



Siebel Incentive Compensation Management Installation Guide for Microsoft Windows

Version 7.5.3
December 2003

Siebel Systems, Inc., 2207 Bridgepointe Parkway, San Mateo, CA 94404
Copyright © 2003 Siebel Systems, Inc.
All rights reserved.
Printed in the United States of America

No part of this publication may be stored in a retrieval system, transmitted, or reproduced in any way, including but not limited to photocopy, photographic, magnetic, or other record, without the prior agreement and written permission of Siebel Systems, Inc.

Siebel, the Siebel logo, TrickleSync, Universal Agent, and other Siebel names referenced herein are trademarks of Siebel Systems, Inc., and may be registered in certain jurisdictions.

Other product names, designations, logos, and symbols may be trademarks or registered trademarks of their respective owners.

PRODUCT MODULES AND OPTIONS. This guide contains descriptions of modules that are optional and for which you may not have purchased a license. Siebel's Sample Database also includes data related to these optional modules. As a result, your software implementation may differ from descriptions in this guide. To find out more about the modules your organization has purchased, see your corporate purchasing agent or your Siebel sales representative.

U.S. GOVERNMENT RESTRICTED RIGHTS. Programs, Ancillary Programs and Documentation, delivered subject to the Department of Defense Federal Acquisition Regulation Supplement, are "commercial computer software" as set forth in DFARS 227.7202, Commercial Computer Software and Commercial Computer Software Documentation, and as such, any use, duplication and disclosure of the Programs, Ancillary Programs and Documentation shall be subject to the restrictions contained in the applicable Siebel license agreement. All other use, duplication and disclosure of the Programs, Ancillary Programs and Documentation by the U.S. Government shall be subject to the applicable Siebel license agreement and the restrictions contained in subsection (c) of FAR 52.227-19, Commercial Computer Software - Restricted Rights (June 1987), or FAR 52.227-14, Rights in Data—General, including Alternate III (June 1987), as applicable. Contractor/licensor is Siebel Systems, Inc., 2207 Bridgepointe Parkway, San Mateo, CA 94404.

Proprietary Information

Siebel Systems, Inc. considers information included in this documentation and in Siebel eBusiness Applications Online Help to be Confidential Information. Your access to and use of this Confidential Information are subject to the terms and conditions of: (1) the applicable Siebel Systems software license agreement, which has been executed and with which you agree to comply; and (2) the proprietary and restricted rights notices included in this documentation.

Contents

Chapter 1: Overview of Siebel Incentive Compensation Management

Who Should Read This Manual	5
The Siebel Incentive Compensation Management Implementation Process	5
Related Documents	8

Chapter 2: Understanding Siebel Incentive Compensation Management

Siebel Incentive Compensation Management Architecture	9
Web and Application Tier	9
Data Tier	10

Chapter 3: Siebel Incentive Compensation Management Installation

Siebel ICM Platform Deployment Overview	11
Post-Database-Installation Instructions for Oracle 8i Users	11
Post-Database-Installation Instructions for Oracle 9i Users	11
Process for Installing Siebel ICM	12
Unpacking the Software	12
Configuring the Server Properties Files	13
Configuring Database Property Files	15
Configuring the SQL Server Database Properties Files	15
Configuring the Oracle 8i/9i Database Properties Files	17
Installing Siebel ICM Application Server and Web Server	18
Installing the Siebel ICM Database Tier	19
Installing the Siebel ICM Database Tier on SQL Server	19
Installing the Siebel ICM Database Tier on Oracle	20
Completing the Siebel ICM Server Installation	20
Jasper Reports Target Configuration and Execution	20
Verifying Proper Installation of Database Tiers	22
Distributed Processing Mode	23

Process for Configuring Authentication Modes	26
Netegrity Siteminder	27
NT/Active Directory	28
Using IIS as a Front End HTTP Server	28
HTTP access to Siebel ICM using IIS	29
HTTPS/SSL access to Siebel ICM using IIS	30
Running Siebel ICM	31

Chapter 4: Encrypted Passwords, User Names, and Log Files

Encrypted Passwords and User Names	35
Encrypted Log Files	36

Chapter 5: Glossary

1

Overview of Siebel Incentive Compensation Management

Thank you for selecting Siebel Incentive Compensation Management, the premier system for designing and administering incentive compensation plans. Siebel Incentive Compensation Management provides financial administrators a powerful, one-stop system for managing and reporting multilevel compensation schemas. Siebel Incentive Compensation Management is typically used by financial administrators and corporate managers to provide a company's employees with bonuses, commissions, and other incentives based on individual or group performance benchmarks. Siebel Incentive Compensation Management can also manage incentive plans for channel partners, value-added resellers, or any group or person for whom commissions and rewards are an essential part of the business relationship.

Access to data, reports, and metrics is through a zero-footprint, Web browser-based client. No additional client-side software is required to use Siebel Incentive Compensation Management.

Who Should Read This Manual

This guide is for system administrators and database administrators responsible for the installation, configuration, and maintenance of Siebel Incentive Compensation Management host servers and databases. This guide contains technical information on the planning and implementation of Siebel Incentive Compensation Management, and does *not* address advanced database configuration, Siebel Incentive Compensation Management customization, or user-level features.

This document assumes a basic familiarity with Windows 2000, and SQL Server and Oracle database administration. While important commands and steps related to Siebel Incentive Compensation Management installation are described in detail, some commands may not be familiar to junior administrators. In addition, Siebel Incentive Compensation Management contains additional database and server components that require advanced technical setup.

The Siebel Incentive Compensation Management Implementation Process

As is the case with any business-critical enterprise application, installing Siebel Incentive Compensation Management requires a protracted and considered process of planning and implementation. Important decisions must be made at each step, and each decision is based on several variables. Siebel Incentive Compensation Management has developed a five-step rollout process that considers each aspect of an enterprise implementation, from budget to support.

Each phase of this process is just as crucial as the next. [Table 1](#) briefly examines each phase.

