Boldon James
A QINETIQ company

Classifier Reporting Starter Guide

UM643801

October 2019

Gold Microsoft Partner

Customer Documentation

Contents

1 INTRODUCTION

This document is intended to help prepare a Classifier Reporting Database for a demonstration or an evaluation. It explains how to use the **DataCreator** program to create sample windows events and how to load the events into the database. It also identifies a SQL script that processes the data in the database and identifies a set of dashboards and reports that could be used to demonstrate the sample data.

2 CREATING SAMPLE EVENT DATA

Classifier Reporting Services should be installed as described in the Classifier Reporting Services Guide section called **Installing Classifier Reporting Services**. The Classifier Reporting Services contains a program called the **DataCreator** that generates sample windows events that can be loaded into the Classifier Reporting database. The **DataCreator** does not create all the event data that can be generated by Classifier products but is useful for evaluation purposes.

2.1 Configuring DataCreator

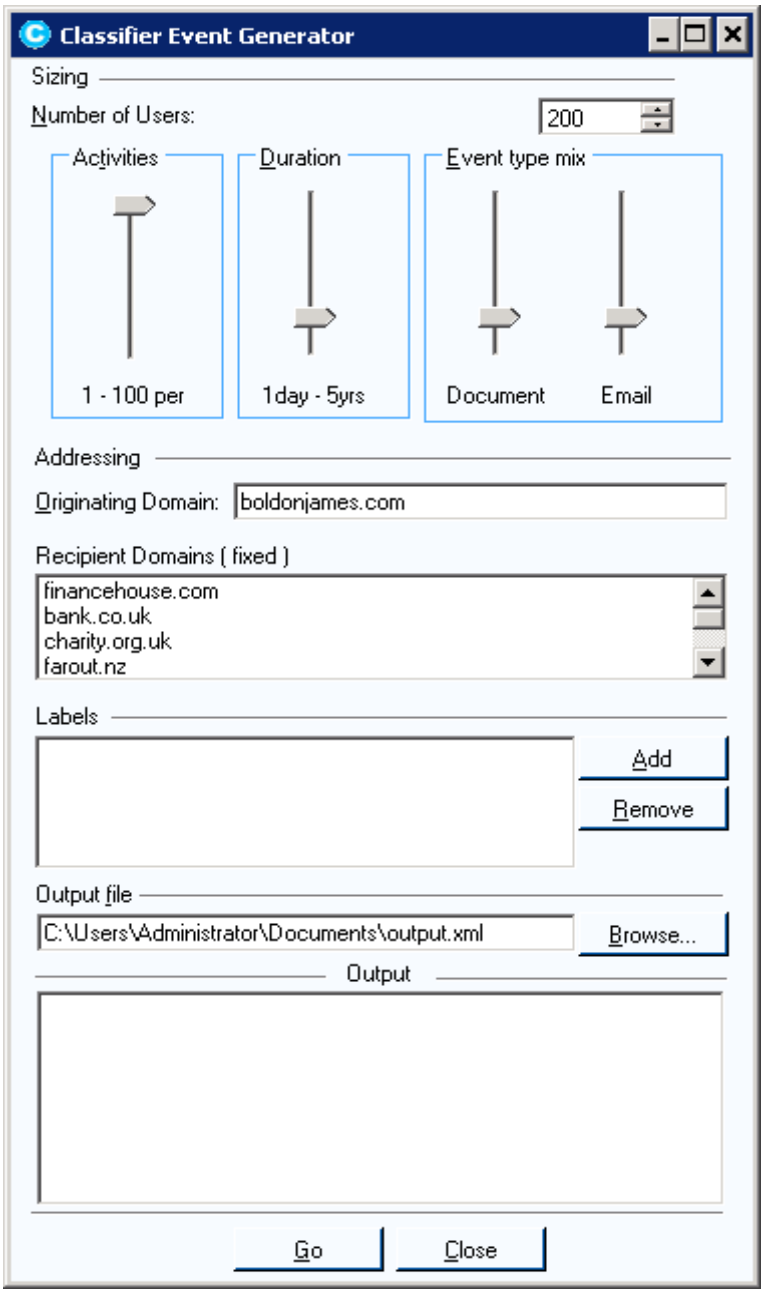
1. The **DataCreator** program must have access to a published Classifier Configuration so that it can access definitions of labels and policies needed to parse event labels into individual selector values. Parsing labels into individual selector values enable users of the **Classifier Reporting Console** to drill-down into labels on dashboards.
2. The label marking format used for event labels is defined in the Classifier configuration by the Custom format for 'Classifier Auditing' setting – see Classifier Administration Guide > General Settings for more details. To improve the parsing of individual selector values, the marking prefix and suffix of selector elements in the marking format, should not be a space character.
3. Classifier configurations can be published to either a local file store or to an Active Directory. The **DataCreator** program uses the same mechanisms as other Classifier components to access the configuration as defined by registry keys that must be established before it is run.
4. You must supply registry key values for LabelConfiguration, Policy, ServerFileSystemRoot (if using a fileshare) and ServerRootType. You must provide a policy name from your Classifier configuration for the Policy key value. You may use any Classifier policy name from your configuration.
5. The Boldon James tracing tool (BJTRACE) can be used to diagnose configuration problems. In particular tracing the following common Classifier libraries may be useful.
    - ConfigHelper
    - UIDefinitions
    - BJLabellerLabelFormats
    - RulesEngine
    - BJSettingsEngine
    - BJLabberLabel
    - BJPreDefinedLabels
    - BJLabellerControlLib
    - ConfigManager
    - BJLabellerSpif

Note: The DataCreator does not support Service Mode Registry Settings.

