Note

Before using this information and the product it supports, read the information in "Notices" on page 99.

Product Information

This document applies to IBM Cognos Incentive Compensation Management Version 8.0.4 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 requirements .......... 3
  Setting Up IBM Cognos Incentive Compensation Management as the database owner for Microsoft SQL Server 4
  Changing the DEFAULT_SCHEMA through Microsoft SQL Server Management Studio .......................... 4
  Changing the DEFAULT_SCHEMA using a query ........................................ 5

Chapter 2. Install the IBM Cognos Incentive Compensation Management Client and Service ............................................... 7
Installing the IBM Cognos Incentive Compensation Management Client ............................................... 7
Installing the Windows Service .............................................. 7
  Setting the IBM Cognos Incentive Compensation Management Windows Service to start automatically 7
Edit the configuration files .................................................. 8
  Editing the IBM Cognos Incentive Compensation Management Client configuration file ............................. 8
  Edit the IBM Cognos Incentive Compensation Management Service configuration file ........................... 9
Upgrade IBM Cognos Incentive Compensation Management .......... 16
  Standard upgrade .......................................................... 16
  Running simultaneous instances of IBM Cognos Incentive Compensation Management .......................... 20
Verify the installation of the Client ........................................ 21
  Opening an existing model ................................................. 22
  Creating a new model ...................................................... 22
Integrate LDAP with the client ............................................ 23
  Configuring the Windows Service configuration file for LDAP authentication ........................................... 24
  Granting LDAP users or LDAP groups access to the Client ............................................................. 24
Enable Data Tier Performance Optimization ............................ 25
  CLR integration .......................................................... 25
  Enabling Data Tier Performance Optimization in the Client .............................................. 25

Chapter 3. Install and use IBM Cognos Incentive Compensation Management Client tools .................................................. 27
IBM Cognos Incentive Compensation Management Console Service .............................................. 27
  Installing the Console Service .............................................. 27
  Editing the Console Service configuration file ............................ 27
  Starting the Console Service .............................................. 27
IBM Cognos Incentive Compensation Management configuration file encryption ................................ 28
  Install the IBM Cognos Incentive Compensation Management Configuration File Encrypter tool .................. 28
  Running the IBM Cognos Incentive Compensation Management Configuration File Encrypter .................. 28
IBM Cognos Incentive Compensation Management Model Converter .................................................. 28
  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 .................................................... 29
  Using the Enterprise Size Optimization feature ....................... 30
Use certificates with IBM Cognos Incentive Compensation Management .................................................. 31
  Required software to use digital certificates ............................ 31
  Generating certificates for IBM Cognos Incentive Compensation Management ........................................ 31
  Setting up Microsoft Management Console to use digital certificates .................................................... 33
  Import certificates for use with IBM Cognos Incentive Compensation Management ............................... 33
  Identify the server IP address and port .................................. 34
  Configure IBM Cognos Incentive Compensation Management to use certificates ................................... 36

© Copyright IBM Corp. 2005, 2014
Chapter 4. Install and configure the IBM Cognos Incentive Compensation Management web client .............................................. 59
Installing the IBM Cognos Incentive Compensation Management web client using the Solaris operating system .................................. 59
Apache Tomcat deployment .................................................................................................................................................. 59
Installing and configuring Java ............................................................................................................................................... 59
Installing and configuring Apache Tomcat .............................................................................................................................. 59
Deploying the application using Apache Tomcat ....................................................................................................................... 60
Configuring database access using Apache Tomcat .................................................................................................................. 60
Configuring multi-language and Unicode data support for Apache Tomcat .......................................................................... 61
JBoss deployment .................................................................................................................................................................... 62
Installing and configuring Java for JBoss ................................................................................................................................ 62
Installing and configuring JBoss ................................................................................................................................................. 62
Configuring database access for JBoss .................................................................................................................................. 62
Deploying the IBM Cognos Incentive Compensation Management web client with JBoss ....................................................... 63
Configuring multi-language and Unicode data support for JBoss ............................................................................................. 64
WebSphere 7 deployment .......................................................................................................................................................... 64
Downloading the IBM Cognos Incentive Compensation Management Web Application ................................................................. 64
Configuring database access using WebSphere ........................................................................................................................ 65
Using the WebSphere Admin Console to start the web application ......................................................................................... 66
Setting a web container custom property on WebSphere .......................................................................................................... 66
Configuring multi-language and Unicode data support for WebSphere .................................................................................. 67
WebSphere 8 Deployment .......................................................................................................................................................... 67
Property file encryption .............................................................................................................................................................. 69
Obtaining encrypted passwords .................................................................................................................................................. 70
Configuring IBM Cognos Incentive Compensation Management web client ....................................................................... 70
Configuring IBM Cognos Incentive Compensation Management web client password encryption in a Windows environment ............................................................................................................................... 71
Deployment of the IBM Cognos Incentive Compensation Management web client with encrypted passwords .......................................................... 71
Multi-language and Unicode data support .................................................................................................................................. 71
Emailing users when an inquiry is pending .................................................................................................................................. 72
Preventing Presenter reports from loading with a large amount of data ................................................................................... 73
Change the appearance of the IBM Cognos Incentive Compensation Management web client .................................................. 73
Web tab configuration ................................................................................................................................................................. 73
Changing the web client theme .................................................................................................................................................... 75

Chapter 5. Authentication and Sign On ................................................................................................................................. 77
IBM Cognos Incentive Compensation Management communication path options ........................................................................ 77
IBM Cognos Incentive Compensation Management Client to application server ........................................................................ 77
IBM Cognos Incentive Compensation Management application server to database server .................................................................. 77
Web client to IBM Cognos Incentive Compensation Management web application .................................................................... 78
IBM Cognos Incentive Compensation Management web application to database server .......................... 78
Authentication options ............................................ 78
SiteMinder configuration with IBM Cognos Incentive Compensation Management .......................... 79
Configuring the IBM Cognos Incentive Compensation Management web client for CA SiteMinder .... 79
Access the web client with SiteMinder configured .......... 79
OpenSSO configuration ............................................ 80
  Downloading and installing OpenSSO .......................... 80
  Configuring OpenSSO ......................................... 81
  Identity provider (IDP) configuration ......................... 81
  Service Provider configuration ............................... 82
LDAP configuration for the web client ......................... 83
  Validation requirements ..................................... 84
  Configuring the ldap.properties file ....................... 84
  Configuring the Web.xml file ................................ 85
Chapter 6. Integration ........................................... 87
Configuring the IBM Cognos Incentive Compensation Management web client for Salesforce ............. 87
Accessing IBM Cognos Incentive Compensation Management from Salesforce.com ......................... 87
Integrate the IBM Cognos Incentive Compensation Management web client with Oracle CRM .......... 88
  Configuring the IBM Cognos Incentive Compensation Management Client for integration with Oracle CRM 89
  Configuring the IBM Cognos Incentive Compensation Management web client for use with Oracle CRM 89
Change the appearance of IBM Cognos Incentive Compensation Management to Salesforce .......... 90
  Changing the theme of the IBM Cognos Incentive Compensation Management to Salesforce.com .... 90
Integrate with Microsoft's IIS web server .................... 90
  Configuring the IBM Cognos Incentive Compensation Management web client ......................... 91
  Configuring Apache Tomcat to accept proxied requests ..................................................... 91
  Configuring IIS to forward requests to IBM Cognos Incentive Compensation Management .......... 91
Integration with IWA ............................................. 94
  Setting up for Internet Explorer .............................. 94
  Setting up for Firefox ....................................... 95
  Setting up for Google Chrome ............................... 95
  Creating a Kerberos configuration file ..................... 95
  Configuring the Service Principal Name and keytab ..................................................... 96
  Setting up the IBM Cognos Incentive Compensation Management web client ........................ 96
Notices ......................................................... 99
Glossary ........................................................ 103
A ............................................................................ 103
C ............................................................................ 103
D ............................................................................ 104
F ............................................................................ 104
I ............................................................................ 104
J ............................................................................ 104
L ............................................................................ 105
M ............................................................................ 105
O ............................................................................ 105
P ............................................................................ 105
Q ............................................................................ 105
R ............................................................................ 106
S ............................................................................ 106
V ............................................................................ 106
W ............................................................................ 106
Index ..................................................................... 109
Introduction

This document is intended for use with IBM® Cognos® Incentive Compensation Management Version 8.0.4.

