



User Guide Classifier Reporting Console

May 2021



Copyright Terms and Conditions

Copyright Help/Systems LLC and its group of companies.

The content in this document is protected by the Copyright Laws of the United States of America and other countries worldwide. The unauthorized use and/or duplication of this material without express and written permission from HelpSystems is strictly prohibited. Excerpts and links may be used, provided that full and clear credit is given to HelpSystems with appropriate and specific direction to the original content. HelpSystems and its trademarks are properties of the HelpSystems group of companies. All other marks are property of their respective owners.

202105260144

Table of Contents

About this product	4
About this guide	4
Before you start	4
Installing the Reporting Console	5
Configuring and Running the Classifier Reporting Console	5
Configuring a Database Connection	6
Configuring the Console (SQL Connection Editor)	6
Configuring the Classifier Reporting Console via the registry	8
SQL Connection string	8
Dashboard and Reports Folders	8
Configuring Classifier Reporting Console via Group Policy	9
Usage	9
Console Tile Files	11
Reporting Console Dashboards and Reports	12
Dashboards	12
Reports	15
Extending the Console	22
Creating Dashboards	22
Configuring a Connection String in the Simple Report Editor	22
Extending the “drill-down” level in Dashboards	23

About this product

The Boldon James Classifier Reporting Console provides dashboards and reports that enables administrators and managers to see how Classifier components are being used in their organisations.

About this guide

This document describes how to install and operate the Classifier Reporting Console.

Before you start

Ensure you have access to a working Classifier Events Database with entries in the Working Tables before installing this product.

Installing the Reporting Console

When you install the Reporting Console, you can choose to install the Dashboard Editor and Report Editor now or later.

1. Double-click **Classifier Reporting Console.exe**.
2. Click **Next**.
3. Read and accept the license agreement.
4. If you do not want to install the Dashboard Editor or Reporting Editor now, click **Next**, then click **Install**.

NOTE:

If you want to install the Dashboard Editor and Reporting Editor now, select the drop-down arrow next to Classifier Reporting Console, and select **Entire feature will be installed on local hard drive**. If you want to install them one at a time, select the individual editor, and select **Will be installed on local hard drive**.

1. Run Classifier Reporting Console.exe.
2. Click Next, then click Modify.
3. If you want to install the Dashboard Editor and Reporting Editor now, select the drop-down arrow next to Classifier Reporting Console, and select **Entire feature will be installed on local hard drive**. If you want to install them one at a time, select the individual editor, and select Will be installed on local hard drive.
4. Click **Next**, then click **Install**.
5. When the installation is complete, click **Finish**.

5. When the installation is complete, click **Finish**.

NOTE:

If you want to use the command line:

- To install the Console and the Report Editor, enter `msiexec /i "Classifier Reporting Console.msi" ADDLOCAL=REP_EDITOR`
- To install the Console and the Dashboard Editor, enter `msiexec /i "Classifier Reporting Console.msi" ADDLOCAL=DASH_EDITOR`
- To install the Console and the Dashboard Editor and Report Editor, enter `msiexec /i "Classifier Reporting Console.msi" ADDLOCAL=ALL`

Configuring and Running the Classifier Reporting Console

The Classifier Reporting Console displays dashboards and reports containing data read from the Classifier Reporting Database. The Console needs to configure a SQL Connection string to access the database.

Configuring a Database Connection

You must define a login that has access to the Classifier Reporting Database. Then grant permission to the login to read data from the database by mapping the account to the ClassifierConsumerRole or the ClassifierMaskedConsumerRole to restrict access to sensitive data.

NOTE: The database instance has to be configured for both SQL Server and Windows Authentication mode if you want to define a login using SQL Server authentication. To run the service using Windows Authentication, use a Windows domain account.

1. Open SQL Server Management Studio, right-click Security and select New > Login.
2. From the General tab, enter a Login name and either associate it to a Windows domain account or configure it to use SQL Server Authentication.
3. From the User Mapping tab, select the checkbox in the Map column next to ClassifierEventsDB.
4. In the Database role membership for: ClassifierEventsDB section, select ClassifierConsumerRole or ClassifierMaskedConsumerRole.

