IBM Opportunity Detection
Version 9 Release 1
October 25, 2013

Administrator's Guide

Note

Before using this information and the product it supports, read the information in “Notices” on page 25.

This edition applies to version 9, release 1, modification 0 of IBM Opportunity Detection (product number 5725-D16) and to all subsequent releases and modifications Opportunity Detection (product number 5725-D16) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. About IBM Opportunity Detection

IBM® Opportunity Detection enables you to look for specified customer behaviors and patterns in your customer data and respond to them. You define the transactions and patterns that Opportunity Detection looks for, and the data that is written to the database when those criteria are met.

You use Opportunity Detection components to build trigger systems in workspaces where you apply your marketing business logic to your transaction and profile data. When you run a trigger system, it processes streams of data from your transaction and profile data feeds.

Batch and real time modes

Opportunity Detection has two modes: batch and real time.

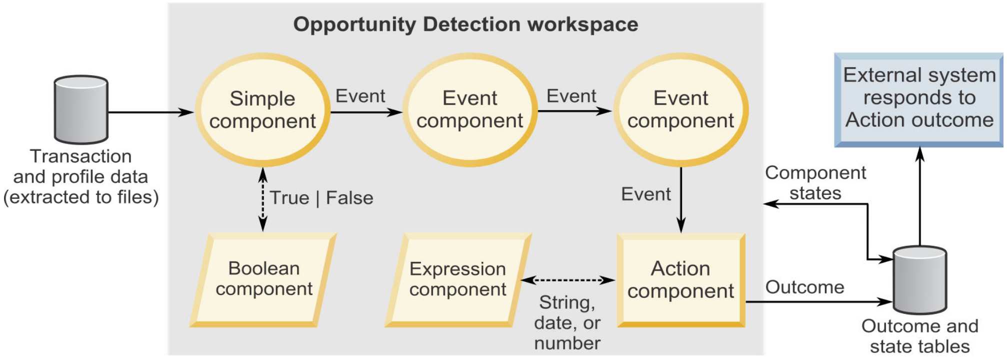
- When installed in a stand-alone configuration, Opportunity Detection processes streams of data in batches.
- When Opportunity Detection is integrated with IBM Interact, it is also possible to apply Pattern component logic to data in real time.

  To learn more about this integration, see the IBM Interact Administrator's and User's Guides.

Trigger system basics

A trigger system is comprised of configurable components. When a trigger system runs, it produces state and outcome data. State data is the saved results of processing some components; the system uses this information in subsequent runs. Outcome data can be used by external systems to respond to customer activity.

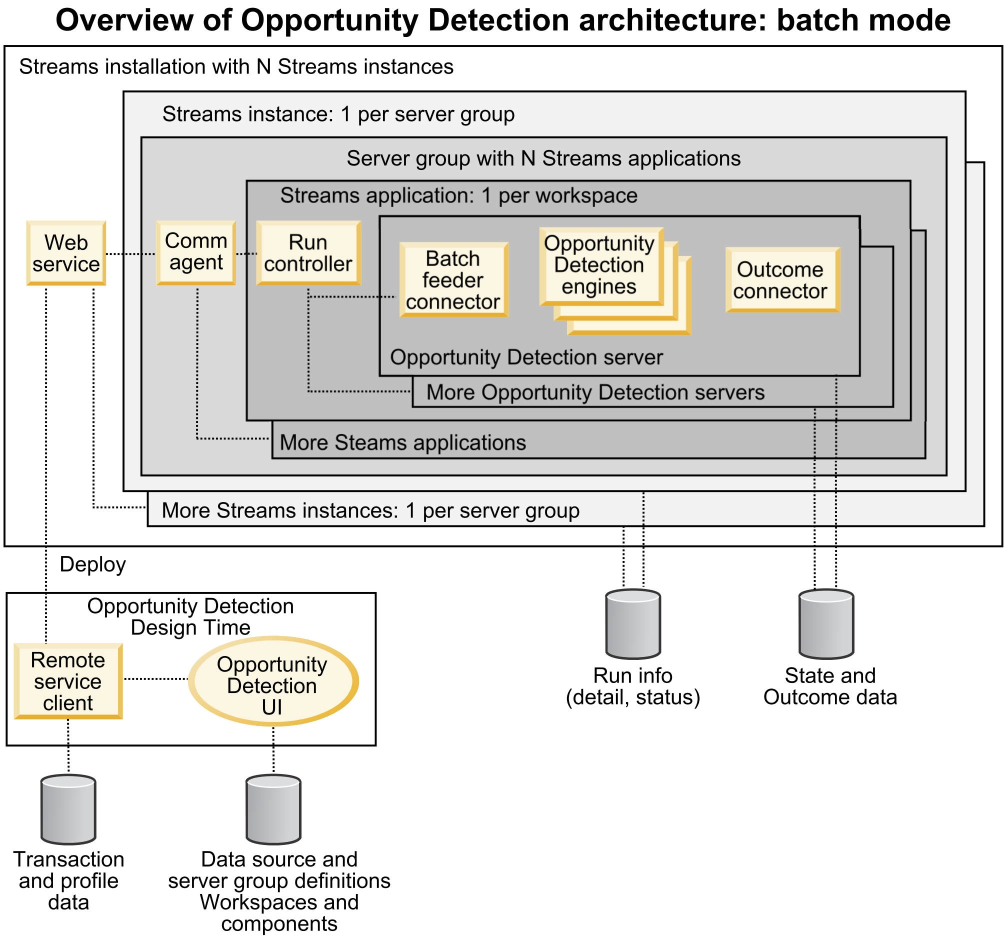
The following diagram illustrates a basic trigger system.



