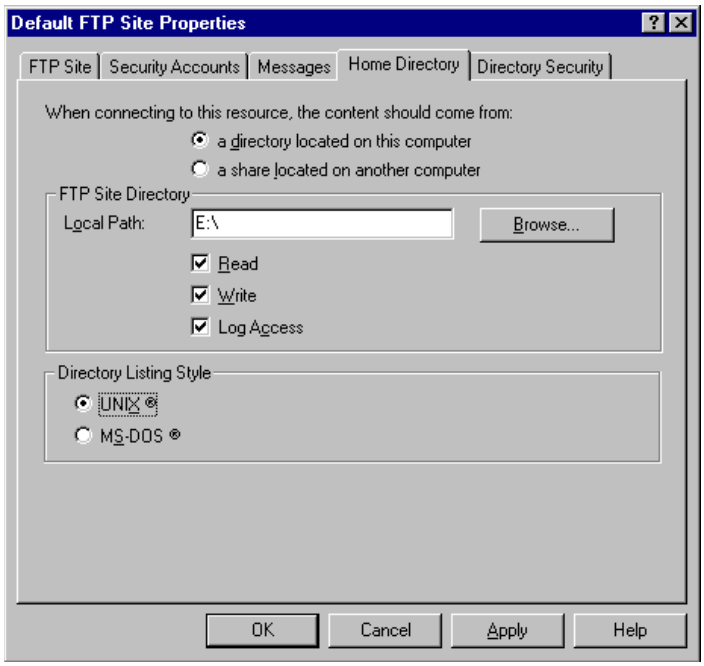
To set the Directory Listing Style:

1. In Windows NT, open the Internet Service Manager.

2. In the left-hand panel, open the Internet Information Server under ‘Console Root.’ Select the proper machine name.



3. Right-click on the ‘Default FTP Site’ that appears in the right-hand panel and go to ‘Properties.’ The Default FTP Site window opens.



4. Click on the **Home Directory** tab.

5. Select **UNIX** under ‘Directory Listing Style’ and click **OK**.

Accelerator Installation (UNIX and Windows NT/2000)

An Accelerator installation script is included with each Accelerator installation archive. After the archive is unpacked, it should reside in the KINTANA_HOME/bin directory. This script needs to be run for each Accelerator that is installed. After running the Accelerator install driver, there may be additional installation instructions. If an accelerator is being installed the Kintana server must be running.

See the installation guide for each Accelerator for more details on installing that particular Accelerator.

If no Kintana Accelerators are being installed, proceed directly to *"Starting the Kintana Server"* on page 40.

Server Modes

The Kintana server supports a "Restricted Mode" feature. The server modes are an important part of an Accelerator install or upgrade that requires an isolated Kintana server.

The following modes are supported.

- Restricted Mode – The server will only allow logins of users with a 'SysAdmin: Server Administrator' access grant. The server will not run scheduled executions, notifications, or the concurrent request manager.
- Normal Mode – The server will run as it runs now, with all enabled users able to logon and all services available according to server.conf parameters.
- Disabled Mode – The server is prevented from being started. This only happens when the Kintana core upgrade has exited prior to finishing.

Kintana supplies script KINTANA_HOME/bin/setServerMode.sh to manually set the server mode in situations where it is desirable to obtain exclusive access to a running server.

Note

If you are running Kintana on an IBM AIX server using Java v1.3.1, then you will need to start the Kintana server with a specific environment when installing Accelerators. This environment setting disables the AIX JIT (just-in-time compiler) as a workaround for a bug in this version of the AIX JIT.

1. Stop the Kintana server using kStop.sh, if it is running.
2. Set the JAVA_COMPILER environment variable:

   ```
   JAVA_COMPILER=NONE; export JAVA_COMPILER
   ```

3. Start the Kintana server using kStart.sh. You should see this output during server startup:

   ```
   Warning: JIT compiler "none" not found. Will use
      interpreter.
   ```

4. Install the Accelerator(s).
5. Stop the Kintana server using kStop.sh.
6. Unset the JAVA_COMPILER environment variable:

   ```
   unset JAVA_COMPILER
   ```

7. Restart the Kintana server. You should no longer see the JIT warning message (from step 3 above) during server startup.

Kintana Solution Installation (UNIX and Windows NT/2000)

The process for installing the Kintana Solutions solution follows the standard Kintana patch process. For new Kintana customers, this process should be employed after the successful Kintana installation.

See the installation guide for each Solution for more details on installing that particular Solution.

Starting the Kintana Server

To start the Kintana server:

UNIX: In the <KINTANA_HOME>/bin directory there is a file named *kStart.sh*. Run this script to start the server.

Windows NT/2000: Open the Services Control Panel, click the Kintana service (Kintana services start with the word “Kintana”) and click **Start** to start the server.

Chapter 3

Accessing the Kintana Client

The Kintana Product Suite features two interfaces: the Kintana interface and the Kintana Workbench interface. The Kintana interface uses HTML and Javascript to provide users with access to many key areas of functionality. The Kintana interface lets users of each product in the suite perform common tasks without requiring a Power License. All Kintana users will logon to the standard Kintana interface.

Kintana also features a Kintana Workbench interface. The Kintana Workbench is a Java applet designed to help Kintana Administrators, product configurers, and Power Users to perform advanced configuring and processing tasks, such as creating entities (like Request Types, Object Types, and Workflows) and administering licenses. The Kintana Workbench is accessed from the menu in the standard Kintana interface.