NOTE: Data masking is only provided if the version of SQL Server you are using supports Dynamic Data Masking (See <https://msdn.microsoft.com/en-us/library/mt130841.aspx> for more details).

Configuring the Console (SQL Connection Editor)

When the Console starts, it looks for a SQL connection string in the SqlConnectionString value in the registry. See [Configuring the Classifier Reporting Console via the registry on page 8](#) for more details. If no SQL connection string is defined in any of the registry keys, the SQL Connection Editor appears asking you to supply the connection needed to construct the SQL connection string.

To configure the SQL Connection string:

1. Open the Classifier Reporting Console.
The SQL Connection Editor opens.
2. If you want to define a custom connection string, go to step 3. Else go to step 4.
3. Select the Use the following SQL connection string checkbox. See [Defining your own SQL Connection String on page 7](#). Go to step 7.
4. Enter the Sever Name of the server hosting the Classifier Reporting database.

If the Classifier Events database has been created in a database instance other than the default instance, add the name of the instance to the server name. For example if your Classifier Reporting database is stored in an instance called Classifier, define the server name as SQLSERVER\Classifier.

If your installation of SQL Server is not listening on the default TCP port, add the port number the SQL Server is listening on to the server name. For example if your SQL Server is listening on port 1434, define the server name as SQLSERVER,1434. If your Classifier Reporting database is stored in an instance called Classifier, define the server name as SQLSERVER\Classifier,1434. Ensure firewall is open on the SQL Server.

5. Log on to the server either using Windows or SQL Server Authentication.
6. Select the database ClassifierEventsDB.
7. Click Test to ensure you can access the database.
8. Click OK.

Defining your own SQL Connection String

If the Use Custom Connection String option is selected, you change the SQL Connection string created by the SQL Connection Editor. For example, if you want to encrypt the SQL connection between the console and the database, add the required keywords to the SQL Connection string.

The SQL Connection strings created by the SQL Connection editor have the following format.

If	Then
Windows Authentication is used	<p>the format is Data Source=<Server name>; Initial Catalog=ClassifierEventsDB;Integrated Security=True</p> <p>where <Server name> is the name of the server hosting the Classifier Reporting database.</p>
SQL Server Authentication is used	<p>the format is Data Source=<Server name>; Initial Catalog=ClassifierEventsDB;Integrated Security=False, User ID=<Login Name>,Password=<Password> where:</p> <ul style="list-style-type: none"> • <Server name> is the name of the server hosting the Classifier Reporting database. • <Login Name> is the name of the SQL Login name created to access the database. • <Password> is the password of the SQL Login.

TIP: Use <https://www.connectionstrings.com/sql-server/> as a reference for SQL Connection strings and <https://docs.microsoft.com/en-us/sql/relational-databases/native-client/applications/using-connection-string-keywords-with-sql-server-native-client?view=sql-server-2017> to see a list of SQL Server SQL Connection string keywords.

NOTE: If you change the SQL Connection string you should always retain the Initial Catalog=ClassifierEventsDB component.

Configuring the Classifier Reporting Console via the registry

The application will search the registry looking for user/policy configuration values for the SQL connection string and the folders holding the dashboard and report definitions.

These searches scan the registry keys in the following order:

1. HKCU\SOFTWARE\Policies\Baldon James\Classifier Reporting Console
2. HKLM\SOFTWARE\Policies\Baldon James\Classifier Reporting Console
3. HKCU\SOFTWARE\Baldon James\Classifier Reporting Console
4. HKLM\SOFTWARE\Baldon James\Classifier Reporting Console
(Use Wow6432Node on 64bit OS e.g. HKLM\SOFTWARE\Wow6432Node\Baldon James\Classifier Reporting Console)

SQL Connection string

The registry value holding the SQL Connection string is called `SQLConnectionString` and is stored in an encrypted form. This value can only be changed by using the SQL Connection Editor.

Dashboard and Reports Folders

The installation will copy the dashboard and report definitions to the folders

“%ProgramFiles%\Baldon James\Classifier Reporting Console\Dashboards” and “%ProgramFiles%\Baldon James\Classifier Reporting Console\Report” respectively.