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 IBM Cognos product documentation on the web, including all translated documentation, access the IBM Cognos Incentive Compensation Management Information Center (http://pic.dhe.ibm.com/infocenter/cicm/v8r0m4/index.jsp). Release Notes are published directly to Information Centers, and include links to the latest technotes and APARs.

You can also read PDF versions of the product release notes and installation guides directly on the IBM Cognos product discs.

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.

Accessibility features

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

IBM Cognos HTML documentation has accessibility features. PDF documents are supplemental and, as such, include no accessibility features.
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.

Application overview

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

The following three applications make up the integrated solution:
1. Client - user interface for getting work done.
2. Application server - contains the business logic, calculation engine, and business event scheduler
3. 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 each model administrator's workstation
• 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 written in C# using the Microsoft .NET framework

The following points outline the details of the application server:
• 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.

In order to use the application, you must install the Client on the administrator's workstation and the Cognos Incentive Compensation Management Windows Service needs to be installed and running on the server. Tools, such as Model Upgrader, Model Converter, CLI, the IBM 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 used in conjunction 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</td>
<td>The Client must be installed to run the application.</td>
</tr>
<tr>
<td>Cognos Incentive Compensation Management Windows Service</td>
<td>ICM-service</td>
<td>The Cognos Incentive Compensation Management Windows Service (or Console Service) must be installed and running for the Cognos Incentive Compensation Management application to work correctly.</td>
</tr>
<tr>
<td>Console Service</td>
<td>ICM-console</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>CLI (Command-Line Interface)</td>
<td>ICM-cli</td>
<td>The CLI installer needs to be run in order to use the CLI tool. It is not required for the core Cognos Incentive Compensation Management application.</td>
</tr>
<tr>
<td>IBM Cognos Incentive Compensation Management add-in for Microsoft Excel</td>
<td>ICM-exceladdin</td>
<td>The IBM Cognos Incentive Compensation Management add-in for Microsoft Excel installer must be run in order 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</td>
<td>The Configuration File Encrypter installer needs to be run in order to use the Configuration File Encrypter tool. It is not required for the core Cognos Incentive Compensation Management application.</td>
</tr>
<tr>
<td>Model Converter</td>
<td>ICM-modelconverter</td>
<td>The Model Converter installer needs to be run to convert models to a different version of Microsoft SQL Server. It is only required for model conversion.</td>
</tr>
<tr>
<td>Model Upgrader</td>
<td>ICM-modelupgrader</td>
<td>The Model Upgrader tool needs to be installed to upgrade your Cognos Incentive Compensation Management model to a newer version. If the Client and Service have been upgraded, existing models also must 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:

- Download the Cognos Incentive Compensation Management installation files
- Install Microsoft .NET Framework 3.5 SP1 on both the server and client (can be downloaded from [http://www.microsoft.com/downloads](http://www.microsoft.com/downloads))
- Install Java™ 6
- Grant administrator access to all computers involved
- Grant sufficient database user rights or be the database owner

Microsoft SQL Server database permission requirements

When deploying 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 in order to access your database.

When installing 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.