Table 1. Implementation Process for Installing Siebel Incentive Compensation Management

Project Phase	Actions	Siebel Incentive Compensation Management Deliverables
Mobilize	<ul style="list-style-type: none"> ■ Ascertain objectives ■ Ascertain budget ■ Align objectives and expectations ■ Create and train project team ■ Determine infrastructure requirements ■ Determine hardware requirements ■ Determine software requirements ■ Ascertain metrics and reporting requirements ■ Solicit feedback from potential users ■ Understand and determine Siebel Incentive Compensation Management configuration options 	<ul style="list-style-type: none"> ■ Engagement Letter ■ Statement of Work ■ Sales Turnover Checklist ■ Project Proposal and Charter ■ Preliminary Project Plan
Discover	<ul style="list-style-type: none"> ■ Evaluate current (as-is) processes ■ Carefully read and understand Siebel Incentive Compensation Management documentation ■ Procure and install adjunctive software (databases, Java support) ■ Procure and prepare server and network hardware 	<ul style="list-style-type: none"> ■ Business requirements definition ■ Integration/Reporting definition ■ Environment specification ■ Risk assessment worksheet ■ Project scope definition ■ Detailed project plan

Table 1. Implementation Process for Installing Siebel Incentive Compensation Management

Project Phase	Actions	Siebel Incentive Compensation Management Deliverables
Design	<ul style="list-style-type: none"> ■ Develop and prepare backup schema ■ Prepare legacy data for import and transfer ■ Prepare operating systems ■ Prepare internal support for end-users ■ Develop process for post-install maintenance ■ Install and configure Siebel Incentive Compensation Management software 	<ul style="list-style-type: none"> ■ Gap solution assessment ■ Configuration design ■ Interface and report designs ■ Installation checklist ■ Unit test scripts ■ Solution acceptance criteria
Configure	<ul style="list-style-type: none"> ■ System adjustments ■ Diligent monitoring of Siebel Incentive Compensation Management systems for potential problems 	<ul style="list-style-type: none"> ■ Configuration specification ■ Integration specifications ■ Reporting specifications ■ Environment management policy ■ System test scripts
Confirm	<ul style="list-style-type: none"> ■ Postmortem of installation ■ Test initial installation ■ Test installation against performance benchmarks with select control group ■ Test client-server relationship from different locations with varying intensity ■ Daily backup of database ■ Support of end-users ■ Develop custom policies and procedures 	<ul style="list-style-type: none"> ■ Acceptance test scripts ■ System policies and procedures ■ Training documentation ■ Support transition checklist ■ Go-live criteria ■ Project summary report

Related Documents

Occasionally, this document will reference other Siebel Incentive Compensation Management manuals and documentation. In addition to the Siebel Incentive Compensation Management's online help, these documents that describe the various aspects of Siebel Incentive Compensation Management, from implementation to every day use, are also included with Siebel Incentive Compensation Management.

- *Siebel Incentive Compensation Management Configuration Guide*: This is a guide for system administrators or financial planners responsible for configuring the Siebel Incentive Compensation Management environment for a group or company after a successful installation.
- *Siebel Incentive Compensation Management Administration Guide*: This guide details Siebel Incentive Compensation Management's essential functionality, and is designed for financial planners, payroll staff, or anyone needing client-level access to Siebel Incentive Compensation Management.

2

Understanding Siebel Incentive Compensation Management

The Siebel Incentive Compensation Management system is comprised of three tiers of integrated components, self-contained for adaptability and scalability. In a *stand-alone configuration*, all three tiers are hosted on the same server. As needs grow, any tier can be migrated to a dedicated server or upgraded without affecting other aspects of the system. A Siebel Incentive Compensation Management system with one or more tiers on its own dedicated server is called an *enterprise configuration*.

Siebel Incentive Compensation Management uses the Java 2 Enterprise Edition (J2EE) platform and Enterprise JavaBeans (EJB) to promote maximum flexibility during initial rollout and upgrading. This method enables any company to leverage its unique performance requirements and IT infrastructure when implementing Siebel Incentive Compensation Management.

Siebel Incentive Compensation Management supports Microsoft Windows 2000 Server (Standard, Advanced, and Datacenter), Sun Microsystems Solaris 8 or later, and IBM AIX 4.3.3 or later.

Siebel Incentive Compensation Management Architecture

The *Web Tier* serves as the portal to Siebel Incentive Compensation Management, providing individuals with proper access, and the ability to obtain and add information through the use of Microsoft Internet Explorer. The *Application Tier* is home to the software that processes business logic and transaction rules. The Application Tier is able to interface with many external legacy systems, including Enterprise Resource Planning (ERP) and Contact Relationship Management (CRM) software. Finally, the *Data Tier* contains Siebel Incentive Compensation Management's database and all related raw data.

Web and Application Tier

The *Web Tier* provides access to the information contained in Siebel Incentive Compensation Management through a combination of a Web server, Java *servlets*, and Java *Server Pages* (JSP). The Web Tier utilizes the Tomcat Web server to process JSPs and to send rich, formatted data to client browsers.

The *Application Tier* makes up the bulk of Siebel Incentive Compensation Management, and includes the analytical engine, security features, the user management interface, the transaction rules engine, and other components that process the raw data and statistics. This tier uses the JBoss application server. JBoss uses Enterprise JavaBeans to process Siebel Incentive Compensation Management's business logic and to interact with legacy systems.

Data Tier

The *Data Tier* is home to Siebel Incentive Compensation Management's transactional and analytics databases. The data schema operates under an Oracle 8i, Oracle 9i relational database instance. These components are not bundled with Siebel Incentive Compensation Management and must be procured and licensed separately.

NOTE: It is recommended that Siebel Incentive Compensation Management and its adjunctive applications be installed on a disk partition separate from the partition that hosts the operating system and system logs. It is not necessary to place tiers on individual partitions.

3

Siebel Incentive Compensation Management Installation

This section provides instructions for installing a stand-alone configuration of Siebel Incentive Compensation Management. All three tiers, including the application servers and databases, are hosted on the same machine.

Siebel ICM Platform Deployment Overview

Siebel ICM is a n-tier J2EE based platform. The following tiers need to be installed and configured: Web Server, Application Server, and Database Server. All tiers can be deployed on a single machine, or on multiple machines.

For a complete list of supported platforms, see *System Requirements and Supported Platforms* on Siebel SupportWeb.

Post-Database-Installation Instructions for Oracle 8i Users

After the Oracle instance is installed and verified, you must run a script before moving on to install the Siebel ICM software. This script populates the Product user Profile information required by SQL*Plus. Instructions are as follows.

To run the Product User Profile population script

- 1 On the transaction database host, launch SQL*Plus.
- 2 Log in with the "system" user name and password.
- 3 Execute `$ORACLE_HOME/sqlplus/admin/pupbld.sql`

Example: `sqlplus system/manager @$ORACLE_HOME/sqlplus/admin/pupbld.sql`

Post-Database-Installation Instructions for Oracle 9i Users

After the Oracle instance is installed and verified, you must run a script before moving on to install the Siebel ICM software. This script populates the Product user Profile information required by SQL*Plus. Instructions are as follows.

To run the Product User Profile population script

- 1** On the transaction database host, launch SQL*Plus.
- 2** Log in with the "system" username and password.
- 3** Execute \$ORACLE_HOME/sqlplus/admin/pupbld.sql

Example: sqlplus system/manager @\$ORACLE_HOME/sqlplus/admin/pupbld.sql

Process for Installing Siebel ICM

Installing Siebel ICM consists of unzipping three files, configuring your application server properties, and either Oracle or SQL Server properties, then running an install script.

