IBM Cognos Incentive Compensation Management
Version 9.0.0

Installation and Configuration Guide

IBM
Note

Before using this information and the product it supports, read the information in “Notices” on page 97.

Product Information

This document applies to IBM Cognos Incentive Compensation Management Version 9.0.0 and may also apply to subsequent releases.

Licensed Materials - Property of IBM


US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
Contents

Introduction .............................................................................. vii

Chapter 1. Client installation preparation ................................. 1
Application overview ................................................................. 1
Installation files ....................................................................... 2
Preinstallation checklist ............................................................. 3
Microsoft SQL Server database permission and component requirements 
  Setting Up IBM Cognos Incentive Compensation Management as the database owner for Microsoft SQL Server 
  Changing the DEFAULT_SCHEMA through Microsoft SQL Server Management Studio 
  Changing the DEFAULT_SCHEMA using a query .......................... 4

Chapter 2. IBM Cognos Incentive Compensation Management client and Windows Service ............................................ 7
Installing the client ................................................................... 7
Installing the Windows Service .................................................... 7
  Setting the Windows Service to start automatically....................... 7
Configuration files ..................................................................... 8
  Client configuration file. ............................................................. 8
  Service configuration file .......................................................... 9
Upgrades .................................................................................. 15
  Standard upgrades .................................................................. 15
  Running simultaneous instances of IBM Cognos Incentive Compensation Management ................................. 20
Installation verification ............................................................ 21
  Opening an existing model to verify the installation ....................... 21
  Adding a model to verify the installation ...................................... 21
LDAP integration with the client ................................................... 22
  Configuring the Windows Service configuration file for LDAP authentication ......................................................... 23
  Granting LDAP users or LDAP groups access to the client .......... 24
Data Tier Performance Optimization ........................................... 24
  Common language runtime (CLR) integration ................................... 25
  Enabling Data Tier Performance Optimization in the client ........... 25

Chapter 3. Client tools ............................................................... 27
Console Service ....................................................................... 27
  Installing the Console Service .................................................. 27
  Editing the Console Service configuration file ............................. 27
  Starting the Console Service .................................................... 27
Configuration file encryption ...................................................... 28
  Installing the Configuration File Encrypter ................................. 28
  Running the Configuration File Encrypter ................................... 28
Model Converter ..................................................................... 29
  Installing the Model Converter tool .......................................... 29
  Converting a model from Microsoft SQL 2000 or 2005 to 2008 .... 29
  Converting a Microsoft SQL Standard Model to an Enterprise Model .......................................................... 30
  Converting a Microsoft SQL 2005 Standard Edition model to a 2008 Enterprise Edition model ......................... 30
  Reducing database size and calculation times ........................... 31
Certificates .............................................................................. 31
  Required software to use digital certificates ............................... 31
  Generating digital certificates for testing or troubleshooting ....... 32
  Setting up Microsoft Management Console to use digital certificates ............................................................ 33
  Root and server certificates ...................................................... 34
  Server IP address and port ...................................................... 35
  Configuring IBM Cognos Incentive Compensation Management to use certificates ........................................ 36
Command line interface ............................................................ 37
  Preparing for command-line interface installation ....................... 37
Installing IBM Cognos Incentive Compensation Management command-line interface ........................................ 38
Configuring digital certificates with the CLI ........................................................................................................ 38
Connecting to a model using the CLI .................................................................................................................. 38
Command-line interface commands .................................................................................................................. 39
Return code from the command-line interface .................................................................................................. 40
API ................................................................................................................................................................... 41
API architecture ................................................................................................................................................. 41
API access .......................................................................................................................................................... 42
API specifications for processing and calculation ............................................................................................... 43
API specifications for data management ............................................................................................................. 44
API specifications for data store ........................................................................................................................ 47
Object definitions .............................................................................................................................................. 48
Exception definitions ........................................................................................................................................ 51
Add-in for Microsoft Excel .................................................................................................................................. 52
Service-side setup for installing the Microsoft Excel add-in ............................................................................. 52
Client-side setup for installing the add-in ........................................................................................................... 54

Chapter 4. The IBM Cognos Incentive Compensation Management web client .................................................. 57
Installing the web client on the Solaris operating system ................................................................................... 57
Deployment of the web client with Apache Tomcat ............................................................................................ 58
Installing and configuring Java ............................................................................................................................ 58
Installing and configuring Apache Tomcat ........................................................................................................ 58
Using Apache Tomcat to deploy the web client ................................................................................................. 58
Using Apache Tomcat to configure database access ....................................................................................... 58
Configuring multi-language and Unicode data support for Apache Tomcat .................................................... 59
Deployment of the web client with JBoss .............................................................................................................. 60
Installing and configuring Java for JBoss ........................................................................................................... 60
Installing and configuring JBoss ........................................................................................................................ 60
Configuring database access for JBoss ............................................................................................................... 60
Using JBoss to deploy the web client ................................................................................................................ 61
Configuring multi-language and Unicode data support for JBoss ............................................................... 62
Deployment of the web client with IBM WebSphere 7 ...................................................................................... 62
Deploying the web client on WebSphere 7 .......................................................................................................... 63
Configuring database access using WebSphere 7 ............................................................................................. 63
Using the WebSphere Admin Console to start the web client ..................................................................... 64
Setting a web container custom property on WebSphere .............................................................................. 64
Configuring multi-language and Unicode data support for WebSphere ...................................................... 65
Deployment of the web client with WebSphere 9 ............................................................................................... 65
Property file encryption ..................................................................................................................................... 67
 Obtaining encrypted passwords ........................................................................................................................ 68
 Configuring web client password encryption ................................................................................................ 68
 Configuring web client password encryption in a Windows environment ................................................. 69
 Deployment of the web client with encrypted passwords ............................................................................... 69
 Configuring multi-language and Unicode data support for locale .............................................................. 69
 Emailing users when an inquiry is pending ...................................................................................................... 70
 Preventing Presenter reports from loading with a large amount of data ..................................................... 70
 Presenter report data grid row limits ................................................................................................................ 71
 Disabling collection of Presenter report information ..................................................................................... 71
 Web client appearance ..................................................................................................................................... 71
 Web tab configuration ....................................................................................................................................... 72
 Changing the web client theme ......................................................................................................................... 74

Chapter 5. Authentication and sign on .................................................................................................................. 75
Communication path options ............................................................................................................................. 75
 Security options for communications between the client and the application server .................................. 75
 Security options for communications between the application server and the database server .................. 75
 Communication methods between the web client and the web application ............................................... 76
 Encryption methods for communication between the web application server and the database server .... 76
 Authentication options ...................................................................................................................................... 76
 SiteMinder configuration .................................................................................................................................. 77
Introduction

This document is intended for use with IBM® Cognos® Incentive Compensation Management Version 9.0.0.

IBM Cognos Incentive Compensation Management enables organizations to automate the process of administering, calculating, reporting, and analyzing variable-based pay programs. The solution simplifies incentive compensation management for organizations by increasing accuracy, reducing costs, and improving visibility into sales performance and compensation plans.

Audience

This guide is intended for users who will be installing and configuring the IBM Cognos Incentive Compensation Management client and web client.

Finding information

To find documentation on the web, including all translated documentation, access IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter).

Publication date

This document was published on April 13, 2017.

Accessibility features

Accessibility features help users who have a physical disability, such as restricted mobility or limited vision, to use information technology products.

Forward-looking statements

This documentation describes the current functionality of the product. References to items that are not currently available may be included. No implication of any future availability should be inferred. Any such references are not a commitment, promise, or legal obligation to deliver any material, code, or functionality. The development, release, and timing of features or functionality remain at the sole discretion of IBM.
Chapter 1. Client installation preparation

IBM Cognos Incentive Compensation Management is a valuable tool that can be used to manage payment for individuals receiving variable compensation, including the sales force, management, or distribution channels.

Cognos Incentive Compensation Management enables organizations to design, manage, and automate the calculation of variable payment for dozens of plans and thousands of employees simultaneously. The application includes several context sensitive dialogs and wizards designed to guide you through performing tasks.

To review an up-to-date list of environments supported by Cognos Incentive Compensation Management, such as operating systems, browsers, web servers, database servers, and application servers, see Software Requirements (http://www.ibm.com/support/docview.wss?uid=swg27041272).

Application overview

IBM® Cognos® Incentive Compensation Management is a distributed N-Tier application.

The following applications make up the integrated solution:

Client Contains the user interface for getting work done.

Application server Contains the business logic, calculation engine, and business event scheduler.

Database server Stores data for the Cognos Incentive Compensation Management model, such as dimension information and computed results.

A number of different database servers, including Microsoft SQL Server (2005, 2008, or 2012), are supported.

The following points outline the details of the client:

• Provides the model administrator with several administrative options, including new model creation, table customization, data import, calculation, and multiple reporting modes
• Resides on the workstation of each model administrator
• Communicates with the server in a true distributed environment and uses a configuration file to specify the location of the application server
• Communicates with the application server through an encrypted channel that is written in C# using the Microsoft .NET framework

The following points outline the details of the application server:

• The application layer can be run as a process on one or more servers to provide scalability
• Contains the business logic for the model
• Houses the calculation engine for processing data
• Uses the data layer to communicate with the specified database
Contains the Cognos Incentive Compensation Management Scheduler, which schedules and executes business events

Written in C# using the Microsoft .NET framework, which results in a highly stable product

### Installation files

The IBM® Cognos® Incentive Compensation Management application comes with several installation files.

To use the application, the client must be installed on the administrator's workstation, and the Cognos Incentive Compensation Management Windows Service must be installed and running on the server. Tools such as Model Upgrader, Model Converter, CLI, the Cognos Incentive Compensation Management add-in for Microsoft Excel, and Configuration File Encrypter can be installed but are not required for running the core application.

All tools and components of the client must be on the same product version. If you are upgrading the client and service, all other Cognos Incentive Compensation Management tools that are used with the core administrative application must be upgraded as well.

#### Table 1. Installation Files

<table>
<thead>
<tr>
<th>Application Components and Tools</th>
<th>Installation File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cognos Incentive Compensation Management client</td>
<td>ICM-client.exe</td>
<td>The Cognos Incentive Compensation Management client must be installed to run the application.</td>
</tr>
<tr>
<td>Cognos Incentive Compensation Management Windows Service</td>
<td>ICM-service.exe</td>
<td>The Cognos Incentive Compensation Management Windows Service (or Console Service) must be installed and running.</td>
</tr>
<tr>
<td>Console Service</td>
<td>ICM-console.exe</td>
<td>The Console Service can be run as an alternative to the Cognos Incentive Compensation Management Windows Service. It is not required if the Cognos Incentive Compensation Management Windows Service is being used.</td>
</tr>
<tr>
<td>Command-Line Interface (CLI)</td>
<td>ICM-cli.exe</td>
<td>The Command-Line Interface installer must be run to use the CLI tool. It is not required for the core application.</td>
</tr>
<tr>
<td>Cognos Incentive Compensation Management add-in for Microsoft Excel</td>
<td>ICM-exceladdin.exe</td>
<td>The Cognos Incentive Compensation Management add-in for Microsoft Excel installer must be run to use the tool. It is not required for the core application.</td>
</tr>
</tbody>
</table>
Table 1. Installation Files (continued)

<table>
<thead>
<tr>
<th>Application Components and Tools</th>
<th>Installation File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration File Encrypter</td>
<td>ICM-encrypter.exe</td>
<td>The Configuration File Encrypter installer must be run to use the Configuration File Encrypter. It is not required for the core application.</td>
</tr>
<tr>
<td>Model Converter</td>
<td>ICM-modelconverter.exe</td>
<td>The Model Converter installer must be run to convert models to a different version of Microsoft SQL Server. It is required only for model conversion.</td>
</tr>
<tr>
<td>Model Upgrader</td>
<td>ICM-modelupgrader.exe</td>
<td>The Model Upgrader tool must be installed to upgrade your model to a newer version. If the client and service are upgraded, existing models must also be upgraded to work on the new version of the software.</td>
</tr>
</tbody>
</table>

Preinstallation checklist

Before installing the IBM Cognos Incentive Compensation Management application, you must perform some preinstallation tasks.

Before beginning the installation, make sure you have performed the following steps:

1. Download the Cognos Incentive Compensation Management installation files.
2. Install Microsoft .NET Framework 4.5 on both the server and client (can be downloaded from [http://www.microsoft.com/downloads](http://www.microsoft.com/downloads)).
4. Grant administrator access to all computers involved.
5. Grant sufficient database user rights or be the database owner.

Microsoft SQL Server database permission and component requirements

When you deploy IBM® Cognos® Incentive Compensation Management on a Microsoft SQL Server, Cognos Incentive Compensation Management does not require administrative access to the database server, but database ownership rights must be granted to access your database.

When you install a model, make sure that Cognos Incentive Compensation Management is set up as the database owner (dbo).

If it is not possible to grant dbo rights, a user with the following minimum permission requirements must be created:

- Connect
- Create Table
• Create View
• Execute
• Select
• Delete
• Insert
• Update
• View Database State

**Important:** Granting Cognos Incentive Compensation Management dbo rights is preferred.

You must also install the following components within Microsoft SQL Server. These components must be installed on the same server where the Varicent Service is being installed:
• Client Tools Connectivity
• Integration Services
• Client Tools Backwards Compatibility
• Client Tools SDK

SSIS components must be installed on the application server, where the Cognos Incentive Compensation Management service is hosted, and not on the database server. To install these components, you must run the Microsoft SQL Server installer and select the check boxes next to each component in the Feature Selection step. These components can also be installed in the same way on pre-existing installations of SQL Server.

**Important:** The Windows Service for SQL Server Integration Services does not need to be started to import data into Cognos Incentive Compensation Management. In this way, you can free up more memory on the application server.

**Setting Up IBM Cognos Incentive Compensation Management as the database owner for Microsoft SQL Server**

You must create a database user to be used by Cognos Incentive Compensation Management to access the database, and then make this user the database owner.

**Procedure**
1. Create a database user (ICMDBUser) to be used by Cognos Incentive Compensation Management to access the database.
2. Log in to Microsoft SQL Server as an administrator.
3. Connect to the database used by Cognos Incentive Compensation Management (ICMDBase).
4. Run the following script:
   ```sql
   USE [ICMDBase]
   GO
   IF EXISTS (SELECT*FROM dbo.sysusers WHERE name=N'ICMDBUser')
   EXEC dbo.sp_revokedbaccess N'ICMDBUser';
   GO
   sp_changedbowner N'ICMDBUser'
   ```
5. If you are using Microsoft SQL Server 2005, there are the following additional security options:
   • ICMDBUser needs to have database creation rights to the ICMDBase
ICMDBUser must have the `DEFAULT_SCHEMA` property set to `dbo`. This can be done either through Microsoft SQL Server Management Studio or with a query.

**Changing the DEFAULT_SCHEMA through Microsoft SQL Server Management Studio**

The default schema for the IBM® Cognos® Incentive Compensation Management database user can be changed to database owner through the Microsoft SQL Server Management Studio.

**Procedure**

1. In Microsoft SQL Server Management Studio, expand the `ICMDatabase` folder.
2. Expand the `Security` folder.
3. Expand the `Users` folder.
4. Right-click the `ICMDBUser` and click `Properties`.
5. Type or select `dbo` in the `Default Schema` field.

**Changing the DEFAULT_SCHEMA using a query**

The default schema of the IBM® Cognos® Incentive Compensation Management database user can be changed to the database owner through a query.

**Procedure**

1. Connect to the `ICMDatabase` with an SQL client.
2. Log in with an administrator account.
3. Run the following query:
   ```sql
   ALTER USER "ICMDBUser" WITH DEFAULT_SCHEMA dbo;
   ```
Chapter 2. IBM Cognos Incentive Compensation Management client and Windows Service

Both the IBM® Cognos® Incentive Compensation Management client and the Windows Service must be installed and running before you can use the Cognos Incentive Compensation Management application.

The client is required to allow authorized users to create models, customize tables, import data, create calculations, and report on results. For the client to run properly, the service (or Console Service) must also be installed and running.

Installing the client

The IBM Cognos Incentive Compensation Management client must be installed in order to run the application. The client should be installed on the administrator’s desktop.

Procedure
1. Double-click the ICM-client.exe installation file located in your release folder.

   Important: If you are upgrading Cognos Incentive Compensation Management, refer to the instructions on upgrading.
2. Complete the steps in the installation wizard.

Installing the Windows Service

The IBM® Cognos® Incentive Compensation Management Windows Service must be installed and running on the server for the application to run properly.

About this task

The Windows Service must be installed on the application server. You must have the Cognos Incentive Compensation Management Windows Service or the Console Service installed and running to log in to the client.

Procedure
1. Double-click the ICM-service.exe installation file in your release folder.
2. Select the Default installation option and click Next on the installer welcome screen.

   Important: If you are upgrading Cognos Incentive Compensation Management, see the instructions on upgrading.
3. Complete the steps in the installation wizard.

   Important: By default, the Cognos Incentive Compensation Management Windows Service startup type is set to manual, which means that you must manually start the Service each time that you want to open the client.

Setting the Windows Service to start automatically

You can change the startup type of the IBM Cognos Incentive Compensation Management Windows Service from manual to automatic.
Procedure
2. In the Services panel, select IBM Cognos ICM Service.
3. Right-click and select Properties.
4. Select Automatic as the Startup type.

Configuration files
When installing or upgrading IBM Cognos Incentive Compensation Management, you must edit the configuration files.

The following configuration files must be modified:
- IBM Cognos ICM.exe.config on the administrator's workstation
- IBM Cognos ICM Windows Service.exe.config on the application server

If you are upgrading an existing version of Cognos Incentive Compensation Management, save a copy of the IBM Cognos ICM Windows Service.exe.config file and IBM Cognos ICM.exe.config file to use for comparison with the upgraded configuration files. Make sure that the application settings in the new configuration files match the settings in the saved configuration file from the previous version.

Attention: You can comment out lines in the configuration file, that is lines that you do not want to use, by adding <!-- to the beginning of those lines. If you are commenting lines out, make sure that you comment out the entire section and not just the first line of that section.

Client configuration file
You must edit the IBM Cognos ICM.exe.config file to specify how the IBM® Cognos® Incentive Compensation Management client communicates with the application server.

When you install Cognos Incentive Compensation Management, you must replace all instances of localhost with the name or IP address of your application server. This change must be made to the configuration file that is located in the same directory as the IBM Cognos ICM.exe file.

The following configuration sections in the IBM Cognos ICM.exe.config file must be edited:
- Environments
- appSettings

Configuring the environments for your models
You can specify the environments for your models in the Environments section of the IBM® Cognos® Incentive Compensation Management Windows Service configuration file.

Procedure
1. Edit the environment name.
   This can be any name you give to your environment, such as Production, Development, or Quality Assurance.
2. Edit the securityMode. This determines how communication is to be encrypted between the client and Windows Service. The following three settings are available:
Transport layer security mode
Clients are unauthenticated by the Windows communication framework. The server must provide a trusted certificate for authentication.

Window security mode
Clients and servers are authenticated via Kerberos using the domain controller as a trusted third party. No certificates are required.

Unprotected mode
All security is disabled.

3. Edit the serviceAddress.
This indicates the port that the Service is using. Each environment must be configured to use a different port.

Important: Security settings for both the Service configuration file (IBM Cognos ICM Windows Service.exe.config) and the client configuration file (IBM Cognos ICM.exe.config) must be configured to run on the same security mode. Update both files accordingly.

AppSettings configuration
In the IBM Cognos Incentive Compensation Management configuration file, the AllowMultipleInstances value determines whether multiple models can be open simultaneously on one computer. The default language of the client can also be set in this section.

Typically, users only need one client instance to be open on a computer. Some clients, however, must run the client on a terminal server and have multiple clients.

The following example shows an IBM Cognos ICM.exe.config file configuration that allows users to have multiple models open at the same time on one computer:

```xml
<appSettings>
  --> Allowing Multiple Instance -->
  <add key="AllowMultipleInstances" value="true"/>
</appSettings>
```

To set the default language of the client, uncomment and edit the following setting:

```xml
<add key="DefaultLanguage" value="EnglishUS"/>
```

Service configuration file
The IBM Cognos Incentive Compensation Management Service configuration file indicates how the application server communicates with the database server.

The Service configuration file (IBM Cognos ICM Windows Service.exe.config) is in the same directory as the Cognos Incentive Compensation Management configuration file (IBM Cognos ICM Windows Service.exe).

Configuring database server settings
You must edit the <databaseServers> block in the IBM Cognos Incentive Compensation Management Windows Service configuration file to correspond with your database server. By default, the file is set up to connect to a Microsoft SQL Server 2008 database.

Procedure
1. Open the IBM Cognos Windows Service.exe.config file.
2. In the databaseServers section, complete the following steps:
a. Edit the database server name.
   This can be an arbitrary name, such as Super Server, and is intended to identify and distinguish the database server. If your database is a Microsoft SQL Server 2000 named instance, or if you are using a Microsoft SQL Server 2005 database, the value for the DB Server field must use the following format: SERVER_NAME\INSTANCE_NAME.

b. Edit the User.
   User is the same as the database user. For Microsoft SQL Servers, Cognos Incentive Compensation Management requires SQL Authentication or Windows Authentication to connect. Therefore, you must use a local database user to connect. If you are using Windows Authentication, both the user and password values must remain blank.

c. Type the Password.
   This is the password that corresponds to the database user.

d. Edit the Address.
   This address points to the location of the database. Use the following format for the address: SERVER_NAME\INSTANCE_NAME. If SQL Server is not using the default port 1433, you must add the port number to the server address field (for example, SERVER_NAME\INSTANCE_NAME, PORT_NUMBER).

e. Edit the Type of database.

f. Edit the DiskPath.
   This is the location where databases are created and stored.

g. Edit the LogPath.
   This is the location where the log file is created and stored.

h. Modify the TimeoutSeconds.
   This is the number of seconds before a timeout occurs. The database timeout default is 90 seconds. This is the minimum amount of time that clients must wait before Cognos Incentive Compensation Management can warn of a network or server issue. For models with long calculation times, you can increase this time to avoid a database timeout during calculation.

**Configuring access to multiple databases**
If you have multiple database servers, you can configure multiple database settings in the IBM Cognos ICM Windows Service.exe.config file.

**About this task**

When you configure multiple database settings, you can access both Unicode and non-Unicode SQL models with a single service. By default, there is only one section in the configuration file, but others can be added. All models that are contained on each database server in the service configuration file are accessible from the login screen.

**Procedure**

2. Complete a <databaseServer> section for each of your servers.

   **Important:** Cognos Incentive Compensation Management cannot run without a service. It is not possible to enter database information in the IBM Cognos ICM.exe.config file to bypass the service and access the database directly.
The following example shows a configuration for a non-Unicode Microsoft SQL server model and a Unicode Microsoft SQL Server model to run on the same Cognos Incentive Compensation Management Windows Service.

```xml
<databaseServers>
  <databaseServer Name="NonUnicodeModel"
    Address="(local)"
    Type="SQLServer2008"
    User="sa"
    Password=""
    DiskPath="D:\"
    LogPath="D:\"
    TimeoutSeconds="90">
  </databaseServer>
  <databaseServer Name="UnicodeModel"
    Address="(local)"
    Type="SQLServer2008unicode"
    User="sa"
    Password=""
    DiskPath="D:\"
    LogPath="D:\"
    TimeoutSeconds="90">
  </databaseServer>
</databaseServers>
```

Configuring Windows Service settings
After configuring database server settings, you can modify different sections in the IBM Cognos Incentive Compensation Management Windows Service configuration file to suit your Cognos Incentive Compensation Management Windows Service requirements.

Procedure
1. Modify the `ServiceAddress` value and `port` value to point to the server name and port where the Cognos Incentive Compensation Management Windows Service is located and running, such as localhost:13105.
2. Modify the `SecurityMode` value. This determines how communication is to be encrypted between the client and the Windows Service. The following settings are available:
   - Transport layer security (TLS) mode
     Clients are unauthenticated by the Windows communication framework. The server must provide a trusted certificate for authentication.
   - Windows security mode
     Clients and servers are authenticated via Kerberos using the domain controller as a trusted third party. No certificates are required.
   - Unprotected mode
     All security is disabled.

Attention: Security settings for both the Cognos Incentive Compensation Management Windows Service (IBM Cognos ICM Windows service.exe.config) and the Cognos Incentive Compensation Management Client (IBM Cognos ICM.exe.config) must be configured to run on the same security mode. Update both files accordingly.
3. If you are using TLS mode, modify the `ServiceCertificateName` to the subject name of a certificate stored in the Windows Personal Certificate Store to be used for authentication in the Cognos Incentive Compensation Management Windows Service.
4. If you are using the Cognos Incentive Compensation Management API Service, modify the **APIAddress** and **value** to point to the server name and port where the Cognos Incentive Compensation Management API Service is located and running, such as localhost:13115.

5. If you are using certificates with the IBM Cognos ICM API Service, modify the **APISecureAddress** and **value** to the server name and port where the Cognos Incentive Compensation Management API Service is located, running securely, and requiring certificate authentication, such as MobileAPI:13125.

6. If you are using certificates with the Cognos Incentive Compensation Management API Service, modify the **APICertificateName** to the subject name of a certificate (CN) stored in the Windows Personal Certificate Store to be used for authentication in the API Service.