**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 (ICMDatabase).
4. Run the following script:
   ```sql
   USE [ICMDatabase]
   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 ICMDatabase
   - 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 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 select **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 on with an administrator account.
3. Run the following query:

   ```sql
   ALTER USER "ICMDBUser" WITH DEFAULT_SCHEMA dbo;
   ```
Chapter 2. Install the IBM Cognos Incentive Compensation Management Client and Service

Both the Cognos Incentive Compensation Management Client and 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 IBM Cognos Incentive Compensation Management Client

The 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.

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 located 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, refer to the instructions on upgrading.
3. Complete the steps in the installation wizard.

   Important: By default, the Cognos Incentive Compensation Management Service startup type is set to manual, which means that users will manually have to start the service each time they want to start the Client.

Setting the IBM Cognos Incentive Compensation Management Windows Service to start automatically

You can change the startup type of the 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.

**Edit the 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.

**Editing the IBM Cognos Incentive Compensation Management Client configuration file**

You must modify the IBM Cognos ICM.exe.config file to specify how the Client will communicate with the application server.

When installing Cognos Incentive Compensation Management, you will 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 different settings are available:

- **Transport layer security 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.

3. **Edit the serviceAddress.**
   This indicates the port that the service is using. Each environment needs to be configured to use a different port.

**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.

**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.

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 to be open at the same time on one computer:

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

**Edit the IBM Cognos Incentive Compensation Management Service configuration file**
The Cognos Incentive Compensation Management Service configuration file indicates how the application server will communicate with the database server.

This change should be made to the file that is in the same directory as the IBM Cognos ICM Windows Service.exe file.

**Configuring the 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 for connection to a Microsoft SQL Server 2008 database.

**Procedure**
1. Open the **IBM Cognos ICM Windows Service.exe.config** file.
2. In the `databaseServers` section, do the following tasks:
a. Modify 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. Modify the **User**.
   This is the same as the database user. For Microsoft SQL Servers, Cognos Incentive Compensation Management requires SQL Authentication or Windows Authentication in order to connect. Therefore, you must connect using a local database user. If you are using Windows Authentication, both the user and password values should remain blank.

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

d. Modify the **Address**.
   This address points to the location of the database. The Address should use the following format: 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, SEVER_NAME\INSTANCE_NAME, PORT_NUMBER).

e. Modify the **Type** of database.

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

g. Modify 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 very long calculation times, this time may be increased to avoid a database timeout during calculation.

**Configuring access to multiple databases**

If you have multiple database servers, the IBM Cognos ICM Windows Service.exe.config file allows multiple database sections to be configured.

This allows you to 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 contained on each database server configured in the service configuration file are accessible from the login screen.

**Procedure**


2. Complete a `<databaseServer>` section for each of your servers.
   **Attention:** 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 in order 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 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 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 the 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** vale 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 used to authenticate the Cognos Incentive Compensation Management environment and database.

4. Change the **CommunicationMode** and **SecurityMode** values in the Cognos Incentive Compensation Management client configuration file to the same values as those in the Windows service configuration file.
   a. 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.

**Attention:** 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 IBM Cognos Incentive Compensation Management settings**

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

**Procedure**

1. In the IBM Cognos ICM section, edit the **SchedulerUser** and **SchedulerPassword** values to match the user ID and password of the user given the Scheduler role in the Manage Users window in the Cognos Incentive Compensation Management Client.
If the SchedulerUser and SchedulerPassword are not updated here after being changed in the Client, the scheduled processes will not run.

**Attention:** In order to run Scheduler, the Cognos Incentive Compensation Management Windows Service must be run as a Windows Service. Make sure that Scheduler and Cognos Incentive Compensation Management API Windows Service are started before scheduling any process.

2. You can modify the **SchedulerRefreshSeconds** value to indicate how often Scheduler will update to include any changes that the user has made in the Scheduler module.

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

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

5. You can modify the **AllowAnonymousModelCreation** value to determine whether or not administrators can create new models.
   If this is set to **False**, new models cannot be created.

6. You can modify the **Language** value to the language you want to be used in the Audit module logs.
   Setting the Language to **EnglishUS** will set the date format to month/day/year. Setting the Language to **EnglishGB** will set the date format to day/month/year.

7. You can uncomment and modify the **Saved Import File Directory** value to point to the location where Cognos Incentive Compensation Management will look 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.

8. You can uncomment and modify the **Saved Publisher File Directory** value to point to the location where Cognos Incentive Compensation Management will place published files that have been scheduled for publishing via Scheduler.
   This setting has to be determined before publishing can be scheduled and must refer to a directory on the same computer as the Windows Service.

9. You can uncomment and modify the **Saved Image File Directory** value to point to the location where Cognos Incentive Compensation Management will look 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 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 are to be scheduled by Scheduler will have to reside in the External Tools Directory.
Procedure
1. Uncomment and modify the ExternalToolDirectory section to point to the location where Cognos Incentive Compensation Management will look for items used outside of Cognos Incentive Compensation Management.
2. To modify the maximum run time Scheduler will allot for the tool to run, click the Properties button in the Schedule module in the Cognos Incentive Compensation Management Client.
   After that time is up, Scheduler will continue down the list of actions to perform.

Configuring email SSL settings
If the server is configured to send emails, then the connection to the email server can be encrypted with 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 entered 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 will usually be set to the administrator's email address. When Portal Access emails are generated, they are sent from the email address indicated here.

To send emails from Portal Access the following section of the Cognos Incentive Compensation Management Windows Service configuration file must be configured:
Setting the email address of the IBM Cognos Incentive Compensation Management administrator

The email address of the Cognos Incentive Compensation Management administrator must be set in the Client.

Procedure

1. Log in to the Cognos Incentive Compensation Management Client.
2. Select 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.password=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.
Upgrade IBM Cognos Incentive Compensation Management

The 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 install a new service to run parallel with the initial installation.

**Standard upgrade**

A standard upgrade will replace 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 will no longer be available on your computer after the upgrade. Before the new version of Cognos Incentive Compensation Management can be installed, the previous version of Cognos Incentive Compensation Management must be removed. All tools and components in Cognos Incentive Compensation Management must be the same version in order for Cognos Incentive Compensation Management to work properly. 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 upgrading your IBM Cognos Incentive Compensation Management installation, there are some steps you should follow to ensure your upgrade is successful.

Back up any existing Cognos Incentive Compensation Management models before you upgrade. Save copies of your configuration files prior to upgrading 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 will need to be manually updated.

**Procedure**

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

   **Attention:** 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, as well as any other Cognos Incentive Compensation Management tools you may have installed, such as the Cognos Incentive Compensation Management add-in for Microsoft Excel, Cognos Incentive Compensation Management CLI, and Configuration File Encrypter.

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

A database backup duplicates all the data contained 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 the backup completed.

Backing up a database:

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

Procedure

1. Using Microsoft SQL Server Enterprise Manager, from the Tools menu, select Backup Database.
2. Select one of the following Backup Types:
   - Complete backup: makes a full backup of your database. You will almost always need to start your backup strategy with a full back up of your database.
   - Differential backup: stores all changes that have occurred to the database since the last full backup.
3. You can modify 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 used in the IBM Cognos Incentive Compensation Management database. Upon restoring 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. Select Restore Database from the Tools menu.
2. The Restore as Database field is the name of your newly restored database. It does not have to be identical to the name of the original (backed up) database.
3. Define your restoration parameters by selecting the original database name and the stored backup you want to be restored.

Using back up 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 IBM Cognos Incentive Compensation Management application
After you have performed the upgrade preparation steps and uninstalled your current version of Cognos Incentive Compensation Management, you are ready to install the new version.

Procedure
1. Install the Cognos Incentive Compensation Management Client.
   For more information, see “Installing the IBM Cognos Incentive Compensation Management Client” on page 7.
2. Install the Cognos Incentive Compensation Management Windows Service.
   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 “Edit the configuration files” on page 8.
4. Install any additional Cognos Incentive Compensation Management tools, such as the CLI.

Upgrade your IBM Cognos Incentive Compensation Management model
The Cognos Incentive Compensation Management Model Upgrader is a tool that allows Cognos Incentive Compensation Management database models to be upgraded so they are compatible with the upgraded version.

After you have completed upgrading an existing version of Cognos Incentive Compensation Management, you will need to upgrade your models to the new version as well.

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

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

Attention: If you have a previous version of Model Upgrader installed, make sure you have removed the older Model Upgrader before installing the new one.
Procedure
1. Double-click the **ICM-modelupgrader.exe** installation file located in your release folder.
2. Complete the steps in the installation wizard.

**Running Model Upgrader:**

After Model Upgrader has been installed, you will need to start the Model Upgrader tool to upgrade your current model to be compatible with the new version of IBM Cognos Incentive Compensation Management.

Procedure
1. In the location specified during the installation of the Model Upgrader tool, double-click the **ModelUpgrader.exe** file.
   The Model Upgrader tool will open.
2. Type the **Server Name**.
   This is the name of the database server containing 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 should follow this format: SERVER_NAME\INSTANCE_NAME.
3. Select the **Database Type** from the drop-down menu.
   This is the type of database that you are connecting to, such as Microsoft SQL Server 2000 or 2005.
4. Type in the **Database Name**.
   This is the name of the database containing your Cognos Incentive Compensation Management model.
   a. If you do not know the database name, click **Browse**.
   b. Select a model.

   **Tip:** The database version is listed in brackets beside each model.
5. Type a value in the **Database Timeout** field.
   The default is 90 seconds and probably does not need to change. However, you should change it here if you have increased the default timeout in the Cognos Incentive Compensation Management Windows Service configuration file.
6. Type your **UserID** 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 select the Options button when running the IBM Cognos Incentive Compensation Management Model Upgrader tool, you are able to set error protection.

The following error protection options are available:

- **None** - This option uses the least amount of resources but offers no protection for the model should an error occur. If an error occurs during the upgrade process, the model being upgraded is unsalvagable and must be restored from a backup.
Attention: A backup must be created prior to using this option.

- **Partial** - If a model fails to upgrade and the partial protection option is selected, it is possible that the error can be resolved without restoring the original backup of the model. Also, upgrades that fail may always safely be restarted when using this option. This option uses less resources than the Complete option but more than the None option.