Once the Kintana server is running, users can logon to Kintana from their desktop computers. To access a logon screen, simply run Netscape or Internet Explorer and browse to the Web access point. See the following sections for details:

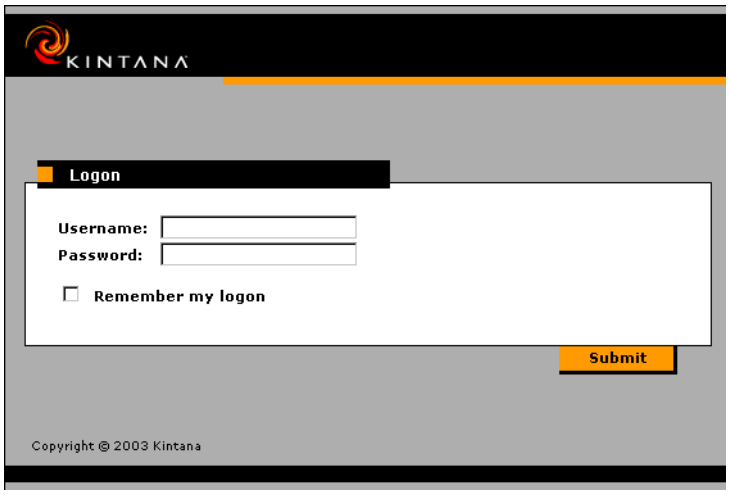
- *Logging onto Kintana*
- *Launching the Kintana Workbench*

Logging onto Kintana

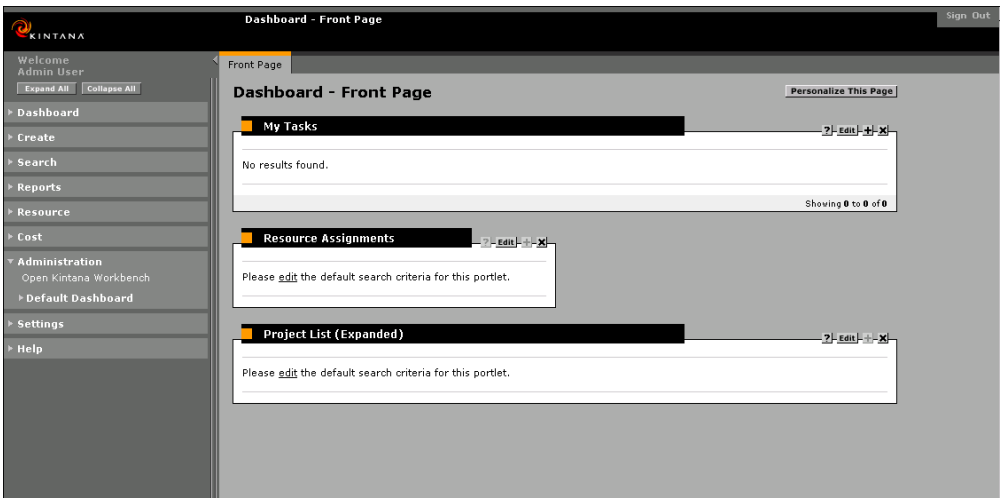
All Kintana users will logon to the Kintana using the same URL. The URL for Kintana is formed by taking the value of the BASE_URL parameter as configured in *Table 5-2 on page 51* and appending "/kintana/html/kintanaHome.html" to it, as in this example:

```
http://wwwserver.mydomain.com:port/kintana/html/kintanaHome.html
```

Enter the URL for your site. The Kintana logon screen appears.



The Kintana suite provides a default account for logging on the first time. Enter username “admin” and password “admin,” and click **Logon**. The Kintana client will be displayed in the window. It is recommended that the password of the “admin” account is disabled or changed once accounts for all of users have been generated.



Accounts (users and licenses) for the Kintana HTML interface are set in the Kintana Workbench’s Users window. See the *"Kintana Security Model"* document for more information on configuring licenses and user access.

Launching the Kintana Workbench

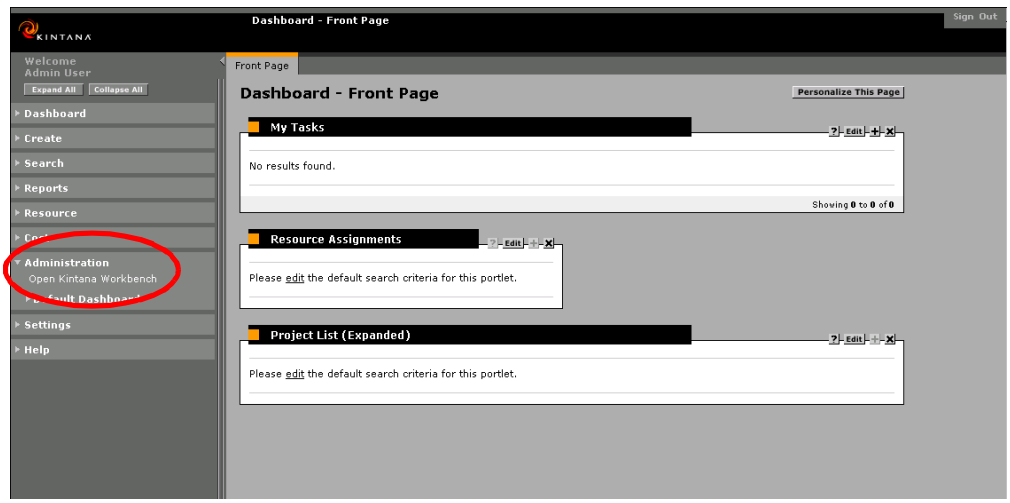
The Kintana Workbench provides an interface accessing advanced processing and configuration functionality in Kintana. This interface is available to users with a product Power License. For detailed information on the Kintana licensing as it relates to the Kintana interface and user permissions, see the *"Kintana Security Model"* document.

Note

If you have installed a pop-up blocker in your web browser, the Kintana Workbench will not open.

The Kintana Workbench is launched from within the standard Kintana interface. To launch the Workbench:

1. Logon to Kintana.



2. Select **ADMINISTRATION > OPEN KINTANA WORKBENCH** from the menu.

When the Workbench is accessed for the first time, Kintana detects whether or not the correct version of Java Plug-in is installed on their computer. If it is not, users are taken through a procedure for installing the Java Plug-in. This procedure only needs to be performed once.