IBM Opportunity Detection architecture

IBM Opportunity Detection uses IBM InfoSphere Streams, a high-performance computing platform. Multiple instances of the Opportunity Detection engine can run in servers in a Streams instance. You can define multiple server groups and specity the data they can access. You can also specify which server group processes your Opportunity Detection workspace.

The following diagram provides a high-level overview of Opportunity Detection architecture for batch mode.


Overview of Opportunity Detection architecture: batch mode
Streams installation with N Streams instances
Streams instance: 1 per server group
Server group with N Streams applications
Streams application: 1 per workspace
Web service
Comm agent
Run controller
Batch feeder connector
Opportunity Detection engines
Outcome connector
Opportunity Detection server
More Opportunity Detection servers
More Steams applications
More Streams instances: 1 per server group
Deploy
Opportunity Detection Design Time
Remote service client
Opportunity Detection UI
Run info (detail, status)
State and Outcome data
Transaction and profile data
Data source and server group definitions Workspaces and components

Chapter 2. Opportunity Detection roles and permissions

The permissions assigned to users in Opportunity Detection determine what areas of the application they can access and the actions they can perform.

Reference: Permissions for Opportunity Detection

The following table describes permissions that you can assign to roles in Opportunity Detection.

All permissions that have the **Not Granted** status are treated as **Denied**.

Table 1. Permissions in Opportunity Detection

Permission	Description
View only	Access all of the user interface, in view-only mode.
Design triggers	Create workspaces and design trigger systems in batch mode. Allows the following. • Create, modify, and delete all trigger related resources. • Access Workspace, Component, Audience Level, Data Source, Named Value List pages. Can not access Server Groups and Deployment Configuration, and cannot set off a batch run.
Run for testing	• Deploy deployment configurations and run batch deployment configurations on server groups not designated for production. • Can access Server Group and Deployment Configuration pages,but can not designate a server group for production. Can not access any production related resources.
Run for production	• Deploy deployment configurations and run batch deployment configurations on any server group. • Perform all actions on the Server Groups, Deployment Configuration and Batch Run pages, including designating a server group for production.
Administer real time	Manage objects that the web service creates when Opportunity Detection is integrated with Interact to enable real time mode. Allows the following. • Delete workspaces and components created by the web service. • Start and stop real time deployment configurations and update their log level. The user with this permission alone can not start runs for real time deployment configurations. No one, even with this permission, can do any of the following. • Delete and update audience levels, data sources, named value lists, server groups, or deployment configurations created by the web service. • Create and deploy deployment configurations created by the web service.

Built-in roles in Opportunity Detection

Four built-in roles are included with Opportunity Detection.

In addition, you can create roles with permissions that you specify. See the *IBM Marketing Platform Administrator's Guide* for details on creating custom roles.

The following table shows the permissions assigned to each built-in role.

Table 2. Built-in roles in Opportunity Detection

Role	**Permissions**
OpDetectViewer	• View only
OpDetectTestDesigner	• View only • Design triggers • Run for testing
OpDetectProductionDesigner	• View only • Design triggers • Run for production
OpDetectAdmin	• View only • Design triggers • Run for testing • Run for production • Administer real time

Chapter 3. Setting up data sources in Opportunity Detection

To set up data sources for IBM Opportunity Detection, you configure them in the user interface, including setting up connections to the databases that hold run detail, component state, and outcome data. To develop data feeds, you must identify the operational systems, databases, and tables that hold the feed data you want to use, and plan to extract this data into flat files in the required format, with the required file names.

You configure Opportunity Detection to access the following feed files and databases.

Table 3. Types and formats of data used in Opportunity Detection

Type	Required format
Input data	
Transaction data about customer activities, obtained from your organization's operational system. At least one transaction data source is required to run a workspace.	Flat file
Profile data, which is information about customer attributes, rather than customer activities. Examples of profile data are age, home address, and telephone number. Optional.	Flat file
Output data	
State data needed for component processing. You can share state tables with multiple workspaces for development and test purposes, and set up one or more state tables for exclusive use by the production environment.	Database tables
Outcome data produced by trigger systems, for use by external systems. You can share outcome tables with multiple workspaces for development and test purposes, and set up one or more state tables for exclusive use by the production environment.	Database tables
Run detail data produced by the engine, containing information about workspace runs.	Database tables

Data source configuration roadmap

You configure data sources in Opportunity Detection as described in this roadmap.