**Changing Windows Service communication to HTTP or HTTPS**

The communication method between the IBM® Cognos® Incentive Compensation Management client and the Windows Service can be changed to HTTP or HTTPS communication by editing the settings in the Windows Service configuration file and client configuration file. By default, TCP communication is used.

**Procedure**

1. In the Cognos Incentive Compensation Management Windows Service configuration file, uncomment the **HTTP Communication mode** section and comment out the **TCP Communication mode** section.

2. To use HTTP communication, change the **SecurityMode** value to **None**.

3. To use HTTPS communication, change the **SecurityMode** value to **TLS**.
   a. Change the **HttpsDefaultUsername** and **HttpsDefaultPassword** values to the user name and password that are used to authenticate the Cognos Incentive Compensation Management environment and database.

4. Change the **CommunicationMode** and **SecurityMode** values in the client configuration file to the same values as those in the Windows Service configuration file. If you are using HTTPS communication, change the **HttpsDefaultUsername** and **HttpsDefaultPassword** values in the client configuration file to the same values as those in the Windows Service configuration file.

   **Important:** Security settings for both the Cognos Incentive Compensation Management Windows Service (IBM Cognos ICM Windows Service.exe.config) and client (IBM Cognos ICM.exe.config) must be configured to run on the same security mode. Update both files accordingly.

**Configuring settings**

After you configure database access, you can configure settings for Scheduler and Task Manager in the IBM® Cognos® Incentive Compensation Management Windows Service configuration file.

**Procedure**

1. In the **ICM** section, edit the **SchedulerUser** and **SchedulerPassword** values to match the user ID and password of the user who has the Scheduler role in the Manage Users window in the Cognos Incentive Compensation Management client. If **SchedulerUser** and **SchedulerPassword** are not updated here after they are changed in the client, the scheduled processes cannot run.

   **Important:** To run Scheduler, the Cognos Incentive Compensation Management Windows Service must be run as a Windows Service. Make sure that Scheduler
and the Cognos Incentive Compensation Management API Windows Service are started before you schedule any process.

2. You can edit the SchedulerLogPath value to update the location of the Scheduler log. By default, this log is in the Service directory. The SchedulerLogPath must be updated if the Windows Service is not installed to the default directory.

3. You can edit the TaskManagerLogPath value to update the location of the Task Manager log. By default, this log is in the Service directory. The TaskManagerLogPath must be updated if the Windows Service is not installed to the default directory.

4. You can edit the AllowAnonymousModelCreation value to determine whether administrators can create new models. If this value is set to False, new models cannot be created.

5. You can edit the Language value to the language that you want to use in the Audit module logs.
   - If you set the Language to EnglishUS, the date format is set to month/day/year.
   - If you set the Language to EnglishGB, the date format is set to day/month/year.

6. You can uncomment and edit the Saved Import File Directory value to point to the location where Cognos Incentive Compensation Management looks for source files for any of its data imports. This setting must be determined before any imports can be saved within Cognos Incentive Compensation Management and must refer to a directory on the same computer as the Windows Service.

7. You can uncomment and edit the Saved Publisher File Directory value to point to the location where Cognos Incentive Compensation Management places published files that are scheduled for publishing in Scheduler. This setting must be determined before publishing can be scheduled, and the setting must refer to a directory on the same computer as the Windows Service.

8. You can uncomment and edit the Saved Image File Directory value to point to the location where Cognos Incentive Compensation Management looks for image files to be used as header graphics for scheduled PDF file publishing. This setting must refer to a directory on the same computer as the Windows Service.

Configuring external tools
The External Tools Directory section determines the items that can be used to schedule and run processes that exist outside of IBM® Cognos® Incentive Compensation Management. Any external tools that you plan to schedule by Scheduler must be in the External Tools Directory.

Procedure
1. Uncomment and edit the ExternalToolDirectory section to point to the location where Cognos Incentive Compensation Management looks for items that are used outside of Cognos Incentive Compensation Management.

2. To modify the maximum run time that Scheduler allocs for the tool to run, click the Properties button in the Scheduler module in the Cognos Incentive Compensation Management client. After that time expires, Scheduler continues down the list of actions to complete.
Configuring email SSL settings
If the server is configured to send emails, the connection to the email server can be encrypted with Secure Sockets Layer (SSL) in IBM® Cognos® Incentive Compensation Management.

Procedure
1. Uncomment the line under Email SSL Settings.
2. Set the EnableSSLForServerEmails entry to True.

Configuring IBM Cognos Incentive Compensation Management mobile settings
Cognos Incentive Compensation Management can be configured to send data to handheld devices.

Procedure
1. To enable handheld device configuration in Cognos Incentive Compensation Management, set the EnableHandheld value to True and uncomment the line.
2. You can modify the MobileDataSynchFrequency value to indicate how frequently (in seconds) data on a handheld device running Cognos Incentive Compensation Management Mobile will be synchronized with the data accessible through the Cognos Incentive Compensation Management API Service, such as 3600.

Mail settings configuration
To use the Portal Access email reminder system, the mail settings must be configured in the IBM® Cognos® Incentive Compensation Management Windows Service configuration file.

Your system administrator can provide you with details of your company’s mail server.

The Cognos Incentive Compensation Management web client uses the email address and server in the Cognos Incentive Compensation Management Windows Service configuration file for sending out emails from Scheduler, for example, when a task fails for Portal Access period posts or when an administrator forces the approval of a period.

The smtp from field is usually set to the administrator’s email address. When Portal Access emails are generated, they are sent from this email address.

To send emails from Portal Access, edit the following section of the Cognos Incentive Compensation Management Windows Service configuration file:

```
<system.net>
 <mailSettings>
 <smtp from="softco@softco.com">
 <!-- Set defaultCredentials="false" if using SSL for Email -->
 <network host="mail.softco.com" port="25" username="username" password="password"
 defaultCredentials="true"/>
 </smtp>
 </mailSettings>
</system.net>
```

Setting the email address of the administrator
The email address of the IBM® Cognos® Incentive Compensation Management administrator must be set in the client.
**Procedure**

1. Log in to the Cognos Incentive Compensation Management client.
2. Click **Admin > Manage Users**.
3. Select the administrator.
4. Click **Edit**.
5. Set the email address.

**Managing Portal Access email settings**

You can choose to email users about sign offs and inquiries available for review in the IBM Cognos Incentive Compensation Management web client.

Emails to users when a sign off is pending are initiated from the client, so email settings must be configured in the Cognos Incentive Compensation Management Windows Service (or Console Service) configuration file. Emails to users when an inquiry is pending are initiated from Cognos Incentive Compensation Management web client, so email settings must be configured in the `mail.properties` file.

**Procedure**

1. To send emails to users when a sign off is pending, you must configure the email settings in the Cognos Incentive Compensation Management Windows Service configuration file.
   - If you are using the Console Service, the email setting must be configured in the Console Service configuration file.
2. To send emails to users when an inquiry is pending, you must configure the email settings in the `mail.properties` file.
   - The `mail.properties` file is located in the following directory: `...\webapps\IBM Cognos ICM\WEB-INF`. You must make changes to the following section:
     ```
     mail.host=smtp.yourdomain.com
     mail.port=25
     mail.username=username
     mail.passowrd=secret
     mail.from=varicent@yourdomain.com
     ```
3. In the Client, select **Admin > Administrative Options**.
4. Under the **Portal Access** tab, select **Email users when a sign off is pending** or **Email users when an inquiry is pending** or both.
5. Click **OK**.
   - **Attention:** You must reload the ICM.war file after making changes to the `mail.properties` configuration file.

**Upgrades**

The IBM® Cognos® Incentive Compensation Management application can be updated with the latest fixes and enhancements.

There are two ways to upgrade. You can perform a standard upgrade to replace the initial installation, or you can install a new service to run parallel with the initial installation.

**Standard upgrades**

A standard upgrade replaces the existing version of IBM® Cognos® Incentive Compensation Management with a new version.
For example, if you upgrade from version 7 to version 8, version 7 is no longer available on your computer after the upgrade. If you upgrade a model older than version 8.1.0, before you can install the new version of Cognos Incentive Compensation Management, the previous version of Cognos Incentive Compensation Management must be removed. When you upgrade version 8.1.0 models or newer, the upgrade process overwrites the existing version.

All tools and components in Cognos Incentive Compensation Management must be the same version. Therefore, even optional tools, such as the Cognos Incentive Compensation Management add-in for Microsoft Excel and Cognos Incentive Compensation Management CLI, must be removed and replaced with the newer version.

**Preparing to upgrade**

Before you upgrade your IBM® Cognos® Incentive Compensation Management installation, you must prepare to ensure that your upgrade is successful.

**About this task**

Back up any existing Cognos Incentive Compensation Management models before you upgrade. Save copies of your configuration files so that database and environment settings can be compared with the settings in the configuration files in the upgraded version. When you upgrade, the settings in the Cognos Incentive Compensation Management Windows Service configuration file and the Cognos Incentive Compensation Management configuration file must be manually updated.

**Important:** If you are upgrading a model that contains star schemas that were created with calculations, you receive an error message when you try to upgrade your model. As of version 8.0.4, star schemas must be created with data stores. Before you upgrade your model, you must delete any star schemas that were created with calculations and create them with data stores.

**Procedure**

1. Back up your configuration files. If you are upgrading an existing version of Cognos Incentive Compensation Management, you must back up the following files:
   - IBM Cognos ICM.exe.config
   - IBM Cognos ICM Windows Service.exe.config
   - jdbc.properties

   **Important:** You cannot use your existing configuration files with an upgraded version.

2. Uninstall the current version of Cognos Incentive Compensation Management, the Cognos Incentive Compensation Management Application Server, the client, and the Model Upgrader, and any other Cognos Incentive Compensation Management tools, such as the Cognos Incentive Compensation Management add-in for Microsoft Excel, Cognos Incentive Compensation Management CLI, and Configuration File Encrypter.

   If you upgrade a version 8.1.0 or newer model, you do not need to uninstall the current version. The upgrade process overwrites the current version as of version 8.1.0.

3. Back up your Cognos Incentive Compensation Management models.
Microsoft SQL Server database backup and restoration

A database backup duplicates all the data in the IBM® Cognos® Incentive Compensation Management database and creates a copy of the full database.

You can then recreate the entire database in one step by using the restore command. The restored database is an exact match of the database at the time that the backup completed.

Backing up a database:

You can use Microsoft SQL Server Enterprise Manager to back up the IBM® Cognos® Incentive Compensation Management database.

Procedure
1. In Microsoft SQL Server Enterprise Manager, click Tools > Backup Database.
2. Select one of the following Backup Types:
   - **Complete backup**: Makes a full backup of your database. Start your backup process with a full back up of your database.
   - **Differential backup**: Stores all changes that occurred to the database since the last full backup.
3. You can edit the backup file destination. By default, the backup file is stored in the following location: C:\Program Files\Microsoft SQL Server\MSSQL\BACKUP.
   
   **Tip**: The database can remain online and accessible to users while the backup is being made.

Restoring a database backup:

In the backup file, Microsoft SQL Server stores the names and locations of the files that are used in the IBM® Cognos® Incentive Compensation Management database. After you restore the database, SQL Server recreates all the necessary files and the database is restored to the point in time that the backup finished.

Procedure
1. In Microsoft SQL Server Enterprise Manager, click Tools > Restore Database.
2. The **Restore as Database** field is the name of your newly restored database. It does not need to be identical to the name of the original (backed up) database.
3. To define your restoration parameters, select the original database name and the stored backup that you want to restore.

Using backup and restore to transfer databases between servers:

You can restore a backup of an IBM Cognos Incentive Compensation Management database on a new server by creating a backup of a database and saving it to a location that is accessible from the server where you are performing the restoration.

Procedure
1. From the server that you want the database transferred to, open Enterprise Manager.
2. From the Tools menu, select Restore Database.
3. Type the name that you want the database to be restored with in the Restore as database field.
4. Select the From device option.
5. Select File name and type the location of the backup file.

Upgrading the application
After you complete the upgrade preparation steps, you are ready to install the new version of IBM® Cognos® Incentive Compensation Management.

Procedure
1. Install the Cognos Incentive Compensation Management client.
   For more information, see “Installing the client” on page 7.
2. Install the Cognos Incentive Compensation Management Windows Service by selecting the Maintain or Upgrade an existing instance option.
   For more information, see “Installing the Windows Service” on page 7.
3. Edit the IBM Cognos ICM.exe.config and IBM Cognos ICM Windows Service.exe.config files to match the saved versions from the previous model.
   For more information, see “Configuration files” on page 8.
4. Install any additional Cognos Incentive Compensation Management tools, such as the CLI.

Model upgrades
You can use the IBM® Cognos® Incentive Compensation Management Model Upgrader tool to upgrade models so that they are compatible with the upgraded version.

After you finish upgrading an existing version of Cognos Incentive Compensation Management, you must upgrade your models to the new version.

Upgrade options give you control over the upgrade process for Microsoft SQL Server models and can reduce the size of transaction log files on the Microsoft SQL server.

Tip: If you are completing a new installation of Cognos Incentive Compensation Management, you do not need to upgrade models. Models must be upgraded only when Cognos Incentive Compensation Management is upgraded.

Installing Model Upgrader
The Model Upgrader tool is required to upgrade your IBM® Cognos® Incentive Compensation Management model to be compatible with your upgraded application.

About this task
If you have a previous version of Model Upgrader installed, removed the older version before you install the new one. If you upgrade a version 8.1.0 or newer model, you do not need to uninstall the current version. The upgrade process overwrites the current version as of version 8.1.0.

Procedure
1. Double-click the ICM-modelupgrader.exe installation file in your release folder.
2. Complete the steps in the Installation wizard.
Running Model Upgrader
After Model Upgrader is installed, you must run it to upgrade your current model so that it is compatible with the new version of IBM® Cognos® Incentive Compensation Management.

Procedure
1. In the location that was specified during the installation of the Model Upgrader tool, double-click the ICM-modelupgrader.exe file.
2. In the Model Upgrader tool, type the server name. This is the name of the database server that contains your model. If your database is a Microsoft SQL Server 2000 named instance, or if you are using a Microsoft SQL Server 2005 database, the value for the DBServer field must follow this format: SERVER_NAME\INSTANCE_NAME.
3. Select the database type from the menu. This is the type of database that you are connecting to, such as Microsoft SQL Server 2000 or 2005.
4. Type the database name. This is the name of the database that contains your Cognos Incentive Compensation Management model.
   a. If you do not know the database name, click Browse.
   b. Select a model.
5. Type a value in the Database Timeout field. The default is 90 seconds and probably does not need to change. However, change it here if you increased the default timeout in the Cognos Incentive Compensation Management Windows Service configuration file.
6. Type your user ID and password. This refers to the database user with database altering permissions. This is not the same as the Cognos Incentive Compensation Management administrator password.
7. Click Upgrade.

Model Upgrader options
If you click the Options button when you run the Model Upgrader tool in IBM® Cognos® Incentive Compensation Management, you can set error protection.

The following error protection options are available:

None  This option uses the least resources but offers no protection for the model if an error occurs. If an error occurs during the upgrade process, the model that is being upgraded cannot be salvaged, and must be restored from a backup.

Important: If you plan to use this option, create a full backup first.

Partial  If a model fails to upgrade and the Partial protection option is selected, an error might be resolved without restoring the original backup of the model. Upgrades that fail can always be restarted. This option uses fewer resources than the Complete option but more than the None option.

Important: If you plan to use this option, create a full backup first.

Major Release  If the upgrade fails, this option rolls back the database to the last successful database version that corresponds to a major release. Users can then install the matching major Cognos Incentive Compensation Management release and make the necessary changes to the model to allow it to upgrade. After the changes are made, Model Upgrader can be safely run again.
Important: If you plan to use this option, back up the model first.

Complete
The Complete protection level guarantees that your model is usable no matter what errors are encountered during the upgrade process. If your model cannot be completely upgraded to the database version of your choice, your model is left unchanged. This is the safest option, but it is also the option that uses the most resources.

Target database version
The target database version in the IBM® Cognos® Incentive Compensation Management Model Upgrader tool is an integer that indicates the specific database version that you are upgrading to.

The database version is different from the software version. There is a particular database version for every software version, but there is not a software version for every database version.

You might want to select a database version to control the level of error protection at different points during the upgrade. When you select a target version, you can run the upgrade in smaller increments to avoid running out of disk space.

Running simultaneous instances of IBM Cognos Incentive Compensation Management
If necessary, you can run previous versions of IBM® Cognos® Incentive Compensation Management along with a new version.

About this task
You can have multiple Cognos Incentive Compensation Management Windows Services (including Scheduler) installed on one computer. When you use this upgrade option, previously installed services do not need to be uninstalled. You must stop the Windows Service, Scheduler Service, and API before you install more Windows Services.

Procedure
1. Double-click the ICM-service.exe file in your release folder.
   a. Select the Install a new instance option.
   b. Select the Named Instance option, and specify an instance name for the new service, for example, Service2. Instance names must be unique for all Windows Services, regardless of version number.
   c. Specify a directory to save the new Windows Service in. The directory name must be unique for each Windows Service installation. For example, type C:\Program Files\IBM Cognos ICM\Service2.
   d. Click Install.
   e. If the installation is not successful, uninstall and reinstall the Windows Service.
2. Repeat the previous steps for each Windows Service that you want to install.
4. Scroll down in the Services window and find ICM Windows Service. There should be the same number of IBM Cognos ICM Windows Services, IBM Cognos ICM APIs, and Schedulers as you installed in the previous steps.
5. Right-click the Windows Service. For example, click IBM Cognos ICM Windows Service (SERVICE2), and select Properties.

6. Make sure that the file path in the Path to executable field points to the new Windows Service installation.

7. Repeat steps the previous two steps for the other Windows Services that you installed.

**Editing the Windows Service configuration files**

You must edit the IBM® Cognos® Incentive Compensation Management Windows Service configuration files to indicate how the application server communicates with the database server. You must also add the service instances and configure each service to run on a different port.

**Procedure**

1. Open the new Service folder. For example, open the Service 2 folder.
2. Open the IBM Cognos ICM Windows Service.exe.config configuration file and edit the databaseServer section.
3. Edit the `<add key="ServiceAddress" value="localhost:13105"/>` line so that the service uses a different port from the other services. For example, change the line to `<add key="ServiceAddress" value="localhost:13106"/>`.
4. In the Service instance name section, make sure that the `<add key="ServiceInstanceName" value="myinstance"/>` line is uncommented and the value of the name of the service instance is updated. For example, `<add key="ServiceInstanceName" value="Service2"/>

5. When you finish editing, save and close the configuration file.
6. Repeat for any other service folders that you created.
7. Start the IBM Cognos ICM Windows Services.

**Installation verification**

Once you install or upgrade IBM Cognos Incentive Compensation Management, log in to the client to make sure it is working properly.

**Opening an existing model to verify the installation**

If you upgraded your IBM® Cognos® Incentive Compensation Management model, log in to the client to verify whether the upgrade was successful.

**Procedure**

1. Open the client.
2. Select the Model Name from the menu.
3. Type your User ID and Password.
4. Click Login.

**Adding a model to verify the installation**

To verify whether the IBM® Cognos® Incentive Compensation Management client was installed successfully, you can open the client and create a model.

**Procedure**

1. Open the client.
2. Click Options to change the language of the client and set the date format.
• If you set the language to **EnglishUS**, the date format is set to month/day/year.
• If you set the language to **EnglishGB**, the date format is set to day/month/year.

3. In the login window, click **New Model**. Use the New Model wizard to add and customize a new model.

4. Name the model. Cognos Incentive Compensation Management removes all spaces and punctuation from your model name and uses it as the database name on your database server. The model name can be changed at any time from within the Cognos Incentive Compensation Management client, but the database name that is set initially remains for the life of the database.

5. Select the beginning fiscal year. Cognos Incentive Compensation Management uses this date and the number of payroll periods to construct a default calendar for the new model. The default calendar can be edited and refined from within the client, or replaced entirely if necessary.

6. Select the number of payroll periods. Select whether your organization pays employees weekly (52), biweekly (26), semimonthly (24), or monthly (12). The number of pay periods is used to create the default calendar, which is used to set payment schedules for calculated earnings. The default calendar can be edited or replaced entirely later.

7. Select the currency. A currency is used for either collection or payment. You can select more than one currency from the list, if necessary.

8. Optional: You can add another currency, if necessary.
   a. To add another currency, select the **Other Currencies** check box.
   b. Click **Add**.
   c. Type the currency ID and the currency name.
   d. Click **OK**.

   **Tip:** You can add currencies without using the New Model wizard, so the list can be expanded later.

9. Click **Finish**.

---

**LDAP integration with the client**

You can set up the IBM Cognos Incentive Compensation Management client to allow users to sign in using LDAP authentication.

LDAP users and groups must be configured in the Cognos Incentive Compensation Management Windows Service configuration file and the client. Users can only log in to the client if they have been mapped to a Cognos Incentive Compensation Management role, or if they are a member of an LDAP group that has been mapped to a Cognos Incentive Compensation Management role. LDAP users must be assigned to a user role, configured in the LDAP settings of the Cognos Incentive Compensation Management Windows Service configuration file, and added to the LDAP tab in the client. Then, the users are able to log in to the client with their LDAP user IDs and passwords. LDAP groups must be assigned to a Cognos Incentive Compensation Management role, configured in the LDAP settings of the Cognos Incentive Compensation Management Windows Service configuration file, and added to the LDAP tab in the client. Then, LDAP users who are part of that LDAP group can log in to the client using their SAMAccountName and LDAP password.
Each employee or group in LDAP has a Distinguished Name (DN) that uniquely identifies it. The DN is composed of attribute-value pairs (for example, CN=Quality Assurance, OU=Internal, OU=Groups, OU=HQ, DC=hq, DC=IBM Cognos ICM, DC=com). The first attribute of a DN is the Common Name (CN). Each user or group has a CN to identify them (for example, CN=Dan Huddle or CN=Quality Assurance). Users also have the attributes SAMAccountName, which acts like a username (for example, SAMAccountName=dhuddle), and memberOf, which describes the groups that the employee belongs to (for example, memberOf=All,All Development,Quality Assurance).

The following rules apply to LDAP users for Cognos Incentive Compensation Management:

- LDAP users cannot log in if there is a pending password change in the account.
- LDAP users cannot log in if there account is disabled.
- LDAP users cannot log in twice in the same model.
- If there is a Cognos Incentive Compensation Management user with the same username as the LDAP user, the Cognos Incentive Compensation Management user takes priority (for example, Cognos Incentive Compensation Management will ignore the existence of the LDAP user, and the rules that apply to the Cognos Incentive Compensation Management user remain).
- If the LDAP user is mapped to different Cognos Incentive Compensation Management roles, the union of the permission are given.
- The administrator role can be renamed and mapped to any LDAP group and any user in this group will have all administrator permissions.
- If an LDAP user is logged in to the client, the change password menu item is disabled.
- LDAP users can write web messages and upload web documents.
- An LDAP user can be the Scheduler (the same rules for a Scheduler user apply).
- An LDAP user can log in to perform migrations.

**Configuring the Windows Service configuration file for LDAP authentication**

You must make a few changes in the IBM Cognos Incentive Compensation Management Windows Service configuration file to allow for users to log in to the client using LDAP authentication.

**Procedure**

1. In the IBM Cognos ICM Windows Service.exe.config file, uncomment the ldapSettings section.
2. Edit the ProviderUrl value to point to the address of the LDAP server that should be searched.
3. Edit the ManagerDn value.
   - This is the account that should be used to perform the LDAP tree search.
4. Edit the ManagerPassword value.
   - This is the password of the ManagerDn account.
5. Edit the UserSearchFilter value.
   - This is the LDAP attribute that an LDAP user should enter as the user ID in the Cognos Incentive Compensation Management Client login window.
6. Edit the UserGroupAttribute value.
This is the LDAP attribute that should be used when attempting to determine LDAP group membership.

7. Set the **UseKerberos** value to true to obtain and use the Kerberos token for authentication.

Set the **UseKerberos** value to False to use LDAP for authentication. When the **UseKerberos** field is set to true, the **ManagerDn** and **ManagerPassword** fields are ignored. Instead, the user under which the Cognos Incentive Compensation Management Windows Service runs is used to perform the search of the LDAP tree.

**Attention:** If your network is set up using IWA and you want to authenticate as a user other than the user you are logged into your network as, you must use NTLM and not Kerberos. Kerberos will only authenticate the currently logged in user.

8. Set the **UseSSL** value to True to use SSL (LDAPS) to communicate with the LDAP server. Set the **UseSSL** value to False if you do not want to use SSL (LDAPS) to communicate with the LDAP server.

**Attention:** When using LDAP authentication in a multi-domain environment, the **UseKerberos** field and **UseSSL** field cannot both be simultaneously set to True. Either SSL or Kerberos can be used on their own (or both can be set to False); however, setting both to True will not work in a multi-domain environment.

### Granting LDAP users or LDAP groups access to the client

LDAP users or LDAP groups must be added and granted access in the IBM Cognos Incentive Compensation Management client. The LDAP user or group must be associated with a Cognos Incentive Compensation Management user role.