Depending on the client's connection to the server, this may take several minutes. Subsequent logons will be much quicker, as the client does not have to install any additional components on their machine.

Java Plug-In Required for All Workbench Users

Kintana requires the Java Plug-in for accessing the Kintana Workbench. Installing the Java Plug-in means that Kintana users are not dependent on any specific version of JVM to run Kintana on their Internet browsers. The Java Plug-in is fully compatible with the Kintana client.

The first time Kintana users access the Workbench, Kintana detects whether or not the correct version of Java Plug-in is installed on their computer. If it is not, users are taken through a procedure for installing the Java Plug-in. This procedure only needs to be performed once.

To support this feature, the following server configuration parameters are defaulted in the server.conf file:

Server Parameter Name	Default
JAVA_PLUGIN_VERSION	1.4.1_02
JAVA_PLUGIN_PATH_IE	http://java.sun.com/products/plugin/autodl/jinstall-1_4_1_02-windows-i586.cab
JAVA_PLUGIN_PATH_NS	http://java.sun.com/j2se/1.4.1/

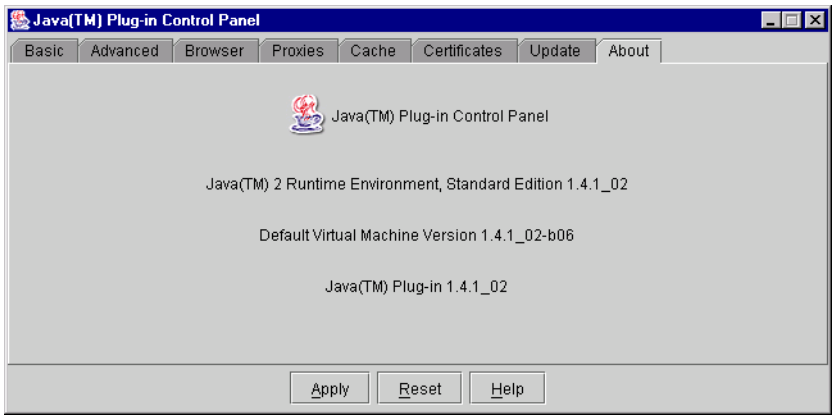
Java Plug-In Defaulting Issues

Users of the Kintana Workbench may run into issues resulting from the Java Plug-In setting itself as the default JVM for their browser.

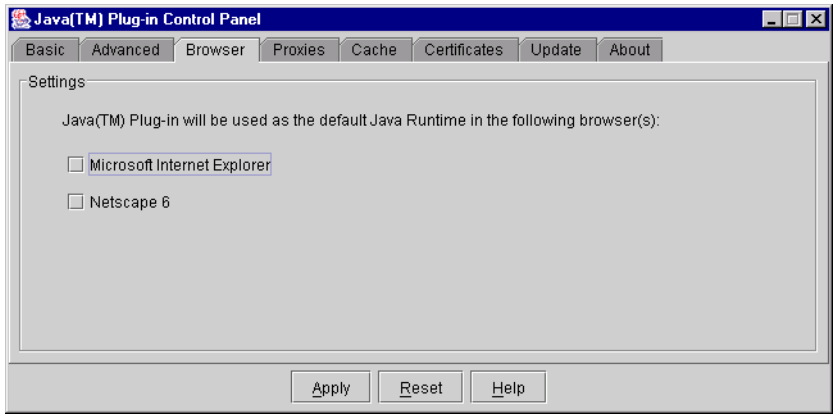
- The Kintana Workbench may throw a “class not found” exception error.
- The user may have other applications requiring different versions of the Java Plug-In.

To resolve these issues, remove the default browser associations for all versions of the Java Plug-In.

1. Open your Windows Control Panel and find the Java Plug-In icon. Each Plug-in version will have a icon, but by opening them and inspecting the **ABOUT** tab you can readily identify the newly installed Java Plugin 1.4.1_02.



2. Click the **BROWSER** tab and uncheck the default browser associations.



3. After you apply the changes, your other applications will be able to use their desired version of the Java Plug-in and the Workbench will function properly.

Chapter 4

Server Administration Notes

This chapter details some specific concerns of Kintana server administration. The following topics are discussed:

Server Administration Notes

A Kintana administrator needs access to server log files and tools to start, stop, and report on the state of the server. This section presents the organization of the server directory tree, and describes the administrative tools which are provided.

The Kintana server generally requires very little maintenance. However, as is the case with virtually all client-server applications, a server that runs for long periods of time can require periodic attention. To ensure continued smooth operation it is recommended that the server be periodically (once per month is recommended) stopped and restarted.

To help familiarize administrators with the server directory structure, the following list briefly describes the files and subdirectories contained in <KNTA_HOME>:

- **Server configuration file**: server.conf contains the values of all of the server parameters provided when the server configuration utility was run in *"Server Configuration"* on page 26. It is automatically generated by the configuration utility, using the file server.conf.dist as a basis. Anytime configuration changes are required, it is recommended that the server configuration utility is used and the instructions outlined in *"Server Configuration"* on page 26 are followed.

However, it is sometimes more convenient to edit the server.conf file directly. If this is done, run the script kUpdateHtml.sh in the /bin/ subdirectory to propagate the changes. The Kintana server reads the values from server.conf each time it is started, and writes them to a database table for quick runtime access. Because of this, anytime the value of a server parameter is changed, or a new server parameter is added, the server must be stopped and restarted for the configuration changes to be applied.

- **HTML files**: KintanaWorkbench.html and KintanaHome.html are located in the `<KNTA_HOME>/html` directory and are accessed directly from clients through the Web to logon to Kintana. DO NOT EDIT these files. They are automatically generated when the server configuration utility is run, as described in *"Server Configuration"* on page 26, using the *.dist files. Any manual changes are overwritten the next time the server configuration utility is run. The file about_knta.html contains the page displayed when the **Help -> About Kintana** menu item is selected from the Java client.