You can access all of the configuration tools mentioned here by navigating to the **Settings > Opportunity Detection Settings** page.

Table 4. Data source configuration roadmap

Step	Where to find details
Configure audience codes on the Audience Levels page.	“Configuring audience level codes” on page 6
Create display names for pre-defined values in your transaction and profile data sources on the Named Value Lists page. Optional.	“Creating display names for pre-defined field values” on page 7
Identify the fields in your transaction and profile data sources and specify display names on the Data Sources page. Required.	“Defining transaction and profile data sources” on page 8

Table 4. Data source configuration roadmap (continued)

Step	Where to find details
Define database connections, data source connectors, and server groups, and map connectors to data sources on the Server Groups page. Required.	"Configuring server groups and data source connections" on page 9
Set up your transaction and profile data files, ensuring that they meet the requirements for data used in Opportunity Detection. Required.	Chapter 3, "Setting up data sources in Opportunity Detection," on page 5
Set up your state and outcome database tables. Required.	"To set up state and outcome tables" on page 16

When you have finished this process, you can build, deploy, and run trigger systems. The data configuration described above makes the data available for use when you configure components and deploy workspaces.

Configuring audience level codes

Audience codes represent the various audience levels defined in your data. You specify audience codes on the **Settings > Opportunity Detection Settings > Audience Levels** page. The audience code is always a single alphanumeric ASCII character, lower case (0-9, a-z except i). Opportunity Detection groups data sources based on the audience code associated with them.

About audience levels

An audience level is composed of a key or database table field that uniquely identifies a member of that audience level. For example, your organization could use the audience levels Household, Customer, and Account. Each of these levels represents a different view of your marketing data.

Audience levels are typically organized hierarchically. Using the examples above, you might have the following hierarchy.

- Household is at the top of the hierarchy, and each household can contain multiple customers.
- Customer is next in the hierarchy, and each customer can have multiple accounts.
- Account is at the bottom of the hierarchy.

Other, more complex examples of audience hierarchies exist in business-to-business environments, where audience levels may need to exist for businesses, companies, divisions, groups, individuals, accounts, and so on.

These audience levels may have different relationships with each other, for example one-to-one, many-to-one, or many-to-many. By defining audience levels, you allow these concepts to be represented within Opportunity Detection, so users can manage the relationships among these different audiences for targeting purposes. For example, although there might be multiple customers per household, you might want to limit contact to one customer per household.

Note: IBM Services can advise you on the audiences you need to define for your system.

How audiences are associated with data sources

When you define your data sources on the Data Sources page, you specify the fields you want to use in Opportunity Detection. When you specify an audience ID field, you associate that field with an audience.

Also, when you create data source connectors on the Server Groups page, you associate an audience level with each transaction and profile data source.

Audience codes for internal use

Opportunity Detection includes a pre-defined audience code: `n`. The `n` code is used internally by the system and is read-only. You must create additional audience codes to represent the audience levels in your data.

Also, the letter i is reserved for real time mode, and signifies the audience used for the audience level used by Interact when integration is enabled. You should not use i when configuring your audience levels for batch mode.

Creating display names for pre-defined field values

When business users work with components to build trigger systems, they select items from drop-down lists in the component editors. If a data source includes fields with pre-defined values, you can use the **Settings > Opportunity Detection Settings > Named Value Lists** page to assign display names to these values.

These display names are what the user sees when working with component editors. Display names make the component-building process more intuitive and efficient for business users.

Named value lists are reusable. For example, you might have several transaction data sources that have a Boolean field where the pre-defined values are `0` and `1`, where `1=true` and `0=false`. In this case, you can create a named value list that you associate with these fields in several transaction data sources.

Named value list example

For example, you might have a field in a data source that is named `FREQUENCY`. This field contains three pre-defined values, which have the following significance.

- `F` for customers who interact with your company frequently
- `A` for customers whose interaction frequency is average
- `I` for customers who interact with your company rarely

To help users understand what these values signify, you can map each value to a display name. You might create a named value list called Frequency and map the values as follows.

Table 5. Mapping data to display names

Value	Display name
F	Frequent customer
A	Average customer
I	Infrequent customer

After you map the values, you can associate the list with the FREQUENCY field when you define the data source. Then, when a user selects this field in a component editor, the drop-down list that contains the pre-defined values shows the display names, which are more meaningful to the user than the actual values in the data source.

Obtaining required information

As the example illustrates, you must obtain the following information about your data when you create a named value list and use it in a data source definition.

- Pre-defined values - You need these when you create the named value list.
- Name of the field in your data source that contains pre-defined values - You need this when you associate the named value list to your data source. You must associate the list with the field that contains the pre-defined values.

Creating, modifying, and deleting lists

Before you can delete a list, you must either delete all of the components that use any of its items, or edit those components to remove the reference to the list item.