  Attention: A backup must be created prior to using this option.

- **Major Release** - If the upgrade should fail, this option will roll 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 have been made, Model Upgrader can be safely run again.

  Attention: Make a model backup prior to selecting this option.

- **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 indicating the specific database version that you are upgrading to.

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

You may want to select a database version to control the level of error protection at different points during the upgrade. Selecting a target version also allows you to perform the upgrade in smaller increments to avoid running out of disk space.

### Running simultaneous instances of IBM Cognos Incentive Compensation Management

If it is necessary, you can keep previous versions of Cognos Incentive Compensation Management running along with a new version.

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

**Procedure**

1. Double-click the **ICM-service.exe** file located in your release folder.
   a. Select **Named Instance** and specify an instance name for the new service. For example, Service2.

      **Attention:** Instance names must be unique for all Windows Services, regardless of version number.

   b. 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.

c. Specify a Start menu folder.
The Start menu folder must be unique for each Windows Service installation. For example, type IBM Cognos ICM\Service2.

d. Click Install.

**Important:** If the installation is not successful, uninstall and re-install the Windows Service.

2. Repeat the steps above for each Windows Services that you want to install.


4. Scroll down in the Services window and find IBM Cognos 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 above steps.

5. Right-click the Windows Service, for example, IBM Cognos ICM Windows Service (SERVICE2), and select Properties.

6. Make sure the Path to executable is correct and pointing to the new Windows Service installation.

7. Repeat steps 5 and 6 for the other Windows Services you installed.

### Editing the IBM Cognos Incentive Compensation Management Windows Service configuration files

You will need to make some changes to the Cognos Incentive Compensation Management Windows Service configuration files to indicate how the application server will communicate 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 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 IBM Cognos ICM Windows Service instance name section, make sure the `<add key="ServiceInstanceName" value="myinstance"/>` line is uncommented and the value of the name of the Service instance has been updated.
   For example, `<add key="ServiceInstanceName" value="Service2"/>`.

5. Make any other edits and changes required, and then save and close the configuration file.

6. Repeat steps 1-5 for any other Service folders you created.

7. Start the IBM Cognos ICM Windows Services.

### Verify the installation of the Client

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

If you upgraded your IBM Cognos Incentive Compensation Management model, log in to the Client to make sure the upgrade was successful.

Procedure
1. Open the Client.
2. Select the Model Name from the drop-down menu.
3. Type your User ID and Password.
4. Click Login.

Creating a new model

Open the IBM Cognos Incentive Compensation Management Client and create a model to make sure the Client has been installed successfully.

Procedure
1. Open the Client.
2. Click Options to change the language of the Client and set the date format. Select EnglishGB to set the date format to day/month/year, or select EnglishUS to set the date format to month/day/year.
3. Click New Model.
4. Name the model.
   Cognos Incentive Compensation Management will remove all spaces and punctuation from your model name and use that as the database name on your database server. The model name can be changed at any time from within Cognos Incentive Compensation Management, but the database name that is set initially will remain for the life of the database.
5. Select when Your current fiscal year began.
   This is the first day in the current fiscal year. Cognos Incentive Compensation Management will use this date and the number of payroll periods to construct a default calendar for this new model. The default calendar can be modified and refined from within the Client, or replaced entirely if a mistake is made.
6. Select the Number of payroll periods.
   This is how many times per year your organization pays employees, either 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 modified or replaced entirely once the new model is created.
7. Select the currency.
   A currency should be added if it is used for either collection or payment. More than one currency can be selected. If you require a currency that is not in the pick list, you can add additional currencies by clicking Other Currencies.
   Attention: Currencies can be added without using the New Model wizard, so the list can be expanded at a later time.
8. Select any Cognos Incentive Compensation Management hierarchies.
   Defining hierarchies specifies the columns that are used to define the data tables within Cognos Incentive Compensation Management. Columns for payees, accounts, date, and value are automatically generated. If your data file contains more required columns, such as, products, customers, territories, or promotion codes, you can add those items to the list of hierarchies by either checking the appropriate box or typing their names in the text box.
Attention: It does not matter whether the data for these columns exists in a single data file or if you are loading multiple data files.

9. Click Finish.

**Integrate LDAP 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:

1. LDAP users cannot log in if there is a pending password change in the account.
2. LDAP users cannot log in if there account is disabled.
3. LDAP users cannot log in twice in the same model.
4. 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).
5. If the LDAP user is mapped to different Cognos Incentive Compensation Management roles, the union of the permission are given.
6. The administrator role can be renamed and mapped to any LDAP group and any user in this group will have all administrator permissions.
7. If an LDAP user is logged in to the client, the change password menu item is disabled.
8. LDAP users can write web messages and upload web documents.
9. An LDAP user can be the Scheduler (the same rules for a Scheduler user apply).
10. 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. Modify the `ProviderUrl` value to point to the address of the LDAP server that should be searched.
3. Modify the `ManagerDn` value.
   This is the account that should be used to perform the LDAP tree search.
4. Modify the `ManagerPassword` value.
   This is the password of the ManagerDn account.
5. Modify 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. Modify 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.

Enable Data Tier Performance Optimization

The Data Tier Performance Optimization feature in IBM Cognos Incentive Compensation Management can improve calculation performance, especially in models that have a large number of calculations that perform multiplication and division operations.

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.

CLR integration

In order to use the Data Tier Performance Optimization feature in IBM Cognos Incentive Compensation Management, the common language runtime (CLR) integration feature in Microsoft SQL Server needs to 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.

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

Enabling Data Tier Performance Optimization in the Client

After enabling the common language runtime (CLR) integration feature, performance optimization needs to be turned on in the IBM Cognos Incentive Compensation Management Client.

Procedure
1. Go to Admin > Administrative Options.
2. Click the Calculation tab.
3. Select the Enable data tier performance optimization check box.
Chapter 3. Install and use IBM Cognos Incentive Compensation Management 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.

IBM Cognos Incentive Compensation Management Console Service

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

It is possible to run multiple console services on the same computer, as long as each service is installed in a separate directory and is configured to use a different port.

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 located in your release folder.
2. Complete the steps of 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 be the same as the security settings in the Client.

Starting the Console Service

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

Procedure
1. Start a command prompt.
2. In the directory that the Console Service is located in, type ConsoleService.
   A message displays reporting that the service is running.
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 in order to bypass the service and access the database directly.

IBM Cognos Incentive Compensation Management configuration file encryption

The Cognos Incentive Compensation Management Configuration File Encrypter tool 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 (IBM Cognos ICM Windows Service.exe.config) and Console Service (ConsoleService.exe.config) configuration files: DBPassword, DBUser, SchedulerPassword, and SchedulerUser.

Install the IBM Cognos Incentive Compensation Management Configuration File Encrypter tool

Before running the Cognos Incentive Compensation Management Configuration File Encrypter tool, 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 IBM Cognos Incentive Compensation Management Configuration File Encrypter

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

Procedure

1. Launch the Configuration File Encrypter tool located in the IBM Cognos ICM release folder.
2. Click Browse to search for the IBM Cognos ICM Windows Service.exe.config or ConsoleService.exe.config file to be encrypted.
3. Click Encrypt.
4. Click Exit.
5. To decrypt a file, repeat the above steps but select Decrypt in Step 3.

Important: Encrypting a file will encrypt both sets of user names and passwords in the file (database and scheduler). You cannot choose to encrypt one or the other.

IBM Cognos Incentive Compensation Management Model Converter

The Model Converter tool allows Cognos Incentive Compensation Management models created in Microsoft SQL 2000 or 2005 to be converted to Microsoft SQL 2008 models, and models created in Microsoft SQL Standard edition to be converted to Microsoft SQL Enterprise.
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

An IBM Cognos Incentive Compensation Management model can be converted from Microsoft SQL Server 2000 to a Microsoft SQL Server 2008 model.

Procedure

1. Install Microsoft SQL Server 2008.
   
   **Attention:** The Cognos Incentive Compensation Management Windows Service must be running when using the Model Converter tool.
2. Restore your Microsoft SQL 2000 or 2005 model on to the Microsoft SQL 2008 server.
3. Launch the Model Converter tool.
4. Type the name of the SQL 2008 server in the **Server Name** field.
   
   This can be an arbitrary name, such as Super Server, and is intended 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 should be in the following format: `SERVER_NAME\INSTANCE_NAME`.
5. Select the appropriate **Database Type** for the model you want to convert.
   
   If you convert a Unicode model, it will remain a Unicode model after the conversion.
   
   **Attention:** Because you have restored your model onto a Microsoft SQL 2008 Server, you will need to 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.
7. Select **Microsoft SQL Server 2008** from the **Convert to** menu.
8. Type your Microsoft SQL Server login credentials.

Converting a Microsoft SQL Standard Model to an Enterprise Model

An IBM Cognos Incentive Compensation Management model can be converted from Microsoft SQL Standard to a SQL Enterprise Model.
Procedure
1. Install Microsoft SQL Server Enterprise Edition.
2. Restore your Microsoft SQL Standard Edition model on to the SQL Enterprise server.
3. Launch the Model Converter tool.
4. Type the name of the Microsoft SQL Enterprise Edition server in the Server Name field. 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 SQL Server 2000 named instance or if you are using a SQL Server 2005 database, the value for the Database Server field should be in the following format: SERVER_NAME\INSTANCE_NAME.
5. Select the appropriate Database Type for the model you want to convert. This is the Microsoft SQL Server version that you are converting from. If you convert a Unicode model, it will remain a Unicode model after the conversion.
6. Browse for the model you want to convert.
7. Select Microsoft SQL Server Enterprise Edition from the Convert to menu.
8. Type your Microsoft SQL Server login credentials.

Converting a Microsoft SQL 2005 Standard Edition model to a 2008 Enterprise Edition model
You can convert an IBM Cognos Incentive Compensation Management model from a Microsoft SQL 2005 Standard Edition model to a Microsoft SQL 2008 Enterprise Edition model.

You need to perform this conversion in the following two phases:

Procedure

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

This 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 alternate storage format that can be used to minimize the disk space 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 created prior to version 7.0, complete the following steps:
1. Upgrade to Cognos Incentive Compensation Management version 7.0 or higher.
   
   **Attention:** 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.

3. Using Model Converter, select **Enterprise Size Optimization** from the **Convert To** drop-down menu.

### Use certificates with IBM Cognos Incentive Compensation Management

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.

You will require the following software to work with certificates:

- **.NET Framework Redistributable**
  
  Go to [http://msdn.microsoft.com](http://msdn.microsoft.com) to download this software.

  **Important:** Version 3.5 SP1 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 this software.

  **Important:** The .NET Framework SDK has been superseded by the Windows SDK. Obtain the SDK appropriate for the versions of the Windows operating system and .NET Framework being used.

You will likely need administrator privileges for the Windows computer (server) where your digital certificates will be configured in order to successfully complete the configuration steps in this document.

### Generating certificates for IBM Cognos Incentive Compensation Management

You can generate your own digital certificates for testing or troubleshooting purposes.

**Attention:** 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 generated by the steps below can compromise the security of your production environment.

The Certificate Creation Tool (Makecert.exe) included in the .NET Framework\Windows SDK is used to generate a default self-signed (root) certificate (called "Root Agency") and a certificate signed by this root certificate.
1. Run the installed SDK Command Prompt and type the following command. You need to 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
```