- **Kintana logs directory**: The `logs/` subdirectory of <KNTA_HOME> contains all logs generated by the Kintana product suite. As the server runs, logging messages are generated and written into the file serverLog.txt. When this file reaches the size indicated by the ROTATE_LOG_SIZE server parameter, it is renamed to serverLog_<timestamp>.txt, and a new serverLog.txt is started. In addition, the Java servlets used to serve the Web pages generate their own logfiles, named servletLog.txt. The amount of information present in the server logfiles depends on the debugging level set in the server configuration. The server parameters SERVER_DEBUG_LEVEL and DEFAULT_USER_DEBUG_LEVEL control this. If a problem arises and it is necessary to obtain more information in the logs, it is best to logon as an Administrator to the Kintana Workbench and set the server debug level to high from the menu (Edit -> Server Settings).

  The `logs/` directory contains the subdirectory `reports/`, which contains a logfile for each Kintana report that is run, and directories named `PKG_<number>/` and `REQ_<number>/`. These subdirectories contain execution logs for Kintana Deliver Packages and Kintana Create Requests, respectively. The <number> in the directory name corresponds to the ID of the Package or Request that is being executed

- **Server administration and configuration tools**: The `bin/` subdirectory of KNTA_HOME contains all of the scripts necessary to configure and administer the server. Some of these have already been discussed earlier in this document (for example, kConfig.sh in *"Server Configuration"* on page 26). Other key scripts are listed below:

a. kStart.sh: Used only on UNIX systems to start the Kintana server as a background process. See *"Starting the Kintana Server"* on page 40 for more details about starting the server.

b. kStop.sh: Stops the Kintana server. This script requires some arguments. When stopping the server, it is possible to choose to stop it now with the -now flag, or after a delay of a certain number of minutes with the flag -delay <# minutes>. Using the -delay option results in a message automatically being sent to all currently-connected Kintana users suggesting that the server will stop after the specified delay. In addition, this script may require authentication (if the server parameter REMOTE_ADMIN_REQUIRE_AUTH has been set to "True"). In this case, the flag -user <username> is also required.

c. kCancelStop.sh: If the server has been scheduled to stop by a command such as kStop.sh -delay 10 (which stops the server in 10 minutes), the stop request can be cancelled by running this script. Authentication may be required to do this, which works in the same way as for kStop.sh. Use the -user <username> flag.

d. kStatus.sh: Run this script to check to check the state of the Kintana server at any time.

e. kWall.sh: To send out a message to all users currently logged on to the Workbench, use kWall.sh. When this script is run, it prompts for the Kintana username and password and the desired message text. The message is displayed in a dialog on the monitor screen of anyone who is logged onto Kintana at that time.

f. kRunServerAdminReport.sh: Runs diagnostic reports on the Kintana server. Run kRunServerAdminReport.sh to view a list of reports to choose from. This utility provides a picture of how much activity is currently on the system, how many database connections are being made, etc.

g. kUpdateHtml.sh: Updates the Logon HTML files with the latest configuration. This script is automatically run by the server configuration utility. If any changes are made to server.conf by hand, this script should be run to make sure the changes are propagated.

- ***.jar, *.cab files**: These are archives of the Kintana Java client code. They are automatically downloaded by an end-user's browser when that user connects to Kintana.

- Other: the /sql/ subdirectory contains source code for the built-in Kintana reports. This can be used as a reference for generating custom reports. The /reports/ subdirectory contains the HTML files for all reports that have been run through the client. The /classes/ subdirectory contains all of the server Java code. The /transfers/ subdirectory is used as temporary storage for files being transferred between the server and remote computers. Other directories contain reference files as indicated by their name, and it is likely that they do not need to be accessed.

If You Need Additional Help...

It is strongly recommended that a Kintana Product Consultant assist in the installation of the Kintana product suite. Additional questions or issues about the installation process should be addressed to Kintana support. Contact information can be found on the Kintana support website (http://www.kintana.com/support/support.htm)

Chapter 5

Optional Configuration

You can enable certain features in Kintana by making changes to the server.conf file. Kintana Administrators should decide whether or not to use these features in their system. The additional features:

Logon ID

The Kintana Administrator can now set a parameter in the server.conf file that changes the text on the logon screen interface and lets the Administrator enter any unique name they choose for both the user's logon ID and username.

The Administrator must make the following edit in the server.conf file:

```
com.kintana.core.server.LOGON_METHOD=LOGON_ID
```

The following changes occur in the product:

- A new field titled 'Logon Id' displays on the **User Information** tab of the User window. This lets the Administrator enter unique names in the Logon ID and Username fields and differentiate between the user's logon ID and username. The Administrator can enter a meaningful username, such as the Employee ID number, instead of an automatically generated username which would be cryptic and have no meaning to the user.
- A new field entitled 'Enter New Logon Id' displays on the Copy User window. This also lets the Administrator differentiate between the user's logon name and username when copying a user's information.

- The username defined by the Administrator appears in the Created By and Assigned To fields.
- For both the Workbench and the HTML interface, the text on the logon screen interface changes from 'Username' to 'Logon ID.'
- Users must enter their logon ID on the Logon screen to access the product.

One Way Password Hash

Kintana Administrators have the option of implementing one-way hashes for user passwords if they want to have additional security for user passwords. This is done by adding a new parameter to the server.conf file.

After converting the user password encryption to a one-way hash, the user password encryption can later be converted back to a standard encryption. However, converting the user password back to standard encryption will lose all of the users passwords. The Administrator will need to assign a new default password for all Kintana users.