#### Procedure

1. In the Client, go to **Admin > Manage Users**.
2. Click **Add** to add an LDAP user or group.
3. Select either **LDAP User** or **LDAP Group** from the **Type** drop-down menu.
4. If you selected **LDAP User**, type the user ID that matches the value of the LDAP attribute specified in the user’s LDAP profile in the Windows Service configuration file (by default, the attribute is `SAMAccountName`).
   a. Select the **Role** from the drop-down menu.
      This is the Cognos Incentive Compensation Management user role that is associated with the user.

5. If you selected **LDAP Group**, type the **Group CN** value that matches the value of the **UserGroupAttribute** in the Cognos Incentive Compensation Management Windows Service configuration file.
6. Select the **Role** from the drop-down menu.
   This is the Cognos Incentive Compensation Management user role that is associated with the group.

7. Click **Save**.

---

### Data Tier Performance Optimization

The Data Tier Performance Optimization feature in IBM® Cognos® Incentive Compensation Management can improve calculation performance, especially in models that contain many multiplication and division calculations.
This feature allows a larger portion of calculations to be processed by the database and reduces the need for transfers between the database and Cognos Incentive Compensation Management Windows Service.

**Common language runtime (CLR) integration**

When you use the Data Tier Performance Optimization feature in IBM® Cognos® Incentive Compensation Management, the common language runtime (CLR) integration feature in Microsoft SQL Server must be enabled by running a script to install a user-defined data type.

To enable CLR integration, use the `clr enabled` option of the `sp_configure` stored procedure.

```sql
sp_configure 'clr enabled', 1;
GO
RECONFIGURE;
GO
```

**Enabling Data Tier Performance Optimization in the client**

After you enable the common language runtime (CLR) integration feature, the Data Tier Performance Optimization feature must be enabled in the IBM® Cognos® Incentive Compensation Management client.

**Procedure**

1. Click Admin > Administrative Options.
2. Click the Calculation tab.
3. Select the Enable data tier performance optimization check box.
Chapter 3. Client tools

Cognos Incentive Compensation Management comes with several additional tools that are not required for the application to run when initially setting up your model but can be installed later to perform various functions.

The functions that these tools can perform include; converting your model, importing data from your model into Microsoft Excel, and communicating with Cognos Incentive Compensation Management using a command-line interface.

Console Service

The Console Service tool is a version of the IBM® Cognos® Incentive Compensation Management Windows Service that is run from a command prompt. It uses the same configuration information as the Windows Service.

If each Console Service is installed in a separate directory and is configured to use a different port, you can run multiple instances of the Console Service on the same computer.

Installing the Console Service

The IBM® Cognos® Incentive Compensation Management Console Service can be used to run the client and must be installed on the application server.

Procedure

1. Double-click the ICM-console.exe installation file in your release folder.
2. Complete the steps in the Installation wizard.

Editing the Console Service configuration file

The IBM® Cognos® Incentive Compensation Management Console Service configuration file must be edited to allow the application server to communicate with the database server.

Procedure

1. Edit the databaseServer section in the ConsoleService.exe.config file to point to the correct database.
2. Edit the ServiceAddress value to point to a port that is different from any other service (<add key="ServiceAddress" value="localhost:13112"/>).
3. Edit the security settings to match the security settings in the client.

Starting the Console Service

After the IBM® Cognos® Incentive Compensation Management Service configuration file is edited, the Console Service must be started.

About this task

Cognos Incentive Compensation Management cannot run without a service. You cannot enter database information in the IBM Cognos ICM.exe.config file to bypass the service and access the database directly.
**Procedure**

1. Start a command prompt.
2. In the directory that contains the Console Service, type `ConsoleService`.

**Results**

A message reports that the service is running.

---

**Configuration file encryption**

The Configuration File Encrypter tool in IBM® Cognos® Incentive Compensation Management can be used to encrypt settings in the Cognos Incentive Compensation Management Windows Service configuration file and the Console Service configuration file.

You can encrypt the following settings in the Windows Service configuration file (IBM Cognos ICM Windows Service.exe.config) and the Console Service configuration file (ConsoleService.exe.config):

- DBPassword
- DBuffer
- SchedulerPassword
- SchedulerUser
- LDAP user name and password
- Mail server user name and password

The Configuration File Encrypter encrypts any blank user names and passwords.

---

**Installing the Configuration File Encrypter**

Before running the Cognos Incentive Compensation Management Configuration File Encrypter, you must first install it using the installation file.

**Procedure**

1. Double-click the ICM-encrypter.exe installation file.
2. Complete the steps of the installation wizard.

---

**Running the Configuration File Encrypter**

After the Configuration File Encrypter tool is installed in IBM® Cognos® Incentive Compensation Management, you can use it to encrypt settings in the Windows Service and Console Service configuration files.

**Procedure**

1. Start the Configuration File Encrypter file in the release folder.
2. Click Browse to search for the IBM Cognos ICM Windows Service.exe.config or ConsoleService.exe.config file that you want to encrypt.
3. Click Encrypt.
4. Click Exit.
5. To decrypt a file, repeat the procedure, but select Decrypt in step 3.

**Important:** When you encrypt a file, you encrypt both sets of user names and passwords in the file (database and Scheduler). You cannot choose to encrypt just one or the other.
Model Converter

You can use the Model Converter tool to convert models in IBM® Cognos® Incentive Compensation Management that were created in Microsoft SQL 2000 or 2005 to Microsoft SQL 2008. You can also use the Model Converter to convert models that were created in Microsoft SQL Standard edition to Microsoft SQL Enterprise.

The Model Converter tool changes the compatibility level of your model during a conversion. This too helps to prevent compatibility errors during a conversion.

Installing the Model Converter tool

Before running the IBM Cognos Incentive Compensation Management Model Converter tool, you must first install it using the Model Converter installation file.

Procedure

1. Double-click the ICM-modelconverter.exe installation file located in your release folder.
2. Complete the steps in the installation wizard.

Important: Models created in a Microsoft SQL Standard edition can be restored on a Microsoft SQL Enterprise edition but the Model Converter is required to use Enterprise features. Enterprise edition models cannot be restored on a standard version of SQL. Models created on a 2000 or 2005 edition of SQL can be restored on Microsoft SQL Server 2008, but the Model Converter tool is required for Microsoft SQL Server 2008 features to be available on those models.

Converting a model from Microsoft SQL 2000 or 2005 to 2008

You can use the Model Converter to convert a model in IBM® Cognos® Incentive Compensation Management from Microsoft SQL Server 2000 to Microsoft SQL Server 2008.

Before you begin

The Cognos Incentive Compensation Management Windows Service must be running when you use the Model Converter tool.

Procedure

1. Install Microsoft SQL Server 2008.
2. Restore your Microsoft SQL 2000 or 2005 model on to the Microsoft SQL 2008 server.
3. Start the Model Converter tool.
4. Type a name of the SQL 2008 server in the Server Name field. This name can be an arbitrary name, such as Super Server, to identify and distinguish the database server. If your database is an SQL Server 2000 named instance or if you are using an SQL Server 2005 database, the value for the database server field must be in the following format: SERVER_NAME\INSTANCE_NAME.
5. Select the appropriate Database Type for the model that you want to convert. If you convert a Unicode model, it remains a Unicode model after the conversion.
Important: Because you restored your model on a Microsoft SQL 2008 Server, you must select either Microsoft SQL Server 2008 or Microsoft SQL Server 2008 Unicode, even if your original model was Microsoft SQL Server 2000 or 2005.

6. Browse for the model that you want to convert.
8. Type your Microsoft SQL Server login credentials.
9. Click Convert.

Important: The Model Converter tool changes the compatibility level of the database if it is not set correctly when a conversion is being run.

Converting a Microsoft SQL Standard Model to an Enterprise Model

You can use the Model Converter to convert a model in IBM® Cognos® Incentive Compensation Management from Microsoft SQL Standard to SQL Enterprise.

Procedure
1. Install Microsoft SQL Server Enterprise Edition.
2. Restore your Microsoft SQL Standard Edition model on to the SQL Enterprise server.
3. Start the Model Converter tool.
4. Type a name of the Microsoft SQL Enterprise Edition server in the Server Name field. This can be an arbitrary name, such as Super Server to identify and distinguish the database server. If your database is a SQL Server 2000 named instance or if you are using a SQL Server 2005 database, the value for the Database Server field must be in the following format: \SERVER_NAME\INSTANCE_NAME.
5. Select the appropriate Database Type for the model that you want to convert. This version is the Microsoft SQL Server version that you are converting from. If you convert a Unicode model, it remains a Unicode model after the conversion.
6. Browse for the model that you want to convert.
8. Type your Microsoft SQL Server login credentials.

Converting a Microsoft SQL 2005 Standard Edition model to a 2008 Enterprise Edition model


About this task
You must complete the conversion in two phases.

Procedure
Reducing database size and calculation times

You can use the Enterprise Size Optimization feature in the Model Converter tool in IBM® Cognos® Incentive Compensation Management on Microsoft SQL Enterprise Edition models (both 2005 and 2008) to make the database size smaller and potentially reduce calculation times.

About this task

The Enterprise Size Optimization feature converts a Microsoft SQL Server column type that uses more space (decimal type) to a Microsoft SQL Server column type that uses less space (vardecimal type). The vardecimal data type is an alternative storage format that can be used to minimize the disk space that is needed to store existing decimal and numeric data types. Disk space can be saved by storing decimal and numeric data as variable length columns as opposed to the fixed number of bytes in decimal type storage.

Procedure

To use the vardecimal data type on models that were created before version 7.0, complete the following steps:

1. Upgrade to Cognos Incentive Compensation Management version 7.0 or higher.
   
   **Important:** As of Cognos Incentive Compensation Management version 7.2, all newly created Microsoft SQL 2005 and 2008 Enterprise Edition models do not have the vardecimal data type enabled by default.

2. If your model was created on a Standard Edition of SQL, convert it to Enterprise Edition.


Certificates

This section will guide you through the process of generating digital Secure Sockets Layer (SSL) certificates and configuring them for use with Cognos Incentive Compensation Management applications, including Cognos Incentive Compensation Management and Cognos Incentive Compensation Management Command Line Interface (CLI).

Required software to use digital certificates

To use digital certificates with IBM® Cognos® Incentive Compensation Management, you must install additional software.

To successfully complete the configuration, you probably need administrator privileges for the Windows computer (server) where your digital certificates will be configured.

You need the following software to work with certificates:

**NET Framework Redistributable**

Go to [http://msdn.microsoft.com](http://msdn.microsoft.com) to download the software.

**Important:** Version 4.5 and higher versions are necessary for use with Cognos Incentive Compensation Management applications.

**NET Framework SDK\Windows SDK**

Go to [http://msdn.microsoft.com](http://msdn.microsoft.com) to download the software.
Important: The .NET Framework SDK is superseded by the Windows SDK. Obtain the appropriate SDK for the versions of the Windows operating system and .NET Framework that you are using.

Generating digital certificates for testing or troubleshooting
You can use the Certificate Creation tool to generate your own digital certificates for testing or troubleshooting purposes in IBM® Cognos® Incentive Compensation Management.

About this task
Complete this task for testing or troubleshooting purposes only. In a production environment, use only digital certificates that are purchased from a trusted certificate authority (CA), such as Thawte or VeriSign. Using the digital certificates that are generated by the following steps can compromise the security of your production environment.

The Certificate Creation tool (Makecert.exe) that is included in the .NET Framework\Windows SDK is used to generate a default self-signed (root) certificate that is called Root Agency and a certificate that is signed by this root certificate.

Procedure
Run the installed SDK command prompt and type the following command. You must run CMD as the administrator.

```
makecert -r -pe -n CN="<name of certificate>" -b 01/01/2000 -e 01/01/2036 -eku 1.3.1.5.5.7.3.1 -ss my -sr localmachine -sky exchange -sp "Microsoft RSA SChannel Cryptographic Provider" -sy 12
```

Related concepts:
"Root and server certificates" on page 34
A root certificate and server certificate must be placed into the proper logical stores using the Microsoft Management Console (MMC) window.

Related tasks:
"Preparing for command-line interface installation" on page 37
Before you can install the IBM® Cognos® Incentive Compensation Management command-line interface (CLI), you must complete several other steps.

Command-line switches
To define your digital certificate for use with IBM® Cognos® Incentive Compensation Management, you can use several command-line options.

You can use the following command-line options.

- **-r** Creates a self-signed certificate. A self-signed certificate is a certificate that is not signed by a certificate authority. Because it is not signed by a certificate authority, it can be used for encryption that is required in SSL, but it cannot be used for server authentication.

- **-pe** Marks the private key exportable.

- **-n** Specifies the server name. This name must comply with the X.500 standard. The simplest form is CN="Name" and must specify the name of the server (case-insensitive) or the IP address where it is used. For example, for a server that is named Apple, the certificate subject name is CN="Apple". 
-b Date value in mm/dd/yyyy format that specifies the start of the validity period for the certificate. The default date is the creation date of the certificate.

-e Date value in mm/dd/yyyy format that specifies the end of the validity period for the certificate. If not otherwise set, the default date is 12/31/2039 11:59:59 GMT.

-eku Specifies a list of comma-separated, enhanced key usage object identifiers (OIDs) into the certificate. For SQL Server, an SSL certificate that is valid for server authentication that has an OID of 1.3.6.1.5.5.7.3.1 is required.

-ss Specifies the certificate store where the created certificate is saved. Save this information in the my store, or anywhere in the certificate store.

-sr Specifies the certificate store where the certificate is located. The location can be either currentuser (the default), or localmachine. Because this certificate is being created for a service, it must be placed in the local computer.

-sky Specifies the certificate key type. For RSA public key exchange algorithm, exchange is required here. This key is the type of key that is used to encrypt and decrypt session keys.

-sp Specifies the CryptoAPI provider name. For certificates that are created for SQL Server, this key can be set to Microsoft RSA SChannel Cryptographic Provider.

-sy Specifies the CryptoAPI provider type. When the provider is Microsoft RSA SChannel Cryptographic Provider, the provider type is 12.

Use the corresponding command to generate the digital certificate, for example:

makecert -n "CN=Apple" -ss "My" -sr "LocalMachine" -pe -a sha1 -sky exchange Apple.cer

The generated digital certificate is stored in a file that is called Apple.cer in the directory where the previous command is run. To examine this digital certificate, double-click the file in Windows Explorer and view its details.

The Apple certificate appears below the Root Agency root certificate. This location indicates that the Root Agency root certificate issued and signed the Apple certificate, thereby verifying its authenticity.

Setting up Microsoft Management Console to use digital certificates

You can use Microsoft Management Console (MMC) to view the digital certificates for IBM® Cognos® Incentive Compensation Management that are installed in the local certificate repository. You can also import new digital certificates into the local certificate repository.

Procedure

1. From the Windows Start menu, click Run.
2. Type mmc and click OK.
3. Click File > Add/Remove Snap-in.
4. Click Add.
5. Select Certificates and click Add.
6. Select Computer account and click Next.
7. Leave the Local computer option selected and click Finish.
Root and server certificates

A root certificate and server certificate must be placed into the proper logical stores using the Microsoft Management Console (MMC) window.

Expand the Certificates node in the MMC window to view the logical stores in the local certificate repository.

You will need to import at least two digital certificates into the following logical stores:

- A root certificate into the Trusted Root Certification Authorities store.
- A server certificate signed by the root certificate into the Personal store.

If you have generated test certificates using the steps in “Generating digital certificates for testing or troubleshooting” on page 32, then these digital certificates have already been imported into the correct logical stores.

If you have purchased digital certificates from a trusted certificate authority, these digital certificates need to be imported into the local certificate repository. Purchased digital certificates are usually delivered in one Public-Key Cryptography Standards (PKCS) #12 certificate file (with either a PFX or P12 extension) containing all of the necessary digital certificates and a private key for the signed server certificate. This file is usually protected by a password.

**Related tasks:**

“Generating digital certificates for testing or troubleshooting” on page 32

You can use the Certificate Creation tool to generate your own digital certificates for testing or troubleshooting purposes in IBM® Cognos® Incentive Compensation Management.

**Importing the necessary digital certificates contained in a PKCS #12 file**

To use certificates with IBM® Cognos® Incentive Compensation Management, the server certificate in the PKCS #12 file must be imported into the Personal store.

**Procedure**

1. Expand the Personal store.
2. Select the child Certificates node.
3. Right-click and click All Tasks > Import.
4. Click Next.
5. Click Browse and find the PKCS #12 file. Change the Files of type selection to Personal Information Exchange.
6. After you find the file, select it and click Open.
7. Click Next.
8. Type the private key password and click Next.
9. Leave the Place all certificates in the following store option selected.
10. Click Next.
11. Review the import settings, if necessary, and click Finish.

All of the digital certificates that are contained in the PKCS #12 file are now in the Personal store, but only the server certificate belongs in this store. The server certificate can be identified as the certificate with the server's name, such as Apple, specified under the Issued To column.
12. You can double-click this certificate to examine its details and make sure that the Certification path is complete and that the Certificate status indicates that the certificate is Okay.

13. Move the root certificate, which is the topmost certificate in the Certification path, such as Root Agency, from the Personal store to the Trusted Root Certification Authorities store by dragging and dropping or by cutting and pasting it.

**Server IP address and port**

To configure certificates for use with IBM® Cognos® Incentive Compensation Management, the IP address of the server where the digital certificates are now installed is necessary to properly configure the server to identify itself. An unused port number is also necessary to listens for SSL connections that are initiated by clients.

If a host name is being used instead of an IP address, the host name must be mapped with the IP address in the host file.

**Identifying the IP address of the server**

When you configure certificates for use with IBM® Cognos® Incentive Compensation Management, if you do not know the IP address of the server, you can ping the server from the command prompt window to find the IP address.

**Procedure**

1. Open the command prompt window.
2. In the command prompt window, type: ping <server_name>, where <server_name> is the name of the server, such as Apple.
3. Note the IP address where the ping replies from.

**Editing the hosts file**

When you configure the use of certificates with IBM® Cognos® Incentive Compensation Management, if a host name is used instead of an IP address, the host name must be mapped with the IP address in the host file.

**Procedure**

1. Open the hosts file in the following directory: C:\Windows\System32\drivers\ etc\.
2. Map the certificate to the IP address of the server where the certificate was imported. For example, add the following text to the file: 127.0.0.1 <name of certificate>
3. Save and close the file.

**Identifying an unused port number on the server**

When configuring certificates for use with IBM Cognos Incentive Compensation Management, if you need to find an unused port on the server, you can type a command in the command prompt window to identify one.

**Procedure**

1. Open the command prompt window.
2. Type the following command in the Command Prompt window: telnet <server_name><port_number>, where <server_name> is the name of the server, such as Apple, and <port_number> is the port number to test for.
3. If the connection cannot be opened to the server using the given port number, this port number is not being used. Make a note of this port number.

Attention: By default, Cognos Incentive Compensation Management applications use port numbers 13105, 13115, and 13125.

**Binding the certificate to the port**

When you configure certificates for use with IBM Cognos Incentive Compensation Management, the SSL certificate must be bound to the API port.

**Procedure**

1. Open the Microsoft Management Console. For more information, see “Setting up Microsoft Management Console to use digital certificates” on page 33.
2. Expand Certificates > Personal > Certificates.
3. Double-click the certificate that you added.
4. On the Details tab, scroll to the bottom of the list and click Thumbprint.
5. Copy the value in the window.
6. Paste the value into a text editor and remove all the spaces from the thumbprint value.
7. Click Start > All Programs > Microsoft Windows SDK > CMD Shell (run as administrator).
8. In the command prompt, type the following command: `uuidgen`.
9. Copy the **GUID** value that is displayed and paste it into a text editor.
10. In the text editor, place braces around the **GUID** value, and then copy it so that you can paste it into the command that you create in the next step. For example, type the following text: `{ec8d236c-9a4e-9d9f-2166f1b0ca29}`.
11. In the command prompt, type the following command:

   ```bash
   netsh http add sslcert ipport=0.0.0.0:13125 certhash=<thumbprint> appid=<GUID> clientcertnegotiation=enable
   ```

   - **ipport** The IP address that is configured in the hosts file.
   - **certhash** The value of the thumbprint with the spaces removed.
   - **appid** The **GUID** value with braces around it.

**Configuring IBM Cognos Incentive Compensation Management to use certificates**

After you finish configuring certificates, you are ready to use the configured digital certificates to work with either IBM Cognos Incentive Compensation Management or the Cognos Incentive Compensation Management CLI.

**Configuring the IBM Cognos Incentive Compensation Management client and Windows Service to use certificates**

You can configure IBM Cognos Incentive Compensation Management to use digital certificates.

**Procedure**

1. Open the IBM Cognos ICM Windows Service.exe.config service configuration file.
2. Edit the **APISecureAddress** value, where localhost is the name of the server and 13125 is the port number that is configured to listen for SSL connections.
3. Edit the `APICertificateName` value, where CommonName specifies the common name of the configured server certificate, which must also be the name of the certificate.

The following example shows the configuration for the Service to use a certificate that is called MobileAPI and port number 13125.

```xml
<add key="APISecureAddress" value="MobileAPI:13125"/>

<add key="APICertificateName" value="MobileAPI"/>
```

4. Save the Cognos Incentive Compensation Management Windows Service configuration file changes.

5. Open the IBM Cognos ICM Client.exe.config file.

6. Edit the `serviceAddress` value, to contain the same server name and port number as the values that are specified in the IBM Cognos ICM Windows Service.exe.config file.

7. Save the IBM Cognos ICM Client.exe.config configuration file.

8. Stop the Cognos Incentive Compensation Management services in the following order:
   a. Cognos Incentive Compensation Management API
   b. Cognos Incentive Compensation Management Scheduler
   c. Cognos Incentive Compensation Management Windows Service

9. Start the Cognos Incentive Compensation Management services in the following order:
   a. Cognos Incentive Compensation Management Service
   b. Cognos Incentive Compensation Management Scheduler
   c. Cognos Incentive Compensation Management API

---

**Command line interface**

Cognos Incentive Compensation Management CLI is a command-line interface that connects to models through the Cognos Incentive Compensation Management API Windows Service.

The command-line interface can be used to perform various actions in the model.

**Preparing for command-line interface installation**

Before you can install the IBM® Cognos® Incentive Compensation Management command-line interface (CLI), you must complete several other steps.

**About this task**

Before the command-line interface can connect to models on a configured database, you must first complete the following steps.

**Procedure**

2. Specify values for the `APIAddress`, `APISecureAddress`, and `APICertificateName` keys in the IBM Cognos ICM Windows Service.exe.config file.
3. Start the Cognos Incentive Compensation Management API Service.
4. Install a certificate on the computer that runs the CLI and point the endpoint addresses in the CLI configuration file to where the API service is running.)
Related tasks:
“Generating digital certificates for testing or troubleshooting” on page 32
You can use the Certificate Creation tool to generate your own digital certificates for testing or troubleshooting purposes in IBM Cognos Incentive Compensation Management.

Installing IBM Cognos Incentive Compensation Management command-line interface
Before you can use the IBM® Cognos® Incentive Compensation Management command-line interface (CLI), you must install the CLI application.

Procedure
1. Double-click the ICM-cli.exe installation file in your release folder.
2. Complete the steps in the installation wizard.

Configuring digital certificates with the CLI
You can configure the Cognos Incentive Compensation Management CLI to use digital certificates.

Procedure
1. Open the IBM Cognos ICM Windows Service.exe.config file.
2. Modify the APISecureAddress value to point to the server and port number configured to listen for SSL connections, such as MobileAPI:13125.
3. Modify the APICertificateName value to specify the common name of the configured server certificate, which should also be the name of the server.
4. Save the Cognos Incentive Compensation Management Windows Service configuration file changes.
5. Start (or restart) the Cognos Incentive Compensation Management Windows Service for the service configuration file changes to take effect.
6. Start (or restart) the API service for the service configuration file changes to take effect.
7. Open the ICM-CLI.exe.config configuration file.
8. Modify the ServiceAddress value, where the server name and port number are the same as the values specified in the IBM Cognos ICM Windows Service.exe.config file.
9. Save the configuration file changes.
10. Run the CLI from within a command prompt window.

Connecting to a model using the CLI
To connect to a IBM Cognos Incentive Compensation Management model using the CLI, you need to know the model name, username, and the password (if a password has been set).

Procedure
1. Open the command prompt window.
2. Navigate to the directory where the CLI is located.
   For example, type cd C:\Program Files\IBM Cognos ICM\CLI.
3. From the command-line, type:
   IBM Cognos ICM CLI -server <server name> -model <model name> -user <username> -pass <password>
Where

<server name> is the name of the database server that the model resides on as defined in the configuration file (not necessarily the true name of the server).

<model name> is the name of the database containing the Cognos Incentive Compensation Management model.

<username> is the user name used to log in to the model.

<password> is the password used to log in to the model.

Attention: If no password has been set up for the user, omit the <password> component.

Command-line interface commands

You can use the IBM® Cognos® Incentive Compensation Management command-line interface (CLI) to run several processes in the client.