Before you can delete a list item, you must either delete all of the components that use it, or edit those components to remove the reference to the list item.

The three lists that are populated by default can not be modified or deleted.

Defining transaction and profile data sources

Use the **Settings > Opportunity Detection Settings > Data Sources** page to a define each transaction and profile data source that you want to use in IBM Opportunity Detection.

When you define a data source, you do the following.

- For each transaction or profile data source, specify every field that you want to make available for use in building trigger systems.

  You must define an audience field and a date field for every transaction data source. Profile data sources require only an audience field.
- Specify display names for the data source and the fields.

See “Fields on the Data Sources page” for information on how to complete the fields on the Data Sources page.

Creating, modifying, and deleting data sources

The Data Sources page lists any components that are using the data source. If you want to edit a data source that is being used by a component, you must either delete the components that use the data source, or edit those components to remove the reference to the data source.

Fields on the Data Sources page

You define transaction and profile data sources on the Data Sources page. If you are unsure of how to complete the fields, use the information provided here.

Table 6. Fields on the Data Sources page

Field	Description
Properties	
Content Type	Select one of the following options. • **Transaction**—Customer transactions. At least one Transaction data source is required to run a workspace. • **Profile**—Data such as address, age, and gender in an external database table.
Name	Enter a descriptive name for the data source. The name does not have to match the actual flat file or database table name.
Description	Provide a description of the data source.
Add Field	
Name	Provide the physical name of the field in the source database table or flat file.
Display Name	Provide a descriptive name. This appears in component editors.
Description	Provide a description of the data source field.
App Type	Select the attribute type from the following options. The options available depend on the Content Type selected for the data source. • Audience Id–Select this for audience level fields. • Audience Level–If you select Audience Id as the App Type, select the audience level you want to associate with this field. • Profile Attribute–Choose this type for profile fields that are not audience or date fields. • Transaction Attribute–Choose this type for transaction fields that are not audience or date fields. • Transaction Date–Choose this type for date fields. One date field is required for each transaction data source.
Audience Level	If you selected Audience Id as the App Type, enter the audience level code that applies for the field.
Data Type	Select the type of the data in the field. The options available depend on the App Type selected for the field, and also on the custom data types defined on the Custom Data Types page, if any. The following are the default options. • Boolean • Date • Double • Integer • String
Name Value List	If you have created named value lists, they are displayed here. If a field contains pre-defined values, and if you have created a named value list for it, you can select the list here.

Configuring server groups and data source connections

Use the **Settings & Opportunity Detection Settings > Server Groups** page to define server groups and connect them to data sources you have configured. Server groups are comprised of servers that are set up during installation, and database connections and data source connectors that you configure.

Typically, organizations use different server groups for their development, test, and production environments. Development and test server groups often share outcome and state tables, while the production server group normally has its own, exclusive outcome and state tables.

Follow the steps in the order shown below to configure data source connections and server groups.

1. The first time you use the Server Groups page, and whenever you add a new server, click **Synchronize with changed streams configuration** on the Servers tab to refresh the list of servers.
2. On the Database Connections tab, configure a connection for every database containing run time detail tables, outcome tables, and state tables you plan to use with Opportunity Detection.
3. On the Data Source Connectors tab, configure a connector for every database table and flat file you plan to use with Opportunity Detection. This includes your transaction and profile data, and your outcome and state tables.
4. On the Server Groups tab, configure server groups as follows.
   a. Select an available Streams server and instance.
   b. Select one or more run time databases for run detail data.
   c. Map transaction and profile data sources and your outcome and state tables to data source connectors.

      Table connectors and flat file connectors enable the system to connect to your outcome and state database tables and your transaction and profile files.

      These connectors are where you specify the actual physical names of your database tables and flat files.

      For transaction and profile files, you also specify which audience level a data source is associated with, and the encoding and locale used in the file. Opportunity Detection constructs the required file name, and you must ensure that your data files use this name.

See "Fields on the Server Groups page" for help in completing the fields on the various tabs on the Server Groups page.

Fields on the Server Groups page

If you are unsure of how to complete the fields on the Server Groups page, use the information provided here.

Table 7. Server Groups page: Servers tab

Field	Description
Synchronize with changed streams configuration	Click to refresh the list of servers and stream instances.

Table 8. Server Groups page: Database Connections tab

Field	Description
Add	Click to open a panel where you can add a database connection.
Name	Enter a descriptive name for this database.
Database Type	Select a database type from the drop-down list of supported databases.

Table 8. Server Groups page: Database Connections tab (continued)

Field	**Description**
Database Name	Enter the name of the database as shown in your database management client. This must exactly match the name as shown in the client. Case-sensitive.
Server Name	Enter the fully qualified name or IP address of the machine that hosts the database server. For example, machine.mycompany.com.
Port	Enter the port on which the database listens. The default port for DB2 is 50000.
User Id	Enter the user name of the database account you want Opportunity Detection to use to access to this database.
Password, Confirm Password	Enter the password for the account you entered in the **User ID** field. **Tip:** If a database connection error occurs, verify that the password entered in these fields is correct.