Administrators can select one of the following options for using passwords:

- To convert user passwords to one-way hashing so they cannot be decrypted:

  a. Run the kConvertUserPasswords.sh script. The script prompts you to select a password option. Based on your selection, the script tells you to add a new parameter to the server.conf file.

  b. Add the following line to the server.conf file:

  ```
  com.kintana.core.server.USER_PASSWORD_ENCRYPTION=HASH
  ```

- To convert user passwords to standard encryption:

  a. Run the kConvertUserPasswords.sh script. The script prompts you to select a password option. Based on your selection, the script tells you to add a new parameter to the server.conf file.

  b. Add the following line to the server.conf file:

  ```
  com.kintana.core.server.USER_PASSWORD_ENCRYPTION=STANDARD
  ```

If you are currently using LDAP, you can continue to use LDAP successfully after the user passwords are set to one-way hashing. However, if the Kintana administrator converts the user passwords back to standard encryption, all the LDAP user passwords will be lost.

Appendix A
Server Configuration Parameters

Table A-1 lists the server configuration parameters used in the server.conf file. The Required column shows whether the server parameter is a required parameter for setting up a Kintana Server. A value of TRUE in this column indicates that the parameter is required. A value of FALSE in this column indicates that the parameter is optional. A condition in this column indicates that the parameter is required based on the condition of another parameter. For example, the KINTANA_LDAP_ID parameter is only required when the AUTHENTICATION_MODE parameter is set to LDAP.

In a Server Cluster configuration, required parameters must be set for the primary server. Secondary servers will inherit the parameter value from the primary server. To override the inherited value, set the parameter to the desired value in the appropriate secondary server section of the server.conf file. For more information on setting up Kintana Servers in a Server Cluster configuration, see *"Configuring the Primary and Secondary Kintana Servers"* on page 31.

Use forward slashes (/) when entering directory paths in the server.conf file, regardless of the operating system being used. Kintana applications automatically use the appropriate path separators when communicating with Windows. Under any circumstance, do NOT use back-slashes (\) when entering directory path in the server.conf file, since Kintana applications will not recognize back-slashes.

Table A-1. Server configuration parameters

Parameter	Description	Required	Valid Values	Default	Example
ALLOW_SAVE_REQUEST_DRAFT	Allows Requests to be saved without automatically submitting them in the Kintana HTML interface.	FALSE	TRUE FALSE	FALSE	FALSE
ATTACHMENT_DIRNAME	Absolute pathname of the directory where attached documents will be stored. This directory: • Must give read/write access to web browsers • Should be outside the Kintana directory tree when using an external web server	TRUE			c:/kintana/attachments
ATTACHMENT_ROOT_URL	URL where attached documents can be accessed using a web browser. This URL should: • Begin with http:// or https:// • Be a web alias pointed to the directory specified by the ATTACHMENT_DIRNAME parameter • Point to the web server—and should not contain the /kintana prefix—when using an external web server.	TRUE			http://wwwserver.mydomain.com/kintana/attachments
AUTHENTICATION_MODE	Required for the Kintana Server to determine the user authentication method. Specify multiple modes by using a comma-delimited list of valid values.	TRUE	KINTANA LDAP NTLM SITEMINDER	KINTANA	KINTANA KINTANA, LDAP
BASE_PATH	Full directory where the Kintana Server is installed.	TRUE			c:/Kintana/

Table A-1. Server configuration parameters

Parameter	Description	Required	Valid Values	Default	Example
BASE_URL	Web location of the Kintana Server. This URL should point to the top directory in which the Kintana Server is installed <Kintana_Home>.	TRUE			http://www.mydomain.com:8080
CONC_LOG_TRANSFER_PROTOCOL	Transfer protocol to use when transferring Concurrent Request logs and patching README files.	If ORACLE_APPS_ENABLED = TRUE	FTP SCP		FTP
CONC_REQUEST_PASSWORD	Password of the Concurrent Request user.	If ORACLE_APPS_ENABLED = TRUE			fnd (encrypted)
CONC_REQUEST_USER	Any valid user on the system containing the Oracle Applications Server that can be used to retrieve concurrent request output files (via FTP or SCP, as specified by the CONC_LOG_TRANSFER_PROTOCOL parameter).	If ORACLE_APPS_ENABLED = TRUE			applmgr
DATE_NOTIFICATION_INTERVAL	Determines the interval (in minutes) that the Kintana Server will check to send date-based notifications.	FALSE		60	60
DAYS_TO_KEEP_INTERFACE_ROWS	Defines the duration (in days) that rows in the open interface tables will be kept before they are purged.	If ENABLE_INTERFACE_CLEANUP = TRUE		1	5

Table A-1. Server configuration parameters

Parameter	Description	Required	Valid Values	Default	Example
DB_PASSWORD	Password of the database schema containing Kintana tables as specified by the DB_USERNAME parameter. The server configuration utility automatically encrypts the password value. To manually edit this value, surround the encrypted password with the #!# delimiter.	TRUE			#!#password#!#
DB_USERNAME	Database schema containing Kintana tables.	TRUE			knta
DEFAULT_USER_DEBUG_ LEVEL	Specifies the default debug level of a user's client session. This parameter controls the verbosity of a user's logs on the client, application server, and database. The value may be different for different client sessions, and can be changed through the front-end GUI as a user preference. Available settings include: • NONE: no debugging information (corresponds to the default value of 0) • LOW: normal debugging information (corresponds to the value 10 in the Server Configuration report) • HIGH: maximum debugging information (corresponds to the value 70 in the Server Configuration report)		NONE LOW HIGH	NONE	NONE
EMAIL_NOTIFICATION_ CHECK_INTERVAL	Determines the interval (in seconds) that the Kintana Server will check if there are notifications waiting to be sent out.			20	20