The following installation tasks are included in this section:

- "Unpacking the Software" on page 12
- "Configuring the Server Properties Files" on page 13
- "Configuring Database Property Files" on page 15
- "Installing Siebel ICM Application Server and Web Server" on page 18
- "Installing the Siebel ICM Database Tier" on page 19
- "Distributed Processing Mode" on page 23
- "Process for Configuring Authentication Modes" on page 26
- "Netegrity Siteminder" on page 27
- "NT/Active Directory" on page 28
- "Using IIS as a Front End HTTP Server" on page 28
- "HTTP access to Siebel ICM using IIS" on page 29
- "HTTPS/SSL access to Siebel ICM using IIS" on page 30
- "Running Siebel ICM" on page 31

Unpacking the Software

The following steps need to be performed to unpack the ICM software. During this process you will also download and install the Mozilla Rhino and iText. Mozilla Rhino is the Netscape Javascript Execution Engine. This component executes rule logic and is required. iText generates PDF reports from Jasper report definitions.

To unpack the ICM software

- 1** Download JBoss 3.0.3/Tomcat 4.1.12 from http://prdownloads.sourceforge.net/bulldog/jboss3.0.3_tomcat4.1.12-MOD.zip?download

- 2 Unzip the JBoss3.0.3/Tomcat 4.1.12 zip file to a location of your choice, for example d:\SiebelICM\. This location will be known as the INSTALLATION_ROOT.
- 3 Extract the Siebel_ICM-Main.zip file to INSTALLATION_ROOT.
- 4 Overwrite existing files.

To install Mozilla Rhino

- 1 Download Mozilla Rhino from: [ftp://ftp.mozilla.org/pub/mozilla.org/js/older-packages/rhino15R2.zip](http://ftp.mozilla.org/pub/mozilla.org/js/older-packages/rhino15R2.zip)

Put the unzipped zip file in <INSTALLATION_ROOT>\jboss-3.0.3_tomcat-4.1.12\server\default\lib

To install iText

- 1 Download iText from <http://prdownloads.sourceforge.net/itext/itext-0.96.jar?download>

Put it in <INSTALLATION_ROOT>\jboss-3.0.3_tomcat-4.1.12\server\default\lib

To install JDBC drivers

- 1 **Oracle users:** If you are using Oracle as the RDBMS, place the Oracle Driver zip file in INSTALLATION_ROOT/etc/jboss/dist/**oracle9i** for Oracle 9i and INSTALLATION_ROOT/etc/jboss/dist/oracle8i for Oracle 8i.

NOTE: Siebel Systems does not provide the Oracle Driver zip file; you must acquire it yourself either from your Oracle installation, or through the Oracle TechNet Web site.

- 2 **SQL Server users:** If you are using SQL Server the RDBMS, place the opta2000.jar driver jar file, version 5.0.1 in INSTALLATION_ROOT/etc/jboss/dist/**sqlserver** directory.

NOTE: Siebel Systems does not provide the Opta 2000 driver jar file, you must acquire it yourself from Inet.

Configuring the Server Properties Files

Edit install.properties as follows:

- 1 Set your java.home path. For example: C:/j2sdk1.4.0_04.

NOTE: When you set the "java.home" property, the path must be specified using forward slashes "/" for the directory separators. This is because a back-slash is treated as a character in Java and in Java properties files.

- 2 Specify the database you are using. For example, db = sqlserver.

No matter which database you specify, for instance Oracle, or SQL Server, you must configure that properties file, either oracle.properties or sqlserver.properties respectively.

- 3** Make sure the `app.host`, `transactionDB.host`, and `analyticsDB.host` fields point to the location of your Application Tier, Database Tier, and Analytics DB tier respectively.

Definitions of these values are as follows:

- **app.host.** The name of the machine running your application server, for example, JBoss.
- **transactionDB.host.** The name of the machine running your transaction database.
- **analyticsDB.host.** The name the machine running your analytics database.

- 4** If you want to run the Tomcat/JBoss integrated stack, uncomment the next line. If you are running Tomcat and JBoss on separate machines, comment it out by putting a “#” at the beginning of the line.

`integrated.stack=true.`

- 5** Specify the JDK version you want Siebel ICM to use. For example, `jdk.version = jdk1.3`

- 6** Set Java Memory tuning setting.

Definitions of these settings are as follows:

- **jvm.memory.init.** Set to the initial size of the Java heap. For example:
`jvm.memory.init=128m`
- **jvm.memory.max.** Set to the maximum size of the Java heap. For example:
`jvm.memory.max=512m.`

NOTE: Never exceed the total amount of physical memory on your machine, or your performance will suffer.

- 7** Locate the Application Network Port Configuration section of the file and adjust the port settings as appropriate. You must change these settings if you are using multiple application servers and Web servers on the same server, otherwise, there will be a conflict between the ports.

AJP13 is used by tomcat4

AJP12 is used by tomcat3

- `jboss.port.NamingService=1099`
- `jboss.port.WebService=8083`
- `jboss.port.RMI=4444`
- `tomcat.port.HttpConnector=8080`
- `tomcat.port.AJP13Connector=8009`
- `tomcat.port.AJP12Connector=8007`
- `jboss.port.HtmlAdaptorServer=8082`

- 8** Set your application thread control setting.

For example: `jboss.mdb.pool.size=2`

9 Locate the dashboard.customization property.

Set this value to true to allow dashboard customization through Jetspeed.
(dashboard.customization)

Set this value to false to disable the automatic Jetspeed setup and user creation for dashboards when an OU is created. (dashboard.create.ou.portal)

The global setting, if set to true, will cause the default dashboard configurations to be used. This setting does not change the behavior of per-OU dashboard configuration creation through the bootstrap URL or the regular UI, only dashboard.create.ou.portal controls that. It does mean that the create-on-demand on first-time login feature for populated/migrated OUs will be disabled, however. (dashboard.test.mode)

Recommended values are as follows:

- dashboard.customization=true
- dashboard.create.ou.portal=true
- dashboard.test.mode=false

10 Locate the dashboard.test.mode property. Make sure the value of this property is false.

11 Locate the dashboard.create.ou.portal property. Make sure the value of this property is true.

NOTE: This setting will create unique dashboard layouts per Operating Unit. The remaining parameters in the install.properties are advanced in nature. It is recommended you not change any other parameters.

12 Set the parameters for Performance tuning. Leave the default value, 2.

service.extract.newline.numberchars=2

13 Save install.properties.

Configuring Database Property Files

The following two tasks outline the way in the way in which you configure database property files for SQL Server, and for Oracle Database.

Configuring the SQL Server Database Properties Files

- 1** Open sqlserver.properties in a plain text editor.
- 2** Each database, transactionDB, and analyticsDB has a section that defines the database name, the database user name, and the database user password.
 - a** transactionDB.name=SiebelICM
 - b** transactionDB.user=siebelicm
 - c** transactionDB.password=siebel2003
 - d** analyticsDB.name= SiebelICM _DW

- e analyticsDB.user= siebelicm_dw
- f analyticsDB.password= siebel2003

Change the values for these fields as necessary.