You can use the following commands. All CLI commands are case-sensitive.

calcall
Calculate all objects in the model.

runproc <process>
Run a saved process that is named <process>.

enablewebuser "true" -payeeid <"payeeID of web user to enable"> -webpw <"web user's password">
Enable a user for the Cognos Incentive Compensation Management web client.

enablewebuser "false" -payeeid <"payeeID of web to disable">
Disable a web user.

changepassword -payeeid <"payeeID of web user to change password for"> -webpw <"web user's password">
Change a web user's password.

optimize
Optimizes the model. This command is used to ensure favorable calculation time after data is updated in the model. For more information, see the IBM Cognos Incentive Compensation Management User Guide.

enabledto "true"
Enables the data tier performance optimization feature. To disable the feature, use the enabledto "false" command. For more information, see “Data Tier Performance Optimization” on page 24.

The command must be typed after the model connection information.

The following command connects to the SoftCo model and calculates all objects in the model on a server named MyServer:

IBM Cognos ICM CLI -server "MyServer" -model "SoftCo" -user admin -calcall

The following command connects to the SoftCo model and calculate all objects in the model and run a saved process that is called Imports on a server called MyServer:

IBM Cognos ICM CLI -server "MyServer" -model "SoftCo" -user admin -pass secret -runproc Imports
The following command connects to the SoftCo model and enable a user for the Cognos Incentive Compensation Management web client in the model on a server named MyServer:

```
IBM Cognos ICM CLI -server "MyServer" -model "SoftCo" -user admin -pass secret -enablewebuser "true" -payeeid "E1000" -webpw "1234"
```

The following command connects to the SoftCo model and disable a Cognos Incentive Compensation Management web client user in the model on a server named MyServer:

```
IBM Cognos ICM CLI -server "MyServer" -model "SoftCo" -user admin -pass secret -enablewebuser "false" -payeeid "E1001"
```

The following command connects to the SoftCo model and change a user's password for Cognos Incentive Compensation Management web client in the model on a server named MyServer:

```
IBM Cognos ICM CLI -server "MyServer" -model "SoftCo" -user admin -pass secret -changewebuserpassword -payeeid "E1000" -webpw "4321"
```

The following command connects to the SoftCo model and optimize the model on a server named MyServer:

```
IBM Cognos ICM CLI -server "MyServer" -model "SoftCo" -user admin -pass secret -optimize
```

The following command connects to the SoftCo model and enable the data tier performance optimization feature in the model on a server named MyServer:

```
IBM Cognos ICM CLI -server "MyServer" -model "SoftCo" -user admin -pass secret -enabledto "true"
```

The following command connects to the SoftCo model and disable the data tier performance optimization feature in the model on a server named MyServer:

```
IBM Cognos ICM CLI -server "MyServer" -model "SoftCo" -user admin -pass secret -enabledto "false"
```

**Return code from the command-line interface**

To determine the result of running the IBM® Cognos® Incentive Compensation Management command-line interface (CLI), you can check the value that is returned to the caller, either the operating system or another process or tool.

The third-party tool that is used to call Cognos Incentive Compensation Management through the CLI might need to know whether the called process was able to complete successfully. The following values can be returned:

- A value of 0 (integer) indicates a successful execution
- A value of -1 (integer) indicates failed execution

The procedure for collecting a return code depends on the method that is used to start the Cognos Incentive Compensation Management application. It is up to the caller of Cognos Incentive Compensation Management CLI to capture these values so that this information can be used to take further action.
The Cognos Incentive Compensation Management API is implemented by writing function calls in the program, which provides the linkage required for execution.

The API allows Cognos Incentive Compensation Management modules to be available or linked into an existing program to perform the required tasks.

The intent of this API section is to provide client organizations that want to access Cognos Incentive Compensation Management in a programmatic way with an interoperable option. Some common uses include the following scenarios:

- Client organizations that want to retrieve calculated or statistical data from Cognos Incentive Compensation Management for use in other downstream applications, such as portal applications, reporting, or other systems
- Client organizations that want to leverage web services to more tightly integrate systems
- Client organizations that want to programically trigger Cognos Incentive Compensation Management with existing third-party scheduling or application management software
- Partner organizations that want to integrate their solution more closely with Cognos Incentive Compensation Management
- Client or partner organizations that want to enable the Cognos Incentive Compensation Management mobility application

The above scenarios involve querying Cognos Incentive Compensation Management, retrieving data from the system, updating data within the system, and adding data to the system.

Typically, the data is either of the following types:

- Portal Access-related (for example, access rights, inquiries, approvals, or denials)
- Statistical (for example, transactions, rates, quotas, compensation amounts, hierarchical, or data)

All of this information is accessible via calls embedded in the Cognos Incentive Compensation Management API.

**API architecture**

IBM® Cognos® Incentive Compensation Management provides a WS-I compliant API implemented using the Windows Communication Foundation (WCF) introduced in Microsoft’s .NET Framework 3.0.

WCF supports WS-* security standards through configurable bindings and behaviors. This makes sure that web services are interoperable while incorporating transaction support, end-to-end security, and reliability.

**Transactions**

WCF supports WS-AtomicTransaction and WS-Coordination, enabling two-phase commit transactions.

**Security**

WCF supports WS-SecureConversation, WS-Security, and WS-Trust, enabling both transport-level and message-level security.
Reliability

WCF supports WS-ReliableMessaging, enabling reliable end-to-end communication.

Any WS-I compliant application should be able to inter-operate with the Cognos Incentive Compensation Management API. Both .NET and java-based client applications have been tested.

A custom web services extension can be written for your deployment. To discuss this option, speak with an Cognos Incentive Compensation Management sales representative.

API access

The API is hosted as a Windows Service, called IBM Cognos Incentive Compensation Management API.

The Cognos Incentive Compensation Management API Windows Service must be started in order to obtain access. Certificates also need to be installed and configured properly in order to provide a secure connection between the service and an API-aware client (see "Certificates" on page 31).

After the API service is started, connect an API-aware client to the following addresses:

- https://localhost:13125/API/Calculations
- https://localhost:13125/API/Table
- https://localhost:13125/API/Scheduler

After you are connected, a username and password are required to gain access. The username is given in the following format:

<server>/<database>/<user_type>/<username>

where:

- server is the database server name specified in the Cognos Incentive Compensation Management Windows Service configuration file.
- database is the database name of the Cognos Incentive Compensation Management model you want to connect to.
- user_type is Web (indicating a web-enabled user) except when accessing the Scheduler and data store API, where the user_type is Administrator.
- username is the email address of a web-enabled user.

The password is the password specified for the web-enabled user.

The following example contains an arbitrary user name and password:
User name: Local/TestModel/Web/jsmith@corporation.com
Password: secret

To obtain the WSDL file, connect a web browser to the following addresses:

- https://localhost:13125/API/Table?wsdl
API specifications for processing and calculation

The following tables outline the API specifications for running processes and calculations in IBM Cognos Incentive Compensation Management.

Table 2. RunProcess

<table>
<thead>
<tr>
<th>RunProcess</th>
<th>(WSDL Address: <a href="https://localhost:13125/API/Scheduler?wsdl">https://localhost:13125/API/Scheduler?wsdl</a>)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Run saved process (folder) in Scheduler</td>
</tr>
<tr>
<td>Input</td>
<td>Process (folder) name (string)</td>
</tr>
<tr>
<td>Output</td>
<td>None</td>
</tr>
<tr>
<td>Note</td>
<td>Administrator users only</td>
</tr>
<tr>
<td>Exceptions</td>
<td>InvalidArgumentException, InvalidDataException, RetiredEndpointException, TokenException</td>
</tr>
</tbody>
</table>

Table 3. ComputeAll

<table>
<thead>
<tr>
<th>ComputeAll</th>
<th>(WSDL Address: <a href="https://localhost:13125/API/Calculations?wsdl">https://localhost:13125/API/Calculations?wsdl</a>)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Compute all calculations</td>
</tr>
<tr>
<td>Input</td>
<td>None</td>
</tr>
<tr>
<td>Output</td>
<td>None</td>
</tr>
<tr>
<td>Note</td>
<td>Administrator users only</td>
</tr>
<tr>
<td>Exceptions</td>
<td>RetiredEndpointException, TokenException</td>
</tr>
</tbody>
</table>

Table 4. ComputePlan

<table>
<thead>
<tr>
<th>ComputePlan</th>
<th>(WSDL Address: <a href="https://localhost:13125/API/Calculations?wsdl">https://localhost:13125/API/Calculations?wsdl</a>)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Compute results for given compensation plan</td>
</tr>
<tr>
<td>Input</td>
<td>Plan ID (string)</td>
</tr>
<tr>
<td>Output</td>
<td>None</td>
</tr>
<tr>
<td>Note</td>
<td>Administrator users only</td>
</tr>
<tr>
<td>Exceptions</td>
<td>InvalidArgumentException, RetiredEndpointException, TokenException</td>
</tr>
</tbody>
</table>

Table 5. ComputeTailoredReport

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Compute results for given tailored report</td>
</tr>
<tr>
<td>Input</td>
<td>Tailored report ID (String)</td>
</tr>
<tr>
<td>Output</td>
<td>None</td>
</tr>
<tr>
<td>Note</td>
<td>Administrator users only</td>
</tr>
<tr>
<td>Exceptions</td>
<td>InvalidArgumentException, RetiredEndpointException, TokenException</td>
</tr>
</tbody>
</table>
Table 6. ComputePayee

<table>
<thead>
<tr>
<th>Description</th>
<th>Compute results for given payee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input</td>
<td>Payee ID (string)</td>
</tr>
<tr>
<td>Output</td>
<td>None</td>
</tr>
<tr>
<td>Note</td>
<td>Administrator users only</td>
</tr>
<tr>
<td>Exceptions</td>
<td>InvalidArgumentException, RetiredEndpointException, TokenException</td>
</tr>
</tbody>
</table>

Table 7. ComputeWebReport

<table>
<thead>
<tr>
<th>Description</th>
<th>Compute results for given web report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input</td>
<td>Web Report ID (number)</td>
</tr>
<tr>
<td>Output</td>
<td>None</td>
</tr>
<tr>
<td>Note</td>
<td>Administrator users only</td>
</tr>
<tr>
<td>Exceptions</td>
<td>InvalidArgumentException, RetiredEndpointException, TokenException</td>
</tr>
</tbody>
</table>

Table 8. ComputeWebForm

<table>
<thead>
<tr>
<th>Description</th>
<th>Compute results for given web form</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input</td>
<td>Web Form ID (number)</td>
</tr>
<tr>
<td>Output</td>
<td>None</td>
</tr>
<tr>
<td>Note</td>
<td>Administrator users only</td>
</tr>
<tr>
<td>Exceptions</td>
<td>InvalidArgumentException, RetiredEndpointException, TokenException</td>
</tr>
</tbody>
</table>

API specifications for data management

The following tables outline the API specifications for data management in IBM Cognos Incentive Compensation Management.

Table 9. TableExists

<table>
<thead>
<tr>
<th>Description</th>
<th>Determine if a table with the given name exists in the model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input</td>
<td>Table name (string)</td>
</tr>
<tr>
<td>Output</td>
<td>The value True (boolean) if the table exists in the model and False (boolean) otherwise</td>
</tr>
</tbody>
</table>
Table 9. TableExists (continued)

<table>
<thead>
<tr>
<th>TableExists</th>
<th>(WSDL Address: <a href="https://localhost:13125/API/Table?wsdl">https://localhost:13125/API/Table?wsdl</a>)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note</td>
<td>Administrator users only</td>
</tr>
<tr>
<td>Exceptions</td>
<td>InvalidArgumentException, RetiredEndpointException, TokenException</td>
</tr>
</tbody>
</table>

Table 10. GetTableSchema

<table>
<thead>
<tr>
<th>GetTableSchema</th>
<th>(WSDL Address: <a href="https://localhost:13125/API/Table/wsdl">https://localhost:13125/API/Table/wsdl</a>)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Get the schema for the given table, including column types and key fields</td>
</tr>
<tr>
<td>Input</td>
<td>Table name (string)</td>
</tr>
<tr>
<td>Output</td>
<td>TableSchema object containing the table name (string) and a list of ColumnSchema objects containing column name (string), column type (string) and whether column is a key column (boolean)</td>
</tr>
<tr>
<td>Note</td>
<td>Column types can be one of the following types: Text Box, Date, Pick List, Numeric, Email, URL, Comment</td>
</tr>
<tr>
<td></td>
<td>Administrator users only</td>
</tr>
<tr>
<td>Exceptions</td>
<td>InvalidArgumentException, InvalidDataException, RetiredEndpointException, PermissionDeniedException, TokenException</td>
</tr>
</tbody>
</table>

Table 11. GetTableRow

<table>
<thead>
<tr>
<th>GetTableRow</th>
<th>(WSDL Address: <a href="https://localhost:13125/API/Table?wsdl">https://localhost:13125/API/Table?wsdl</a>)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Get a single data row from the given table</td>
</tr>
<tr>
<td>Input</td>
<td>Table name (string) and list of ColumnValuePair objects that uniquely identifies the row</td>
</tr>
<tr>
<td>Output</td>
<td>DataRow object that contains a list of ColumnValuePair objects that correspond to each column and its value</td>
</tr>
<tr>
<td>Note</td>
<td>Administrator users only</td>
</tr>
<tr>
<td>Exceptions</td>
<td>InvalidArgumentException, InvalidDataException, RetiredEndpointException, PermissionDeniedException, TokenException</td>
</tr>
</tbody>
</table>

Table 12. AddRow

<table>
<thead>
<tr>
<th>AddRow</th>
<th>(WSDL Address: <a href="https://localhost:13125/API/Table?wsdl">https://localhost:13125/API/Table?wsdl</a>)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Add a row to the given table</td>
</tr>
</tbody>
</table>
Table 12. AddRow (continued)

<table>
<thead>
<tr>
<th>AddRow</th>
<th>(WSDL Address: <a href="https://localhost:13125/API/Table?wsdl">https://localhost:13125/API/Table?wsdl</a>)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input</strong></td>
<td>Table name (string), and list of ColumnValuePair objects</td>
</tr>
<tr>
<td><strong>Output</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Administrator users only</td>
</tr>
<tr>
<td><strong>Exceptions</strong></td>
<td>InvalidArgumentException,</td>
</tr>
<tr>
<td></td>
<td>InvalidDataException,</td>
</tr>
<tr>
<td></td>
<td>RetiredEndpointException,</td>
</tr>
<tr>
<td></td>
<td>PermissionDeniedException,</td>
</tr>
<tr>
<td></td>
<td>TokenException</td>
</tr>
</tbody>
</table>

Table 13. UpdateRow

<table>
<thead>
<tr>
<th>UpdateRow</th>
<th>(WSDL Address: <a href="https://localhost:13125/API/Table?wsdl">https://localhost:13125/API/Table?wsdl</a>)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Update values for an existing row in the given table</td>
</tr>
<tr>
<td><strong>Input</strong></td>
<td>Table name (string), list of original ColumnValuePair objects that correspond to a row in the table, and a list of new ColumnValuePair objects that contain new values</td>
</tr>
<tr>
<td><strong>Output</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Administrator users only</td>
</tr>
<tr>
<td><strong>Exceptions</strong></td>
<td>InvalidArgumentException,</td>
</tr>
<tr>
<td></td>
<td>InvalidDataException,</td>
</tr>
<tr>
<td></td>
<td>RetiredEndpointException,</td>
</tr>
<tr>
<td></td>
<td>PermissionDeniedException,</td>
</tr>
<tr>
<td></td>
<td>TokenException</td>
</tr>
</tbody>
</table>

Table 14. DeleteRow

<table>
<thead>
<tr>
<th>DeleteRow</th>
<th>(WSDL Address: <a href="https://localhost:13125/API/Table?wsdl">https://localhost:13125/API/Table?wsdl</a>)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Delete a row from the given table</td>
</tr>
<tr>
<td><strong>Input</strong></td>
<td>Table name (string) and list of ColumnValuePair objects that correspond to a row in the table</td>
</tr>
<tr>
<td><strong>Output</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Administrator users only</td>
</tr>
<tr>
<td><strong>Exceptions</strong></td>
<td>InvalidArgumentException,</td>
</tr>
<tr>
<td></td>
<td>InvalidDataException,</td>
</tr>
<tr>
<td></td>
<td>RetiredEndpointException,</td>
</tr>
<tr>
<td></td>
<td>PermissionDeniedException,</td>
</tr>
<tr>
<td></td>
<td>TokenException</td>
</tr>
</tbody>
</table>

**Tip:** You must provide full column names to update or delete a row or to do both. To get the full column name, call GetTableRow with the table name and key columns to get the entire row.
### API specifications for data store

The following tables outline the API specifications for data store calls in IBM Cognos Incentive Compensation Management.

**Service Address:** https://localhost:13125/API/DataStore

**WSDL:** http://localhost:13115/API/DataStore/?wsdl

#### Table 15. GetDataStoreID

<table>
<thead>
<tr>
<th>Description</th>
<th>Get ID of the DataStore for the given name</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input</strong></td>
<td>DataStore name (string)</td>
</tr>
<tr>
<td><strong>Output</strong></td>
<td>The ID value (integer) for the given DataStore name</td>
</tr>
<tr>
<td><strong>Exceptions</strong></td>
<td>TokenException, PermissionDeniedException</td>
</tr>
</tbody>
</table>

#### Table 16. GetDataStoreName

<table>
<thead>
<tr>
<th>Description</th>
<th>Get name of the DataStore for the given ID</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input</strong></td>
<td>DataStore ID (integer)</td>
</tr>
<tr>
<td><strong>Output</strong></td>
<td>The name value (string) for the given DataStore Name</td>
</tr>
<tr>
<td><strong>Exceptions</strong></td>
<td>TokenException, PermissionDeniedException</td>
</tr>
</tbody>
</table>

#### Table 17. GetDataStoreIDToNameMapping

<table>
<thead>
<tr>
<th>Description</th>
<th>Get mapping of entire DataStore ID to DataStore name</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input</strong></td>
<td>DataStore ID (integer)</td>
</tr>
<tr>
<td><strong>Output</strong></td>
<td>The value 'true' (boolean) if the table exists in the model and 'false' (boolean) otherwise</td>
</tr>
<tr>
<td><strong>Exceptions</strong></td>
<td>TokenException, PermissionDeniedException</td>
</tr>
</tbody>
</table>

#### Table 18. GetDataStoreSchema

<table>
<thead>
<tr>
<th>Description</th>
<th>Get table schema of the DataStore</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input</strong></td>
<td>DataStore ID (integer)</td>
</tr>
<tr>
<td><strong>Output</strong></td>
<td>TableSchema (TableSchema) of the DataStore with the given ID</td>
</tr>
<tr>
<td><strong>Exceptions</strong></td>
<td>TokenException, PermissionDeniedException</td>
</tr>
</tbody>
</table>

#### Table 19. GetDataStoreRowRange

<table>
<thead>
<tr>
<th>Description</th>
<th>Get rows for the given DataStore ID</th>
</tr>
</thead>
</table>
Table 19. GetDataStoreRowRange (continued)

<table>
<thead>
<tr>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>DataStore ID (integer)</td>
<td>Array of DataRow (DataRow[])</td>
</tr>
<tr>
<td>Restrictions (RestrictionBase)</td>
<td></td>
</tr>
<tr>
<td>StartIndex (integer)</td>
<td></td>
</tr>
<tr>
<td>Length (integer)</td>
<td></td>
</tr>
</tbody>
</table>

Exceptions
- TokenException
- InvalidArgumentException
- InvalidDataException
- LargeDataException
- PermissionDeniedException

Table 20. GetDataStoreRowCount

<table>
<thead>
<tr>
<th>Description</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get the number of rows for the given DataStore ID</td>
<td>Number of Rows in the DataStore (integer)</td>
</tr>
</tbody>
</table>

Exceptions
- TokenException
- InvalidArgumentException
- InvalidDataException
- PermissionDeniedException

Object definitions
The following objects are represented as class definitions written in C#.

**ColumnSchema**

```csharp
public class ColumnSchema
{
    public string Name;
    public string Type;
    public bool IsKey;
}
```

**Earnings**

```csharp
public class Earnings
{
    public string PayeeName;
    public string PlanID;
    public string Amount;
}
```

**EarningsDetails**

```csharp
public class EarningsDetails
{
    public string[] ColumnHeaders;
    public EarningsDetailsRow[] Details;
}
```
public class EarningsDetailsRow
{
    public string[] ColumnData;
    public string Payout;
}

public class Inquiry
{
    public int ID;
    public string Object;
    public PayeeName Creator;
    public PayeeName Assignee;
    public string CreationDate;
    public string Status;
    public string Category;
    public InquiryComment[] Comments;
}

public class InquiryComment
{
    public PayeeName Author;
    public string CreationDate;
    public string CommentText;
}

public class NameValue
{
    public string Name;
    public string Value;
}

public class PayeeName
{
    public string ID;
    public string Name;
}

public class PeriodEarnings
{
    public string PeriodType;
    public PeriodEarningsRow[] Earnings;
}

public class PeriodEarningsRow
{
    public string Period;
    public string Amount;
}

public class PlanEarnings
{
    public PayeeName PayeeName;
    public string PlanID;
    public string Earnings;
}
PlanName
public class PlanName
{
    public string ID;
    public string Name;
}

PlanPosted
public class PlanPosted
{
    public PlanName PlanName;
    public string LastPostedPeriod;
}

SignOff
public class SignOff
{
    public int ID;
    public string Name;
    public int NodeID;
    public string StartDate;
    public string Object:
    public string[] Signees;
}

TableData
public class TableData
{
    public TableSchema Schema;
    public TableDataRow[] Rows;
}

TableDataRow
public class TableDataRow
{
    public string[] Values;
}

TableSchema
public class TableSchema
{
    public string Name;
    public ColumnSchema[] Columns;
}

WorkflowStatus
public class WorkflowStatus
{
    public PayeeName PayeeName;
    public int ApprovalStatus;
    public bool HasOpenInquiries;
}

DataRow
{
    public ColumnValuePair[] Values;
}
(ColumnValuePair
public class ColumnValuePair
{
    public string Column;
    public string Value;
}

DataStore Object Definitions
Public abstract class RestrictionBase
{
}
Public abstract class RestrictionGroup : RestrictionBase
{
    Public RestrictionBase[] RestrictionItems;
}
Public class AllGroup : RestrictionGroup
{
}
Public class AnyGroup : RestrictionGroup
{
}
Public class Restriction : RestrictionBase
{
    Public ColumnSchema Column;
    Public Operator OperatorType;
    Public string Right;
}
Public enum Operator
{
    LessThan,
    LessThanEquals,
    Equals,
    NotEquals,
    GreaterThan,
    GreaterThanEquals,
    IsNull,
    IsNotNull
}

Exception definitions
The following objects are represented as class definitions written in C#.

APIException
public class APIException
{
    public string Message;
}

Description: A base object that all exception objects extend to inherit the Message member, which is used to store a description of the error causing the exception.

InvalidArgumentException
public class InvalidArgumentException : APIException
{
}

Description: This is thrown when an invalid argument (parameter value) for a method is discovered.
InvalidDataException
public class InvalidDataException : APIException
{
}

Description: This is thrown when invalid (non-existent) data is discovered.

RetiredEndpointException
public class RetiredEndpointException : APIException
{
}

Description: This is thrown when an endpoint (service method) is retired (i.e. no longer exists).

UserTypeException
public class UserTypeException : APIException
{
}

Description: This is thrown when the user type for the user currently logged in is deemed incorrect or invalid.

PermissionDeniedException
public class PermissionDeniedException : APIException
{
}

Description: This is thrown when the user does not have permission to perform the operation.

Add-in for Microsoft Excel
You can install the IBM® Cognos® Incentive Compensation Management add-in for Microsoft Excel 2003 or 2007 and 2010. The add-in gives users an easy way to do self-reporting with up-to-date results.

When users are logged in to Cognos Incentive Compensation Management through Microsoft Excel, they can select from a list of Cognos Incentive Compensation Management star schemas that can be included in the report. Users can use typical pivot functionality to define what to include along the Y-axis and the X-axis, and what values to report on. Users can also refresh the data with up-to-date Cognos Incentive Compensation Management data.

Service-side setup for installing the Microsoft Excel add-in
To set up the Windows Service for the Microsoft Excel add-in, you must set up certificates on the computer that runs the IBM® Cognos® Incentive Compensation Management Windows Service. You must also edit the Windows Service configuration file.

Setting up certificates for the Microsoft Excel add-in
To set up the Windows Service for the IBM® Cognos® Incentive Compensation Management add-in for Microsoft Excel, you must import a digital certificate into the Trusted Root Certification Authorities store and the Personal store.
Procedure

1. From the Windows Start menu, click Run.
2. Type mmc and click OK.
3. Click File > Add/Remove Snap-in.
4. Click Add.
5. Select Certificates and click Add.
6. Select Computer account and click Next.
7. Leave the Local computer option selected and click Finish.
8. Click Close and then OK.
9. Expand Certificates and expand Trusted Root Certification Authorities.
10. Select the Certificates folder under Trusted Root Certification Authorities, right-click, and click All Tasks > Import.
11. In the Certificate Import wizard, click Next.
12. Click Browse.
13. Open the folder that contains the certificate and click Files of type > All Files.
14. Select the certificate and click Open.
   For this example, the certificate is called MobileAPI.
15. Click Next.
16. Type the password for the private key, if one is required, and click Next.
17. Leave the Place all certificates in the following store option selected.
18. Click Next.
19. Review the import settings and click Finish.
20. Expand the Personal folder.
21. Select the Certificates folder, right-click, and click All Tasks > Import.
22. Complete the steps to import the certificate.