2.2 Running DataCreator

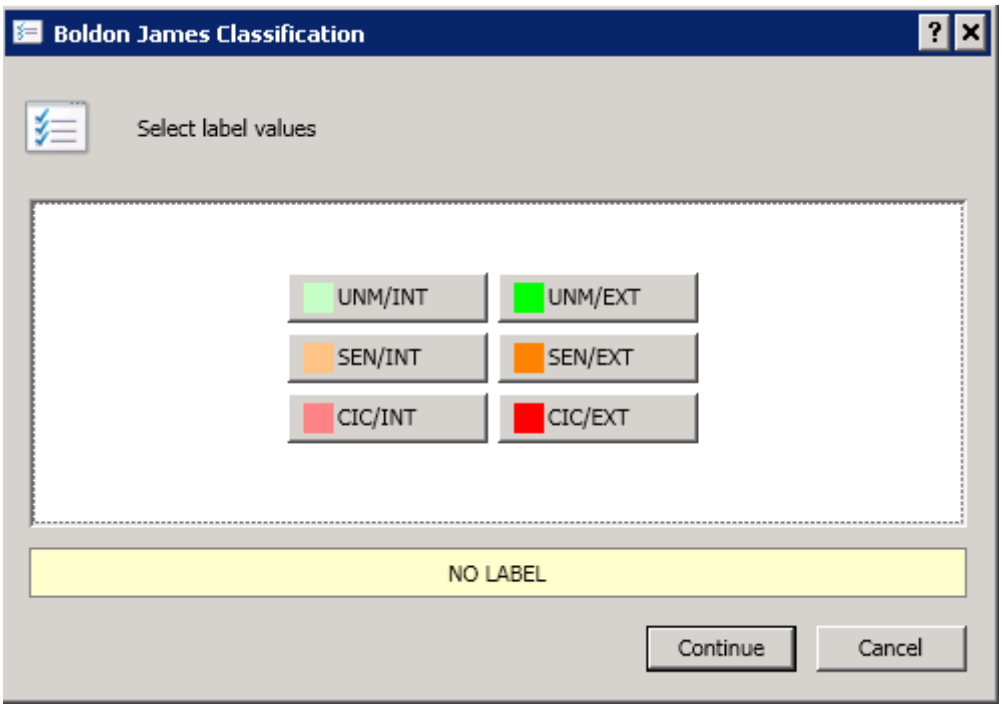
1. **DataCreator** is installed into the installation directory (typically **C:\Programs Files (x86)\Boldon James\Classifier Reporting Services)**. It creates a XML file called **output.xml** containing sample windows events that can be loaded into the Classifier Reporting Database and a file called **output_manifest.xml** that provides an overview of the generated sample window events.

Note: The output_manifest.xml file should be viewed in a XML editor.



Data Creator

2. The number of sample windows events it creates is determined by the following settings
   - The **Number of Users**
   - The **Activities** or number of events in a day.
   - The **Duration** or length of the simulated period.
   - The proportion of each type of events, Document or Email. Note that Management Agent events are not supported.
3. It is possible to set the value of the domain portion of the user and computer names in the event originator fields, by defining the **Originating Domain** value.
4. The set of recipient domains of email events are defined by the values in the ***<Domains>*** in the file **Data.xml** in the installation directory (typically ***C:\Program Files (x86)\Boldon James\Classifier Reporting Services\Data.xml).***
5. To select labels to be used in the generated sample events press the **Add** button. If the **DataCreator** has been configured with access to a published Classifier Configuration, the **Boldon James Classification** selection screen will be displayed with your labelling configuration values. See the sample below.