- 3 The analytics stored procedures will also need to be pointed to the databases called out above. Locate the Analytics Stored Procedures section of the file and update the DW_PREFIX and the TX_PREFIX with the names of the databases as changed above.
- 4 To improve performance when running the UpdateAnalytics service, adjust the analyticsService.readingCommitSize parameter. This parameter size is calculated by finding the record type with the most number of custom fields and multiplying the number of fields by the number of records in the system.

For Example: The combined number of custom fields on a transaction header and transaction line profile is 5, and the anticipated number of transactions to be processed in a single batch is 50,000. Multiply 5 X 50,000 and set this parameter to a value of 250000.

This value (250000) requires that you have a large enough rollback segment and tablespace in Oracle or transaction log in SQL to support this parameter. If the rollback segment/tablespace or transaction logs are limited by available hardware space, reduce the value of this parameter as appropriate.

- 5 Adjust the analyticsService.commitSize parameter. This parameter size is calculated as follows:
Identify the one entity that will have the most number of records from the following tables in the transaction database:

- SALESTRANS_LINE
- ATTRIBUTE_DEF_EFDT
- SALESTRANS_SALESREP

For example:

- SALESTRANS_LINE -50000 records
- ATTRIBUTE_DEF_EFDT - 20000 records
- SALESTRANS_SALESREP - 25000 records

The optimal value for this attribute is a number greater than 50000 as the SALESTRANS_LINE table has the most number of records. This value (50000) requires that you have a large enough rollback segment and tablespace in Oracle or transaction log in SQL to support this parameter. If the rollback segment/tablespace or transaction log are limited by available hardware space, reduce the value of this parameter as appropriate.

- 6 Locate the sqlserverDataFilesDir.dosstyle= field. Edit the default directory to match the location in which the transaction or analytics database resides.

NOTE: You must use double back slashes "\\" in this path.

Example: sqlserverDataFilesDir.dosstyle=C:\\Program Files\\Microsoft SQL Server\\MSSQL\\Data

- 7 Save sqlserver.properties.

Configuring the Oracle 8i/9i Database Properties Files

Edit oracle.properties as follows:

- 1** Adjust the transaction database variables as follows:
 - transactionDB.SID=SIEBELICM
 - transactionDB.user=siebelicm
 - transactionDB.password=siebel2003
 - transactionDB.data_tablespace=siebelicm_data
 - transactionDB.data_dir=/oradata/Siebel/data
 - transactionDB.index_tablespace=siebelicm_indexes
 - transactionDB.index_dir=/oradata/Siebel/indexes
 - transactionDB.temp_tablespace=temp
 - transactionDB.ltable_size=2500k
 - transactionDB.mtable_size=1000k
- 2** Set the transaction database jdbc connection information as follows:
 - jdbc.url.port=1521
- 3** Adjust the analytics database variables as follows:
 - analyticsDB.SID=SIEBELICM
 - analyticsDB.user= siebelicm_dw
 - analyticsDB.password= siebel2003
 - analyticsDB.data_tablespace=siebelicm_data_analytics
 - analyticsDB.data_dir=/oradata/SiebelICM/data
 - analyticsDB.index_tablespace=siebelicm_indexes_analytics
 - analyticsDB.index_dir=/oradata/SiebelICM/indexes
 - analyticsDB.temp_tablespace=temp
 - analyticsDB.ltable_size=2500k
 - analyticsDB.mtable_size=1000k
- 4** Set analytics database jdbc connection information as follows:
 - dwJdbc.url.port=1521
- 5** Adjust the database variables for the analytics stored procedures to match those set above:
 - DW_PREFIX= siebelicm_dw.
 - DW_SUFFIX=
 - TX_PREFIX= siebelicm.
 - TX_SUFFIX=

- 6** Adjust the `analyticsService.readingCommitSize` parameter to improve performance when running the `UpdateAnalytics` service.

This parameter size is calculated by finding the record type with the most number of custom fields and multiplying the number of fields by the number of records in the system.

For example: The combined number of custom fields on a transaction header and transaction line profile is 5, and the anticipated number of transactions to be processed in a single batch is 50,000. Multiply 5 X 50,000 and set this parameter to a value of 250,000. This value (250000) requires that you have a large enough rollback segment and tablespace in Oracle or transaction log in SQL to support this parameter. If the rollback segment/tablespace or transaction log are limited by available hardware space, reduce the value of this parameter as appropriate.

- 7** Adjust the `analyticsService.commitSize` parameter. This parameter size is calculated as follows:
Identify the one entity that will have the most number of records from the following tables in the transaction database:

- `SALESTRANS_LINE`
- `ATTRIBUTE_DEF_EFDT`
- `SALESTRANS_SALESREP`

For example:

- `SALESTRANS_LINE` - 50000 records
- `ATTRIBUTE_DEF_EFDT` - 20000 records
- `SALESTRANS_SALESREP` - 25000 records

The optimal value for this attribute is a number greater than 50000 as the `SALESTRANS_LINE` table has the most number of records. This value (50000) requires that you have a large enough rollback segment and tablespace in Oracle or transaction log in SQL to support this parameter. If the rollback segment/tablespace or transaction log are limited by available hardware space, reduce the value of this parameter as appropriate.

- 8** Save `oracle.properties`.

Installing Siebel ICM Application Server and Web Server

- 1** From the host server, open a command window by clicking Start > Run and then typing `cmd`.
- 2** Change directory to `INSTALLATION_ROOT`.
- 3** To set up the Web tier, type `setup.bat tomcat` in the command window.

This will copy the Tomcat files from the installation directory to `INSTALLATION_ROOT \Jboss-3.0.3_tomcat-4.1.12\tomcat-4.1.12`. Action results and errors are displayed in the command window.

- 4 To set up the application tier, type `setup.bat jboss` in the command window.

This step copies the JBoss files from the installation directory to `INSTALLATION_ROOT \Jboss-3.0.3_tomcat-4.1.12\tomcat-4.1.12`. Action results and errors are displayed in the command window.

Installing the Siebel ICM Database Tier

The following two tasks outline the way in the way in which you install the Siebel ICM database tier on the SQL Server database, and the Oracle Database.

Installing the Siebel ICM Database Tier on SQL Server

You can remotely install the database tier from the windows server even if it is on a UNIX Oracle instance. You must have the Oracle client tools installed on the windows machine in order to do this. If you do not, or cannot install the Oracle client tools on the windows machine, you must follow the instructions for installing the database tier on the UNIX host machine. See the UNIX Installation guide for instructions on how to do this.

You can remotely install the database on a SQL Server database with no additional work required.

- 1 From the host server, open a command window by clicking Start > Run and then typing `cmd`.
- 2 To set up the data tier, type `setup.bat transactionDB <dbusername> <dbpassword>` in the command window. `<dbusername>` is the database server's system administration user name, `<dbpassword>` is the database server's system administration password (Use "" if the system administration password is null), This copies the necessary database files from the installation directory to the hard drive.