Results

The MobileAPI certificate is stored in both folders.

Modifying the IBM Cognos Incentive Compensation Management Windows Service configuration file

To use the Cognos Incentive Compensation Management add-in for Microsoft Excel, in the Cognos Incentive Compensation Management Windows Service configuration file, you will need to set up a secure API address and port and add the certificate required for access.

Procedure

1. Under API secure address and port, change the Value to equal [certificate name]:[port number].
   For example, <add key="APISecureAddress" value="MobileAPI:13125"/>
2. Under API certification required for access, change the Value to equal the certificate name.
   For example, <add key="APICertificateName" value="MobileAPI"/>.
Configuring the identity of the server hosting the service for the Microsoft Excel add-in
To set up the Windows Service for the IBM® Cognos® Incentive Compensation Management add-in for Microsoft Excel, you must configure the identity of the server that hosts the service in the hosts file.

Procedure
1. Go to C:\Windows\system32\drivers\etc and open the hosts file in Notepad.
2. Type the IP address of the computer that hosts the service and type the certificate name. The IP address and the certificate name must be separated by at least one space, for example, 127.0.0.1 MobileAPI.
3. Save and close the file.

Identifying the server certificate for the Microsoft Excel add-in
To set up the Windows Service for the IBM® Cognos® Incentive Compensation Management add-in for Microsoft Excel, you must use the HTTP Configuration Utility to identify the server certificate.

Procedure
1. Run the HTTP Configuration Utility.
2. Select the SSL tab and click Add.
3. Type the IP address of the server in the IP Address field and a port number in the Port field.
   Important: If a host name is used instead of an IP address, the host name must be mapped with the IP address in the host file. Go to C:\windows\system32\drivers\ to make this change.
4. Click Browse and select the server certificate.
5. Click OK.
6. Select the Permissions tab and make sure that permissions are granted for the appropriate group of users.
7. Click OK in the SSL Configuration dialog box.
8. Click OK to close the HTTP Configuration Utility.

Client-side setup for installing the add-in
If the server is using a private (self-signed) certificate, you will need to set up the certificates, identify the server certificate and configure the identity of the server hosting the service on the computer that runs the Cognos Incentive Compensation Management Client using the same steps that were used in the Service-side setup.

Certificates are required on both sides for the Service to access the Cognos Incentive Compensation Management Client. However, if the server is using a trusted certificate, it is not necessary to add certificates to the computer that runs the Client. You will need to install software to run the Cognos Incentive Compensation Management add-in for Microsoft Excel; then install the Cognos Incentive Compensation Management add-in for Microsoft Excel itself on the computer that runs the Client.

Required software to run the Microsoft Excel add-in
Before you install the IBM® Cognos® Incentive Compensation Management add-in for Microsoft Excel, you must install additional required software.
Users must have the following software installed on their computers to run the Cognos Incentive Compensation Management add-in for Microsoft Excel 2007 or 2010:

- Office Primary Interop Assemblies tools
- Microsoft Visual Studio Tools for the Microsoft Office system (version 3.0 Runtime) (x86), which can be found at www.microsoft.com
- Microsoft Visual Studio Tools for the Microsoft Office System (version 3.0 Runtime) Service Pack 1 (x86), which can be found at www.microsoft.com

Users must have the following software installed on their computers to run the Cognos Incentive Compensation Management add-in for Microsoft Excel 2003:

- Office Primary Interop Assemblies tools
- Microsoft Visual Studio 2005 Tools for Office Second Edition Runtime (VSTO 2005 SE) (x86), which can be found at www.microsoft.com

**Installing Office Primary Interop Assemblies tool for the Microsoft Excel add-in**

To run the IBM® Cognos® Incentive Compensation Management add-in for Microsoft Excel, you must have the Office Primary Interop Assemblies tool installed.

**Procedure**

1. In the Control Panel, select Add or Remove Programs.
2. Select Microsoft Office and click Change.
4. Click the arrow and select Run from My Computer.
5. Click Continue.
6. When the configuration process is complete, click Close.

**Certificates and services**

When installing the IBM Cognos Incentive Compensation Management add-in for Microsoft Excel, certificates and services must be set up on the client-side if the server is using a private (self-signed) certificate. If the server is using a Trusted certificate, you do not need to set up certificates and services on the client.

Complete the following tasks to set up certificates and services on the client-side:

- “Setting up certificates for the Microsoft Excel add-in” on page 52
- “Identifying the server certificate for the Microsoft Excel add-in” on page 54
- “Configuring the identity of the server hosting the service for the Microsoft Excel add-in” on page 54

**Important:** Setting up certificates and services on the client-side is only necessary when the server is using a private (self-signed) certificate

**Installing and connecting the add-in**

After all the requirements have been met, you can install the Cognos Incentive Compensation Management add-in for Microsoft Excel.
Attention: Before installing the Cognos Incentive Compensation Management add-in for Microsoft Excel, make sure the Cognos Incentive Compensation Management Windows Service has been stopped and restarted after the changes to the Cognos Incentive Compensation Management Windows Service configuration file were made, and make sure that the Cognos Incentive Compensation Management API Service is running.

Procedure

1. Run the ICM-exceladdin installer provided in the release and follow the steps in the installation wizard.

2. Open Microsoft Excel.
   A quick Add-in installation runs.

3. After running the Cognos Incentive Compensation Management add-in, you will see an IBM Cognos Incentive Compensation Management tab on the menu bar in Microsoft Excel.

4. Click the IBM Cognos Incentive Compensation Management tab.

5. To connect to a model, type in the Service Address.
   This is the same address that you specified in the Cognos Incentive Compensation Management Windows Service configuration file, for example, MobileAPI:13125.

6. Type the server name.
   This is the server name that you specified in the databaseServers section of the Cognos Incentive Compensation Management Windows Service configuration file, for example, SQLServer2005 (local).

7. Type the database name.
   This is the name of the database containing the model that you want to connect to, for example, Rivacent.

8. Click Log in Information.

9. Type your user name and password for the Cognos Incentive Compensation Management Client and click Save.

10. Click Import Star Schema or Import Data Store to download data into Microsoft Excel from your Cognos Incentive Compensation Management model.
Chapter 4. The IBM Cognos Incentive Compensation Management web client

If you are using a Microsoft Windows operating system, you can install and configure the IBM® Cognos® Incentive Compensation Management web client with Apache Tomcat, JBoss, or WebSphere®.

If you are using other operating systems, the steps are similar. You can also set up multi-language and Unicode data support and how to configure the appearance of the web client.

The web client requires the Cognos Incentive Compensation Management Windows service (or the Console Service tool) to be installed and running on a server along with a model.

Installing the web client on the Solaris operating system

The IBM® Cognos® Incentive Compensation Management web client can be installed on a Solaris operating system.

Procedure

1. Copy the ICM.war file to your deployment location.
2. Create a directory.
3. Move the ICM.war file to the directory.
4. Extract the ICM.war file.
5. Deploy according to Windows instructions.

Deployment of the web client with Apache Tomcat

You can use Apache Tomcat, versions 6 or 7, to deploy the IBM® Cognos® Incentive Compensation Management web client.

The deployment consists of the following tasks:

- Install and configure Java
- Install and configure Apache Tomcat
- Deploy the ICM WAR file and configure database access

Installing and configuring Java

For Apache Tomcat to deploy the IBM® Cognos® Incentive Compensation Management web client correctly, Java, version 6 or 7 JRE must be downloaded and installed.

Procedure

Installing and configuring Apache Tomcat

Apache Tomcat must be installed and running on your computer before the IBM® Cognos® Incentive Compensation Management web client can be deployed.

Procedure

Download and install Apache Tomcat, version 6 or 7 from http://tomcat.apache.org/download-60.cgi:

1. If you are installing the web client on Windows, download and run the Windows Service Installer Tomcat distribution.
2. If you are not installing the web client on Windows, install Tomcat with the archive on the following website: http://tomcat.apache.org.

Important: When Tomcat is run as a service, no tray icon is present while Tomcat is running, except if you opt to run Tomcat at the end of the installation process. In this situation, the installer creates shortcuts for starting and configuring Tomcat. The Tomcat web administration application can be used only when Tomcat is running.

Using Apache Tomcat to deploy the web client

You can use Tomcat Manager to deploy the IBM® Cognos® Incentive Compensation Management web client.

Procedure


   Tip: By default, Apache Tomcat runs on port 8080, but if you specified a different port number during the installation of Tomcat, use that port number instead.
2. Click the Tomcat Manager link and log in with the user name and password that you specified during the Tomcat installation.
3. In the Deploy section of the Tomcat Manager page, click Browse.
4. Find the ICM.war file and click Deploy.

   When the page refreshes, an /ICM link opens under the Applications heading.

   Important: Cognos Incentive Compensation Management requires uniquely named WAR files when you deploy the WAR file as part of an upgrade. Either uninstall your current WAR file before you deploy a new one, or change the name of the new WAR file.
5. Click the /ICM link to verify deployment.

Results

When you verify the deployment, you might see a Cognos Incentive Compensation Management web client window that describes an internal error. This message indicates that the web client was deployed, but access to the Cognos Incentive Compensation Management database must be configured.

Using Apache Tomcat to configure database access

After you install and configure Apache Tomcat, you must edit the web client configuration file to point to your model in IBM® Cognos® Incentive Compensation Management.
About this task

After the application is deployed in Tomcat, the jdbc.properties file must be edited. It can be found in C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps\ICM\WEB-INF\jdbc.properties.

Procedure

1. Open the jdbc.properties file with a text editor such as WordPad.

Restriction: Do not use Notepad because it does not support UNIX text format.

2. Edit the Server parameter with the host name of your SQL Server computer, such as localhost:1433. 1433 is the default SQL Server port, but the port number might be different if you are connecting to a named instance. For example, a named instance at \DBserver\SQL2000 runs on port 2140). Use SQL Server Configuration Manager to check the port number.

3. Edit the database name with the name of the database that contains the model. The name is case-sensitive.

4. Edit username and password with the user name and password of the SQL Server account with appropriate rights to access the Cognos Incentive Compensation Management database.

5. Save the updated jdbc.properties file.

Tip: You can also save a copy of the file in another location to use for reference when the application is redeployed, such as when you upgrade to a newer version.

6. Go back to Tomcat Manager and click the Reload link to propagate the changes.

7. Go to http://localhost:8080/ICM.

Results

If your server is running Cognos Incentive Compensation Management Windows Service with an existing model, all the users who are set up in Portal Access through the .NET client can now log in.

Configuring multi-language and Unicode data support for Apache Tomcat

To support UTF-8 encoding or to access a link that contains accented characters in the IBM® Cognos® Incentive Compensation Management web client, the web server must be configured to interpret URIs as UTF-8. If you are using Apache Tomcat as your web server, the default is not UTF-8, so you must change this setting.

Procedure

1. Go to C:\Program Files\Apache Software Foundation\Tomcat 6.0\conf

2. Open the server.xml file.

3. Find the connector that is using the HTTP protocol.

4. Add the following line: URIEncoding="UTF-8"
   The server.xml file now contains the following code:
   <Connector port="8080" protocol="HTTP/1.1"
   connectionTimeout="20000"
   redirectPort="8443"
   URIEncoding="UTF-8"/>
Deployment of the web client with JBoss

You can use JBoss to deploy the IBM® Cognos® Incentive Compensation Management web client.

The deployment consists of the following tasks:
• Install and configure Java
• Install and configure JBoss
• Deploy the ICM WAR file and configure database access

Installing and configuring Java for JBoss

When you deploy the IBM® Cognos® Incentive Compensation Management web client on the latest JBoss release, you must have the Java Software Development Kit 5.0 or higher.

Procedure


Installing and configuring JBoss

When your Java environment is in place, you can go to the JBoss website to download the application server for use with the IBM® Cognos® Incentive Compensation Management web client.

Procedure

2. From the Downloads page, select the JBoss Application Server version that you want to download.
3. Download the appropriate file and extract it to the appropriate directory.

Configuring database access for JBoss

You must edit the IBM Cognos Incentive Compensation Management web client configuration file to point to your Cognos Incentive Compensation Management model.

The jdbc.properties file needs to be pre-configured so that once the application has been deployed, the jdbc.properties file can be copied and pasted into the ICM WAR file. JBoss will not automatically expand the Cognos Incentive Compensation Management web WAR file.

Procedure

1. Navigate to the location where your Cognos Incentive Compensation Management WAR file is stored.
2. Rename the WAR file to ICM.zip.
   This allows you to navigate to within the WAR file.
3. Open the ZIP file and navigate to the WEB-INF folder.
4. Copy the jdbc.properties file.
5. Navigate back out of the ZIP folder and paste the jdbc.properties file.
6. Rename the ZIP folder to ICM.war.
7. Open the jdbc.properties file using a text editor such as, WordPad.
   Do not use Notepad because it does not support UNIX text format.
8. Modify Server with the hostname of your SQL Server machine, for example, localhost:1433.
   1433 is the default SQL Server port, but the port number may be different if you are connecting to a named instance (for example, a named instance at \DBserver\SQL2000 runs on port 2140). Use SQL Server Configuration Manager to check the port number.
9. Modify the database name with the name of the database containing the Cognos Incentive Compensation Management model (it is case-sensitive).
10. Modify username and password with the username and password of the SQL Server account with appropriate rights to access the Cognos Incentive Compensation Management database.
11. Save the updated jdbc.properties file.
   You may also want to save a copy of the file in an alternate location to use for reference when the application is redeployed, such as when upgrading to a newer version.

Using JBoss to deploy the web client

After Java and JBoss are installed and the jdbc.properties file is configured, the IBM® Cognos® Incentive Compensation Management web client must be manually deployed.

About this task

JBoss does not automatically deploy the WAR file, so you must configure the Cognos Incentive Compensation Management web client.

Procedure

1. Create a file that is called jboss-web.xml and save it in an accessible location.

   Tip: It is a good idea to save this file with your ICM.war file and your pre-configured jdbc.properties file.

   a. In WordPad or a similar application, copy the following text into the jboss-web.xml file:

   

   ```
   <jboss-web>
   <!-- Uncomment the security-domain to enable security. You will need to edit the htmladaptor login configuration to setup the login modules used to authenticate users. -->
   <security-domain>java:/jaas/jmx-console</security-domain>
   -->
   </jboss-web>
   ```

   b. Save the jboss-web.xml file.

2. Copy the version of the WAR file into \jboss-[version].GA\server\default\deploy\.

   Tip: You can rename the WAR file to something other than ICM for usability.

3. To navigate within the file to \WEB-INF, change the file extension from .war to .zip.
4. Replace the jdbc.properties file with the pre-configured jdbc.properties file.

5. Paste the jboss-web.xml file into the WEB-INF folder.

6. In \jboss-[version].GA\server\default\deploy, change the file extension from .zip back to .war.

7. Start JBoss by running the run.bat file in \..\jboss-[version].GA\bin\run.bat

8. Navigate to http://localhost:8080/ICM, where ICM is the name of the WAR file.

Configuring multi-language and Unicode data support for JBoss

To support UTF-8 encoding or to access a link that contains accented characters in the IBM® Cognos® Incentive Compensation Management web client, the web server must be configured to interpret URIs as UTF-8. If you are using JBoss as your web server, the default is not UTF-8, so you must change this setting.

Procedure

1. Go to the following location: C:\Program Files\JBoss\jboss-[version].GA\server\default\deploy\jboss-web.deployer\
2. Open the server.xml file.
3. Find the connector that is using the HTTP protocol.
4. Add the following line: URIEncoding="UTF-8"
   The server.xml file now contains the following code:
   ```xml
   <Connector port="8080" address="${jboss.bind.address}"
   maxThreads="250" maxHttpHeaderSize="8192"
   emptySessionPath="true" protocol="HTTP/1.1"
   enableLookups="false" redirectPort="8443" acceptCount="100"
   connectionTimeout="20000"
   disableUploadTimeout="true" URIEncoding="UTF-8"
   />
   ```
5. Save the file.
6. Restart the file.

Deployment of the web client with IBM WebSphere 7

You can use IBM WebSphere 7 to deploy the IBM® Cognos® Incentive Compensation Management web client.

After you install and configure WebSphere, you must install the Cognos Incentive Compensation Management WAR file and configure the jdbc.properties file.

You can find the web client log file in the following WebSphere installation directory: <WebSphere installation>\profiles\<Server Profile>.

Deploying the web client on WebSphere 7

After you install IBM WebSphere, you can deploy the IBM® Cognos® Incentive Compensation Management web client from the WebSphere Admin Console.

Procedure

1. Log in to the Admin Console and select Applications.
2. Select New Applications.
4. Browse to the WAR file that you want to deploy and click Next.
5. Select Detailed - Show all installation options and parameters and click Next.
6. Click Continue on the Application Security Warning screen.
7. Specify Application name, such as ICM803.
8. Highlight All File Permissions and click Next.
9. On Step 2, check the select box and click Next.
10. On Step 3, click Next.
11. On Step 4, check the selection box that corresponds with the current application and click Next.
12. On Step 5, check the selection box that corresponds with the current application and click Next.
13. On Step 6, check the selection box and click Next.
14. Specify a unique context root for the WAR file, such as /ICM803, and click Next.
15. Click Finish on the Summary page.
16. Click Save.
18. Click New.
19. Specify the name as java.awt.headless and set the value to False.
20. Click Apply, and then click OK.
21. Select the Save directly to the master configuration option.

Configuring database access using WebSphere 7

After you deploy the WAR file, you must edit the jdbc.properties file in two locations to configure access to the IBM Cognos Incentive Compensation Management database.

About this task

For Windows systems, the file can be found in the following locations:
- C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\config\cells\ [server name]Node01Cell\ applications\CONTEXT ROOT_war.ear\deployments\ CONTEXT ROOT_war\CONTEXT ROOT.war\WEB-INF
- C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\installedApps\ ..\..\ ICM.war\WEB-INF

For UNIX-like systems, the file can be found in the following locations:
- /AppServer/profiles/AppSrv01/installedApps/../../ICM.war/WEB-INF
- /AppServer/profiles/AppSrv01/installedApps/../../WEB-INF
- /AppServer/profiles/AppSrv01/config/cells/../../WEB-INF

Procedure
1. Open the jdbc.properties file using a text editor such as WordPad.
   Do not use Notepad because it does not support UNIX text format.
2. Modify **Server** with the hostname of your SQL Server computer, for example, localhost:1433.

   The default SQL Server port is 1433, but the port number may be different if you are connecting to a named instance (for example, a named instance at \DBserver\SQL2000 runs on port 2140). Use SQL Server Configuration Manager to check the port number.

3. Modify **database name** with the name of the database containing the Cognos Incentive Compensation Management model (it is case sensitive).

4. Modify **username** and **password** with the username and password of the SQL Server account with appropriate rights to access the Cognos Incentive Compensation Management database.

5. Save the updated jdbc.properties file.

   You may also want to save a copy of the files in an alternate location to use for reference when the application is redeployed, such as when upgrading to a newer version.

### Using the WebSphere Admin Console to start the web client

After WebSphere has been installed and the IBM Cognos Incentive Compensation Management web client has been deployed, you can launch the web client from the WebSphere Admin Console.

**Procedure**

1. Log in to the Admin Console.
2. Select **Applications > Application Types > Websphere enterprise applications**.
3. Select the Cognos Incentive Compensation Management application.
4. Click **Start**.
   
   **Attention:** If you forget the associated context root, select the application name. Select the Context Root for Web Modules option.
5. Open an internet browser on your local computer.
   
   For example: http://server:9080/CONTEXT_ROOT/login.html

### Setting a web container custom property on WebSphere

To avoid the WebSphere error Error 404:SRVE0190E:File not found: /j_spring_security_check when attempting to log in to the IBM Cognos Incentive Compensation Management web client, the following property must be set to true: com.ibm.ws.webcontainer.invokefilterscompatibility = true.

**Procedure**

1. In the administrative console, click **Servers > Application Servers**.
2. Click the server to which the custom property is to be applied.
3. Under **Configuration > Container Settings**, select **Web Container Settings > Web Container**.
4. Under **Configuration > Additional Properties**, select **Custom Properties**.
5. In the **Custom Properties** page, click **New**.
6. In the **Settings** page, type the name of the custom property to be added in the **Name** field and the value to be set for the custom property in the **Value** field.
   
   **Attention:** Some properties are case-sensitive.
7. Click **Apply** or **OK**.
8. Restart the server for the custom property to take effect.

**Configuring multi-language and Unicode data support for WebSphere**

In order to support UTF-8 encoding or when accessing a link that contains accented characters in the IBM Cognos Incentive Compensation Management web client, the web server must be configured to interpret URIs as UTF-8. If you are using WebSphere as your web server, the default is not UTF-8 so you must change this setting.

**Procedure**

1. Go to the following location: \Program Files\IBM\WebSphere\AppServer\properties\
2. Open the encoding.properties file.
3. Replace "en=ISO-8859-1" with "en=UTF-8".
4. Save the file.
5. Restart the web service.

**Deployment of the web client with WebSphere 9**

The IBM Cognos Incentive Compensation Management web client can be deployed using WebSphere 8.

After installing and configuring WebSphere, you will need to install the Cognos Incentive Compensation Management WAR file and configure the JDBC properties file.

**Configuring WebSphere 8**

Before deploying the IBM Cognos Incentive Compensation Management web client on WebSphere, you will need to create an application server profile and start the server.

**Procedure**

1. Go to Start > All Programs > IBM WebSphere Application Server V8.0 > Tools > Profile Management Tools.
2. Click Create.
3. Select Application server and click Next.
4. Select Typical profile creation and click Next.
5. Clear Enable administrative security and click Next.
6. Note the Administrative console port and the HTTP transport port number that is listed.
7. Click Create.
8. Click Finish.
   The WebSphere Application Server - First Steps - <server name> window is displayed.
9. Click Start the Server.

**Deploying the web client on WebSphere 8**

The IBM Cognos Incentive Compensation Management web client can be deployed from the WebSphere Admin Console.
Procedure

1. In your browser, navigate to the WebSphere Admin Console and log in. The default address is localhost:9060/ibm/console.
2. On the left pane, go to Servers > Server Types > WebSphere Application Servers.
3. Click your server.
6. Click New.
   a. In the Name field, type com.ibm.ws.webcontainer.initFilterBeforeInitServlet.
   b. In the Value field, type true.
7. Click New.
   a. In the Name field, type com.ibm.ws.webcontainer.invokeFilterInitAtStartup.
   b. In the Value field, type true.
8. Click the Save directly to master configuration link.
9. On the left pane, go to Applications > Application Types > WebSphere enterprise applications.
10. Select the three default applications and click Uninstall.
11. Click Install.
12. Click Browse and navigate to the ICM.war file.
13. Click Next.
14. Select the Fast Path option and click Next.
15. Leave the default settings selected in step 1, 2, 3, and 4.
16. Click Finish.
17. Click the Save directly to master configuration link.
18. Click the ICM_war link.
19. Click Session management.
   a. Select Override session management.
   b. Enable cookies and URL rewriting.
20. Click Request dispatcher properties.
   a. Select Allow dispatching includes to remote resources.
   b. Select Allow servicing includes from remote resources.

Configuring database access using WebSphere 7

After you deploy the WAR file, you must edit the jdbc.properties file in two locations to configure access to the IBM Cognos Incentive Compensation Management database.

About this task

For Windows systems, the file can be found in the following locations:

- C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\config\cells\[server name]Node01Cell\applications\CONTEXT ROOT_war.ear\deployments\CONTEXT_ROOT_war\CONTEXT_ROOT_war\WEB-INF
- C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\installedApps..\..\..\ICM.war\WEB-INF
For UNIX-like systems, the file can be found in the following locations:

- `/AppServer/profiles/AppSrv01/installedApps/../../ICM.war/WEB-INF` For example, `/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/installedApps/../../ICM.war/WEB-INF`
- `/AppServer/profiles/AppSrv01/config/cells/../../WEB-INF` For example, `/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/config/cells/../../WEB-INF`

**Procedure**

1. Open the `jdbc.properties` file using a text editor such as WordPad. Do not use Notepad because it does not support UNIX text format.
2. Modify `Server` with the hostname of your SQL Server computer, for example, `localhost:1433`. The default SQL Server port is 1433, but the port number may be different if you are connecting to a named instance (for example, a named instance at `\DBserver\SQL2000` runs on port 2140). Use SQL Server Configuration Manager to check the port number.
3. Modify `database name` with the name of the database containing the Cognos Incentive Compensation Management model (it is case sensitive).
4. Modify `username` and `password` with the username and password of the SQL Server account with appropriate rights to access the Cognos Incentive Compensation Management database.
5. Save the updated `jdbc.properties` file.

Using the WebSphere Admin Console to start the web client

After WebSphere has been installed and the IBM Cognos Incentive Compensation Management web client has been deployed, you can launch the web client from the WebSphere Admin Console.

**Procedure**

1. Log in to the Admin Console.
2. Select `Applications > Application Types > Websphere enterprise applications`.
3. Select the Cognos Incentive Compensation Management application.
4. Click `Start`. **Attention:** If you forget the associated context root, select the application name. Select the Context Root for Web Modules option.
5. Open an internet browser on your local computer.