**Command-line switches**

There are several command-line options that can be used to define your digital certificate for use with IBM Cognos Incentive Compensation Management.

- `-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 required in SSL but cannot be used for server authentication.

- `-pe` marks the private key as exportable.

- `-n` specifies the server name. This name must comply with the X.500 standard. The simplest form is CN="Name" and should specify the name of the server (case-insensitive) or the IP address where it is used. For example, for a server named "Apple" the certificate subject name should be CN="Apple".

- `-b` date value in mm/dd/yyyy format that specifies the start of the validity period for the certificate. The default for this 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 for this 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 in the my store, or anywhere in the certificate store.

- `-sr` specifies the certificate store where the certificate is located. Location can be either: currentuser (the default), or localmachine. Because this certificate is being created for a service, it should be placed in the local computer.

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

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

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

Use the corresponding command to generate the digital certificate. For example, you could type a command similar to the following command:

```
makecert -n "CN="Apple" -ss "My" -sr "LocalMachine" -pe -a sha1 -sky exchange Apple.cer
```
The generated digital certificate is stored in a file called Apple.cer in the directory from which the above command is executed. You can examine this digital certificate by opening the file (double-clicking it in Windows Explorer) and viewing its details.

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

Setting up Microsoft Management Console to use digital certificates

Microsoft Management Console (MMC) can be used to view the digital certificates for use with IBM Cognos Incentive Compensation Management installed in the local certificate repository, as well as import new digital certificates into the local certificate repository.

Procedure

1. From the Windows Start menu, click Run.
2. Type in mmc and click OK.
3. Go to the File menu and select 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.

Import certificates for use with IBM Cognos Incentive Compensation Management

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 certificates for IBM Cognos Incentive Compensation Management" on page 31, 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.
Importing the necessary digital certificates contained in a PKCS #12 file

In order to use certificates with IBM Cognos Incentive Compensation Management, the server certificate contained 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 select All Tasks > Import.
4. Click Next.
5. Click Browse and locate the PKCS #12 file.
   Change the Files of type selection to Personal Information Exchange.
6. After you have located 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 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.

Identify the 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 have now been installed is necessary in order to properly configure the server to identify itself.

An unused port number is also necessary to listen for SSL connections initiated by clients.

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

Identifying the IP Address of the server

When configuring 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 configuring the use of certificates with IBM Cognos Incentive Compensation Management, if a hostname is used instead of an IP address, the hostname 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\n
2. Map the certificate to the IP address of the server to which 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**
The SSL certificate must be bound to the IBM Cognos Incentive Compensation Management 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 displayed in the window.

6. Paste the value into a text editor and remove all the spaces from the thumbprint value.

7. Go to **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:
   ```
   Netsh http add sslcert ipport=0.0.0.0:13125 certhash=<thumbprint>
   appid=<GUID> clientcertnegotiation=enable
   ipport  The IP address configured in the hosts file.
   certhash  The value of the thumbprint with the spaces removed.
   appid  The GUID value with braces around it.
   ```

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

You are now ready to use the configured digital certificates to work with either 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 Cognos Incentive Compensation Management to use digital certificates.

**Procedure**

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

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

   ```
   <add key="APISecureAddress" value="MobileAPI:13125"/>
   <!-- API certificate required for access -->
   <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. Modify the serviceAddress value, to contain the same server name and port number as the values specified in the IBM Cognos ICM Windows Service.exe.config file.
7. Save the Cognos Incentive Compensation Management Client configuration file.
8. Stop the Cognos Incentive Compensation Management services in the following order:
   - IBM Cognos Incentive Compensation Management API
   - IBM Cognos Incentive Compensation Management Scheduler
   - IBM Cognos Incentive Compensation Management Windows Service
9. Start the Cognos Incentive Compensation Management services in the following order:
   • IBM Cognos Incentive Compensation Management Windows Service
   • IBM Cognos Incentive Compensation Management Scheduler
   • IBM Cognos Incentive Compensation Management API

IBM Cognos Incentive Compensation Management CLI

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.

IBM Cognos Incentive Compensation Management CLI preinstallation checklist

You must perform a few steps before installing the CLI.

In order for the Cognos Incentive Compensation Management CLI to connect to models on a configured database, you must first perform the following steps:
   • Start the Cognos Incentive Compensation Management Windows Service
   • Specify values for the APIAddress, APISecureAddress, and APICertificateName keys in the IBM Cognos ICM Windows Service.exe.config file
   • Start the Cognos Incentive Compensation Management API Service
   • 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 (see “Generating certificates for IBM Cognos Incentive Compensation Management” on page 31)

Installing IBM Cognos Incentive Compensation Management CLI

Before you can use the Cognos Incentive Compensation Management CLI, you must install the command-line interface application.

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

Configuring IBM Cognos Incentive Compensation Management 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, 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, and <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.

Executing CLI commands
Several processes can be run in the IBM Cognos Incentive Compensation Management Client using the CLI.

The following execution commands are currently available:
• calcall: Calculate all objects in the model
• runproc <process>: Run a saved process 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
• changewebuserpassword -payeeid <"payeeID of web user to change password for"> -webpw<"web user's password">: Change a web user's password

Attention: All CLI commands are case-sensitive.
The command should be typed after the model connection information.

The following command will connect to the SoftCo model and calculate all objects in the model on a server named MyServer:

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

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

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

The following command will connect 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 will connect 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 will connect 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"
```

**Return code from the CLI**

Determining the result of executing the IBM Cognos Incentive Compensation Management CLI can be done by checking the value that is returned to the caller (either the operating system or another process or tool).

The third-party tool being used to call Cognos Incentive Compensation Management through the CLI may need to know if the called process was able to complete successfully or if it failed. 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 entirely on the method used to launch 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.

**IBM Cognos Incentive Compensation Management API**

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 programmatically 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 overview**

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 "Use certificates with IBM Cognos Incentive Compensation Management" on page 31). Once 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

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

```text
<server>/<database>/<user_type>/<username>
```

*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 address:

- https://localhost:13125/API/Table?wsdl
# API specifications - 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>
</tr>
</thead>
<tbody>
<tr>
<td>(WSDL Address: <a href="https://localhost:13125/API/Scheduler?wsdl">https://localhost:13125/API/Scheduler?wsdl</a>)</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>Input</td>
</tr>
<tr>
<td>Output</td>
</tr>
<tr>
<td>Note</td>
</tr>
<tr>
<td>Exceptions</td>
</tr>
</tbody>
</table>

## Table 3. ComputeAll

<table>
<thead>
<tr>
<th>ComputeAll</th>
</tr>
</thead>
<tbody>
<tr>
<td>(WSDL Address: <a href="https://localhost:13125/API/Caculations?wsdl">https://localhost:13125/API/Caculations?wsdl</a>)</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>Input</td>
</tr>
<tr>
<td>Output</td>
</tr>
<tr>
<td>Note</td>
</tr>
<tr>
<td>Exceptions</td>
</tr>
</tbody>
</table>

## Table 4. ComputePlan

<table>
<thead>
<tr>
<th>ComputePlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>(WSDL Address: <a href="https://localhost:13125/API/Calculations?wsdl">https://localhost:13125/API/Calculations?wsdl</a>)</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>Input</td>
</tr>
<tr>
<td>Output</td>
</tr>
<tr>
<td>Note</td>
</tr>
<tr>
<td>Exceptions</td>
</tr>
</tbody>
</table>

## Table 5. ComputeTailoredReport

<table>
<thead>
<tr>
<th>ComputeTailoredReport</th>
</tr>
</thead>
<tbody>
<tr>
<td>(WSDL Address: <a href="https://localhost:13125/API/Calculations?wsdl">https://localhost:13125/API/Calculations?wsdl</a>)</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>Input</td>
</tr>
<tr>
<td>Output</td>
</tr>
<tr>
<td>Note</td>
</tr>
<tr>
<td>Exceptions</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 - 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 &quot;true&quot; (boolean) if the table exists in the model and &quot;false&quot; (boolean) otherwise</td>
</tr>
</tbody>
</table>
Table 9. TableExists (continued)

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

Table 10. GetTableSchema

<table>
<thead>
<tr>
<th>GetTableSchema</th>
</tr>
</thead>
<tbody>
<tr>
<td>(WSDL Address: <a href="https://localhost:13125/API/Table?wsdl">https://localhost:13125/API/Table?wsdl</a>)</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>Input</td>
</tr>
<tr>
<td>Output</td>
</tr>
<tr>
<td>Note</td>
</tr>
<tr>
<td>Exceptions</td>
</tr>
</tbody>
</table>