Also it will record these installation paths to the registry string values “DashboardPath” and “ReportPath” using the registry path: `HKLM\SOFTWARE\Baldon James\Classifier Reporting Console`.

You can overwrite this setting by configuring the “DashboardPath” and “ReportPath” values in either:

- `HKCU\SOFTWARE\Policies\Baldon James\Classifier Reporting Console`
- `HKLM\SOFTWARE\Policies\Baldon James\Classifier Reporting Console`

NOTE: As this is the installation folder, these dashboards and reports will be updated in future installations. If you modify the documents in this folder, we recommend saving them to a new filename.

Configuring Classifier Reporting Console via Group Policy

Group Policy templates are supplied to allow Administrators to remotely configure the SQL connection string, Dashboards and Reports file paths of the Classifier Reporting Console. Two templates are supplied - one for per MACHINE settings and the other for per USER settings.

The installation media (not installed) contains a sub-folder "Group Policy templates" containing two Group Policy (GP) template files and associated resource files located in a sub-folder.

The two GP template files affect different registry locations on the client PC:

Filename	Associated Registry Key Name on client PC
CRC-MACHINE Policy.admx	HKEY_LOCAL_MACHINE\Software\Policies\Boldon James\Classifier Reporting Console
CRC-USER Policy.admx	HKEY_CURRENT_USER\Software\Policies\Boldon James\Classifier Reporting Console

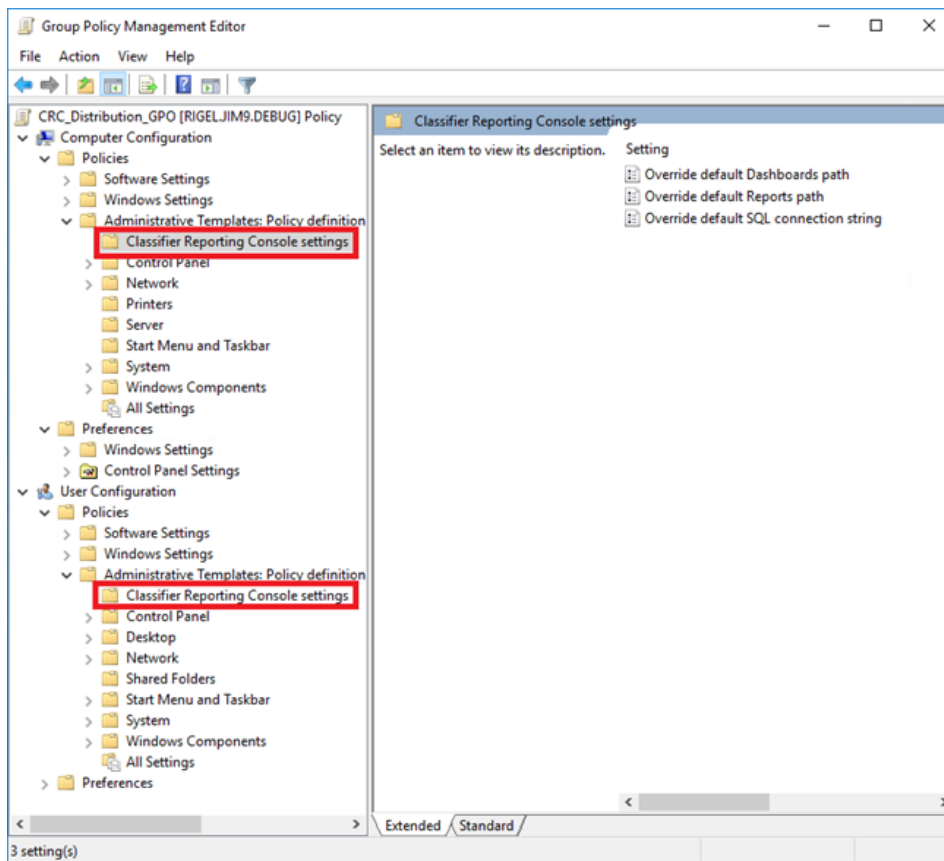
Usage

From the installation media, copy the required ADMX template files and associated ADML resource files and place in the following folders on the server:

Per MACHINE (Computer) configuration	
Installation media file	Server folder
\$. \Group Policy templates\CRC-MACHINE Policy.admx	C:\Windows\PolicyDefinitions
\$. \Group Policy templates\en-US\CRC-MACHINE Policy.adml	C:\Windows\PolicyDefinitions\en-US

Per USER configuration	
Installation media file	Server folder
\$. \Group Policy templates\CRC-USER Policy.admx	C:\Windows\PolicyDefinitions
\$. \Group Policy templates\en-US\CRC-USER Policy.adml	C:\Windows\PolicyDefinitions\en-US

When using the MS Group Policy Management Editor MMC, the Administrative Templates: Policy definition under User Configuration should appear as Classifier Reporting Console settings (same as under Computer Configuration):



Each setting can individually be enabled, disabled, or not configured (default).

When a setting is enabled, it will override the default setting that was applied during previous product installation of Classifier Reporting Console on the client PCs.

The following settings are provided:

Setting	Description
Override default Dashboards path	This setting allows you to define where the Dashboard files are read from.
Override default Reports path	This setting allows you to define where the Report files are read from.
Override default SQL connection string	This setting allows you to define the SQL connection string.

NOTE: If you supply another SQL Connection string in an un-encrypted state, you can encrypt the value using the SQL Connection editor.

After configuring a template on the server, issue the command “gpupdate /force” to update the Group Policy.

For the client PCs to immediately pickup Group Policy changes, issue the command “gpupdate /force”. You may need to log out / reboot to apply the changes.

Console Tile Files

The files “DashTiles.XML”, and “ReportTiles.xml” found in the Dashboard and Reports folders respectively control how the console load the report and dashboard files.

These files have a section for each dashboard or report file in the corresponding folder. Each dashboard or report has a corresponding “<Tile>” section in the form:

```
<Tile>
  <Title>Overview</Title>
  <Name>Overview.xml</Name>
  <ToolTipTitle>Classification activity over the last n days</ToolTipTitle>
  <ToolTip>
    A breakdown of usage:
    .
    Emails sent by classification.
    Documents saved by classification.
    All policy checks that have been triggered.
    Policy checks that have been ignored.
  </ToolTip>
  <id>l</id>
  <Icon>l</icon>
</Tile>
```

The xml elements are used as follows;

<Title>	Title of the item shown in Navigation bar (left hand panel)
<Name>	Filename of the Xml dashboard definition file
<ToolTipTitle>	Tool tip title (emboldened)
<ToolTip>	Dashboard descriptive text
<id>	Currently not used
<icon>	Associated ICON key displayed in the Navigation bar
	ICON key 0: Pie Chart 1: Pie Chart with arrow (Drill Down) 2: Bar Chart 3: Bar Chart with arrow (Drill Down) 4: Filter (funnel) Any other: Report (clip board)
<hide>	Add this element and set to true to prevent the report being displayed.

The dashboard files are loaded in the console, using the order with which they appear in this file. If they are not in the file, they will appear at the end of the list with default parameters.

Reporting Console Dashboards and Reports

This section describes the standard dashboards and reports provided by the Classifier Reporting Console. These dashboards and reports can be altered and new dashboards and reports can be added. See [Extending the Console on page 22](#).

Dashboards

Dashboards are automatically displayed by the Console for the previous 28 days when selected by a user. The user can re-display the dashboards for other pre-defined time ranges or by specifying and start and end time. The following pre-defined time ranges are supported.

Time period	Description
Last Calendar Month	Displays the activity for the previous month. For example if a dashboard was created on the 5 th of July, selecting this time period would create a dashboard for June.
Last 3 Calendar Months	Displays the activity for the previous 3 months. For example if a dashboard was created on the 5 th of July, selecting this time period would create a dashboard for April, May and June.
Last Month to Date	Displays the activity from the start of the previous month to the current date. For example if a dashboard was created on the 5 th of July, selecting this time period would create a dashboard from the start of June to the time the report is created.
Last 7 Days	Displays the activity for the previous 7 days. For example if a dashboard was created on the 5 th of July, selecting this time period would create a dashboard from 28 th June to the time the report is created.
Last 14 Days	Displays the activity for the previous 14 days. For example if a dashboard was created on the 5 th of July, selecting this time period would create a dashboard from 21 st June to the time the report is created.
Last 28 Days	Displays the activity for the previous 28 days. For example if a dashboard was created on the 5 th of July, selecting this time period would create a dashboard from 7 th June to the time the report is created.
Last 365 Days	Displays the activity for the previous 365 days. For example, if a dashboard was created on the 5 th of July, selecting this time period would create a dashboard from 5 th July in the previous year to the time the report is created.