Example: `setup.bat transactionDB user password`

- 3 To set up analytic and reporting functions, type `setup.bat analyticsDB <dbusername> <dbpassword>` in the command window. `<dbusername>` is the database server's system administration user name, `<dbpassword>` is the database server's system administration password (Use "" if the system administration password is null).

Example: `setup.bat analyticsDB user password`

- 4 Link the transaction and analytic databases by typing `setup.bat finishDB <dbusername> <dbpassword>`. `<dbusername>` is the database server's system administration user name, `<dbpassword>` is the database server's system administration password (Use "" if the system administration password is null).

Example: `setup.bat finishDB user password`

Installing the Siebel ICM Database Tier on Oracle

You can remotely install the database tier from the windows server even if it is on a UNIX Oracle instance. You must have the Oracle client tools installed on the windows machine in order to do this. If you do not, or cannot install the Oracle client tools on the windows machine, you must follow the instructions for installing the database tier on the UNIX host machine. See the UNIX Installation guide for instructions on how to do this.

You can remotely install the database on a SQL Server database with no additional work required.

To install the Siebel ICM database tier

- 1** From the host server, open a command window by clicking Start > Run and then typing cmd.
- 2** To set up the data tier, type setup_ora.bat transactionDB
Example: setup_ora.bat transactionDB
- 3** To set up analytic and reporting functions, type setup_ora.bat analyticsDB
Example: setup_ora.bat analyticsDB
- 4** Link the transaction and analytic databases by typing setup_ora.bat finishDB
Example: setup_ora.bat finishDB

Completing the Siebel ICM Server Installation

- 1** Start the server by executing the batch file located in INSTALLATION_ROOT \jboss-3.0.3_tomcat-4.1.12\bin\run.bat. The server is run in a separate command prompt window.
- 2** Populate the database by typing setup.bat populateSystem. This steps seeds the Siebel ICM instance with language/locale information as well as the symbol table.

All lingual dictionaries are populated in this step.

NOTE: At this point you will have a working Siebel ICM server accessible by browser at: <http://HOSTMACHINENAME:8080/Siebel>

You will now need to access the files. For more information, see *Siebel Incentive Compensation Management Configuration Guide*.

Jasper Reports Target Configuration and Execution

The Jasper files, report_groups.txt and report_acl.txt are located in following directories:

- {Siebel ICM Install Directory} \jboss-3.0.3_tomcat-4.1.12\reports\security\report_groups.txt
- {Siebel ICM Install Directory} \jboss-3.0.3_tomcat-4.1.12\reports\security\reports_acl.txt

The report_groups.txt defines groups of reports for display in the report menu. The file is a set of comma-separated lists with the following format:

■ <OUCode>.<Group Name>, <ReportName1>, <ReportName2>, <ReportNameN>

The Group Names for a given OU will always appear in alphabetical order in the UI. The Report Names will always appear in alphabetical order in the UI, as follows:

mainOU.Payout, CommissionDetailsByCustomer, PayoutStatement, PlanParticipantPayout

mainOU.ParticipantPerformance, ParticipantCumulatedPerformance,
ParticipantPerformanceCurrentPeriod

mainOU.Performance, ParticipantCreditRankingByOrganization,
ParticipantCumulatedPerformance, ParticipantPerformanceCurrentPeriod

mainOU.Transaction, TransactionSumForEventByProduct, ParticipantTransactionsByPeriod

mainOU.Modeling, CommissionDetailsByCustomer, RevenuePayoutAllPeriods

mainOU.ParticipantTransaction, ParticipantTransactionsByPeriod,
TransactionSumForEventByProduct

The report_acl.txt file relates the report groups defined in report_groups.txt to Operating Unit-specific security roles. The file appears in the following format:

■ <OUCode>.<SiebelICM Security Role Code>, <GroupName1>, <GroupName2>,
<GroupNameN>

The Group Names for a given OU and Role will always appear in alphabetical order in the UI, as follows:

mainOU.Participant, Payout, ParticipantPerformance, ParticipantTransaction

mainOU.Manager, Payout, Performance, Transaction

mainOU.Executive, Payout, Performance, Transaction

mainOU.ADMIN ROLE: mainOU, Payout, Performance, Transaction

To run configureAllRepots command

- 1 Run the setup_ora.bat set up step and select 'configureAllReports' under the JASPER REPORTING FRAMEWORK - REPORT INSTALLATION.

This will allow you to compile and publish all reports.

Verifying Proper Installation of Database Tiers

To verify proper installation of database tiers

- 1 Run the setup [tier] script once for each tier of your installation:

And verify the following tiers.

Tier	Description
tomcat	Installs web/JSPs into Tomcat4. In multiple application server (distributed) mode installation, this step must be performed for EACH server.
jboss	Installs EJBs into JBoss3. In multiple application server (distributed) mode installation, this step must be performed for EACH server.
transactionDB	Creates transaction database. (args: [sa user] [sa password]) For multiple application server deployment, execute this step ONLY on the controller application server, NOT for the processor/delegate application servers.
analyticsDB	Creates analytics database. (args: [sa user] [sa password]) For multiple application server deployment, execute this step ONLY on the controller application server, NOT for the processor/delegate application servers.
finishDB	Grants access between transaction and analytics databases. Also creates data synchronization procedures. (args: [sa user] [sa password]) For multiple application server deployment, execute this step ONLY on the controller application server, <i>not</i> for the processor/delegate application servers.
populateSystem	Seeds database with initial data. The JBoss/Tomcat application service must be fully started before executing this step. For multiple application server deployment, execute this step ONLY on the controller application server, <i>not</i> for the processor/delegate application servers.

- 2 Then verify Jasper setup by running the following command: `configureAllReports`.
This will compile and publish all reports.

Tier	Description
<code>compileReport</code>	Compiles the report specified in the <code>install.properties</code> file.
<code>fillReport</code>	Fills (runs queries) for the specified report and parameters specified in the <code>install.properties</code> file and produces a <code>.jrprint</code> file.
<code>htmlReport</code>	Reads the <code>.jrprint</code> file for the report specified in the <code>install.properties</code> file and exports it to html. You MUST run compile the report and run the <code>fillReport</code> task before running this task.
<code>pdfReport</code>	Reads the <code>.jrprint</code> file for the report specified in the <code>install.properties</code> file and exports it to PDF. You MUST run compile the report and run the <code>fillReport</code> task before running this task.
<code>viewReportDesign</code>	View the report design.
<code>cleanReports</code>	Deletes all generated files in your <code>reportcompile.dest.dir</code> .

Distributed Processing Mode

Siebel ICM provides the ability to install the application on multiple servers used to distribute the services processing. These servers are called Processors. These processors are grouped together by one central controller application server called Service Controller that can act as a processor as well. The configuration is the heterogeneous distribution system in which the Service Controller maintains the processors service state information and each service run's context information, and functions as Trace/Log master.