Table 9. Server Groups page: Data Source Connectors tab

Field	**Description**
Add	Click to open a panel where you can select the type of connector to add. The options are Table Connector and File Connector.
Table Connector	
Name	Enter a descriptive name for this table connector. It is a good practice to align this name with the name of the data file or database you will associate with the connector.
Type	Select a type from the drop-down list. The options are State and Outcome.
Table Name	Enter the name of the table as shown in your database management client. This must exactly match the name as shown in the client. Case-sensitive.
Description	Enter a description of the table.
Sharable	Select this checkbox if you want to be able to use this table connector on different server groups. For example, you might want to have one connector for outcome and state tables that is not shared and can be used only by the deployment configuration used for production. You might also want table connectors for outcome and state tables that are shared by all test workspaces. Table connectors that are not sharable can be mapped only on the Deployment & Batch Run tab of a workspace.
File Connector	
Name	Enter a descriptive name for the file connector.

Table 9. Server Groups page: Data Source Connectors tab (continued)

Field	Description
File Name	Click the link in this field to open a pop-up window, and complete the following fields. • Name - Enter the base file name for this flat file. Permitted characters are ASCII letters, numbers, and underscore. Do not use spaces or any other special characters • Audience Level - Select from a drop-down list of available audience levels.See "Configuring audience level codes" on page 6 for details. • File name contains a time stamp - Select this box if the file name contains a time stamp (in addition to the date).
Description	Enter a description of this file.
File Encoding	Select the encoding used in the file from the drop-down list. Options are: • Chinese Traditional (Big 5) • Unicode (Little endian) • Unicode (Big endian) • Western European (ISO) • Central European (ISO) • Latin 3 (ISO) • Latin 9 (ISO) • Korean (EUC) • Chinese (GB 18030) • Unicode (UTF-7) • Unicode (UTF-8)
Date Locale	Select from a drop-down list of supported locales. Options are: • English (United States) • Chinese (China) • English (United Kingdom) • French • German • Italian • Japanese (Japan) • Korean • Portuguese (Brazil) • Russian • Spanish • Thai
Currency	Select from a drop-down list of supported locales. Options are the same as for **Date Locale**.

Table 10. Server Groups page: Server Groups tab

Field	Description
Add	Click to open a panel where you can define a server group.
Properties tab	
Name	Enter a descriptive name for the server group.

Table 10. Server Groups page: Server Groups tab (continued)

Field	Description
Stream Instance	Select a stream instance ID. See your administrator if you are not sure which one to select.
Usage	Enter a brief description of how this server group is used. For example, Production or Development.
For Production	Select this checkbox if you want to restrict user's ability to run workspaces on this server, based on their permissions.
Servers tab	
Fully Qualified Name	Double-click in the **# of Engines** column to set the number of Opportunity Detection engines to run on this machine.
Database tab	
Select Runtime database connection	The run time database holds the tables where your run, run details, and run status data is stored. Select the run time database that you want this server group to be able to access.
Select database connections for table connector mapping	The database connections you check here are the ones that are available when you map a table data source to a connector in the Table Data Source Connector Mapping window.
Data Source Mapping tab	
List of datasources	Click the name of a data source to open a pop-up window where you can map the data source to a connector. Only sharable table connectors are available for mapping in the server group page. A connector can be mapped to only one data source.
Data Source Mapping tab: Table data source connector mapping	
Data Source name	This is a read-only field that contains the name of the data source you clicked to open this window.
Connector	Select from a list of previously configured connectors.
Database connection	Select from a list of previously configured database connections.
Data Source Mapping tab: File data source connector mapping	
Data Source name	This is a read-only field that contains the name of the data source you clicked to open this window.
Connector	Select from a list of previously configured file data source connectors.

Naming requirements for profile and transaction files

As part of the process for setting up server groups, you configure a file connector on the Data Source Connectors tab on the Server Groups page. The system uses the name you specify to generate a file name. Ensure that the names of your transaction and profile feed files exactly match the name shown on the Data Source Connectors tab on the Server Groups page.

When you define file data source connectors for server groups, the system creates file names with with the following format, where *data_source_name* is the name you enter.

```
Detect.audience_code.data_source_name.date
```

You must use this name format for the transaction and profile feed files that correspond to the data sources that you configure in Opportunity Detection.

Permitted characters for the name you enter are ASCII letters, numbers, and underscore. Do not use spaces or any other special characters

Date and time_stamp portions of the name

The *date* and *time_stamp* portions of the file name must have this format: `YYYYMMDDhhmmss`

Names of flat files must contain a date. The time stamp (`hhmmss`) is optional, but this provides additional control.

The date and time stamp determine the order in which the files are processed. Files with the same timestamp are processed simultaneously. If you use a profile, you must create one for each set of files with a different timestamp.