**Property file encryption**

The IBM Cognos Incentive Compensation Management web client can be configured to accept encrypted passwords across all properties files, such as the `jdbc.properties` and `ldap.properties` files.
This provides additional local security in the form of obfuscation. Keep in mind that someone must still have knowledge of the encryption key and passwords are transmitted in plain text, unless transmission security, such as SSL, is enabled.

Obtaining encrypted passwords

Using the Java Simplified Encryption (Jasypt) toolset, encrypted strings can be obtained for the passwords to be secured for the IBM Cognos Incentive Compensation Management web client.

Procedure
1. Download the latest Jasypt distribution.
2. Unzip the archive to a location that is easily accessible via command line, such as your Desktop.
3. Make sure the JAVA_HOME environment variable is set and points to the installed Java distribution folder.
4. Open a command prompt window and navigate to the unzipped Jasypt folder.

   Important: If only Java 5 is available, users must also download ICU4J and include the JAR when running the Jasypt CLI tools.

Configuring web client password encryption

The Cognos Incentive Compensation Management web client must be configured to understand property files that contain encrypted values.

Procedure
1. Open the applicationContext.xml file.
2. Edit the file so it looks like the following section of code:

   ```xml
   <!-- Property configuration -->
   <bean id="envConfig" class="org.jasypt.encryption.pbe.config.EncironmentStringPBEConfig">
       <property name="passwordEnvName" value="VARICENT_KEY" />
   </bean>

   <bean id="configEncryptor" class="org.jasypt.encryption.be.StandardPBEStringEncryptor">
       <property name="config" ref="envConfig" />
   </bean>

   <!-- bean id="propertyConfigurer" class="org.jasypt.spring.properties.EncryptablePropertyPlaceholderConfigurer" -->
   <constructor-arg ref="configEncryptor" />
   <property name="locations">
       <list>
           <value>/WEB-INF/jdbc.properties</value>
           <value>/WEBINF/ldap.properties</value>
           <value>/WEB-INF/mail.properties</value>
           <value>/WEB-INF/saml.properties</value>
           <value>/WEB-INF/siteminder.properties</value>
       </list>
   </property>
   </bean>
   ```
Configuring web client password encryption in a Windows environment

A system environment variable containing the encryption password needs to be set before deployment so the Cognos Incentive Compensation Management web client knows how to decrypt the encrypted passwords.

Procedure
1. Right-click My Computer and select Properties.
2. Navigate to the Advanced tab and click Environment Variables.
4. Type VARICENT_KEY in the first field and your password in the second field.
5. Click OK to apply all changes.
6. If the Web application container service is configured to run under the Windows Local System user account, Windows will need to be restarted.

Deployment of the web client with encrypted passwords

To deploy the Cognos Incentive Compensation Management web client, the appropriate property file needs to be configured with the encrypted passwords.

Using jdbc.properties as an example:

```
# Microsoft SQL Server
jdbc.productName=sqlserver
jdbc.driverClassName=net.sourceforge.jtds.jdbc.Driver
jdbc.url=jdbc:jtds:sqlserver://hostname:1433/database

#jdbc.url=jdbc:jtds:sqlserver://localhost:1433/database;instance=SQLEXPRESS
#jdbc.url=jdbc:jtds:sqlserver://localhost:1433/database;domain=DOMAIN;useNTML2=false
jdbc.username=sa
jdbc.password=ENC(1qZ5aIYYQ11TsjiTcQfg==)
```

After saving the file, you will need to restart your the Cognos Incentive Compensation Management web application service, such as the Apache Tomcat service, for the changes to take effect. At this point, the environment variable containing the encryption key can be removed.

Configuring multi-language and Unicode data support for locale

Users can set their locale on the IBM Cognos Incentive Compensation Management web client with a URL parameter equal to a two- or four-letter code that only needs to be passed once on any page. For example, use http://hostname/ICM/home.html?locale=fr to switch to French.

About this task

The following languages are available:
- English: en [Default]. This will also set the language to English and the date format to month/day/year.
- English: en_GB. This will set the language to English and the date format to day/month/year.
- French: fr
- German: de
The following database types can technically be supported:
- SQL Server 2005, SQL Server 2005 Unicode
- SQL Server 2008, SQL Server 2008 Unicode
- SQL Server 2012, SQL Server 2012 Unicode

**Procedure**
1. Edit the database type in the IBM Cognos ICM Windows Service.exe.config file. For example, `<add key="DBType" value="SQLServer2005Unicode"/>`.
2. Edit the database type in the jdbc.properties file. For example, `jdbc.productName=sqlserverunicode`.

**Emailing users when an inquiry is pending**

You can choose to have an email sent automatically to the designated inquiry handler when an inquiry is launched in the IBM Cognos Incentive Compensation Management web client.

You will need to configure settings in the client and the IBM Cognos Incentive Compensation Management web configuration files in order to have the email sent to the correct user after an inquiry is started.

**Procedure**
1. Configure the email settings in the mail.properties file. The mail.properties file is in the following directory: `...\webapps\ICM\WEB-INF`.
2. Reload the ICM.war file after you edit the configuration files.
3. In the admin client, click Admin > Administrative Options, and click the Portal Access tab.
4. Select the Email users when an inquiry is pending check box.
5. Click OK.

**Preventing Presenter reports from loading with a large amount of data**

By configuring the reporting.properties file in the WEB-INF folder of the IBM Cognos Incentive Compensation Management WAR file, you can limit the number of rows displayed by an aggregate transformation in the Cognos Incentive Compensation Management web client.

If a Presenter report contains an aggregate transformation used by a data grid, chart, map, or pick list control, and the aggregate transformation exceeds the row
limit set in the `reporting.properties` file, the report will not be displayed in the Cognos Incentive Compensation Management web client. By default, the value is set to '0', which means that there is no limit that will prevent the report from rendering.

**Procedure**
1. In the ICM.war file, navigate to the WEB-INF folder.
2. Open the `reporting.properties` file.
3. Change the `reporting.aggregateTransformationRowLimit` value to the maximum number of rows the aggregate transformation source can contain to allow the Presenter report to be rendered.
4. Restart the web server application that the Cognos Incentive Compensation Management web client is running on.

**Presenter report data grid row limits**

The number of rows that can be displayed on a Presenter report on the web client is configured in the `reporting.properties` file.

By default, the row limit is set to 15,000 rows. You can increase this value; however, the larger the row limit number, the longer it might take for the report to load on the web client. The `reporting.properties` file is located in the following directory: `C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps\ICM\WEB-INF`.

If you have a large data grid and want to limit the number of rows displayed on the report, you can add restrictions and filters to the source when creating the report.

**Disabling collection of Presenter report information**

By default, the name of the Presenter report and the web user who accessed the report are logged in the IBM Cognos Incentive Compensation Management web client log file. You can disable this setting in the `reporting.properties` file.

**Procedure**
1. In the ICM.war file, navigate to the WEB-INF folder.
2. Open the `reporting.properties` file.
3. Change the `reporting.exceptionShowReportInfo` value to `false`.
4. Restart the web server application that the Cognos Incentive Compensation Management web client is running on.

**Web client appearance**

The way web tabs are displayed to different web users in the web client is configured in the Portal Access module in the Cognos Incentive Compensation Management client.

The color scheme and logo displayed on the login window for the web client can be customized in the web client as well.
Web tab configuration

In the Portal Access module in the Client, administrators can customize the tabs that appear in the IBM Cognos Incentive Compensation Management web client.

Administrators can select the name, type, and sequence of tabs. This allows for administrators to build report-driven home pages that are appropriate for different Portal Access groups.

Web tabs can be created for individual plans, Presenter and tailored reports, and web forms. Module tabs can also be created by selecting either Data Edit, Inquiries, Payee Ledger, Reporting, Web Forms or external URLs. Users can organize tabs into web tab groups, which will create sub-tabs in the Cognos Incentive Compensation Management web client.

The following web tabs are available:
- Compensation Plan
- Draw Assignment
- Draw Report
- External URL
- Module
- Data Edit
- Inquiries
- Payee Ledger
- Reporting
- Web Forms
- Presenter Report
- Tailored Report
- Web Form

When only one object is assigned to a web tab, no sub-tabs are shown, and the plan, report, or form is rendered right away. When more than one object is assigned to a tab group, sub-tabs appear, and selection is required before anything is rendered. After web tabs are created, administrators must assign access to the tab itself and the objects that are included in the tab. If users do not have access to the web tab or the sub-tabs, then they will not see them in the Cognos Incentive Compensation Management web client.

Important: If you are upgrading your version 6.0 model, the tabs you have already set up will be displayed in Portal Access and the Cognos Incentive Compensation Management web client.

Creating a web tab
You must add web tabs in Portal Access so that users can access items in the IBM Cognos Incentive Compensation Management web client.

Procedure
1. In Portal Access, click the Web Tabs tab.
2. Click the Add Web Tab icon or right-click the screen and select Add Web Tab.
3. Name the web tab.
4. Select the Type of web tab.
5. Select the object that is assigned to the type of web tab. For example, if you select the **Compensation Plan** type, you must select a compensation plan.

6. Click **Finish**.

**Tip:** The first tab listed in Portal Access is the first tab that is displayed on the Cognos Incentive Compensation Management web client.

**Moving web tabs**
You can change the order and placement of web tabs after you have created them in the IBM Cognos Incentive Compensation Management client.

**Procedure**
1. In Portal Access, click the **Web Tabs** tab.
2. Press the Shift key and drag the web tab to the location you want.

**Editing a web tab**
After creating a web tab, you can modify the name, type, and object assigned to it in the IBM Cognos Incentive Compensation Management client.

**Procedure**
1. In Portal Access, click the **Web Tabs** tab.
2. Right-click a web tab and select **Edit Web Tab**.
3. Make your changes and click **Finish**.

**Deleting a web tab**
You can remove web tabs that are no longer needed in the IBM Cognos Incentive Compensation Management client.

**Procedure**
1. In Portal Access, click the **Web Tabs** tab.
2. Right-click a web tab, and select **Delete**.

**Adding a web tab group**
Web tab groups can be added to organize web tabs in the IBM Cognos Incentive Compensation Management client.

**Procedure**
1. In Portal Access, click the **Web Tabs** tab.
2. Click the **Add Web Tab Group** icon or right-click in the window, and select **Add Web Tab Group**.
3. Double-click the **New Web Tab Group**, and type in a name.
4. Click a web tab, and drag it to the web tab group.

**Removing a web tab from a group**
You can move a web tab from one group to another in the IBM Cognos Incentive Compensation Management client.

**Procedure**
1. In Portal Access, click the **Web Tabs** tab.
2. Click a web tab and move it above the web tab group while holding down the Shift key.
**Setting access to web tabs**
The user needs access to both the web tab and the objects inside to view them on the IBM Cognos Incentive Compensation Management web client.

For example, if you have a Reporting web tab, you need to set access to the Reporting web tab and to the individual Presenter reports.

**Procedure**
1. In Portal Access, click the **Assignment** tab.
2. Click your mouse under a column to show the drop-down menu arrow.
3. From the drop-down menu, select the **Access** tree for the web tab.

**Changing the web client theme**
The color scheme and logo displayed at the top of the screen in the IBM Cognos Incentive Compensation Management web client can be customized.

**Procedure**
1. In the Cognos Incentive Compensation Management client, select **Tools > Themes**.
2. Select the **Enable Custom Header** check box.
3. Browse for the image you want.
4. Select either **Standard** or **Salesforce.com** for the Web Theme.
5. Click **OK**.

**Attention:** Changes made here are effective in both the Cognos Incentive Compensation Management client and web client. The web deployment may need to be reloaded for the custom header to take effect on the Cognos Incentive Compensation Management web client.
Chapter 5. Authentication and sign on

Various communication and authentication options are available when configuring SiteMinder, Open SSO, or LDAP for IBM Cognos Incentive Compensation Management web client authentication.

Communication path options

There are different communication options between the components of Cognos Incentive Compensation Management.

Cognos Incentive Compensation Management consists of the following components and various communication options are available between each:

- Client
- Application server
- Database server
- Web server
- Web client

Security options for communications between the client and the application server

You can choose different levels of security for the communication between the Cognos Incentive Compensation Management client and the application server.

The following security options are available in the Cognos Incentive Compensation Management Windows Service configuration file:

TLS Security - communication encryption

<!-- Transport Layer Security Mode -->
<!--Clients are unauthenticated by WCF when using TLS. Server must provide a trusted certificate to authenticate itself-->
<add key="SecurityMode" value="TLS"/>
<add key="ServiceCertificateName" value="varicent.com"/>

Windows Domain - trusted network

<!-- Windows Security Mode -->
<!--Clients and servers are authenticated via Kerberos using the domain controller as a trusted 3rd party. No certificates required.-->
<add key="SecurityMode" value="Windows"/>

No Security - no security

<!-- Unprotected Security Mode -->
<!--Set security mode="None" on both client and server to disable all security.-->
<add key="SecurityMode" value="None"/>

Security options for communications between the application server and the database server

You can choose different levels of security for the communication between the Cognos Incentive Compensation Management application server and the database server.

You can select the following levels of security:
Trusted Network
Traditionally, both the Web application server and the database server are on the same trusted network and channel encryption is not used.

Trusted Network and SSL
Our JDBC connector from the Web application to the database server can optionally be configured to use SSL to encrypt communication.

Communication methods between the web client and the web application
There are two different types of communication methods available between the web client and the Cognos Incentive Compensation Management web application.

You can select the following communication methods:

Traditional HTTP (unencrypted communication)
Traditional HTTP is the default communication setting used for communication between the web client and the Cognos Incentive Compensation Management web application.

Secure HTTP (HTTPS) (encrypted communication)
Encrypted communication can be achieved using an SSL certificate that is installed on the web server.

Encryption methods for communication between the web application server and the database server
The web application server and the database server are usually on the same trusted network, but you can choose to use SSL to encrypt communication.

You can select the following encryption methods:

Trusted Network
Traditionally, both the web application server and the database server are on the same trusted network and channel encryption is not used.

Trusted Network and SSL
Our JDBC connector from the web application to the database server can optionally be configured to use SSL to encrypt communication.

Authentication options
There are several different authentication options for use with IBM Cognos Incentive Compensation Management.

Cognos Incentive Compensation Management offers the following authentication options:

Native
Cognos Incentive Compensation Management-specific logins are determined in Portal Access, not single sign on (SSO).

LDAP Directory
Typically, Microsoft Active Directory integration, which allows users to use their network credentials to log in, but does not do so automatically.

Any SAML 2 compliant SSO resource, such as CA SiteMinder, Sun OpenSSO, PingIdentity
Cognos Incentive Compensation Management natively supports SAML2
authentication, automatically authenticating users who have a SAML2 compliant credentialing resource. SSO is a method of access control that enables a user to log in once and gain access to the resources of multiple software systems without being prompted to log in again.

**Custom SSO**
Some clients have developed their own custom authentication options. These are not supported directly by the Cognos Incentive Compensation Management Support team.

---

**SiteMinder configuration**

SiteMinder allows customers to manage users and privileges in an external repository, including an LDAP directory. For more information on this, contact a Cognos Incentive Compensation Management client support representative.

**Configuring the web client for CA SiteMinder**

In order to use SiteMinder to access the Cognos Incentive Compensation Management web client, SiteMinder administrators will need to make sure that the web client is included in the SiteMinder domain.

**Procedure**

1. Open `web.xml` in a text editor.
2. Change `security.xml` to `security-siteminder.xml`.
3. In the `siteminder.properties` file, define what property is being used for authentication purposes.
   
   By default, Cognos Incentive Compensation Management looks at the `SM_USER` attribute in the SiteMinder header and matches the `Email` field to the `Email` field in the Cognos Incentive Compensation Management Payee table. If you want to use a different column for authentication, change the `siteminder.userKeyColumn` value.
   ```
siteminder.userKeyAttribute=SM_USER
siteminder.userKeyColumn=Email_
```
4. Save `web.xml` and `siteminder.properties`.
5. Restart the Cognos Incentive Compensation Management web client by using your web server's management console.

Users can log in to the web client with their CA SiteMinder authentication.

**Web client access with SiteMinder**

To access the IBM Cognos Incentive Compensation Management web client, you must go to the SiteMinder site and enter your user name and password.

Once you are logged on to SiteMinder, you can navigate to the Cognos Incentive Compensation Management web client home page without having to retype their login credentials.

The SiteMinder administrator may provide a link that takes you directly to the Cognos Incentive Compensation Management web client home page from the SiteMinder site. If no link is provided, you can navigate to the Cognos Incentive Compensation Management web client home page yourself after logging in to SiteMinder.

Keep in mind that the URL used to navigate to the Cognos Incentive Compensation Management web client should take you directly to the Cognos
Incentive Compensation Management web client home page (or another post-authentication screen) and not the web client login screen (for example, http://...home.html and not http://...login.html). If you go to the web client pre-authentication screen, you are prompted to re-enter your user name and password.

OpenSSO configuration

IBM Cognos Incentive Compensation Management natively supports authentication via Sun OpenSSO, a SAML 2 compliant identity provider.

The following steps depict how the SAML 2 language and the OpenSSO sign on solution work to authenticate Cognos Incentive Compensation Management users for the Cognos Incentive Compensation Management web client.

Cognos Incentive Compensation Management natively supports all SAML 2 compliant identity providers, so while this document uses the OpenSSO example, the following steps also apply to other SAML 2 compliant identity providers.

1. Browse to the Cognos Incentive Compensation Management web client.
2. The Client is evaluated.
3. Cognos Incentive Compensation Management redirects the browser to SSO URL.
4. The web browser redirects to SSO URL.
5. SAML response is generated by the client network SSO provider.
6. Client returns encoded SAML response to browser.
8. SAML response is verified by Cognos Incentive Compensation Management.
9. User is logged into Cognos Incentive Compensation Management.

OpenSSO can be deployed on a range of platforms and application containers including the following applications:

Oracle Glassfish Server
A free and fully J2EE compliant application server.

Apache Tomcat
The easiest to configure.

This document covers the installation of OpenSSO in an Apache Tomcat environment.

Downloading and installing OpenSSO
OpenSSO can be downloaded and installed in an Apache Tomcat environment for use with IBM Cognos Incentive Compensation Management.

Before you begin
Download the latest version of OpenSSO, as well as Apache Tomcat and Java. For example, download the following items:

- Java 6 Development Kit
- Apache Tomcat 6
• OpenSSO Enterprise 8

**Procedure**

1. Set Tomcat's initial and maximum memory pool to 1024 MB.
2. Navigate to Tomcat Manager and deploy the opensso.war file found in the opensso/deployable-war folder of the OpenSSO distribution.

**Configuring OpenSSO**

During setup of OpenSSO authentication with the IBM Cognos Incentive Compensation Management web client, when the OpenSSO configuration wizard is finished, you must specify an external data store.

**Procedure**

1. Log in to the OpenSSO administration area using amadmin. All URLs that are submitted must contain fully qualified domain names, such as host.domain.com. Short names, such as localhost or host, are unacceptable.
2. A user data store, such as Microsoft Active Directory, can be specified here. OpenSSO provides a built-in service for development and testing use only. For production, Oracle's free OpenDS is recommended if no existing data store is available. The built-in service can be used temporarily for this deployment until an external data store can be properly configured at a later time.

**Identity provider (IDP) configuration**

During setup of OpenSSO authentication with the IBM Cognos Incentive Compensation Management web client, to configure the identity provider, the OpenSSO Keystore must be set up.

**Keystore setup**

During setup of OpenSSO authentication with the IBM Cognos Incentive Compensation Management web client, before creating a hosted identity provider, you will need to set up the Keystore.

OpenSSO provides a default test key for testing purposes. This key should not be used in production.

**Adding and configuring IDP**

During setup of OpenSSO authentication with the IBM Cognos Incentive Compensation Management web client, you must select the signing key, choose a name for the new circle of trust, and map an attribute to use as the SAML NameID.

**Procedure**

1. From the **Common Tasks** tab under the **Create SAMLv2 Providers** heading, click **Create Hosted Identity Provider**.
   - The IDP name should already be populated.
2. Select the signing key imported previously.
3. Choose a name for the new circle of trust.
4. Map an attribute to use as the SAML NameID.
   - This is usually the user’s email address (the mail attribute).
5. Click **Configure > Finish**.
Important: If an external user data store was not specified in the OpenSSO configuration wizard, a test user will need to be added through the OpenSSO administration interface. The demonstration account can be used, but an email address will still need to be entered in the user's profile.

Service provider configuration

To deploy the IBM Cognos Incentive Compensation Management web client as a SAML service provider, you will need to make some configurations in Apache Tomcat and the Cognos Incentive Compensation Management web client.

Before the Cognos Incentive Compensation Management web client can be deployed as a SAML service provider (SP), the following three things must be obtained from the identity provider (IDP):

- IDP SAML meta data file (usually idp.xml)
- SSL keystore file (usually keystore.jks)
- Signing key credentials in keystore (alias and password)

Begin by deploying the ICM.war file in the web application server.

Endorsed libraries

The IBM Cognos Incentive Compensation Management web client's SAML implementation requires the use of more advanced XML components than what is available in the standard library.

To use these components, the Java Virtual Machine needs to be configured. The Java platform allows users to override standard libraries through the Endorsed Standards Override Mechanism, where the required libraries are copied into a special, endorsed folder.

Apache Tomcat version 6 configuration:

During setup of OpenSSO authentication with the IBM Cognos Incentive Compensation Management web client, the deployed endorsed folder must be copied to a new folder named common in the main Apache Tomcat folder.

Procedure

1. In the main Apache Tomcat folder, create a new folder called common.
2. Copy the deployed <Tomcat Path>/webapps/ICM/WEB-INF/endorsed folder to the main Apache Tomcat folder, so that the endorsed files are in <Tomcat Path>/common/endorsed.
3. Restart the Apache Tomcat service.

Configuring OpenSSO and IBM Cognos Incentive Compensation Management

A few settings must be configured for OpenSSO to work with Cognos Incentive Compensation Management.

Procedure

1. Configure database access in the jdbc.properties file.
2. Edit web.xml and change security.xml to security-saml.xml.
3. Copy the idp.xml and keystore.jks files obtained from the IDP to the deployed/ICM/WEB-INF/saml folder.
4. Edit saml.properties.
Important: When SAML 2.0 is deployed in the web client and used with an IDP provider that does not support the AuthnRequest scoping tag, this tag can now be turned off by setting the `saml.includeScoping` value to `false`.

5. Replace the signing key placeholders with the key alias and password obtained from the IDP.

6. Choose the appropriate Payee table column (specified by `saml.userKeyColumn`) if you are not using an email address as the SAML NameID.

7. Reload Cognos Incentive Compensation Management.

**Registering IBM Cognos Incentive Compensation Management as the service provider**

You must set Cognos Incentive Compensation Management as the service provider.

**Procedure**

1. From the **Common Tasks** tab, under the **Create SAMLv2 Providers** heading, click **Register Remote Service Provider**.

2. Enter the Cognos Incentive Compensation Management SAML meta data URL (see note below) in the first field.

   Make sure it is added to the existing circle of trust, such as ICM, that was created when the IDP was configured (this option is typically selected by default).

3. Verify that the service is running by navigating to the URL in a browser.

   **Important:** The meta data URL, by default, is available in the `/saml/metadata` subdirectory from the installed Cognos Incentive Compensation Management deployment. A typical deployment matches the following pattern:

   `http://<server name>/ICM/saml/metadata`.

4. Add the same attribute mapped in the IDP configuration (this is usually the `mail` attribute).

**Verifying the IBM Cognos Incentive Compensation Management login**

You can make sure the Cognos Incentive Compensation Management web client is configured properly by navigating to web client login page.

**Procedure**


   The browser should automatically be redirected to the OpenSSO login screen.

2. Log in.

   Once a user has been successfully authenticated by OpenSSO, the browser will redirect to the Cognos Incentive Compensation Management web client home page.

   **Important:** The signed-in user can log out of the Cognos Incentive Compensation Management web client, but will not be logged out of single sign-on (SSO) until they log out of the IDP. This means that logging out of the web client and immediately returning to any Cognos Incentive Compensation Management view will automatically log the user back in.

**LDAP configuration for the web client**

For a streamlined log in process, LDAP can be used to define access to the IBM Cognos Incentive Compensation Management web application.
The Cognos Incentive Compensation Management web client can be configured to retrieve user authentication information from an LDAP directory with the following LDAP providers:

- Microsoft Active Directory, Windows 2000 with Service Pack 4
- Microsoft Active Directory, Windows 2003
- Microsoft Active Directory, Windows 2008 R2
- Microsoft Active Directory, Windows 2012
- Open LDAP 2.0.27

**Important:** LDAP can be used to obtain user login credentials for the Cognos Incentive Compensation Management web client, but it is not a SSO solution. Cognos Incentive Compensation Management web users will still need to enter login credentials to access the web application.

### Validation requirements

The LDAP column that is being mapped to IBM Cognos Incentive Compensation Management for validation needs to contain data that matches the corresponding column in Cognos Incentive Compensation Management.

By default, Cognos Incentive Compensation Management looks at the mail attribute in the LDAP directory for validation and matches this field to the email address field in the Payee table. If email addresses are being used by the Cognos Incentive Compensation Management web client for user validation, the payee email addresses that are loaded in the Cognos Incentive Compensation Management Payee table must be identical to the email addresses that are loaded in the LDAP directory.