Table 11. GetTableRow

<table>
<thead>
<tr>
<th>GetTableRow</th>
</tr>
</thead>
<tbody>
<tr>
<td>(WSDL Address: <a href="https://localhost:13125/API/Table?wsdl">https://localhost:13125/API/Table?wsdl</a>)</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>Input</td>
</tr>
<tr>
<td>Output</td>
</tr>
<tr>
<td>Note</td>
</tr>
<tr>
<td>Exceptions</td>
</tr>
</tbody>
</table>

Table 12. AddRow

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

<table>
<thead>
<tr>
<th>Method</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, InvalidDataException, RetiredEndpointException, PermissionDeniedException, TokenException</td>
</tr>
</tbody>
</table>

### Table 13. UpdateRow

<table>
<thead>
<tr>
<th>Method</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, InvalidDataException, RetiredEndpointException, PermissionDeniedException, TokenException</td>
</tr>
</tbody>
</table>

### Table 14. DeleteRow

<table>
<thead>
<tr>
<th>Method</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, InvalidDataException, RetiredEndpointException, PermissionDeniedException, 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 - 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>GetDataStoreRowRange</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input</strong></td>
<td>DataStore ID (integer) ID of the DataStore</td>
</tr>
<tr>
<td></td>
<td>Restrictions (RestrictionBase) Restrictions to filter the data</td>
</tr>
<tr>
<td></td>
<td>StartIndex (integer) start index of the row of the result</td>
</tr>
<tr>
<td></td>
<td>Length (integer) number of the rows to retrieve</td>
</tr>
<tr>
<td><strong>Output</strong></td>
<td>Array of DataRow ([DataRow[]])</td>
</tr>
<tr>
<td><strong>Exceptions</strong></td>
<td>TokenException, IllegalArgumentException, InvalidDataException, LargeDataException, PermissionDeniedException</td>
</tr>
</tbody>
</table>

Table 20. GetDataStoreRowCount

<table>
<thead>
<tr>
<th>GetDataStoreRowCount</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input</strong></td>
<td>DataStore ID (integer)</td>
</tr>
<tr>
<td></td>
<td>Restrictions (RestrictionBase) Restrictions to filter the data</td>
</tr>
<tr>
<td><strong>Output</strong></td>
<td>Number of Rows in the DataStore (integer)</td>
</tr>
<tr>
<td><strong>Exceptions</strong></td>
<td>TokenException, IllegalArgumentException, InvalidDataException, PermissionDeniedException</td>
</tr>
</tbody>
</table>

Object definitions

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

**ColumnSchema**

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

**Earnings**

```java
public class Earnings
{
    public PayeeName PayeeName;
}
```
public string PlanID;

public string Amount;

}

EarningsDetails
public class EarningsDetails
{

public string[] ColumnHeaders;

public EarningsDetailsRow[] Details;

}

EarningsDetailsRow
public class EarningsDetailsRow
{

public string[] ColumnData;

public string Payout;

}

Inquiry
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;

}

InquiryComment
public class InquiryComment
{


public PayeeName Author;
public string CreationDate;
public string CommentText;
}

**NameValue**
public class NameValue
{
}

public string Name;
public string Value;
}

**PayeeName**
public class PayeeName
{
}

public string ID;
public string Name;
}

**PeriodEarnings**
public class PeriodEarnings
{
}

public string PeriodType;
public PeriodEarningsRow[] Earnings;
}

**PeriodEarningsRow**
public class PeriodEarningsRow
{
}

public string Period;
public string Amount;
}

**PlanEarnings**
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,
}
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**

class PermissionDeniedException : APIException

{ }

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

---

**IBM Cognos Incentive Compensation Management add-in for Microsoft Excel**

You can install a Cognos Incentive Compensation Management add-in for Microsoft Excel 2003 or 2007 and 2010 that gives users an easy way to do self-reporting using up-to-date Cognos Incentive Compensation Management results.

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

**Service-side setup for installing the IBM Cognos Incentive Compensation Management add-in for Microsoft Excel**

You must set up certificates on the computer that runs the Cognos Incentive Compensation Management Windows Service and modify the Windows Service configuration file.

**Setting up certificates**

To use 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. Go to 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 then OK.
9. Expand Certificates and expand Trusted Root Certification Authorities.
10. Select the Certificates folder under Trusted Root Certification Authorities, right-click and select All Tasks > Import.
11. In the Certificate Import Wizard, click Next.
12. Click Browse.
13. Open the folder containing the certificate and select All Files from the Files of type drop-down menu.
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 select All Tasks > Import.
22. Complete the steps to import the certificate.
   The Mobile API 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
To use the IBM Cognos Incentive Compensation Management add-in for Microsoft Excel, you must configure the identity of the server hosting the service in the hosts file.

Procedure
1. Go to C:\Windows\system32\drivers\etc and open the hosts file using 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 should be separated by at least one space. For example, 127.0.0.1 MobileAPI.
3. Save and close the file.

Identifying the server certificate
To use the IBM Cognos Incentive Compensation Management add-in for Microsoft Excel, you must identify the server certificate using the HTTP Configuration Utility.
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.
   **Attention:** If a hostname is being used instead of an IP address, the hostname needs to 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 for the appropriate group of users are granted.
7. Click OK in the SSL Configuration dialog.
8. Click OK to close the HTTP Configuration Utility.

Client-side setup for the IBM Cognos Incentive Compensation Management Add-in for Microsoft Excel

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 IBM Cognos Incentive Compensation Management add-in for Microsoft Excel

Before installing the 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 in order to run the Cognos Incentive Compensation Management add-in for Microsoft Excel 2007/2010:

- 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 in order 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
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 drop-down arrow and select Run from My Computer.
5. Click Continue.
6. When the configuration process is complete, click Close.

Set up 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” on page 54
- “Identifying the server certificate” on page 55
- “Configuring the identity of the server hosting the service” on page 55

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 IBM Cognos Incentive Compensation Management add-in for Microsoft Excel
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 Login Information.

9. Type your Username 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. Install and configure the IBM Cognos Incentive Compensation Management web client

The following topics provide instructions for installing and configuring the Cognos Incentive Compensation Management web client using either Apache Tomcat, JBoss, or WebSphere® deployment based on a Microsoft Windows operating system.

If you are using other operating systems, the steps are similar. This chapter also explains multi-language and unicode data support and how to configure the appearance of the web client. Before you begin, note that the web client requires the IBM Cognos Incentive Compensation Management Windows service (or the Console Service tool) to be installed and running on a server along with a Cognos Incentive Compensation Management model in order to function correctly.

Installing the IBM Cognos Incentive Compensation Management web client using the Solaris operating system

The 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. Unzip the ICM.war file.
5. Deploy as per Windows instructions.

Apache Tomcat deployment

The IBM Cognos Incentive Compensation Management web client can be easily deployed using Apache Tomcat version 6 or 7.

In order to successfully deploy the web client using Tomcat Manager, you must already have Java installed.

**Installing and configuring Java**

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

**Procedure**

Download and install Java 6 or 7 JRE from [http://java.sun.com/javase/downloads/index.jsp](http://java.sun.com/javase/downloads/index.jsp)

**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 6 or 7 from the following website: [http://tomcat.apache.org/download-60.cgi](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 using the archive provided on the following website: [http://tomcat.apache.org](http://tomcat.apache.org)

**Important:** When Tomcat is run as a service, there will not be a tray icon present while Tomcat is running. An exception to this rule occurs when opting to run Tomcat at the end of the installation process. Then the installer will create shortcuts for starting and configuring Tomcat. The Tomcat Web administration application can only be used when Tomcat is running.

**Deploying the application using Apache Tomcat**

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

**Procedure**

   
   Apache Tomcat runs on port 8080 by default, but if you specified a different port number during the installation of Tomcat, navigate to that port number instead.

2. Click the **Tomcat Manager** link and log in using the user name and password specified during the Tomcat installation.

3. On the Tomcat Manager page in the **Deploy** section, click **Browse**.

4. Find the **ICM.war** file and then click **Deploy**.
   
   When the page refreshes, an /ICM link displays under the Applications heading.

   **Attention:** Cognos Incentive Compensation Management requires uniquely named WAR files when deploying the WAR file as part of an upgrade. Clients will need to either uninstall their current WAR file before deploying a new one or change the name of the new WAR file.

5. Click the /ICM link to verify deployment.

   **Attention:** When you verify the deployment, you may see a Cognos Incentive Compensation Management web client window containing an internal error. This indicates that the web client has been deployed, but access to the Cognos Incentive Compensation Management database needs to be configured.