How flat files are processed

Opportunity Detection uses the *data_source_name* portion of the file name to identify multiple instances of a transaction data source.

You might have a series transaction files, all with exactly the same fields, containing batches of transactions created at different times and using different timestamps in their names. Every time you run a trigger system that uses this data, a file with a different date stamp and/or timestamp would be used.

Location and data requirements for profile and transaction files

Your profile and transaction files must be accessible from the machine on which the Opportunity Detection run time component is installed. In addition, you must follow data format requirements for your profile and transaction files.

Format requirements

Flat files must have the following format.

- One header record followed by zero or more records.
- The first field must be the audience code.
- All record lines must use the pipe (vertical line: `|`) delimiter between fields, but not before the first field in the line or after the last field in the line.
- A pair of delimiters next to one another indicates the absence of data for the field positioned between those two delimiters. If the first field of the record contains no data, then the line begins with the first delimiter, and if the last field contains no data, then the line ends with the last delimiter.
- The pipe delimiter must not be used within data fields.

Date field requirement

For transaction files only, one field must be a date field.

Audience ID field requirement

One field in all data sources must be an ID field used for an audience level, and this must be the first field in each record in the file. More information about audiences is provided in “Configuring audience level codes” on page 6.

Sort order requirement

The records in a flat file must be sorted by audience ID first, then by transaction date and time.

Additional considerations

Note the following considerations.

- Opportunity Detection cannot match fields with NULL values when performing comparisons. You must substitute either a single printable character or a character string for the NULL values if you want to use NULL as a condition in comparisons.
- Date fields must be in system-readable date format even if you want those dates to be empty (NULL). You can represent NULL dates as either very old dates or very future dates .
- The date format in date fields must match the date format that is associated with the date locale used in the file connector.

File examples

Note: The following examples are formatted with constant widths for readability. Actual transaction and profile files must not use constant widths.

Here is an example of a simple transaction file.

```
ID    |NAME    |CALLED_NUMBER|CALL_LENGTH|TRAN_DATE_TIME
001234|David   |732-123-4567 |15         |2012-02-10 09:12:33
001234|David   |732-111-5555 |48         |2012-02-10 10:11:50
002941|Jeremiah|732-777-8888 |40         |2012-02-10 11:22:44
005555|Anthony |732-333-4444 |27         |2012-02-10 03:01:02
005555|Anthony |732-32-8945  |121        |2012-02-10 10:12:30
005555|Anthony |973-597-0022 |2          |2012-02-10 19:00:21
006789|Tom     |732-111-2222 |4          |2012-02-10 06:54:01
```

Here is an example of a simple profile file.

```
ID    |AGE|ZIP
001234|25 |11111
002941|55 |22222
005555|31 |33333
006789|60 |44444
100382|18 |55555
```

Profile data

The following requirements apply to all profile data sources used in trigger systems.

- Profile data is not required. However, if profile data is not defined, all the data used in a trigger system (including any required profile data) must be included in the transaction data.
- When profile data is defined, for every customer represented in your transaction file, there must be a single record for that customer in your associated profile.

  When a transaction file is associated with a profile flat file, the system ignores transaction records without an associated profile record, and ignores profile records without an associated transaction record. In both cases, these orphan records affect processing efficiency.

To set up state and outcome tables

Follow this procedure to edit the SQL scripts provided for creating your state and outcome tables, and then run them against your database.

1. Open the SQL scripts in a text editor and edit them as described in the comments in the files.

   The scripts are located in the `database/DB2/RunTime` directory under your Opportunity Detection run time installation. Edit the following scripts.

   - OutcomeTable.sql
   - StateTable.sql

   You replace a variable with the names you want to give to the state and outcome tables in the database.
2. Run the scripts against the database you have configured to hold your state and outcome data.

Chapter 4. Automating tasks using the RemoteControlCLI utility

The Opportunity Detection command line utility, RemoteControlCLI (CLI), allows you to automate the management of deployment configurations and batch runs. You can use the CLI to perform the same actions you can perform on the Deployment & Batch Run tab of a workspace.

The RemoteControlCLI utility and sample batch or shell scripts are all located in the cli directory under your Opportunity Detection design time installation.

The following sample scripts are provided with your installation.

Table 11. Command line scripts

Script	Usage
encode	Encrypt the password that the CLI uses to connect to the design time database.
deploy	Deploy a deployment configuration.
stop	Stop the deployment of a deployment configuration.
start	Re-start the deployment of a deployment configuration.
startBatch	Start a batch run by starting a deployed deployment configuration.
stopBatch	Stop a batch run by stopping a deployed deployment configuration.

Prerequisites

The following are prerequisites for using the Opportunity Detection command line scripts.

- The computer where you run the scripts must have network access to machines where the Opportunity Detection design time and run time components are installed.
- Java version 6 or higher must be installed on the machine where you run the scripts.
- You must set the JAVA_HOME system environment variable. You can do this either on the machine where you run the scripts, or by editing the scripts to set it temporarily when the scripts run.