Node Specific Installation Instructions

For a Service Controller installation

- 1 Follow the instructions for a standard Siebel ICM installation, but during the ["Configuring the Server Properties Files"](#) on page 13, uncomment (by removing the leading #) and change the following properties in `install.properties`:

Parameter	Setting	Comments
<code>app.service.isSingleServer</code>	false	Setting to false tells the Service Controller that distributed processors exist.
<code>app.service.controller.host</code>	MACHINE_NAME	This is the machine name for the Service Controller.

Parameter	Setting	Comments
app.service.controller.port	1099	The JNDI port.
app.service.controller.isProcessor	True	If you want the Service Controller to also process, set this to true.
service.jms.queueConnectionFactory.jndiName	RMIXAConnectionFactory	Do Not Change.
app.cluster.url	PROCESSOR1:JNDI_PORT, PROCESSOR2:JNDI_PORT, PROCESSOR3:JNDI_PORT	A comma delimited list of Processor Machines. Each Processor must use the same port as the controller.
app.service.isAutoRecoverable	True	Leave this variable value set to true to active the fail over mechanism used by the Service Controller.

Parameter	Setting	Comments
mail.smtp.host	mail.MYCOMPANY.com	If you want the Service Controller to notify an administrator by email when a processor is down, uncomment this parameter and set it to the email address you want notified in the email related configuration section of this file.
app.admin.email	info@MYCOMPANY.com	If you want the Service Controller to notify an administrator by email when a processor is down, uncomment this parameter and set it to the email address you want notified in the email related configuration section of this file.

- 2** Create <MACHINENAME>.properties file and put it in INSTALLATION_ROOT
- 3** In the <MACHINENAME>.properties file, add the following line: app.service.isController=true
- 4** Save and close the install.properties file.
- 5** Continue with the standard installation instructions.

For each Processor machine

- 1** Follow the instructions for a standard Siebel ICM installation, but after the steps detailed in ["Configuring the Server Properties Files" on page 13](#), create a <MACHINENAME>.properties file and put it in INSTALLATION_ROOT.
- 2** In the <MACHINENAME>.properties file, add the following line: #app.service.isController=true
If you want to change the node-specific settings for this machine, you can override settings in install.properties by including one or more of the following overridden properties. These properties would be overridden to accommodate for differences in the machine's resources (CPU, RAM, Port number allocation, and so on).

- jboss.mdb.pool.size=2

- `jvm.memory.init=128`
- `jvm.memory.max=516`
- `jboss.port.NamingService=1099`

3 Save and close the <MACHINENAME> properties file.

4 Continue with the standard installation instructions.

Process for Configuring Authentication Modes

Siebel ICM supports four different Authentication and single sign on modes. To configure authentication modes, edit `INSTALLATION_ROOT\jboss-3.0.3_tomcat-4.1.12\server\default\conf\login-config.xml`

Native

Native Authentication mode ships out of the box. No changes are required to make this work. All user account authentication information is stored in the Siebel ICM database.

Siebel Databean

This allows users to be authenticated against an instance of Siebel Enterprise Server. The options here are used to build the connect string needed by the Siebel Data Bean login method.

Connect String syntax

`siebel[[:transport]][[:encryption]][[:compression]]]://host[:port]/EnterpriseServer/AppObjMgr[/SiebelServer]`

Naming conventions

- `siebelProtocol` = `siebel[[:transport]][[:encryption]][[:compression]]]` where `transport` = {`tcpip|http`} (default = `tcpip`)
- `encryption` = {`none | rsa`} (default = `none`)
- `compression` = {`none | zlib`} (default = `zlib`)
- `gatewayServer` = `hostname:port` where server is installed; aka "plwrk247:2320"
- `enterpriseServer` = "Siebel"
- `appObjManager` = the object manager for the application group you are authenticating against. Example is `FinsObjMgr`
- `siebelServer` = `hostname`
- `language` = Siebel language code. Example = "ENU"

Example XML config for Siebel Database Authentication

```

<login-module code = "com.motiva.ce.security.spi.SiebelLoginModule" flag =
"sufficient">

    <module-option name = "unauthenticatedIdentity">nobody</module-option>

    <module-option name = "multi-threaded">true</module-option>

<module-option name="connectString">siebel.TCPIP.none.NONE://<hostname>:2320/siebel/
FINSObjMgr_enu/<hostname></module-option>

    <module-option name="language">ENU</module-option>

</login-module>

```

Netegrity Siteminder

This module allows users to be authenticated against Netegrity Siteminder.

- 1** Put the login module XML snippet in place of the CastorLoginModule.
- 2** Put the Netegrity SDK jar files in the Jboss/server/default/lib directory. These files are
 - a** netegrity.jar
 - b** smjavaagentapi.jar
 - c** smjavasdk2.jar
- 3** Put the Netegrity SDK dll files are in the Jboss/bin directory. These files are:
 - a** SmAgentAPI.dll
 - b** smjavaagentapi.dll
- 4** Put your siteminder.properties in INSTALLATION_ROOT \Jboss-3.0.3_tomcat-4.1.12\bin directory.

Example XML Config for Siteminder

```

<login-module code = "com.motiva.ce.security.spi.NetegrityLoginModule" flag =
"sufficient">

    <module-option name = "unauthenticatedIdentity">nobody</module-option>

    <module-option name = "multi-threaded">true</module-option>

</login-module>

```

NT/Active Directory

This module which is only available on Windows NT and 2000 allows users to be authenticated against an NT domain. The module will request a user name, password and optionally domain (the domain to use may be named in the configuration file) and attempt to retrieve the user's credentials using them. Depending on settings in the config file the returned Principals may have human readable names (for example, administrator), NT SID format names (for example, S-1-5-32-544) or both.

NOTE: If the system on which authentication is performed is temporarily out of contact with its PDC it will not necessarily be able to return human readable names, but it will be able to return SID format names.

- 1 Put the login module XML snippet before the CastorLoginModule.
- 2 Make sure the NTSysm.dll is in INSTALLATION_ROOT \Jboss-3.0.3_tomcat-4.1.12\bin directory.
- 3 Configure the following parameters in the XML.
 - a returnNames Principals with human readable names will be created optional.
 - b returnSIDs Principals with names in NT SID format will be created optional.
 - c defaultDomain Domain to authenticate against - this is REQUIRED.

Example XML Config for NT/Active Directory Authentication

```
<login-module code = "com.motiva.ce.security.spi.NTLMLoginModule" flag = "sufficient">
  <module-option name = "unauthenticatedIdentity">nobody</module-option>
  <module-option name = "returnNames">true</module-option>
  <module-option name = "returnSIDs">>false</module-option>
  <module-option name = "defaultDomain">CORP</module-option>
  <module-option name = "multi-threaded">true</module-option>
</login-module>
```

Using IIS as a Front End HTTP Server

Configuring Siebel ICM with IIS

Siebel ICM uses Tomcat as the default HTTP Server. Companies requiring secure access to Siebel ICM, or those who have standardized on IIS, can use IIS as the HTTP Server in place of Tomcat. Tomcat will still continue to be used to generate the dynamic pages. Configuring Siebel ICM for use with IIS requires changes to Siebel ICM configuration files as well as manual configuration within IIS. The setup listed below outlines the configuration changes that need to be made for both HTTP and HTTPS access to the application. The steps below assume that IIS has been correctly installed and started.