**Configuring database access using Apache Tomcat**

The web client configuration file must be modified to point to your IBM Cognos Incentive Compensation Management model.

Once the application has been deployed in Tomcat, the jdbc.properties file needs to be edited. It can be found in the following default locations: C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps\ICM\WEB-INF\jdbc.properties.

**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, such as 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.
3. Modify the 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 can also 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.
6. Go back to Tomcat Manager and click the Reload link for /ICM to propagate the changes.
7. Go to http://localhost:8080/ICM.
   If your server is running Cognos Incentive Compensation Management Windows Service with an existing Cognos Incentive Compensation Management model, all the users that have been set up in Portal Access through the .NET client will be able to log in.

Configuring multi-language and Unicode data support for Apache Tomcat

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 Apache Tomcat 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\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"
   You should have the following code now in the server.xml file:
   
   <Connector port="8080" protocol="HTTP/1.1"
   connectionTimeout="20000"
   redirectPort="8443"
   URIEncoding="UTF-8"/>

5. Save the file.
6. Restart the Apache Service.
JBoss deployment

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

The deployment requires 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 deploying 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

Download and install the Java SDK (JDK 6 Update 16) from the following website: [http://java.sun.com/javase/downloads/index.jsp](http://java.sun.com/javase/downloads/index.jsp)

Installing and configuring JBoss

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

Procedure

1. Go to the following JBoss website to download the web server: [http://www.jboss.org/download/](http://www.jboss.org/download/)
2. From the Downloads page, select the JBoss Application Server version you want to download.
3. Download the appropriate file and extract it to the directory of your choice.

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.

---

**Deploying the IBM Cognos Incentive Compensation Management web client with JBoss**

After Java and JBoss have been installed and the **jdbc.properties** file has been configured, the Cognos Incentive Compensation Management web client needs to be manually deployed.

JBoss will not automatically deploy the WAR file, so a few steps need to be followed to configure the Cognos Incentive Compensation Management web client.

**Procedure**

1. Create a file called **jboss-web.xml** and save this in an accessible location.
   It is a good idea to save this file with your ICM.war file and your pre-configured **jdbc.properties** file.
   a. Using WordPad or a similar application, copy the following text into the **jboss-web.xml** file:
      ```xml
      <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\`.
      You may rename the WAR file to something other than ICM for usability.
   3. Change the file extension from **.war** to **.zip**. This allows you to navigate within the file to `\WEB-INF`.
   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, which can be found in the following location: `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**

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 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"`  
   ```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" diableUploadTimeout="true" URIEncoding="UTF-8"
   />
   ```
5. Save the file.
6. Restart the Web Service.

**WebSphere 7 deployment**

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

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

**Downloading the IBM Cognos Incentive Compensation Management Web Application**

After installing 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**.
3. Select **New Enterprise Application**.
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 select box that corresponds with the current application and click Next.
12. On Step 5, check the select 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, then click OK.
21. Select the Save directly to the master configuration option.

Configuring database access using WebSphere

After deploying the WAR file, you will need to 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/..../applications/.../deployments/..../WEB-INF For example, /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/config/cells/..../applications/.../deployments/..../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 the 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 application**

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:SRVE019OE: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.
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 URI's 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: C:\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.

**WebSphere 8 Deployment**

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

After deploying the WAR file, you will need to 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:

- %PROGRAMFILES%\IBM\WebSphere\AppServer\profiles\AppSrv01\config\cells\[server name]Node01Cell\applications\CONTEXT ROOT_war.ear\deployments\CONTEXT ROOT_war\WEB-INF\CONTEXT ROOT\WEB-INF\jdbc.properties
- %PROGRAMFILES%\IBM\WebSphere\AppServer\profiles\AppSrv01\installedApps\..\..\..\ICM.war\WEB-INF\jdbc.properties
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/../../ICM.war/WEB-INF` For example, `/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/config/cells/../../ICM.war/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 the 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 application**

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`

**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.
   
   **Attention:** If only Java 5 is available, users will also have to download ICU4J and include the JAR when running the Jasypt CLI tools.

**Configuring IBM Cognos Incentive Compensation Management web client**

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 IBM Cognos Incentive Compensation Management 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**.
3. Under System Variables, click **New**.
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 IBM Cognos Incentive Compensation Management 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:

```properties
# 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(1qZ2aIYYQ11TsjiTcqfg==)
```

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.

**Multi-language and Unicode data support**

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, 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
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 Servive.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 located in the following directory:
   `...\webapps\ICM\WEB-INF`
   **Attention:** You will need to reload the ICM.war file after making changes to the configuration files.

2. In the admin client, go to **Admin > Administrative Options**, and click the **Portal Access** tab.

3. Select the **Email users when an inquiry is pending** check box.

4. 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.

Change the appearance of the IBM Cognos Incentive Compensation Management web client

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
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 need to select a compensation plan.
6. Click **Finish**.

**Tip:** The first tab listed in Portal Access is the first tab that will be 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.

IBM Cognos Incentive Compensation Management 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

IBM Cognos Incentive Compensation Management Client to 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"/>

IBM Cognos Incentive Compensation Management application server to database server

You can choose different levels of security for the communication between the Cognos Incentive Compensation Management application server and the database server.
1. **Trusted Network** - Traditionally, both the Web application server and the database server are on the same trusted network and channel encryption is not used.

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

### Web client to IBM Cognos Incentive Compensation Management web application

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

1. **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.

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

### IBM Cognos Incentive Compensation Management web application to 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.

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

2. **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:

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

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

3. **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.

4. **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 with IBM Cognos Incentive Compensation Management

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 IBM Cognos Incentive Compensation Management 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.

Access the web client with SiteMinder configured

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.

Attention: 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`.
   
   **Attention:** Keep in mind that all URLs 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 setup the Keystore.

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

**Creating 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.

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**
1. Navigate to `http://<server name>/ICM`. 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
- 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, as well as the port number that is used by the LDAP server.

If the 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 web client can be configured so that it is integrated with, or accessible through external applications, such as salesforce.com.

Configuring the IBM Cognos Incentive Compensation Management web client for Salesforce

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.

Integrate the IBM Cognos Incentive Compensation Management web client with Oracle CRM

Oracle users can install an 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.

   **Attention:** Although enabling each user for web access via 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 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.

---

**Change the appearance of IBM Cognos Incentive Compensation Management to Salesforce**

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 the 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.

---

**Integrate with Microsoft's 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 IBM Cognos Incentive Compensation Management web client**

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 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** 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).
Attention: 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 files `uriworkermap.properties` and `workers.properties.minimal` and 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`
   - `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`, 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` 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.

Attention: 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 using IIS 6.0 or earlier,
   • Right-click Default Web Site (or the Web Site that should be responsible for proxying requests to Cognos Incentive Compensation Management) > Properties.
   • Click the ISAPI Filters tab.
   • 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.
   • Type tomcat as the Filter Name and type the location of the isapi_redirect.dll file for the executable.
   • Click Apply, then OK.

   If using IIS 7.0,
   • Click the Default Web Site (or the Web Site that should be responsible for proxying requests to Cognos Incentive Compensation Management) and click ISAPI Filters.
   • Click the ISAPI Filters icon.
   • 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.
   • Type tomcat as the Filter Name and type the location of the isapi_redirect.dll file.
   • 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 proxying 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.
   c. This can point to any directory.

13. Create a virtual directory for access to the isapi_redirect.dll in IIS in one of the following ways: If using IIS 6.0 or earlier,
   • Right-click Default Web Site (or the Web Site that should be responsible for proxying requests to Cognos Incentive Compensation Management) > New > Virtual Directory.
   • Set the alias to be jakarta.
   • This must point to the directory in which the isapi_redirect.dll is installed. In our example, this is C:\tomcat_iis_connector.
   • Select the Execute check box.

   If using IIS 7.0,
   • Right-click Default Web Site or the Web Site that should be responsible for proxying requests to Cognos Incentive Compensation Management and click Add Virtual Directory.
• Set the alias.

• **Physical Path** must point to the directory in which the isapi_redirect.dll is installed. In our example, this is C:\tomcat_iis_connector.

• Click the alias Virtual Directory and double-click **Handler Mappings**.

• Click **Edit Feature Permissions** in the Action panel.