Table A-1. Server configuration parameters

Parameter	Description	Required	Valid Values	Default	Example
EMAIL_NOTIFICATION_ SENDER	Email address of the default sender of email notifications. This sender will also receive any error messages associated with email notifications.	FALSE			sender@kintana.com
ENABLE_CONSOLE_ LOGGING	Enables the Kintana Server to log messages to the console.		TRUE FALSE		TRUE
ENABLE_INTERFACE_ CLEANUP	Specifies if transitive data in the open interface tables will be purged. When this parameter is set to TRUE, open interface tables will be purged periodically as specified by the DAYS_TO_KEEP_ INTERFACE_ROWS parameter.		TRUE FALSE		TRUE
ENABLE_STATISTICS_ CALCULATION	Specifies if statistics for the cost-based optimizer will be collected automatically to improve system performance. By default, statistics will be rebuilt every Sunday at 1AM.		TRUE FALSE	TRUE	TRUE
HTTP_PORT	Used to identify the port being used to communicate with the built-in HTTP server. This port number must be unique and distinct from the web server, SQL*Net, and RMI ports.	TRUE	Any unique port above 1024	8080	8080
HOURS_TO_KEEP_DEBUG_ MESSAGE_ROWS	Determines the duration (in hours) that rows in the KNTA_DEBUG_MESSAGES table will be kept.	TRUE		24	24
INSTALLATION_LOCALE	Locale information (language and country codes) of the Kintana installation. The language code should match the Kintana installation language.	TRUE	<language_ code>_ <COUNTRY_ CODE>	en_US	en_US de_DE

Table A-1. Server configuration parameters

Parameter	Description	Required	Valid Values	Default	Example
JDBC_URL	Locator for the database that contains the Kintana database schema. This parameter must be specified correctly to enable the Kintana Server to communicate with the database. The JDBC_URL parameter uses the following format: `jdbc:<subprotocol>:<subname>:@<hostname>:<port>:<SID>` The JDBC_URL parameter uses the following variables: • <subprotocol>:<subname> is a directive to Java and must always be oracle:thin. • <hostname> represents the DNS name or IP address of the system running the database. • <port> is the port used by SQL*Net to connect to the database. Obtain the value by referring to the database entry in the tnsnames.ora file. The default value is 1521. • <SID> represents the database system ID.	TRUE			jdbc:oracle:thin:@DBhost.domain.com:1521:SID
KINTANA_LDAP_ID	Kintana account on the LDAP server. Used by the Kintana Server to bind to the LDAP server.	If AUTHENTICATION_MODE=LDAP			

Table A-1. Server configuration parameters

Parameter	Description	Required	Valid Values	Default	Example
KINTANA_LDAP_PASSWORD	Kintana password on the LDAP server. The server configuration utility automatically encrypts this password. To manually edit this value, surround the encrypted password with the #!# delimiter.	If AUTHENTICATION_MODE=LDAP			#!#password#!#
KINTANA_SERVER	Name of the Kintana environment that contains information about the Kintana Server machine (such as host name, username, and password). This environment must be configured before Kintana Migrators or commands involving Secure Copy can run. This parameter can be used interchangeably with the SERVER_ENV_NAME parameter.				
KINTANA_SERVER_NAME	Name of the Kintana Server instance. If multiple Kintana Servers are running on the same machine, this name must be unique for each server. If the server is running on Windows, this name MUST match the name of the Windows service name.	TRUE			Kintana
KINTANA_SESSION_TIMEOUT	Duration (in minutes) before the Kintana Server terminates a user session due to inactivity. A value of 0 denotes no timeout.	TRUE	0 to 720	120	120
LDAP_BASE_DN	Specifies the base in the LDAP server from where the search will start. If not specified, the LDAP server will be queried to determine the base.	If AUTHENTICATION_MODE=LDAP			o=kintana.com

Table A-1. Server configuration parameters

Parameter	Description	Required	Valid Values	Default	Example
LDAP_GROUP_RECURSION_LIMIT	Determines the number of levels of sub-groups traversed when importing users from groups.	If AUTHENTICATION_MODE=LDAP			
LDAP_SSL_PORT	SSL port number on the LDAP server. If LDAP server is SSL-enabled, set this value to the SSL port on the LDAP server to secure all transactions. If not specified, all transactions will be carried over the port specified by the LDAP_URL parameter.	If AUTHENTICATION_MODE=LDAP		636	636
LDAP_URL	Comma-delimited list of LDAP URLs. The Kintana Server will query the URLs in the order specified. If a port number is not specified, the default port number 389 will be used.	If AUTHENTICATION_MODE=LDAP		ldap://ldap.theurl.com:389	ldap://ldap.kintana.com:389

Table A-1. Server configuration parameters

Parameter	Description	Required	Valid Values	Default	Example
LOCAL_IP	If LOCAL_IP is set to the IP address of the machine running the firewall, clients inside the firewall can connect, but clients outside cannot (no route to host). If LOCAL_IP is set to the machine name of the machine running the firewall, clients inside the firewall can connect, but clients outside cannot (cannot resolve host name). If LOCAL_IP is set to an IP address that is different from the machine running the firewall, clients outside the firewall can connect, but clients inside the firewall cannot (since address translation from the different IP address to the IP address on the machine running the firewall is not done). To resolve this issue, register the external IP address on the external DNS server and set LOCAL_IP to the name of the machine running the firewall. Clients running inside the firewall will connect to the internal DNS server and the machine name will be resolved to the IP address. Clients running outside the firewall will connect to an external DNS server and the machine name will be resolved to a different IP address. Both external clients will then be able to connect (each to a different IP address).				