### Configuring the `ldap.properties` file

The `ldap.properties` file defines the configuration details for IBM Cognos Incentive Compensation Management web client authentication with LDAP, such as the LDAP server name and the manager password.

Changes made to this file allow Cognos Incentive Compensation Management to connect to the client’s LDAP directory.

**Procedure**

Enter the LDAP server URL and the port number that is used by the LDAP server. If `DC=yourdomain,DC=com` is not specified here, then it should be specified in the `ldap.managerDn` line:

```
ldap.providerUrl=ldap://localhost:389/dc=example,dc=com
```

**Specifying Distinguished Names (Dn) in the `ldap.properties` file**

The LDAP manager user name and password are defined in the `ldap.properties` file when configuring the IBM Cognos Incentive Compensation Management web client for authentication with LDAP.

**About this task**

`cn` refers to the common name, such as Jane Doe, and `ou` refers to the organizational unit.

When configuring the Cognos Incentive Compensation Management web client to use LDAP authentication, it is often best to use the full distinguished name (Dn) for the `managerDn` and `userSearchBase` attributes:
ldap.managerDn=cn=Administrator,ou=Users,dc=example,dc=com
ldap.userSearchBase=ou=Accounts,dc=example,dc=com

**Important:** The DC components are specified in these strings. If you are using full DNS that specify the DC components in the `managerDn` and `userSearchBase` strings, you should not specify the DC components in the `providerUrl` string as well.

For example, use the following string: `ldap.providerUrl=ldap://localhost:389` and not the following string: `ldap.providerUrl=ldap://localhost:389/ dc=example,dc=com`.

**Procedure**

1. Define the root of the user search tree.
   This information is specific to the client's LDAP setup, and should be provided by their LDAP expert.
   
   ```
   ldap.userSearchBase=ou=Accounts
   ```

2. The `userSearchFilter` field can be used to limit the search to the members of the group.
   This field should not have to be changed.
   
   ```
   ldap.userSearchFilter=(sAMAccountName={0})
   ```

3. Map the LDAP `mail` attribute internally to the appropriate column.
   Typically, the mail attribute maps to email and should not have to be changed.
   
   ```
   ldap.userKeyAttribute=mail
   ldap.userKeyColumn=Email
   ```

**Configuring the web.xml file**

To enable LDAP authentication with the IBM Cognos Incentive Compensation Management web client, the `web.xml` file in the `WEB-INF` folder must be configured.

**Procedure**

1. In the `web.xml` file, change `/WEB-INF/security.xml` to `/WEB-INF/security-ldap.xml` to enable LDAP authentication.

2. Save the `web.xml` and `ldap.properties` files.

3. Restart the Cognos Incentive Compensation Management web client.
   Users can log in to the Cognos Incentive Compensation Management web client with the authentication credentials stored in the LDAP directory.
Chapter 6. Integration

The IBM Cognos Incentive Compensation Management client and web client can be configured so that it is integrated with, or accessible through external applications, such as Salesforce.com.

The Cognos Incentive Compensation Management client can be integrated with the IBM Cognos Territory and Quota Management application and the IBM Cognos Producer Lifecycle and Credential Management application.

Assignment detail reports created in Cognos Territory and Quota Management and tables from Cognos Producer Lifecycle and Credential Management can be imported and used as sources in calculations and reports in Cognos Incentive Compensation Management.

Connecting to IBM Cognos Territory and Quota Management

For the IBM Cognos Incentive Compensation Management client to import data from Cognos Territory and Quota Management, the Cognos Incentive Compensation Management Windows Service configuration file needs to be updated to point to the Cognos Territory and Quota Management instance.

Procedure
1. Open the Cognos Incentive Compensation Management Windows service configuration file.
2. Navigate to the TerritoryManagementServiceAddress section.
3. In the Value field, type the URL that you use to log in to Cognos Territory and Quota Management.
   You must omit the HTTPS:// from the URL and add :8443 to the end of the URL.

Connecting to IBM Cognos Producer Lifecycle and Credential Management

For the IBM Cognos Incentive Compensation Management client to import data from Cognos Producer Lifecycle and Credential Management, the Cognos Incentive Compensation Management Windows Service configuration file needs to be updated to point to the Cognos Producer Lifecycle and Credential Management application.

Procedure
1. Open the Cognos Incentive Compensation Management Windows service configuration file.
2. Navigate to the PLCMServiceAddress section.
3. In the Value field, type the URL that you use to log in to Cognos Producer Lifecycle and Credential Management.
Configuring the IBM Cognos Incentive Compensation Management web client for Salesforce.com

After installing the Cognos Incentive Compensation Management web client, the web.xml web configuration file needs to be modified in order for the web client to be accessible through Salesforce.com.

The Cognos Incentive Compensation Management web client must be deployed first.

Procedure
1. Navigate to the web.xml file found, by default, in the following location: C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps\ICM\WEB-INF.
2. In the Parameters section, change security.xml to security-salesforce-composite.xml.
3. After saving the file, restart the Cognos Incentive Compensation Management web client for the changes to take effect.

Accessing IBM Cognos Incentive Compensation Management from Salesforce.com

You can make the Cognos Incentive Compensation Management application accessible from a tab within Salesforce.

Procedure
1. Log in to Salesforce.com with a user ID that has administrative rights.
2. Select the Setup link from the top of the screen.
3. From the left pane, select Create > Tabs from the App Setup section.
4. Click New in the Web Tabs section. This will allow you to create a custom tab that displays Cognos Incentive Compensation Management content inside the Salesforce window.
5. You have the option of using the full page width to display the Cognos Incentive Compensation Management application or having the Salesforce sidebar displayed.
6. Click Next once you have made your selection.
7. Define the content and display properties for the Cognos Incentive Compensation Management tab by performing the following steps:
   a. In the Tab Content Definition section, select URL from the Tab Type menu.
   b. In the Tab Label field, enter the text that you want displayed on the label.
   c. In the Tab Name field give the tab a unique name. This can be the same as the tab label.
   d. Choose the color of your tab by selecting a Tab Style from the styles screen.
   e. The Content Frame Height field allows you to indicate how tall (in pixels) the Cognos Incentive Compensation Management content frame will be. Specify a frame height of at least 800 pixels.
8. You also have the option of enabling the Cognos Incentive Compensation Management tab for mobile use, specifying a custom splash page, and entering a description for the tab.
These fields, however, are not mandatory.

9. Press the **Next** button after entering the tab content definition and display properties information.

10. From the URL details screen, define the address of the Cognos Incentive Compensation Management web application on the web application server where Cognos Incentive Compensation Management has been deployed.

There is no need to define merge fields on this screen.

11. Enter the **URL** for the Home page of the Cognos Incentive Compensation Management web application and select **Unicode encoding**.

If the Cognos Incentive Compensation Management web client is deployed at https://localhost:8080/ICM, the Cognos Incentive Compensation Management web client URL for Salesforce is the same as the following URL:

https://localhost:8080/ICM/sforce_composite_login?SessionId={!API.Session_ID}&ServerURL={!API.Partner_Server_URL_100}

**Attention:** You must include the underscores in the URL.

12. Click **Next** when complete.

13. From the **Add to Profiles** screen, you can choose which user profiles are able to see the new Cognos Incentive Compensation Management tab.

14. From the **Add to Custom Apps** page, you can choose the custom apps for which the new Cognos Incentive Compensation Management tab will be visible.

15. Click **Save**.

The Cognos Incentive Compensation Management application is now accessible from the newly created tab.

---

**Web client integration with Oracle CRM**

Oracle users can install a Cognos Incentive Compensation Management tab, allowing direct access to Cognos Incentive Compensation Management from the Oracle CRM site.

Users that are logged into Oracle CRM will not have to re-authenticate when navigating to the Cognos Incentive Compensation Management web tab.

**Important:** Once the Cognos Incentive Compensation Management web application is configured for Oracle CRM integration, users are not able to connect directly to the Cognos Incentive Compensation Management web client. The only way to access Cognos Incentive Compensation Management is through the tab in Oracle CRM.

**Configuring the IBM Cognos Incentive Compensation Management client for integration with Oracle CRM**

To integrate Oracle CRM with Cognos Incentive Compensation Management, a column needs to be added to the Payee table that contains Oracle CRM user names for all payees.

**Procedure**

1. In the model that will be accessed through Oracle CRM, add a text column to your Payee table to use for Oracle integration.

For example, add a text column called **Oracle UserID**.
2. For each payee that will be accessing the Cognos Incentive Compensation Management web client through a tab in Oracle CRM, add the payee's Oracle CRM user name to the new column, for example, rivacent/huddle.

3. Create a new web tab in Portal Access and enable users for web access.
   a. Go to Portal Access > Web Tabs and add a Module type web tab with a Data Edit object assigned to it.
   b. Create a Portal Access group containing all payees that will be accessing Cognos Incentive Compensation Management through Oracle CRM. For example, create a group called Oracle Group that contains all your payees.
   c. Create a Portal Access tree and add the Portal Access group to the tree. For example, create a Portal Access tree called Oracle Access Tree that contains the Oracle Group.
   d. From the Assignment tab, give your Oracle Access Tree access to your Oracle web tab.
   e. From the Groups tab, enable all users in your Oracle group with access to the Cognos Incentive Compensation Management web client.

   Tip: Although enabling each user for web access through the Cognos Incentive Compensation Management Client is required, the user will never use the password created in Cognos Incentive Compensation Management to access the Cognos Incentive Compensation Management web client when Oracle CRM integration is in use.

Configuring the IBM Cognos Incentive Compensation Management web client for use with Oracle CRM

In order to configure access to the Cognos Incentive Compensation Management web client by using a tab in Oracle CRM, the crmondemand.properties and web.xml files need to be edited.

If the Cognos Incentive Compensation Management web client is deployed on Apache Tomcat, these files can be found in the following default location:
C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps\ICM\WEB-INF.

Procedure
1. Deploy the ICM.war file and configure the jdbc.properties file to point to your model.
2. Open up the crmondemand.properties file and make the edits to the authenticationURL and userKeyColumn fields.
   a. The authenticationURL field needs to contain the URL for the Oracle CRM instance you are connecting from.
   b. The userKeyColumn field contains the name of the column added to the Cognos Incentive Compensation Management Payee table that contains the Oracle CRM user names.
4. Restart your Cognos Incentive Compensation Management web service.
5. Connect to the Oracle CRM instance, log in as a user referenced in the Payee table column containing Oracle user names, and select the tab that was configured to connect to Cognos Incentive Compensation Management.

For information on adding custom tabs to Oracle instances, see the help section on displaying external pages in tabs in the Oracle CRM On Demand help.
Customization of client appearance to match Salesforce.com

Once the Cognos Incentive Compensation Management tab has been set up in Salesforce, you may want to customize Cognos Incentive Compensation Management's appearance.

This can be done in the Cognos Incentive Compensation Management Client.

Changing the theme of IBM Cognos Incentive Compensation Management to Salesforce.com

When accessing Cognos Incentive Compensation Management from Salesforce, you may want to configure Cognos Incentive Compensation Management's appearance to be more consistent with the rest of Salesforce.

Procedure

1. Select the Themes option from the Tools menu in the Cognos Incentive Compensation Management Client.
2. In the Web Theme section, select salesforce.com.

Integration with Microsoft IIS web server

You can configure Microsoft's IIS web server with the IBM Cognos Incentive Compensation Management web server so that IIS forwards requests on to Cognos Incentive Compensation Management and responses back to the user.

This is useful if you already have IIS running several web pages (for example, http://mycompany.com) and want to integrate Cognos Incentive Compensation Management as just another URL (for example, http://mycompany.com/ICM).

The Cognos Incentive Compensation Management web client is written as a J2EE web application and needs a Java Application Server (servlet container) to run. As IIS does not provide the services of a Java Application Server, it is not possible to deploy the Cognos Incentive Compensation Management web client directly into IIS. It is possible to configure IIS to proxy requests for the Cognos Incentive Compensation Management web client to an application server where Cognos Incentive Compensation Management is deployed. Therefore, if your main website is running in IIS, it is possible to integrate Cognos Incentive Compensation Management into this website.

If you need to integrate the Cognos Incentive Compensation Management web client with IIS, the Cognos Incentive Compensation Management web client needs to be deployed into a Java Application Server that provides IIS integration capability. Apache Tomcat is one of these application servers.

Configuring the web client to prepare for integration with Microsoft IIS web server

Before integrating Microsoft's IIS web server with the Cognos Incentive Compensation Management web server, you must first configure Cognos Incentive Compensation Management and test the deployment.

Procedure

1. Install and configure the Cognos Incentive Compensation Management web client.
2. Deploy the WAR file using Apache Tomcat.

**Configuring Apache Tomcat to accept proxied requests**

You must configure Apache Tomcat to accept proxied requests for IBM Cognos Incentive Compensation Management from IIS and enable the AJP/1.3 Connector in Cognos Incentive Compensation Management.

**Procedure**

1. Enable **AJP/1.3 Connector** in Apache Tomcat.
   a. Edit the server.xml file and make sure that the **AJP/1.3 Connector** is enabled (for example, not commented out).
      The server.xml file is found in the following location by default:
      C:\Program Files\Apache Software Foundation\Tomcat 6.0\conf
   b. Remove the comment symbols (<!- and -->) around the following section in the conf/server.xml file: `<Connector port="8009" protocol="AJP/1.3" redirectPort="8443"/>

2. Restart Apache Tomcat and make sure that no errors regarding used ports appear in the logs or in the Apache Tomcat Console.
3. Make sure that the AJP Connector is listening on the specified port (8009 by default).
   One way to do this is to use the **netstat -na** command in the command window and see if port 8009 is listed in the output.

**Configuring IIS to forward requests to IBM Cognos Incentive Compensation Management**

After deploying the Cognos Incentive Compensation Management web client using Apache Tomcat and configuring Apache Tomcat to accept proxied requests, you must configure IIS to forward Cognos Incentive Compensation Management requests to Apache Tomcat. The following steps must be performed on the computer where IIS is deployed.

**Procedure**

1. Download the ISAPI Redirect DLL file from the Apache site.
2. When downloading, choose the version of Windows that IIS is running on (either win32 or win64), and then choose the latest available jk version (jk-1.2.31). The file to download is named api_redirect_X.X.X.dll, where X.X.X is the version number. You will need to remove the version number from the DLL file (that is, it needs to be named isapi_redirect.dll).
3. Place the DLL and the associated properties files in an installation directory. For example, assume the directory is C:\tomcat_iis_connector. Place the isapi_redirect.dll in this directory.
4. Download the isapi_redirect.properties file and place this in the same directory as the isapi_redirect.dll file.
5. Create a directory called conf in your installation directory (C:\tomcat_iis_connector\conf).
   a. Download the uriworkermap.properties and workers.properties.minimal files.
   b. Place them in the C:\tomcat_iis_connector\conf directory.
6. Create a directory called logs (C:\tomcat_iis_connector\logs).
This is where the logs associated with the isapi_redirect.dll execution will be placed.

7. In the C:\tomcat_iis_connector directory you may need to modify the isapi_redirect.properties file. The isapi_redirect.properties file tells the connector where to find its configuration files and where the DLL can be found in relation to the IIS server. The following properties are in this file:

   - **extension_uri**
     - The path to the virtual directory that contains the isapi_redirect.dll file.

   - **log_file**
     - The path to write the log file to.

   - **log_level**
     - The level at which the logs should be generated.

   - **worker_file**
     - The path to your workers.properties.minimal file in your installation.

   - **worker_mount_file**
     - The path to your uriworkermap.properties file in your installation.

If you install the connector in C:\tomcat_iis_connector and you follow the instructions below for setting up the virtual directory for the isapi_redirect.dll file, then you should not have to change any properties in the provided file.

8. In the C:\tomcat_iis_connector\conf directory, you may need to modify the uriworkermap.properties and the workers.properties.minimal files.

   a. Edit the uriworkermap.properties file and make sure that it contains the following mapping for Cognos Incentive Compensation Management: /ICM/*=worker1.

   b. Edit the workers.properties.minimal file and modify the **worker.ajp13w.host** property if necessary.
      - This property should be set to the host name or the IP address of the computer where Apache Tomcat is running. If Apache Tomcat is running on the same computer as IIS then you can leave the property set to **localhost**. If you have specified a host name as the value of this property, make sure that the IIS computer can correctly resolve it to the appropriate IP address.

      If you have modified the port for the AJP Connector you will need to modify the **worker.ajp13w.port** property.

9. Open Control Panel > Administrative Tools > Internet Information Services. If you are using IIS 7.0, you will need to install ISAPI Extensions and ISAPI Filters.

10. Navigate to Start Menu > All Programs > Administration Tools > Service Manager.
    a. Select Web Server (IIS) > Roles.
    b. Click Add Role Services.

11. Add an ISAPI filter to IIS in one of the following two ways:
    * If you are using IIS 6.0 or earlier, perform the following steps:
      a. Right-click Default Web Site (or the web site that should be responsible for proxying requests to Cognos Incentive Compensation Management) > Properties.
      b. Click the ISAPI Filters tab.
c. Check if there is a filter that points to the  isapi_redirect.dll file and that it is in the right location. If not, click Add and create one.
d. Type tomcat as the Filter Name and type the location of the  isapi_redirect.dll file for the executable.
e. Click Apply and then OK.

- If you are using IIS 7.0, perform the following steps:
a. Click the Default Web Site (or the web site that should be responsible for proxing requests to Cognos Incentive Compensation Management) and click ISAPI Filters.
b. Click the ISAPI Filters icon.
c. Check if there is a filter that points to the  isapi_redirect.dll file and that it is in the right location. If not, click Add and create one.
d. Type tomcat as the Filter Name and type the location of the  isapi_redirect.dll file.
e. Click OK.

12. Create a virtual directory for Cognos Incentive Compensation Management in IIS.
a. Right-click Default Web Site (or the web site that should be responsible for proxing requests to Cognos Incentive Compensation Management) > New > Virtual Directory.
b. Set the alias as the value of the context path, without slashes, that was set in the Configure Cognos Incentive Compensation Management section of this document. This can point to any directory.

13. Create a virtual directory for access to the isapi_redirect.dll file in IIS in one of the following ways:

- If you are using IIS 6.0 or earlier, perform the following steps:
a. Right-click Default Web Site (or the web site that should be responsible for proxing requests to Cognos Incentive Compensation Management) > New > Virtual Directory.
b. Set the alias to be jakarta. This must point to the directory in which the  isapi_redirect.dll file is installed. In our example, this is C:\tomcat_iis_connector.
c. Select the Execute check box.

- If you are using IIS 7.0, perform the following steps:
a. Right-click Default Web Site or the web site that should be responsible for proxing requests to Cognos Incentive Compensation Management and click Add Virtual Directory.
b. Set the alias.
c. Physical Path must point to the directory in which the  isapi_redirect.dll file is installed. In our example, this is C:\tomcat_iis_connector.
d. Click the alias virtual directory and double-click Handler Mappings.
e. Click Edit Feature Permissions in the Action panel.
f. Select the Execute check box.

14. If you are using IIS 6.0 or 7.0, you will need to add the dll as a Web Service Extension in one of the following ways:

- If you are using IIS 6.0, perform the following steps:
b. Type tomcat for the Extension Name.
c. Add the isapi_redirect.dll file to the required files.
d. Select the Set extension status to the Allowed check box.
e. Click OK.

- If you are using IIS 7.0, perform the following steps:
  a. Navigate to the servers and highlight your server.
  b. Navigate to ISAPI and CGI Restrictions.
  c. Add and allow the isapi_redirect.dll extension.

### Integration with IWA

You can configure the IBM Cognos Incentive Compensation Management web client to have single sign on integration with Integrated Windows Authentication (IWA).

Cognos Incentive Compensation Management web users are automatically signed in without having to enter a user name and password. If the authentication fails, then users will have to enter their Windows account user name and password.

### Setting up for Internet Explorer

If you are using Internet Explorer, you must enable Integrated Windows Authentication and add the IBM Cognos Incentive Compensation Management web client address to your local intranet zone.

**Procedure**

1. Go to Tools > Internet Options > Advanced.
3. Restart Internet Explorer.
4. Go to Tools > Internet Options > Security.
5. Select the Local Intranet zone.
6. Click Sites.
7. Click Advanced.
8. Add the website address where the Cognos Incentive Compensation Management web client runs.
9. Click Close then OK.
10. Click Custom Level.
11. Under User Authentication, make sure Automatic logon only in Intranet zone is selected.

   If you would like the webapp to ask you to authenticate manually, select Prompt for user name and password instead.

### Setting up for Mozilla Firefox

If you are using Mozilla Firefox, you must make changes to a few settings to enable IWA functionality for use with IBM Cognos Incentive Compensation Management.

**Procedure**

1. In the address bar, enter about:config as a URL and click Go.
2. If you receive a warning message, click I'll be careful, I promise!
3. In the filter, type network.negotiate-auth.trusted-uris.
4. Double-click network.negotiate-auth.trusted-uris and enter your server address.

**Setting up for Google Chrome**

If you are using Google Chrome, you must make changes to a few settings to enable IWA functionality for use with IBM Cognos Incentive Compensation Management.

**Procedure**

1. Click the **Settings** icon and select **Options**.
2. On the **Under the Hood** tab, click **Change proxy settings**.
3. On the **Advanced** tab, select **Enable Integrated Windows Authentication**.
4. Restart Google Chrome and repeat steps 1 and 2.
5. On the **Security** tab, select **Local Intranet Zone**.
6. Click **Sites**.
7. Click **Advanced**.
8. Add the website address where the Cognos Incentive Compensation Management web client runs to your local intranet zone.
9. On the **Security** tab, select **Custom Level**.
10. Select **Automatic logon only in Intranet zone**.
    
    If you would like the webapp to ask you to authenticate manually, select **Prompt for user name and password** instead.

**Creating a Kerberos configuration file**

You will need to create a Kerberos configuration file that is necessary for IWA configuration with IBM Cognos Incentive Compensation Management.

**Procedure**

1. On your web server, create a krb5.ini file and place it in the Windows directory (for example, C:\Windows). A basic krb5.ini file will look like the following example:

   ```ini
   [libdefaults]
   default_realm = YOURDOMAIN.COM
   default_tkt_enctypes = aes128-cts rc4-hmac des3-cbc-shal des-cbc-md5
des-cbc-crc
   default_tgs_enctypes = aes128-cts rc4-hmac des3-cbc-shal des-cbc-md5
des-cbc-crc
   permitted_enctypes = aes128-cts rc4-hmac des3-cbc-shal des-cbc-md5
des-cbc-crc
   [realms]
   YOURDOMAIN.COM = {
    kdc = kdc.yourdomain.com
    default_domain = YOURDOMAIN.COM
    }
   [domain_realm]
   .YOURDOMAIN.COM = YOURDOMAIN.COM
   ```

2. Replace **YOURDOMAIN.COM** with your organization's domain name.
3. Replace **kdc.yourdomain.com** with the address of your Active Directory Server.
4. Configure the lists of encryption types that you would like to use.
Configuring the Service Principal Name and keytab

For integration of the IBM Cognos Incentive Compensation Management web client with IWA, you will need to configure a Service Principal Name (SPN) for your web server in the Active Directory and generate a keytab file containing a shared secret key. Your organization’s IT department can assist you with this section.

Procedure

1. To create a domain account for the web server in your Active Directory, perform the following steps:
   a. Add account name serviceaccount.
   b. Select a password such as secret.
   c. Deactivate User must change password at next logon.
   d. Activate Password never expires.
2. Create keytab file http-webserver.keytab using ktpass.exe:
   
   ```
   ktpass -out http-webserver.keytab -princ HTTP/webserver.yourdomain.com@YOURDOMAIN.COM
   -mapUser serviceaccount@YOURDOMAIN.COM
   -mapOp set -pass secret -crypto RC4-HMAC-NT -pType KRB5_NT_PRINCIPAL -DesOnly
   ```
   a. Replace webserver.yourdomain.com with the address of your web server.
   b. Replace YOURDOMAIN.COM with your domain name.
   c. Replace secret with the password of the account created in step 1.
   d. Replace RC4-HMAC-NT with the encryption your Kerberos server uses.
3. Copy the keytab file generated in step 2 (http-webserver.keytab) to a secure location on the web server that can only be accessed locally.

   **Attention:** In this case, the Service Principal Name (SPN) chosen is HTTP/webserver.yourdomain.com@YOURDOMAIN.COM. You will need this to configure the Cognos Incentive Compensation Management web client.

Setting up the web client

After your browser has been enabled for IWA functionality, you will have to enable the Cognos Incentive Compensation Management web client for IWA functionality as well.

Procedure

1. Deploy the ICM.war file.
   
   **Important:** All web users must be in the Payee table, have an email address, and be part of a Portal Access group and Portal Access tree in your Cognos Incentive Compensation Management model.
2. Configure database access in the jdbc.properties file.
3. Configure the web.xml file to use SPNEGO security by changing the security.xml param-value to security-spnego.xml,

   By default the file is located in C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps\ICM\WEB-INF.

4. Configure the spnego.properties file for your environment.
By default, it is located in C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps\ICM\WEB-INF.

a. Replace the service principal and keytab location values with the ones you obtained from the previous section.

b. Configure the LDAP settings for your Active Directory.
   By default, the search filter is userPrincipalName and should not be changed unless it is necessary.

c. Configure the Active Directory account attribute (spnego.ldapUserKeyAttribute and spnego.userKeyColumn) that will map to the Payee table column in your model.