The following dashboards are available with this release:

Dashboard	Description
Overview	<p>Shows a quick snapshot of an organisation's classification activity. As with many of the dashboards, you can amend the time period that the dashboard reports against by selecting the parameters button.</p> <ul style="list-style-type: none"> • Emails sent by classification - Quickly see what level of classification is most used within an organisation when emails are sent • Documents saved by classification - Quickly see what level of classification is most used within an organisation when a document is saved • All policy checks - an initial overview of which Classifier 'check' rules are being triggered the most • All ignored policy checks - A high level view of the policy check rules that have been ignored by users
Classification summary	Shows the classification values used in the selected time period for all sent email, saved document and file classifier label events. You can also filter for an Office Application and then drill down through the chart to see who the top 10 users of a specific classification value are.
Heatmap	Shows the total number of classification all sent email, saved document and file classifier label events. Low and high thresholds can be configured that cause the heatmap to present the total number of classification values in alternative colours.
Email classification trends	Allows a user to filter the dates to the desired period and then show the classification trends for sent emails. A trough or peak in the trend line may indicate unusual activity that requires further analysis.
Email classification changes	This dashboard shows the classification values applied to an email that resulted in a warning. If a user has tried to downgrade an email classification value where downgrades are not permitted, it would show in this chart. The report will include changes to classification values made before the email is sent.
Document classification trends	This dashboard allows a user to filter the dates to the desired period and then show the classification trends for saved documents.

Document label downgrades	This dashboard shows the number of document label downgrade events over a selected time period and the ten users who downgrade document labels the most for a selected time period.
SharePoint classifications	This dashboard presents documents that have been uploaded to SharePoint for selected classification values. The name and location of the document, as well as the upload time, are displayed.
File classifier labelled documents	Shows documents that have been labelled by the File Classifier. The classification, name and the location of the document, and the time the document was labelled, are displayed.
Policy distribution	Shows the Classifier policy usage, number of users for each Classifier policy, and other environment information. You can use this dashboard to find out which users are using which Classifier policy.
Policy check activities	Shows the Classifier rules that have been triggered by user activity. The outcome of the rule (for example, audit, warn, prevent) is displayed for each Classifier rule.
Policy checks	<p>Gives a view of the top ten users triggering each Classifier check rule. The Console user can select a time range, application and then double click on the rule to see who triggered the check rule most often and crucially, how they responded. User's responses can be:</p> <ul style="list-style-type: none"> • Warn: The user adhered to the warning. • Prevent: The check prevented the user from completing their action. • Challenge: The user responded to the challenge. • Ignore: The user ignored the warning or challenge. • Success: The rule succeed because the user was compliant. <p>A check rule's response can also be:</p> <ul style="list-style-type: none"> • Audit: A check rule failed but the rule was configured to only be audited. • Suppressed: The check rule did not happen. The can happen, for example, if the rule is triggered when dialogs are suppressed via a macro
Policy warning trends	Provides a trend line of the check rules that resulted in a user being warned or advised by the Classifier client. A trough or peak in the trend line may indicate unusual activity that requires further analysis.

Client issues	Shows any technical issues reported by Classifier clients and Classifier Management Agent: <ul style="list-style-type: none"> • Computers with Classifier issues (Management Agent) – displays various issues reported by the Management Agent such as Office clients running without Classifier • Computers with Classifier issues against time (Management Agent) displays a trend line for reported issues • Computers with Classifier issues – displays various issues reported by the Classifier clients such as invalid configuration location • Computers with Classifier issues against time – displays a trend line for reported issues
Classification issues	Used to identify classification values that are not recognised by the Reporting System. This can occur if administrators are running in test mode with test values.