Label Selection

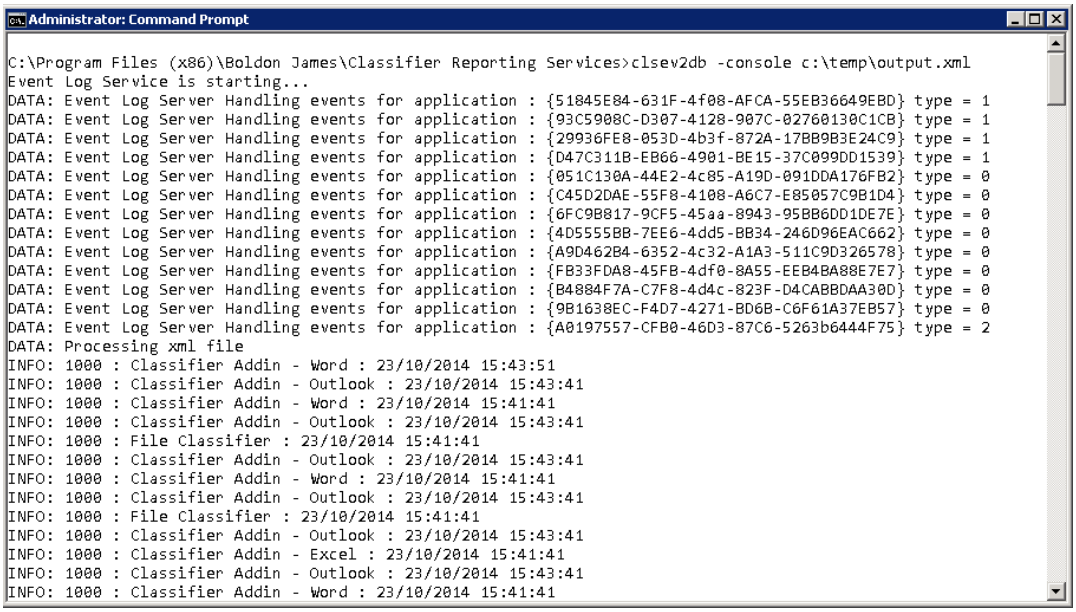
Select one or more of the labels to include in the sample events.

6. Finally configure the location of the **Output file** and press the **Go** button to generate the sample events.

3 LOADING SAMPLE EVENT DATA

The sample event data created by **DataCreator** can be loaded into the Database by the following steps.

1. In a Command prompt window, navigate to the installation folder, typically ***C:\Program Files (x86)\Boldon James\Classifier Reporting Services***
2. Type **clsev2db.exe -console C:\Users\<username>\Documents\output.xml** (or the location of the generated sample event file) and press return



Running clsev2db.exe from the command line

Note: This may take some time. When you see the text "Events: NNNN" you can exit the service by pressing Ctrl-C

3.1 Loading Sample User Data

To accompany this data, a script called **InsertSampleData.sql** is included in the release. This SQL script file loads sample users and computers data into the Classifier Reporting Database and calls the stored procedures to process the sample event data into a form that can be displayed by the **Classifier Reporting Console**. To do this perform the following step.

1. In **SQL Server Management Studio**, load the file **InsertSampleData.sql** from location ***C:\Program Files (x86)\Boldon James\Classifier Reporting Services\SQL*** and press **Execute.**

4 USE OF THE CLASSIFIER REPORTING CONSOLE DURING EVALUATIONS

Organisations evaluating the Classifier Reporting System, either for first time use or for proof-of-concept purposes, may wish to review the following dashboards and reports in the first instance.

1. **Overview dashboard**
   Used for a quick snapshot of an organisation's classification activity. This dashboard will show you the classification values that are being used during the evaluation. If the pie charts are populated, you can be sure that the reporting infrastructure is set up appropriately.

2. **Policy distribution dashboard**
   This dashboard shows the Classifier policy usage, number of users with Classifier-enabled applications and other environment information. If you are using more than one Classifier policy, you can see which users are in which policy.

3. **Classification summary dashboard**
   This dashboard shows which users are interacting most with Classifier products, and which classification values they are using. You can filter by classification value, time range and application types.

4. **Policy checks dashboard**
   This dashboard gives a view of the top 10 users triggering each Classifier check rule. You can select a time range and application and then double click on the Classifier rule to see who triggered the check rule most often and crucially, how they responded (was the user warned, prevented, challenged or did they ignore the check rule).

5. **Client issues dashboard**
   The Client issues dashboard shows you if there are any Classifier issues at your users' endpoints. For example, you can see if the Classifier configuration is always available to users. If you are using Classifier Management Agent, this dashboard will also show you when users are running Classifier-enabled applications (e.g. Word) without Classifier enabled (e.g. Word run in Safe mode). Any entries on this dashboard will likely require further analysis.

6. **Classification issues dashboard**
   This dashboard shows classification values that are not recognised by the reporting system. This can happen frequently in an evaluation period as new values are added to the users' client configurations before the reporting system is updated with the new values. This dashboard should not report unknown values once the Classifier configuration has been consolidated.

7. **Sent emails by classification and domain report**
   Use this report to see the classification values of emails sent to SMTP domains. You can filter by classification value and/or domain name.

8. **Sent emails by classification and username report**
   This report shows the classification values that individual users are using when sending emails. You can filter by username and classification value.

9. **Email classification changes report**

Use this report to see which users are making label changes to their emails. Frequent changes may indicate misclassification or misunderstanding of the classification system.

10. **Saved documents by username and filename report**
    This report displays, for each user, which classification values they have used for saving documents. Each document name and location, and save time is also shown. You can filter by username and/or classification value.

11. **Document classification changes report**
    Use this report to see which users are making label changes to documents. Frequent changes may indicate misclassification or misunderstanding of the classification system.