Password security

The information the CLI uses to connect with the design time database is saved in the RemoteControlCLI.xml file, located in the cli directory. This information includes the user name and password for an account in the database.

You can encrypt the password that is stored in this file, to avoid storing the password in clear text. See “Setting up the database connection for the Opportunity Detection CLI” on page 18 for details.

Setting up the database connection for the Opportunity Detection CLI

You edit the RemoteControlCLI.xml file to enable the CLI to connect with the Opportunity Detection design time database.

1. Open the RemoteControlCLI.xml file, located in the cli directory under your Opportunity Detection design time installation.
2. Obtain the following information about your design time database.
   - The name of the database used with your design time installation.
   - The user name and password for an account with Administrator privileges in the design time database.
   - The URL of your design time installation
   - The URL and class name for the database driver used with your design time database.
3. Run the encode script to encrypt the password for the database account. Copy the resulting string and use it as the value for the ConnectionPassword key in the RemoteControlCLI.xml file.

   This step is optional, but provides optimal security. If you do not encrypt the password, it is stored in clear text in the RemoteControlCLI.xml file.

   If you use an encrypted password, set the ConnectionPasswordEncrypted value to True.
4. Use the database information you obtained in step 2 to complete the values in the rest of the keys in the RemoteControlCLI.xml file.
5. Save and close the RemoteControlCLI.xml file.

You can now run the CLI commands.

RemoteControlCLI XML reference

The values you enter in the RemoteControlCLI.xml file enable the CLI to connect with your Opportunity Detection design time database.

Table 12. Reference for CLI XML keys

XML key	Value
RemoteControlURL	The URL for your Opportunity Detection design time installation. Example: `http://example.com:8080/axis2/services/RemoteControl`
ConnectionDriverName	The class name of the database driver used with your Opportunity Detection design time installation. Example: `com.ibm.db2.jcc.DB2Driver`
ConnectionURL	The URL of the driver used with your Opportunity Detection design time installation. Example: `jdbc:db2://example.com:50000/Detect91:retrieveMessagesFromServerOnGetMessage=true;`
ConnectionUserName	The user name of an account in the Opportunity Detection design time database. Example: `example_user_name`
ConnectionPassword	The password of the same account used for the ConnectionUserName. Example: `example_password`

Table 12. Reference for CLI XML keys (continued)

XML key	Value
ConnectionPasswordEncrypted	A flag that indicates whether the password value used for ConnectionPassword has been encrypted using the `encode script`. If you use an encoded password, set this value to `True`.
Schema	The name of the Opportunity Detection design time database. Example: `http://example.com:8080/axis2/services/RemoteControl`

RemoteControlCLI command reference

Syntax

```
RemoteControlCLI deploy -d deployment configuration ID -v version number
```

```
RemoteControlCLI start -d deployment configuration ID -v version number
```

```
RemoteControlCLI stop -d deployment configuration ID -v version number
```

```
RemoteControlCLI startBatch -d deployment configuration ID -v deployment
configuration version number -w workspace ID -fp path to feed files
[-am Off|EndOfDay|EndOfRun ]
[-ll Off|Trace|Debug]
[-n notification file name]
[-r] [-ri] ID of the batch run to recover
```

```
RemoteControlCLI stopBatch -d deployment configuration ID -v version number
```

You can obtain the help for this utility by entering `-h` by itself or with any of the above commands.

How to specify the deployment version number

You can obtain the version number and ID of the deployment configuration on the Deployment & Batch Run tab of the workspace. Look under the Version and Message columns on the History tab of the Details panel for the deployment configuration. When you run the command, increment the deployment configuration version by 1.

For example, if the deployment version is currently `n`, you would specify a deployment configuration version number of `n+1`.

Command and option details

`RemoteControlCLI deploy -d` *`deployment configuration ID`* `-v` *`deployment configuration version number`*

Deploy a deployment configuration to the Streams server. For a first time deployment, you must use the Deployment & Batch Run tab of the workspace. You can perform subsequent deployments using the CLI.

`RemoteControlCLI start -d` *`deployment configuration ID`* `-v` *`deployment configuration version number`*

Start a deployment configuration.

RemoteControlCLI stop -d *deployment configuration ID* -v *version number*

Stop a deployment configuration.

RemoteControlCLI startBatch -d *deployment configuration ID* -v *deployment configuration version number* -w *workspace ID* -fp *path to feed files*

Start a batch run.

The non-required options for this command allow you to set the same parameters that are available on the Deployment & Batch Run tab, as follows.

- `-am` *Off|EndOfDay|EndOfRun*

  Set the artificial transaction mode
- `-ll` *Off|Trace|Debug*

  Set the logging level for all Streams components
- `-n` *notification file name*

  Set the file used to send notifications about run success or failure
- `-r`

  Run in recovery mode (requires `-ri`)
- `-ri` *ID of batch run*

  Set the ID of the batch run to recover (used with `-r`)

See the *IBM Opportunity Detection User's Guide* for details on these batch run parameters.