Reports

All the reports, except where stated otherwise in the descriptions below, are automatically displayed by the Console.

Some reports are displayed for the previous 28 days and allow the user to select the start and end dates and re-display the report. Some reports show classifier activity for the fixed periods of the previous 7 and 30 days. Some reports provide filters to refine the results. Filters can be either be values entered by the user or can be values selected from a drop-down list. Most filters permit the use of the SQL childcare character %.

Some reports include a User Name parameter and are presented in the report as %<Username>%. These reports can contain a large amount of data and therefore ideally the report should be created for only one user. So for example entering, for example, Francis Green will show all the reports for that user. However the SQL wild card character can still be used, so entering, for example, **Francis**.

The following reports are provided in this release.

Report	Description
Classification activity summary	Shows, for a configurable time period, the number of sent, saved and printed emails at different classification levels. A similar chart is shown for saved and printed documents. The time period's initial value is 28 days.

Unclassified activity over the last 7 and 30 days	Shows the number of saved documents and sent emails that have been classified and the number of saved documents and sent emails that have not been classified in the last 7 and 30 days. If the text that indicates no label has been added to the document or email is supplied, documents and emails marked with that text are excluded from the report.
Classifier activity over the last 7 and 30 days	Shows the number of saved documents and sent emails, grouped by classification, in the last 7 and 30 days. If the text that indicates no label has been added to the document or email is supplied, documents and emails marked with that text are excluded from the report.
Documents and email by classification	<p>Shows, in a table, the total number of saved documents and sent emails, grouped by classifications, for a period starting at the user defined start date until the end of the third month after the start date. The report also shows the totals for the previous quarter. This report is not automatically displayed by the console.</p> <p>For example, if the user defines the start date as 13th March 2018, the report would show the total number of saved documents and sent emails from the 13th March 2018 until the end of May 2018 together with the totals for the previous quarter of October to December 2017.</p> <p>This report requires the Active Directory service to add details of classifier user's departments to the database.</p> <p>The report can be filtered on the user's department.</p>
Classifier checks applied by each user	<p>Shows, for a configurable time period, each classifier check applied by the user. The report shows what document or email the checks were applied to and when the checks were performed. The user must enter a User Name before the report can be created.</p> <p>The time period's initial value is 28 days.</p>

User responses to Classifier challenges	<p>Shows user's responses to classifier rule check challenges. The report shows the user's response for each classification, application and check rule and shows the title of the email or document name that the rule applied to and the date/time that the rule check occurred.</p> <p>The report can be filtered by the classification, the application, the User's name and the User's department. The report can be displayed for a configurable time period.</p> <p>This report requires the Active Directory service to add details of classifier user's departments to the database.</p> <p>The report is not automatically displayed by the console; the user must enter a User name before the report can be created.</p> <p>The time period's initial value is 28 days.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>NOTE: This report has been updated in V1.4.1 of the Console. The earlier version of the report is still released in V1.4.1 but is configured in the ReportsTile.xml file to be hidden. If you want to use the earlier version you can display it in the console by editing the ReportTile.xml file, see Console Tile Files for more details.</p> </div>
Total emails by domains	<p>Shows, in a table, the total number of emails sent, grouped by the domain of the email recipients for a period starting at the user defined start date until the end of the third month after the start date. The report also shows the totals for the previous quarter. This report is not automatically displayed by the console.</p> <p>For example if the user defines the start date as 13th March 2018, the report would show the total number of emails sent from the 13th March 2018 until the end of May 2018 together with the totals for the previous quarter of October to December 2017.</p> <p>This report requires the Active Directory service to add details of classifier user's departments to the database.</p> <p>The report can be filtered by the classification applied to the email and the user's department.</p>
Sent emails by classification and domain	<p>Shows, for a configurable time period, an overview of the emails sent ordered by classification and by domain. This report is not automatically displayed by the console. A domain has to be selected before this report can be created. The report can be filtered on the classification value and/or the SMTP domain name.</p> <p>The time period's initial value is 28 days.</p>