Table A-1. Server configuration parameters

Parameter	Description	Required	Valid Values	Default	Example
LOGON_TRIES_INTERVAL	Logon attempt time interval. Defines the time interval (in minutes) during which logon attempts will be monitored.	TRUE		1	1
MAX_EXECUTION_ MANAGERS	Determines how many command executions can run simultaneously. If one or more package lines are selected for execution, an execution manager is used to run the package lines serially. Installations that process a high volume of packages may require a larger number of execution managers.	TRUE		15	15
MAX_LOGON_TRIES	Maximum number of logon attempts. Defines the maximum number of logon tries that the Kintana Server will accept in the time interval specified by the LOGON_TRIES_INTERVAL parameter.	TRUE		0	1
MAX_RELEASE_EXECUTION_ MANAGERS	Distribution execution dispatcher. Determines how many command executions can run in a Release Distribution simultaneously. This parameter is similar to the MAX_EXECUTION_MANAGERS parameter, except that it is used for Releases only. Installations that process a high volume of packages may require a larger number of execution managers. If the server is overloaded, lowering this value may reduce workload but may cause execution delays.	TRUE	>1	15	15

Table A-1. Server configuration parameters

Parameter	Description	Required	Valid Values	Default	Example
MAX_STATEMENT_CACHE_SIZE	Maximum number of prepared statements that are cached per database connection (prepared statement cache). This is part of the DB connection pool settings.	FALSE	>0		
MAX_WORKER_THREADS	Maximum number of worker threads. Determines how many threads can run simultaneously to process scheduled tasks (such as reports and Request commands). If the server is overloaded, lower this value to reduce the server's workload. If there are a lot of pending scheduled tasks and additional capacity is available on the server, raise this value to improve performance.	TRUE		10	10
MULTICAST_CLUSTER_NAME	Unique name of the Kintana cluster. Do not configure two Kintana Server clusters with the same cluster name running on the same subnet.			BASE_URL value for the primary server	http://wwwserver.mydomain.com/kintana/
MULTICAST_DEBUG	If this parameter is set to TRUE, all incoming and outgoing multicast messages will be logged to the server log.		TRUE FALSE	FALSE	FALSE
MULTICAST_IP	Multicast IP address.		224.0.0.0 to 239.255.255.255	225.39.39.244	225.39.39.244
MULTICAST_LEASE_MILLIS	Time in milliseconds a server sends out heartbeats.			2000 (20 seconds)	1500
MULTICAST_PORT	Multicast IP port.			9000	9000

Table A-1. Server configuration parameters

Parameter	Description	Required	Valid Values	Default	Example
OM_WATCH_DOG_INTERVAL	Do NOT change this parameter unless instructed by Kintana support.	FALSE		1	1
ORACLE_APPS_ENABLED	Indicates whether Kintana Applications will be integrated with Oracle Applications. To use Object*Migrator, GL*Migrator, or Patch*Migrator, this parameter must be set to TRUE.		TRUE FALSE		TRUE
ORACLE_HOME	Full path to the ORACLE_HOME directory on the Kintana Server machine. The ORACLE_HOME/ network/admin directory should contain the proper TNS names, or a file, required to connect to the Kintana database schema.	TRUE			d:/orant
PASSWORD_EXPIRATION_ DAYS	Default expiration period (in days) of passwords for new users.	TRUE	0 to 366	0 (no expiration)	0
PASSWORD_REUSE_ RESTRICTION_DAYS	Duration (in days) to restrict reuse of old password since the last date that password was changed.	TRUE	0 to 2192	0 (no restriction)	0
PENDING_COST_EV_ UPDATE_SERVICE_DELAY	Duration (in seconds) to wait when the Pending Cost EV Update Service completes before restarting.	FALSE	>0	30	30
PENDING_COST_EV_ UPDATE_SERVICE_ENABLED	Enables a service which asynchronously propagates external updates to Kintana Pending Cost EV Updates when updates could not be made immediately	FALSE	TRUE FALSE	TRUE	TRUE

Table A-1. Server configuration parameters

Parameter	Description	Required	Valid Values	Default	Example
PORTLET_EXEC_TIMEOUT	Duration (in seconds) before portlets time out. Used to limit long-running queries in portlets. Adding a portlet without any criteria may cause long-running queries. Using a timeout in this case avoid taking up database CPU when users end their sessions before portlets are completed.			20	20
REMOTE_ADMIN_REQUIRE_AUTH	Determines if user authentication is required for remote administration. If the parameter is set to TRUE, users running kStop.sh to shutdown the server will be required to supply a valid Kintana username and password. If the parameter is set to FALSE, any user with access to kStop.sh will be able shutdown the server.		TRUE FALSE		TRUE
RESOURCE_CACHE_SIZE	Used for caches of internal string resources.	FALSE	>0		
RESTRICT_BYPASS_EXECUTION_TO_MANAGERS	Determines if users can bypass execution when they are eligible to act on a Workflow Step in a Package. If this parameter is set to FALSE, users will always have the option to bypass an execution when they are eligible to act on it. If this parameter is set to TRUE, only users with the Package Manager access grant will have this privilege.		TRUE FALSE		FALSE
RML_PASSWORD	Password of the Oracle schema name as specified by the RML_USERNAME parameter	TRUE			

Table A-1. Server configuration parameters

Parameter	Description	Required	Valid Values	Default	Example
RMI_URL	Uses the following format: rmi://<hostname>:<port>/KintanaServer The Kintana Server will listen on the specified port to initiate RMI client/server communication. The port number must be an unique number, distinct from the web server, SQL*Net, and HTTP ports.	TRUE	<port> must be greater than 1024	<port> is 1099	rmi://platinum. kintana.com:1099 /KintanaServer
RML_USERNAME	Oracle schema name for the Meta Layer schema. This value must be the same as the schema name used during the installation or upgrade process	TRUE			
ROTATE_LOG_SIZE	Kintana Server logs will be rotated when this size (in kBytes) has been reached.	TRUE		150	250
SCHEDULER_INTERVAL	Determines the interval (in seconds) before the scheduler wakes up to verify if there are services ready to run.	TRUE		60	60
SCPCLIENT_TIMEOUT	Duration (in milli-seconds) that SCP clients need to provide feedback after a file transfer has initiated. If the client provides feedback within the specified duration, the program will complete. Otherwise, the program will timeout. To avoid timeouts, set this parameter to the maximum time it would take to transfer a file.				10000