The Jakarta/IIS documentation can be found in the following location:

■ <http://jakarta.apache.org/tomcat/tomcat-4.1-doc/jk2/jk2/installhowto.html>

For additional documentation on the JK2 Connector see:

■ <http://jakarta.apache.org/tomcat/tomcat-4.1-doc/config/jk2.html>

HTTP access to Siebel ICM using IIS

- 1 Open the install.properties file in a text editor. This file is located in INSTALLATION_ROOT.
- 2 Locate the app.host property in this file and replace localhost with your server's network ID.
NOTE: This value is copied into the tomcat41-service.xml file, and the IIS redirect (outlined below) will not work if the value for this property remains localhost.
- 3 Open a command window.
- 4 Navigate to INSTALLATION_ROOT.
- 5 Run setup tomcat.
- 6 Run setup jboss.
- 7 Open the workers2.properties file in a text editor. (Install Dir)\jboss-3.0.3_tomcat-4.1.12\tomcat-4.1.x\conf.
- 8 Change the value of the file property under the [shm] header to the correct location for your installation.
NOTE: Use back-slashes as file separators in this path.
EXAMPLE: file=[installation root]\jboss-3.0.3_tomcat-4.1.12\tomcat-4.1.x\bin\shm.file
file=C:\SiebelICM\jboss-3.0.3_tomcat-4.1.12\tomcat-4.1.x\bin\shm.file
- 9 Save the workers2.properties file.
- 10 Right-click on the IIS-Tomcat-RegEntries.reg file and select edit. (Install Dir)\jboss-3.0.3_tomcat-4.1.12\tomcat-4.1.x\conf
- 11 Set the absolute paths for properties serverRoot and workersFile to the correct locations for your installation (simply change the path to your installation's root directory for both variables).
NOTE: Use double back-slashes (\\) for path separators. The Windows registry requires this syntax.
- 12 Save the IIS-Tomcat-RegEntries.reg file.
- 13 Double-click the IIS-Tomcat-RegEntries.reg file to import the required registry settings.
- 14 Open the IIS management console; Start/Programs/Administrative Tools/Internet Services Manager.
- 15 Expand your machine name.
- 16 Right-click on Default Web Site and select New/Virtual Directory.
The Virtual Directory Creation Wizard window appears.

- 17** Click Next to continue.
- 18** Enter jakarta in the Alias field, then click next.
- 19** Click Browse and navigate to the directory containing the isapi_redirector2.dll file. (Install Dir)\jboss-3.0.3_tomcat-4.1.12\tomcat-4.1.x\bin.
- 20** Click Next.
- 21** On the Access Permissions screen select the following privileges
 - a** Read
 - b** Run scripts
 - c** Execute
- 22** Click Next, then click Finish.
- 23** Right-click on Default Web Site and select Properties.
- 24** Click the ISAPI Filters tab across the top of the Default Website Properties window.
- 25** Click Add.
- 26** Enter jakarta in the Filter Name field.
- 27** In the Executable field, click Browse and navigate to the following directory:
(Install Dir)\jboss-3.0.3_tomcat-4.1.12\tomcat-4.1.x\bin\isapi_redirector2.dll
- 28** Click OK.
- 29** Click OK.

NOTE: To verify that the ISAPI filter was loaded correctly, navigate back to Default Web site\Properties \ISAPI Filters. A green arrow, pointing up, should display next to the new jakarta filter.
- 30** Restart IIS.
- 31** Right-click your machine name in the Internet Information Services window.
- 32** Select Restart IIS.
- 33** Start Siebel ICM.
- 34** Test your configuration by accessing Siebel ICM on default HTTP port 80, <http://<machineID>/Siebel>.

HTTPS/SSL access to Siebel ICM using IIS

When using secure http (HTTPS) to access Siebel ICM you must disable the built-in HTTP connector in Tomcat so that all HTTP requests must go through IIS. If this step is not performed, client browsers will have access to the application on both port 80 (through IIS) and port 8080 (directly to Tomcat).

To disable Tomcat's HTTP listener:

- 1** Open tomcat41-service.xml in a text editor. INSTALLATION_ROOT\etc\jboss
- 2** Locate the HttpConnector entry.
EXAMPLE: <!-- A HTTP Connector on port 8080 -->
- 3** Comment out this entry by inserting an "!" before the text Connector Class.
EXAMPLE: <!--Connector className = "org.apache.catalina.connector.http.HttpConnector"
allowChunking= "false" port = "@tomcat.port.HttpConnector@" minProcessors = "5"
maxProcessors = "25" enableLookups = "false" acceptCount = "10" debug = "0"
connectionTimeout = "60000"/>
- 4** Open a command window.
- 5** Navigate to INSTALLATION_ROOT.
- 6** Run setup jboss.
- 7** A security certificate is required to run SSL with IIS.
NOTE: Security certificates are not provided by or supported by Siebel Client Care.
- 8** To assign your security certificate to the default Web site, right-click on Default Web Site.
- 9** Select Properties.
- 10** Click the Directory Security tab at the top of the Default Website Properties window.
- 11** Click Server Certificate.
The Welcome to the Web Server Certificate window will appear.
- 12** Click Next.
- 13** Select the method you want to use to obtain your security certificate, then click Next.
- 14** Follow the instructions in the Certificate wizard to assign a security certificate to this Web site.
- 15** Restart IIS.
- 16** Right-click your machine name in the Internet Information Services window.
- 17** Select Restart IIS.

Running Siebel ICM

Now that the software is installed on all three tiers, it is time to start the system and proceed to detailed configuration of the environment. Environment configuration is explained in Siebel ICM Advanced Setup. This section describes the procedures for starting up and stopping the Siebel ICM servers.

Starting

- 1** Ensure the transaction database and analytical database are running.

- 2 Open a command window by clicking Start > Run and then typing cmd.
- 3 Change directory to INSTALLATION_ROOT/ Jboss-3.0.3_tomcat-4.1.12/bin.
- 4 Type run to start all Siebel ICM services.

The Command window may be minimized, but not closed. Closing the Command window will shut down the server. In addition, logging out of the current session will also shut down the server. The Command window displays startup messages and errors. Important messages are archived in INSTALLATION_ROOT/Jboss-3.0.3_tomcat-4.1.12/server/default/log.

Stopping

- 1 Open a command prompt and change the directory to INSTALLATION_ROOT/ Jboss-3.0.3_tomcat-4.1.12/bin.
- 2 Type shutdown to stop the Siebel ICM services.