   # SPNEGO
   spnego.kerberosServicePrincipal=HTTP/webserver.yourdomain.com@YOURDOMAIN.COM
   spnego.kerberosKeyTabLocation=d:/secure/http-webserver.keytab

   spnego.ldapProviderUrl=ldap://localhost:389/dc=example,dc=com
   spnego.ldapManagerDn=cn=Administrator,ou=Users
   spnego.ldapManagerPassword=secret
   spnego.ldapUserSearchBase=ou=Accounts
   spnego.ldapUserSearchFilter=(userPrincipalName={0})
   spnego.ldapUserKeyAttribute=mail

   spnego.userKeyColumn=Email
Notices

This information was developed for products and services offered worldwide.

This material may be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service. This document may describe products, services, or features that are not included in the Program or license entitlement that you have purchased.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.
Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Software Group
Attention: Licensing
3755 Riverside Dr.
Ottawa, ON
K1V 1B7
Canada

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.
This Software Offering does not use cookies or other technologies to collect personally identifiable information.

**Trademarks**

IBM, the IBM logo and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “[Copyright and trademark information](https://www.ibm.com/legal/copytrade.shtml)” at www.ibm.com/legal/copytrade.shtml.

The following terms are trademarks or registered trademarks of other companies:

- Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.
Glossary

This glossary includes terms and definitions for IBM Cognos Incentive Compensation Management.

The following cross-references are used in this glossary:

- See refers you from a term to a preferred synonym, or from an acronym or abbreviation to the defined full form.
- See also refers you to a related or contrasting term.

To view glossaries for other IBM products, go to www.ibm.com/software/globalization/terminology (opens in new window).

A

Active Directory (AD)
A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

AD See Active Directory

administrator
A person responsible for administrative tasks such as access authorization and content management. Administrators can also grant levels of authority to users.

aggregate
A calculation that returns a single result value from several relational data rows or dimensional members. Typical examples are total and average.

allocated adjustment
An adjustment to the results of the difference between the original value calculated for a closed period and the value that would be currently calculated based on the new data.

configuration file
A file that specifies the characteristics of a program, system device, system, or network.

certificate
In computer security, a digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority.

component
A container that is used to organize a model. When creating a new model, components should be created first, in order to give the model a framework and ensure that it is easy to navigate. Once components have been created, model elements, such as tables, calculations, and plans can be built.

database (DB)
A collection of interrelated or independent data items that are stored together to serve one or more applications. See also database server

database server
The server on which the database application and database are installed.

XML, and HTML, a name-value pair within a tagged element that modifies features of the element.

C
calculation
The process used to transform a series of records into a new result. Typically a calculation is mathematical, but may also include sorting, shifting, or adding to a prior result. Calculations enable the model admin to select records from their source data, perform operations on the data, segment results, and begin another calculation based on those results.

certificate
In computer security, a digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority.

component
A container that is used to organize a model. When creating a new model, components should be created first, in order to give the model a framework and ensure that it is easy to navigate. Once components have been created, model elements, such as tables, calculations, and plans can be built.

database (DB)
A collection of interrelated or independent data items that are stored together to serve one or more applications. See also database server.

database server
The server on which the database application and database are installed.
**DB**  See *database*

delimiter
A character, such as comma or tab, used to group or separate units of text by marking the boundary between them.

digital certificate
An electronic document used to identify an individual, a system, a server, a company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority.

dimension table
The representation of a dimension in a star schema. Each row in a dimension table represents all of the attributes for a particular member of the dimension.

**F**

fact table
A relational table that contains facts, such as units sold or cost of goods, and foreign keys that link the fact table to each dimension table.

**I**

inbound connection
A resource that is used to import data from selected outbound connections to a component. They are created to specify which component the selected outbound component should connect to.

**J**

join
An action that combines records from two or more tables or calculations based on a point of commonality. Joins are produced by adding columns to the initial data source.

**L**

LDAP  See *Lightweight Directory Access Protocol*.

left outer join
A join whose result consists of the matched rows of the two tables that were joined and the unmatched rows of the first table. See also *join*.

**Lightweight Directory Access Protocol (LDAP)**
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model and that does not incur the resource requirements of the more complex X.500 Directory Access Protocol (DAP). For example, LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

**M**

manual adjustment
A one-time change to a value that is applied in specific scenarios. Administrators can add manual adjustments to any payee for any open period.

**O**

optimization
The process of achieving improved runtime performance or reduced code size of an application. Optimization can be performed by a compiler, by a preprocessor, or through hand tuning of source code.

outbound connection
A resource that is used to export calculation results or table data from a component. They are created from tables, calculations, and other sources.

**P**

parameter (parm)
A value or reference passed to a function, command, or program that serves as input or controls actions. The value is supplied by a user or by another program or process. See also *configuration file*.

parm  See *parameter*.

partition
The division of a single calculated result into sub-results. Partitions are used to define how the results of the calculation will be displayed. For example, if the partitioning is by payee ID, the calculation results will show the calculated amount for each payee.
payee  An individual who is being compensated or is approving the compensation results.

period  A date interval that reported values are saved in. An example of a period is December 2000.

pick list  A list of cell values available to a user when entering data into a cell.

primary key  An object that uniquely identifies an entity bean of a particular type.

Q

query  A request for information from a database that is based on specific conditions: for example, a request for a list of all customers in a customer table whose balances are greater than USD1000.

R

root certificate  The certificate (proof of identity and keys) of the original trusted signer or certificate authority that certifies the authenticity of the end user/entity (or of intermediate signers).

S

server  A software program or a computer that provides services to other software programs or other computers.

server certificate  An electronic stamp stored in the server's key ring file that contains a public key, a name, an expiration date, and a digital signature. The server certificate uniquely identifies the server.

servlet container  A web application server component that invokes the action servlet and that interacts with the action servlet to process requests.

single sign-on (SSO)  An authentication process in which a user can access more than one system or application by entering a single user ID and password.

SQL  See Structured Query Language

SSO  See single sign-on

Structured Query Language (SQL)  A standardized language for defining and manipulating data in a relational database.

V

validation rule  A rule defined on an attribute definition that specifies the criteria that must be met by the data stored in an instance of this attribute for that attribute to be valid.

view  A virtual table that is created by joining two or more tables together. Views can also include the results of calculations.

W

web application server  The runtime environment for dynamic web applications. A Java EE web application server implements the services of the Java EE standard.

web client  An interface where payees can review and approve their compensation payments via a web browser. The Cognos ICM web client runs on a variety of servlet containers.

web server  A software program that is capable of servicing Hypertext Transfer Protocol (HTTP) requests.

workflow  The sequence of activities performed in accordance with the business processes of an enterprise.
Index

Special characters
.NET Framework Redistributable 31
.NET Framework SDK/Windows SDK 31

A
add-in
   See Microsoft Excel add-in
administrator
   setting email address for 15
Anonymous Model Creation
   configuring 12
Apache Tomcat
   configuring database access using 59
   configuring language and Unicode support using 59
   configuring to accept proxied requests through Microsoft IIS web server 90
   configuring to forward requests to IBM Cognos Incentive Compensation Management 90
   deploying application using 58
   installing and configuring 58
   OpenSSO 80
   overview of deployment of web client 57
API
   access to 42
   architecture 41
   configuring settings for 11
   overview 41
   specifications for data management 44
   specifications for data store 47
   specifications for processing and calculation 43
application server
   editing configuration files on 8
   installing Console Service on 27
   installing Windows Service on 7
   JBoss 60
   overview 1
   security options for communications with client 75
   security options for communications with database server 75
   WebSphere 865
authentication
   configuring for web client 83
   database server settings 9
   IWA 93
   LDAP 22
   LDAP for web client 82
   models 8
   OpenSSO 78
   overview 76
   SiteMinder 77
   Windows Service settings 11, 12

B
backups
   database 17
   ICM.exe.config file 17
   restoring data from 17
   transferring databases between servers using 17

C
C#
   exception definitions 51
   object definitions 48
   calculations
      API specifications 43
      improving speed of with Data Tier Performance Optimization 25
      improving speed of with Enterprise Size Optimization 31
   certificates
      binding to ports 36
      configuring for use by client and service 36
      configuring with CLI 38
      generating 32
      generating from command line 32
      identifying for Microsoft Excel add-in 54
      importing for Microsoft Management Console 34
      Microsoft Management Console 34
      required software 31
      setting up client for 54
      setting up for Microsoft Excel add-in in client 55
      setting up for Microsoft Excel add-in in services 53
      setting up Microsoft Management Console to use 33
Chrome
   See Google Chrome
CLI
   configuring digital certificates with 38
   connecting to models with 38
   installation files for 2
   installing 38
   overview 37
   preinstallation checklist 37
   return codes 40
   running commands 39
client
   allowing LDAP users to access 24
   allowing multiple instances 9
   changing appearance to match Salesforce.com 89
   changing theme to match Salesforce.com 89
   configuring for Oracle CRM 87
   configuring to use certificates 36
   enabling Data Tier Performance Optimization in 25
   installation files for 2
   installing 7
   integrating LDAP with 22, 23
   overview 1
   preinstallation checklist 3
   preparation for installation 1
   setting default language for 9
   setting up for Microsoft Excel add-in 54
   tools 27
   Windows Service 7
client tools
   Console Service 27
CLR
   integrating with Data Tier Performance Optimization 25
Cognos Incentive Compensation Management client
   See client
Cognos Incentive Compensation Management Windows Service
   See Windows Service

© Copyright IBM Corp. 2005, 2015
105
colors
changing in web client 71
changing in web client for theme 74
command-line interface
See CL1
common language runtime
See CLR
communications
between client and application server 75
between database server and application server 75
between database server and web application server 76
between web client and web application 76
configuring modes 12
security overview 75
configuration 38
Apache Tomcat 58
Console Service 27
database access for web client using Apache Tomcat 59
database access for web client using JBoss 60
database access for web client using WebSphere 63, 66
digital certificates 38
ICM.exe.config 8
identity of hosting server for Microsoft Excel add-in 54
Java 57
Java for JBoss 60
JBoss 60
Microsoft Excel add-in 53
multilingual support for web client 69
multilingual support for web client using Apache
Tomcat 59
multilingual support for web client using JBoss 62
multilingual support for web client using WebSphere 65
OpenSSO 78, 79
OpenSSO with IBM Cognos Incentive Compensation
Management 80
service providers 80
service.exe.config 8
Unicode support for web client 69
WebSphere 8 for web client 65
Configuration File Encrypter
installation files for 2
installing 28
overview 28
configuration files
ConsoleService.exe.config 28
Console Service
editing configuration file 27
installing 27
overview 2, 27
starting 27
ConsoleService.exe.config file
ingredienting 27
encrypting files 28
encryption 28
currencies
adding 21
Customer Relationship Management
See Oracle CRM

Data Tier Performance Optimization
enabling in client 25
integrating with CLR 25
overview 25
database
changing DEFAULT_SCHEMA through queries 5
database (continued)
changing DEFAULT_SCHEMA through SQL Server
Management Studio 5
configuring access using Apache Tomcat 59
configuring access using JBoss 60
configuring access using WebSphere 63, 66
configuring multiple 10
owner for Microsoft SQL Server 4
selecting target version 20
server overview 1
transferring between servers 17
dbo rights for Microsoft SQL Server 3
DEFAULT_SCHEMA
changing through queries 5
changing through SQL Server Management Studio 5

E
email
configuring 14
configuring email address for administrator 15
configuring settings for 14
managing settings for portal access 15
sending from web client 70
encryption
configuring 11
configuring for web client passwords 68
configuring for web client passwords in Windows 69
HTTP 76
HTTPS 76
overview 28
property files 68
TLS security 75
trusted network 76
trusted network and SSL 75, 76
Windows Domain 75
endorsed libraries
SAML 80
Enterprise Model
converting Standard Edition model to 30
converting Standard model to 30
optimizing size 31
Excel add-in
See Microsoft Excel add-in
exception definitions 51
external tools
configuring 13

F
Firefox
See Mozilla Firefox

G
glossary 101
Google Chrome
setting up for with IWA 94

H
handheld devices
configuring 14
hierarchies
adding 21
hosts file
editing 35
HTTP
configuring for Windows Service 12
unencrypted communication between web client and web application 76
HTTP Configuration Utility
using to identify server certificate 54
HTTPS
configuring for Windows Service 12
encrypted communication between web client and web application 76
IBM Cognos ICM Windows Service.exe.config file
configuring communication modes 12
configuring environments for models in 8
configuring multiple databases in 10
configuring to use certificates 36
editing 21
encrypting files 28
encryption 28
location 9
Model Upgrader 16
preinstallation checklist 37
upgrades 18
IBM Cognos Incentive Compensation Management client
See client
IBM Cognos Incentive Compensation Management Windows Service
See Windows Service
IBM Cognos Producer Lifecycle and Credential Management
integration with 85
IBM Cognos Territory and Quota Management
integration with 85
ICM-cli.exe file
installing CLI 38
ICM-console.exe file
installing Console Service 27
ICM-modelupgrader.exe file
installing Model Upgrader 18
running Model Upgrader 19
ICM-service.exe file
installing the Windows Service 7
running simultaneous instances 20
ICM.exe.config file
backups 17
overview 8
restoring data 17
identity provider
See IDP
IDP
adding and configuring 79
overview 79
IIS web server
See Microsoft IIS web server
installation
Apache Tomcat 58
installation (continued)
checklist 3
client 7
Configuration File Encrypter 28
Console Service 27
files for 2
Java 57
Java for JBoss 60
JBoss 60
Management Model Converter 29
OpenSSO 78
overview 1
Windows Service 7
installation files
ICM-cli.exe 38
ICM-console.exe 27
ICM-modelupgrader.exe 18
ICM-service.exe 7
Integrated Windows Authentication
See IWA
integration with external applications
IBM Cognos Producer Lifecycle and Credential Management 85
IBM Cognos Territory and Quota Management 85
Microsoft IIS web server 89
Oracle CRM 87
overview 85
Salesforce.com 86
Internet Explorer
setting up for with IWA 93
Internet Information Services
See Microsoft IIS web server
IP addresses
identifying 35
IWA
configuring the Service Principal Name and keytab for 95
creating a Kerberos configuration file for 94
enabling web client for 95
integration with web client 93
setting up web client for Google Chrome with 94
setting up web client for Internet Explorer with 93
setting up web client for Mozilla Firefox with 93
setting up web client with 95
J
j_spring_security_check error
avoiding 64
Java
installing and configuring 57
Java for JBoss
installing and configuring 60
JBoss
configuring 60
configuring database access using 60
configuring multilingual and Unicode support using 62
deploying application using 61
installing 60
Java for JBoss 60
overview of deployment of web client 60
jdbc.properties
backing up before upgrades 16
configuring database access using Apache Tomcat 59
jdbc.properties file
configuring database access using WebSphere 63, 66
configuring OpenSSO with IBM Cognos Incentive Compensation Management 80
jdbc.properties file (continued)
  encryption of 68
Model Upgrader 16

K
Kerberos
  authenticating clients and servers through 8
  configuring the Windows Service configuration file for LDAP authentication 23
  setting up configuration file for Windows security mode 11
  keystore
    setting up 79
  keytab
    configuring for web client 95

L
languages
  See multilingual support
LDAP
  allowing users to access client 24
  configuring authentication for web client 83
  configuring client with 23
  configuring for web client 82
  configuring properties for 82
  integrating with client 22
  specifying distinguished names in 82
  validating for web client 82
ldap.properties file
  configuring 82
  encryption of 68
  specifying distinguished names in LDAP 82
Lightweight Directory Access Protocol
  See LDAP
logs
  changing in web client 71
  changing in web client for theme 74
logs
  audit 12
  Scheduler 12
  Task Manager 12

M
Makecert.exe file
  Certificate Creation Tool 32
Management Console
  See Microsoft Management Console
Management Model Converter
  converting models 29
  converting Standard Edition model to Enterprise model 30
  converting Standard model to Enterprise model 30
  installation files for 2
  installing 29
  optimizing Enterprise model size 31
  overview 29
Microsoft Excel add-in
  configuring identity of hosting server 54
  connecting 56
  editing the configuration file for 53
  identifying server certificate for 54
  installation files for 2
  installing 56
Microsoft Excel add-in (continued)
  installing Office Primary Interop Assemblies tool for 55
    overview 52
    setting up certificates for client 55
    setting up certificates for services 53
    setting up client for 54
    setting up service for 52
    setting up services for client 55
    software for 55
Microsoft IIS web server
  configuring Apache Tomcat to accept proxied requests through 90
  configuring to forward requests to IBM Cognos Incentive Compensation Management 90
  configuring web server to prepare for integration with 89
  integration with 89
Microsoft Internet Information Services
  See Microsoft IIS web server
Microsoft Management Console
  certificates for 34
  importing certificates for 34
  setting up to use certificates 33
Microsoft SQL Server
  changing DEFAULT_SCHEMA through SQL Server Management Studio 5
  converting models to 29
  converting models to later versions 29
  database owner 4
  overview 1
  permission requirements for database 3
mobile settings
  configuring 14
Model Converter
  See Management Model Converter
Model Upgrader
  error protection 19
  installation files for 2
  installing 18
  running 19
  target database version 20
  upgrading models with 18
models
  adding 21
  connecting with CLI 38
  opening 21
  upgrading 18
Mozilla Firefox
  setting up for with IWA 93
multilingual support
  configuring for web client 69
  configuring for web client using Apache Tomcat 59
  configuring for web client using JBoss 62
  configuring for web client using WebSphere 65
  select date settings 12
  select language 12
  setting default language 9

O
object definitions 48
Office Primary Interop Assemblies tool
  installing for Microsoft Excel add-in 55
OpenSSO
  Apache Tomcat configuration 80
  configuring 79
  configuring IDP for 79

108  IBM Cognos Incentive Compensation Management Version 9.0.0: Installation and Configuration Guide
OpenSSO (continued)
configuring with IBM Cognos Incentive Compensation Management 80
downloading 78
installing 78
overview 78
Oracle CRM
configuring client for 87
configuring web client for 88
integration with 87
Oracle Customer Relationship Management
See Oracle CRM

P
passwords
configuring encryption for in web client 68
configuring encryption for in web client in Windows 69
deploying web client with encryption 69
encryption for property files 68
obtaining encrypted 68
Portal Access
configuring email settings 14
managing email settings for 15
ports
binding certificates to 36
identifying 35
identifying unused numbers 35
Presenter reports
data grid row limits 71
preventing from loading with a large amount of data 71
properties files
saml.properties 80
siteminder.properties 77
property files
configuring database access for JBoss 60
configuring web client password encryption 68
emailing users when inquiries are pending 70
encrypted passwords for 68
encryption for web client 68
jdbc.properties 16, 59
ldap.properties 82
Portal Access email settings 15
specifying distinguished names in LDAP 82

Q
queries
changing DEFAULT_SCHEMA through 5

R
reporting.properties file
disabling collection of Presenter report information 71
Presenter report data grid row limits 71
reports
data grid row limits in web client 71
Presenter 71
tailored reports 43
web reports 43
restoration of data
from backups 17
overview 17
Salesforce.com
changing appearance of client to match 89
changing theme of client to match 89
configuring web client for 86
integration with IBM Cognos Incentive Compensation Management 86
theme 74
SAML
authentication options 76
configuring IDP for 79
configuring OpenSSO with IBM Cognos Incentive Compensation Management 80
endorsed libraries 80
OpenSSO configuration 78
registering IBM Cognos Incentive Compensation Management as service provider in 81
service provider configuration 80
saml.properties file
configuring OpenSSO with IBM Cognos Incentive Compensation Management 80
Saved Image File Directory
configuring 12
Saved Import File Directory
configuring 12
Saved Publisher File Directory
configuring 12
Scheduler
API access to 42
configuring 12, 13
configuring email settings for 14
Secure Sockets Layer
See SSL
Security Assertion Markup Language
See SAML
security standards 41
servers
configuring identity of server hosting service for Microsoft Excel add-in 54
identifying IP address 35
identifying port 35
identifying unused port numbers on 35
transferring databases between 17
Service Principal Name
configuring for web client 95
service provider
registering IBM Cognos Incentive Compensation Management as 81
service providers
overview 80
service.exe.config file
configuring client with LDAP authentication 23
configuring database server settings 11
configuring database server settings in 9
email SSL settings 14
external tool settings 13
Incentive Compensation Management settings 12
mail settings 14
managing email settings for portal access 15
mobile settings 14
overview 8
setting email address for administrator 15
services
Cognos Incentive Compensation Management for Windows 2
configuring to use certificates 36
Console 2

Index 109
services (continued)
setting up for Microsoft Excel add-in 52
setting up for Microsoft Excel add-in in client 55
setting up for Microsoft Excel add-in in services 53
single sign on
integration with IWA 93
SiteMinder
accessing web client with 77
configuring web client for 77
overview 77
siteminder.properties file
configuring web client for SiteMinder 77
Solaris
installing web client in 57
SQL Server
See Microsoft SQL Server
SSL
configuring for email 14
configuring for LDAP 23
encryption between application server and database server 25
encryption between client and application server 75
encryption between database server and web application server 76
encryption between web client and web application 76
identifying server certificates 54

T
tabs
See web tabs
tailored reports
API specifications for 43
Task Manager
configuring 12
TCP
configuring for Windows Service 12
themes
changing client to match Salesforce.com 89
TLS security
certificates 11
changing Windows Service communication to 12
security options 75
Tomcat
See Apache Tomcat
Transport layer security
See TLS security
trusted network
between application server and database server 75
between application server and database server with SSL 75
between client and application server 75
between client and application server with SSL 75
between database server and web application server 76
between database server and web application server with SSL 76
between web client and web application 76
between web client and web application with SSL 76
Windows Domain 75

U
Unicode
configuring support for web client 69
Unicode (continued)
configuring support for web client using Apache Tomcat 59
configuring support for web client using JBoss 62
configuring support for web client using WebSphere 65
SQL models 10
uninstalling IBM Cognos Incentive Compensation Management 16
upgrades
IBM Cognos ICM.exe.config 16
jdbc.properties 16
models 18
overview 15
performing 18
standard 16
user groups
allowing LDAP user groups to access client 24
users
allowing LDAP users to access client 24

W
web client
access with SiteMinder 77
changing color scheme and logo 71
changing color scheme and logo for theme 74
configuring database access using Apache Tomcat 59
configuring database access using JBoss 60
configuring database access using WebSphere 63, 66
configuring for Oracle CRM 88
configuring for Salesforce.com 86
configuring for SiteMinder 77
configuring language support using Apache Tomcat 59
configuring multilingual support for locale 69
configuring multilingual support using JBoss 62
configuring multilingual support using WebSphere 65
configuring Service Principal Name and keytab 95
configuring Unicode data support using Apache Tomcat 59
configuring Unicode data support using JBoss 62
configuring Unicode data support using WebSphere 65
configuring WebSphere 8 for 65
deploying using Apache Tomcat 58
deploying using JBoss 61
deployment of with encrypted passwords 69
disabling collection of Presenter report information 71
installing and configuring Apache Tomcat 58
installing and configuring Java 57
installing and configuring Java for JBoss 60
installing and configuring JBoss 60
installing in Solaris 57
integration with external applications 85
integration with IWA 93
LDAP configuration 82
LDAP properties 82
LDAP validation 82
obtaining encrypted password 68
overview 57
overview of Apache Tomcat deployment 57
overview of JBoss deployment 60
overview of WebSphere 7 deployment 62
overview of WebSphere 8 deployment 65
password encryption 68
password encryption in Windows 69
presenter data grid row limits in 71
preventing Presenter reports from loading with a large amount of data 71

110 IBM Cognos Incentive Compensation Management Version 9.0.0: Installation and Configuration Guide
web client (continued)
  property file encryption  68
  sending automatic emails from  70
  setting up for Google Chrome with IWA  94
  setting up for Internet Explorer with IWA  93
  setting up for Mozilla Firefox with IWA  93
  setting up Kerberos configuration file  94
  setting web container custom property for WebSphere  64
  setting web reports
    API specifications for  43
  web server
    configuring Apache Tomcat to accept proxied requests
    through Microsoft IIS web server  90
    configuring to prepare for integration with Microsoft IIS
    web server  89
  web tabs
    adding  72
    adding groups  73
    deleting  73
    editing  73
    moving  73
    overview  72
    removing from groups  73
web tabs (continued)
  setting access to  74
WebSphere 7
  configuring database access using  63, 66
  configuring multilingual and Unicode support using  65
  deploying web client  62
  overview of deployment of web client  62
  setting web container custom property for  64
  using Admin Console to start web client  64, 67
WebSphere 8
  configuring database access using  63, 66
  configuring for web client  65
  configuring multilingual and Unicode support using  65
  deploying web client  66
  overview of deployment of web client  65
Windows
  setting to start automatically  8
Windows Domain  75
Windows Service
  configuring  9
  configuring communication modes  12
  configuring database server settings  11
  configuring environments for  8
  configuring external tools  13
  configuring Scheduler and Task Manager  12
  configuring SSL for emails  14
  editing configuration files for  21
  installing  7
  multiple instances  20
WS-I compliance  41