Table A-1. Server configuration parameters

Parameter	Description	Required	Valid Values	Default	Example
SEARCH_TIMEOUT	Determines the duration (in seconds) before searches time out. Used to limit long-running queries in search pages. Submitting a search without entering selective data may cause long-running queries. Using a timeout in this case avoids taking up database CPU when users end their sessions before searches are completed.			60	60
SERVER_DEBUG_LEVEL	Corresponds to the Debug Level drop-down list in the Server section of the SERVER SETTINGS window. Specifies the debug level of the Kintana Server. This parameter controls the verbosity of logs generated by independent server processes (such as EmailNotificationAgent).		NONE LOW HIGH	NONE	NONE
SERVER_ENV_NAME	Name of the Kintana environment that contains information about the Kintana Server machine (such as host name, username, and password). This environment must be configured before Kintana Migrators or commands involving Secure Copy can run. This parameter can be used interchangeably with the KINTANA_SERVER parameter.				
SERVER_LOCALE_DATE_ ORDER	Date format used in the Kintana HTML interface.		MMDDYY DDMMYY		MMDDYY

Table A-1. Server configuration parameters

Parameter	Description	Required	Valid Values	Default	Example
SERVER_LOCALE_TIME_ ORDER	Time format used in the Kintana HTML interface		12 24		12
SERVER_NAME	DNS name or IP address of the machine hosting the Kintana Server	TRUE			wwwserver. mydomain.com
SERVER_TYPE_CODE	Platform where the Kintana Server is installed.		UNIX WINDOWS		WINDOWS
SHOW_BASE_URL_ON_ NOTIFICATION	Indicates if the URL for the Kintana main logon page will be displayed at the top of each email notification.		TRUE FALSE		TRUE
SMTP_SERVER	Hostname of the SMTP-compliant mail server that acts as the gateway for email notifications. To take advantage of Kintana email notification capabilities, this parameter must be configured.	FALSE			mailserver. mydomain.com
SQLPLUS	Name of the command-line SQL*Plus executable (should be located in the ORACLE_HOME/bin directory).	TRUE	sqlplus (Unix) plus33 plus80 (Windows)		plus33
SRUN_HOST	If the Kintana Web Server Module and the Kintana Server are running on separate machines, set this parameter to the name of the host machine running the Kintana Server.				

Table A-1. Server configuration parameters

Parameter	Description	Required	Valid Values	Default	Example
SRUN_PORT	Allows the Kintana Web Server Module to connect to the Kintana Server using the SRUN protocol. This parameter can be set to any unique port greater than 1024. In a Server Cluster configuration, this parameter must be defined for each secondary server.		>1024		
STATS_CALC_DAY_OF_ WEEK	The day of the week the statistics should be calculated. Valid values range from 1 (Sunday) to 7 (Saturday).	If ENABLE_ STATISTICS_ CALCULATIO N=TRUE	1 to 7	1	1
STATS_CALC_INTERVAL	Determines how often the service will wake up to check if it is time to refresh statistics.	If ENABLE_ STATISTICS_ CALCULATIO N=TRUE		3600	3600
STATS_CALC_WAKE_UP_ TIME	The hour of the day the statistics should be calculated. Statistics calculation will begin within an hour of the time given. Valid values range from 0 (midnight) to 23 (11PM).	If ENABLE_ STATISTICS_ CALCULATIO N=TRUE	0 to 23	1	1
STATS_CALC_WEEK_ INTERVAL	The number of weeks that should occur between statistic calculation. If set to 1, statistics will be collected each week; if set to 2, statistics will be calculated every other week.	If ENABLE_ STATISTICS_ CALCULATIO N=TRUE	1 to 52	1	1

Table A-1. Server configuration parameters

Parameter	Description	Required	Valid Values	Default	Example
TIME_ZONE	Time zone of the Oracle database. Set this parameter to the same time zone as the Oracle database, unless if the database and the Kintana Server are in different time zones. In such cases, set this parameter to valid 3-digit standard time zone (such as PST, MST, CST, EST, or GMT). Do not use daylight savings modified time zones (such as EDT or PDT). For assistance in these cases, contact Kintana support.	FALSE			
USER_PASSWORD_MAX_ LENGTH	Maximum length of user passwords	FALSE		16	16
USER_PASSWORD_MIN_ DIGITS	Minimum number of digits required in the user password	FALSE		0	0
USER_PASSWORD_MIN_ LENGTH	Minimum length of user passwords.	FALSE	0 or greater	4	0
USER_PASSWORD_MIN_ SPECIAL	Minimum number of non-alphanumeric special characters required in the user password.	FALSE		0	0
VISUALIZATION_EXEC_ TIMEOUT	Determines the duration (in seconds) that Costing and Resource Management visualizations can run before timing out.	FALSE		60	60
WORKBENCH_ PRESENTATION_KEY	If there are any standalone Workbench users and a custom presentation key is being used, this parameter will need to be added for that installation.	FALSE		knta	knta

Table A-1. Server configuration parameters

Parameter	Description	Required	Valid Values	Default	Example
WORK_ITEM_BREAKDOWN_SERVICE_DELAY	Duration (in seconds) to wait when the Work Item Breakdown Service completes before restarting.	FALSE	>0	30	30
WORK_ITEM_BREAKDOWN_SERVICE_ENABLED	Enables a service which asynchronously decomposes the (scheduled and actual) effort of Work Item assignments into daily units. These daily units provide the building blocks for Resource Management visualizations	FALSE	TRUE FALSE	TRUE	TRUE
WORK_ITEM_UPDATE_SERVICE_DELAY	Duration (in seconds) to wait when the Work Item Update Service completes before restarting.	FALSE	>0	120	120
WORK_ITEM_UPDATE_SERVICE_ENABLED	Enables a service which asynchronously propagates external updates to Kintana Work Items when updates could not be made immediately.	FALSE	TRUE FALSE	TRUE	TRUE

Index

L

N

O

P

R

S

T

U

V

W