Siebel ICM service window will close when the services have been completely shut down.

Running Siebel ICM as a Windows Service

It is possible to run Siebel ICM as a background NT service enabling users to log off the machine when they are not using the application. Additionally this feature allows you to easily restart the application if regular maintenance requires that the server be rebooted.

- 1 Navigate to the installSiebel_ICM.bat file at INSTALLATION_ROOT\jboss-3.0.3_tomcat-4.1.12\bin.
- 2 Double-click the installSiebel_ICM.bat file.

A command window will appear and when the service has been successfully installed, a message will display.
- 3 Close the command window.
- 4 Click Start/Settings/Control Panel.
- 5 Double-click Administrative Tools.
- 6 Double-click Services.
- 7 Navigate down the list to SiebelICM.
- 8 Double-click SiebelICM.
- 9 In the Startup Type drop-down list, select Automatic.

NOTE: This will start the Siebel ICM services automatically when the server is rebooted.
- 10 Click the Start button in the Service Status section of the screen to start your new service.
- 11 Click OK.
- 12 Close the Services window.

For instructions on setting up System Administrator, Enterprise Units, and Operation Units with a working instance of Siebel ICM, see *Siebel Incentive Compensation Management Configuration Guide*.

4

Encrypted Passwords, User Names, and Log Files

This appendix describes features that allow you to encrypt certain data for security purposes. The topics in this appendix are as follows:

- [Encrypted Passwords and User Names](#)
- [Encrypted Log Files](#)

Encrypted Passwords and User Names

Currently, all user names and passwords are in clear text on the file system. This could be considered a security risk. To address this issue, a secure, reconnecting JDBC driver wrapper allows you to do the following:

- Encrypt user names and passwords in the JBOSS (or any application server) connection pool definition
- Have the wrapper decrypt the user names and passwords before connecting
- Reconnect if the database goes down or network connectivity is lost

To encrypt passwords and user names

- 1 In the pool definition (motiva-transactional-jdbc-service.xml) find the properties element and configure as follows:

```
<properties>

    <config-property name="ConnectionURL"
type="java.lang.String">jdbc:siebel:propsfile=D:\jboss-3.0.3_tomcat-
4.1.12\server\default\conf\siebel.jdbc.properties</config-property>

    <config-property name="DriverClass"
type="java.lang.String">com.siebel.jdbc.SecureReconnectingJDBCdriver</config-property>

    <config-property name="UserName" type="java.lang.String">c2E=</config-property>

    <config-property name="Password" type="java.lang.String">c2IYmVsMjAwMw==</
config-property>

</properties>
```

- The JDBC URL must begin with jdbc:siebel
- Point the propsfile= to the place on the disk where the siebel.jdbc.properties file will exist (more on this in step 3)
- The driver type is com.siebel.jdbc.SecureReconnectingJDBCdriver

- For the UserName and Password Elements, you must generate them if using encryption (see step 2), otherwise just enter them cleartext
- 2 If you will be using the encrypted user name/password feature, you need to encrypt the user name and password. Go to the directory that contains the siebeljdbc.jar (in my case this is D:\jboss-3.0.3_tomcat-4.1.12\server\default\lib). Execute the following command:

D:\jboss-3.0.3_tomcat-4.1.12\server\default\lib>java -cp siebeljdbc.jar
com.siebel.jdbc.SecureReconnectingJDBCUtils blah

Input = 'blah'

Encoded = 'YmxhaA=='

Decoded = 'blah'
 - Instead of 'blah' enter the value you want encrypted.
 - Use the Encoded value, in this case YmxhaA== in the appropriate element in the pool configuration file.
 - You must encrypt BOTH the user name and password if encryption is enabled.
- 3 Find and open the siebel.jdbc.properties file you will be using. Make sure it's in the proper location referred to by the "ConnectionURL" element in step 1. The following are the allowed parameters in the properties file:

reconnect.timeout=10000

reconnect.failure.count=100

jdbc.url=jdbc:inetdae7a:localhost:1433?database=OracleSid&sql7=true&useCursorsAlways=false&username=sa&password=siebel2003

driver.classname=com.inet.tds.TdsDriver

encryption.enabled=true

reconnect.timeout: If the database connection is down, how long should the reconnecting driver wait between reconnection attempts (in ms)

reconnect.failure.count: the maximum number of retries

jdbc.url: the actual real JDBC url for the underlying driver

driver.classname: the actual real JDBC driver type you will be using

encryption.enabled: are the user name and password encrypted, and thus they should be decrypted within the driver wrapper

Encrypted Log Files

During execution, the AUDIT log files for service execution could contain sensitive participant payout information. This could be considered a security risk.

To encrypt log files

- In the siebelicm-config.xml file, add the following elements:

```
<property name="logfile.viewer" value="com.motiva.ui.util.EncryptedLogfileviewer">  
<property name="logfile.encrypted" value="true"/>
```

- If logfile.encrypted = true, then the log will be written out encrypted, and a decrypting servlet will be used to view it.
- Large log files will take more time to render, and general processing will be slower, if you are writing out encrypted logs. You cannot process and view encrypted log files at the same speed as the unencrypted versions.

CAUTION: If you “mix modes,” you might experience unpredictable and undesired results. The decryption routines do not know the format of the logs they are decrypting. If you have a combination of encrypted and plaintext logs, the plaintext logs will be run through the decryptor along with the encrypted logs.

5

Glossary

This is a list of important terms used in this manual.

Application Tier

The “logic” tier of the Siebel Incentive Compensation Management system, containing the analytical engine, security features, user management interface, and transaction rules engine. The application tier uses the JBoss application server.

Data Tier

The largest tier of the system that houses the Oracle or Microsoft SQL database.

Enterprise Configuration

A distributed configuration of Siebel Incentive Compensation Management that houses one or more tiers on its own dedicated server.

Java Server Pages (JSP)

A technology that uses Java to modify Web pages before it is sent to a user. JSP technology configures Web page layout through Java servlets.

P.D.I.O.

A four-step plan for enterprise application deployment that stands for Planning, Development, Implementation, and Operation.

Servlet

A small, Java-based program that configures the layout or content of a Java Server Page (JSP).

Snapshot

A method of data backup that makes a full copy of a file system or directory and stores it to a separate file system, typically for a limited period of time. Snapshots are an excellent method of retrieving recently deleted or changed data without the effort and downtime associated with tape backups.

Stand-alone Configuration

A unified configuration of Siebel Incentive Compensation Management that houses all tiers on a single system. Stand-alone configurations are ideal for small groups or companies.

UNC Path

Short for Universal Naming Convention, a method of identifying shared files or directories in a networked environment. Typically takes the format of

```
\\servername\sharename\path\file
```

Web Tier

The tier of Siebel Incentive Compensation Management that serves the processed information from the data and application tiers and sends it to the Siebel Incentive Compensation Management client at the desktop.