RemoteControlCLI stopBatch -d *deployment configuration ID* -v *version number*

Stop a batch run.

Appendix. Opportunity Detection configuration properties

This section describes the Opportunity Detection configuration properties on the Configuration page.

Opportunity Detection

currencyLocale

Description

The locale that governs the way currency is displayed and stored in Opportunity Detection.

Default value

`en_US`

supportedLocales

Description

A list of the locales supported for data storage in this version of Opportunity Detection. Changes to this value have no effect and are not recommended.

Default value

`de,en,fr,ja,es,ko,pt,it,zh`

defaultLocale

Description

The assumed locale for all Opportunity Detection users. Changes to this value are not recommended.

Default value

`[default-locale]`

Opportunity Detection | Navigation

welcomePageURI

Description

The Uniform Resource Identifier of the IBM Opportunity Detection index page. This value is used internally by IBM EMM applications. Changes to this value are not recommended.

Default value

`/index.jsp`

seedName

Description

Used internally by IBM EMM applications. Changes to this value are not recommended.

Default value

`Detect`

type

Description

Used internally by IBM EMM applications. Changes to this value are not recommended.

Default value

`Detect`

httpPort

Description

The port number that is used by the application server for connections to the Opportunity Detection application.

Default value

`7001`

httpsPort

Description

The port number that is used by the application server for secure connections to the Opportunity Detection application.

Default value

`7001`

serverURL

Description

The URL of the Opportunity Detection installation. Accepts either the HTTP or HTTPS protocol. You must use the domain and the machine name (rather than the IP address) when IBM EMM products are installed on more than one machine.

Important: If IBM EMM products are installed in a distributed environment, you must use the machine name rather than an IP address in the navigation URL for all of the applications in the suite.

Default value

[server-url]

logoutURL

Description

Used internally. Changes to this value are not recommended.

IBM Marketing Platform uses this value to call the logout handler of each registered application if the user clicks the logout link in IBM EMM.

serverURLInternal

Description

Used internally. Changes to this value are not recommended.

displayName

Description

Used internally. Changes to this value are not recommended.

Default value

```
Opportunity Detection
```

Opportunity Detection | System | Streams Remote Control Web Service

ServerURL

Description

The URL for the IBM InfoSphere Streams remote control web service. For example, `http://`*`IP_address:port`*`/axis2/services/RemoteControl`.

Default value

```
http://[SRCSHost]:[SRCSPort]/axis2/services/RemoteControl
```

Opportunity Detection | System | Interact Design Service

ServerURL

Description

The URL for the Interact web service. For example, `http://`*`IP_address:port`*`/axis2/services/InteractDesignService`.

Default value

```
http://[InteractServiceHost]:[InteractServicePort]/axis2/services/
InteractDesignService
```

Opportunity Detection | System | Interact Connector

ServerURL

Description

The URL for the Interact web service. For example, `http://`*`IP_address:port`*`/servlets/StreamServlet`.

Default value

```
http://[InteractConnectorHost]:[InteractConnectorPort]/servlets/
StreamServlet
```

Opportunity Detection | logging

log4jConfig

Description

The location of the configuration file that Opportunity Detection uses for logging. If you change this path, you must restart the web application server to apply the change.

Default value

```
[absolute-path]/conf/detect_log4j.properties
```

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information about 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.

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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites 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 Corporation
170 Tracer Lane
Waltham, MA 02451
U.S.A.

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.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

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.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

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.

Privacy Policy and Terms of Use Considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. A cookie is a piece of data that a web site can send to your browser, which may then be stored on your computer as a tag that identifies your computer. In many cases, no personal information is collected by these cookies. If a Software Offering you are using enables you to collect personal information through cookies and similar technologies, we inform you about the specifics below.

Depending upon the configurations deployed, this Software Offering may use session and persistent cookies that collect each user's user name, and other personal information for purposes of session management, enhanced user usability, or other usage tracking or functional purposes. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

Various jurisdictions regulate the collection of personal information through cookies and similar technologies. If the configurations deployed for this Software Offering provide you as customer the ability to collect personal information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for providing notice and consent where appropriate.

IBM requires that Clients (1) provide a clear and conspicuous link to Customer's website terms of use (e.g. privacy policy) which includes a link to IBM's and Client's data collection and use practices, (2) notify that cookies and clear gifs/web beacons are being placed on the visitor's computer by IBM on the Client's behalf along with an explanation of the purpose of such technology, and (3) to the extent required by law, obtain consent from website visitors prior to the placement of cookies and clear gifs/web beacons placed by Client or IBM on Client's behalf on website visitor's devices

For more information about the use of various technologies, including cookies, for these purposes, See IBM's Online Privacy Statement at: http://www.ibm.com/privacy/details/us/en section entitled "Cookies, Web Beacons and Other Technologies."

Printed in USA