• Select the **Execute** check box.

If 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 using IIS 6.0,

• Right-click **Web Service Extensions > Add a new Web Service Extension**.

• Type tomcat for the **Extension Name**.

• Add the isapi_redirect.dll file to the required files.

• Select the **Set extension status to Allowed** check box.

• Click **OK**.

If using IIS 7.0,

• Navigate to the servers and highlight your server.

• Navigate to **ISAPI and CGI Restrictions**.

• 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**.
2. Under **Security**, select **Enable Integrated Window Authentication**.
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 Firefox

If you are using 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.
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.
10. Select Automatic logon only in Intranet zone.

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:

   krb5.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
   }
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. Create a domain account for the web server in your Active Directory with the following settings:
   - Account name: "serviceaccount"
   - Select a password (such as, "secret")
   - Deactivate "User must change password at next logon"
   - 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 IBM Cognos Incentive Compensation Management 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” 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](http://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.

**application server**
A server program in a distributed network that provides the execution environment for an application program.

**attribute**
In markup languages such as SGML, 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.

**configuration file**
A file that specifies the characteristics of a program, system device, system, or network.

---

**D**

**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](#).

dparm  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.
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.

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).

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.

d 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.

Structured Query Language (SQL)  A standardized language for defining and manipulating data in a relational database.

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.

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
Active Directory 96
Admin Client 22, 75
verify installation 22
Apache Tomcat 59, 60, 61, 82, 91
collection with IIS 91
deployment 59
installation 60
API 36, 37, 40, 41, 42, 43, 46, 55
access 41
addresses 41
architecture 40
security standards
WS-I compliant 40
specifications
data management 43
data store 46
processing and calculation 42
application overview 1
application server 1
Application Server 77

C
C# 47, 53
certificate creation tool 31
certificates 31, 32, 33, 34, 36, 37, 54, 55, 56, 57
client-side setup 56
generate 31
import 33
importing certificates 34
IP address 34
Microsoft Management Console window 33
port 34
required software 31
CLI 31, 36, 37, 38, 39
certificates 37
commands 38
connect to model 38
installation 37
return code 39
Client 1, 3, 7, 8, 9, 12, 15, 23, 25, 36, 77, 89, 90
appearance 90
configuration with LDAP 24
configuration with Oracle CRM 89
e-mail 15
install 7
installation 7
LDAP configuration 25
preinstallation configuration 25
preparation for installation 1
Client tools 27
install 27
CLR 25

command-line interface 31, 37, 39
Configuration File Encrypter 28
Configuration File Encrypter tool 28
installation 28
Configuration File Encrypter Tool 28
configuration files 8, 10, 87
IBM Cognos ICM Windows Service.exe.config file 8
IBM Cognos ICM.exe.config file 8
Console Service 27
configuration 27
installation 27
ConsoleService.exe.config file 27

D
Data Tier Performance Optimization 25
database 3, 5, 10, 17, 18, 60, 62, 65, 68
access multiple databases 10
backup 17, 18
database owner 5
database server 77, 78
restore 17, 18
database server 1, 78
definitions
exception definitions 53

e-mail 14, 15, 72
encryption 71
Enterprise Size Optimization 30
environment 8
External Tools 14

G
generate 32

glossary 103

H
hosts file 55
HTTP 12, 78
HTTP Configuration Utility 31, 56
HTTPS 12

I
IBM Cognos ICM API Service 37
IBM Cognos ICM Client.exe.config file 8
IBM Cognos ICM Console Service.exe.config file
ecommon 28
IBM Cognos ICM Service 37
IBM Cognos ICM Windows Service 8
IBM Cognos ICM Windows Service.exe.config 14, 24, 37
mail settings 14
IBM Cognos ICM Windows Service.exe.config file 8, 9, 10, 21, 36
encryption 28

© Copyright IBM Corp. 2005, 2014

109
IBM Cognos ICM.exe.config file  8
ICM Cognos ICM Windows Service.exe.config file  16
ICM Cognos ICM.exe.config file  16
IDP  81
IIS  91
IIS web server  90
inquiry  72
installation files  2
IP address  34
IWA  94, 95, 96
    Firefox  95
    Google Chrome  95
    Internet Explorer  94
    Kerberos configuration file  95

J
JBoss  62, 63, 64
    installation  62
    multi-language  64
    unicode data support  64
JDBC  78

K
Kerberos  8, 95
Keystore  81

L
LDAP  23, 24, 25, 77, 84, 85
    access to Client  25
    configuration  84, 85
    groups  25
    integration with Client  23
    LDAP directory  78
    ldap.properties file  84
    user rules  23
    users  25
    validation requirements  84

M
Microsoft Excel Add-in  54, 55, 56, 57
    client-side setup  57
    install  54
    installation  57
    required software  56
    service-side setup  54
Microsoft Management Console  33, 34, 54
Microsoft SQL Server  3, 4, 5, 10, 17, 29, 30
    database  4
        permission requirements  3
        database backup  17
        database restoration  17
        model conversion  29, 30
        SQL 2005 Standard Edition  30
        SQL 2008 Enterprise Edition  30
        SQL Enterprise Edition  29, 30
        SQL Server 2005  29
        SQL Server 2008  29
        SQL Standard Edition  29, 30
model  22
Model Converter  29, 30
    Enterprise Size Optimization  30

Model Converter (continued)
    installation  29
Model Upgrader  16, 18, 19, 20
    error protection  19
    installation  19
    target database version  20
multi-language  61
multi-language support  71
multiple instances  9

N
Native  78
non-Unicode  10

O
object definitions  47
Office Primary Interop Assemblies Tool  57
Office Primary Interop Assemblies tools  56
Open SSO  77
OpenSSO  80, 81, 82, 83
    Apache Tomcat configuration  82
    configuration  80, 81, 82
    identity provider  81
    install  80
    Keystone setup  81
    service provider  83
Oracle CRM  88, 89

P
port  35
Portal Access  14, 15, 73, 74, 75
    configure email settings  14
    email settings  15
    web tab groups  75
    web tabs  74, 75
Presenter  73

S
Salesforce  87, 90
Salesforce.com  75, 87
    Web Client access  87
SAML  81, 82
SAML 2  78, 80
Scheduler  14
security  77
SFDC  87
single sign on  78, 94
SiteMinder  77, 79
    Web Client access  79
Solaris Operating System  59
SSL  14, 78
SSL encryption  78
star schema  54

T
TCP  12
TLS Security  77
Unicode 10
Unicode data support 61, 71
uninstall 16
upgrade 16, 18, 20
model 18

Web Client (continued)
  service provider configuration 82
  theme 75, 90
  web tabs 73
  WebSphere 8 deployment 68
  WebSphere deployment 64, 65, 66, 67, 68, 69
Web Server 77
  web tab group 75
  web tabs 73, 74, 75
WebSphere 64, 65, 66, 67, 68, 69
deployment 64, 67
  multi-language 67
  Unicode data support 67
WebSphere 8 67, 68
  configure 67
Windows Domain 77
Windows service 7
  installation 7
Windows Service 7, 8, 9, 11, 12, 14, 21, 36
  API configuration 55
  configuration 9
    Anonymous Model Creation 12
    API settings 11, 36
database server settings 11
enable SSL for emails 14
  External Tools 14
  Language 12
  mobile settings 14
Saved Image File Directory 12
Saved Import File Directory 12
Saved Publisher File Directory 12
Scheduler 12
  Task Manager 12
environment configuration 8
install 7
  multiple instances 20
  multiple services 21

WAR file 60, 63, 64, 68, 91
web application 78
Web Client 59, 60, 62, 63, 64, 65, 68, 70, 71, 73, 74, 77, 78, 79, 82, 84, 87, 88, 90, 91, 94, 96
  Apache Tomcat deployment 59, 60, 61
  appearance 73, 90
  configuration 59
    password encryption 71
  configuration with IIS 91
  configuration with SiteMinder 79
customization 73
deployment 59
  inquiry email 72
  installation 59
  integration 87
integration with IIS 90
integration with IWA 94, 96
IWA configuration 96
JBoss deployment 62, 63, 64
jdbc.properties file 60, 65, 68
languages 71
LDAP configuration 84
log in 83
Oracle CRM configuration 89
  password encryption 70, 71
Presenter configuration 73
property file encryption 70

Web Server 77
  web tab group 75
  web tabs 73, 74, 75