<p>Emails sent by user and domains</p>	<p>Shows, for a configurable time period, users and the recipient domains of the emails the users send. For each recipient domain the report can also show the details of each email's subject and time of submission, sent to recipients in each domain.</p> <p>This report requires the Active Directory service to add details of classifier user's departments to the database.</p> <p>The report can be filtered by the classification applied to the email and the user's department.</p> <p>The time period's initial value is 28 days.</p>
<p>Sent emails by classification and username</p>	<p>Shows, for a configurable time period a breakdown of emails, by classification and by user.</p> <p>The user must enter a user name before the report can be created. The report can be filtered on the classification.</p> <p>The time period's initial value is 28 days.</p>
<p>Email classification changes</p>	<p>Shows, for a configurable time period, all email label changes with the old and new labels presented. For each label change it is possible to drill down to the user who made the change, the subject line of the email, and time of the label change.</p> <p>This report is not automatically displayed by the console. A user name has to be entered before this report can be created. The report can be filtered on the classification value.</p> <p>The time period's initial value is 28 days.</p>
<p>Downgraded emails</p>	<p>Shows, for a configurable time period, users and the downgraded classifications the users applied to email. The report also shows the subject of the downgraded email, the time of the downgrade and the reason for the downgrade (if any).</p> <p>This report requires the Active Directory service to add details of classifier user's departments to the database.</p> <p>This report is not automatically displayed by the console. An original classification has to be selected before this report can be created.</p> <p>The report can be filtered by the original classification applied to the email and the user's department.</p> <p>The time period's initial value is 28 days.</p>

<p>Emails sent with unclassified attachments</p>	<p>This report presents, in a table the total number of emails sent with unlabelled attachments together with the user supplied reason for not labelling the attachment, for a period starting at the user defined start date until the end of the third month after the start date. The report also shows the totals for the previous quarter. This report is not automatically displayed by the console.</p> <p>For example if the user defines the start date as 13th March 2018, the report would show the total number of emails sent from the 13th March 2018 until the end of May 2018 together with the totals for the previous quarter of October to December 2017.</p> <p>This report requires the Active Directory service to add details of classifier user's departments to the database.</p> <p>The report can be filtered on the user's department and the message's classification.</p>
<p>Saved documents by classification and username</p>	<p>This report presents, for a configurable time period, a list of classifications and the number of documents the users saved with each classification.</p> <p>The user must enter a user name before the report can be created. The report can be filtered on the classification.</p> <p>The time period's initial value is 28 days.</p>
<p>Saved documents by username, classification and filename</p>	<p>This report presents, for a configurable time period, a list of users, classifications and the name of the documents created, with each classification and by each user. The user must enter a user name before the report can be created. The report can be filtered on the classification.</p> <p>The time period's initial value is 28 days.</p>
<p>Classifier checks applied to each document</p>	<p>This report presents, for a configurable time period, documents and each classifier check applied to the document. The report shows which users performed the checks and when the checks were performed. The user must enter a document name before the report can be created. The report can be filtered on the user's name.</p> <p>The time period's initial value is 28 days.</p>

Document classification changes	<p>This report presents, for a configurable time period, all document label changes with the old and new labels presented. For each label change it is possible to drill down to the user making the change, the name of the document, and time of the label change.</p> <p>This report is not automatically displayed by the console. A user name has to be entered before this report can be created. The report can be filtered on the classification value.</p> <p>The time period's initial value is 28 days.</p>
Downgraded documents	<p>This report is not automatically displayed by the console. An original classification has to be selected before this report can be created.</p> <p>Shows, for a configurable time period, users and the downgraded classifications the users applied to documents. The report also shows the name of the downgraded document, the time of the downgrade and the reason for the downgrade (if any).</p> <p>This report requires the Active Directory service to add details of classifier user's departments to the database.</p> <p>The report can be filtered by the original classification applied to the documents and the user's department.</p> <p>The time period's initial value is 28 days.</p>
Downgraded documents over the last 7 and 30 days	<p>This report presents the number of downgraded documents, grouped by their original classification, in the last 7 and 30 days.</p>
File Classifier labelled documents	<p>This report presents documents labelled by the File Classifier, grouped by user and classification.</p> <p>This report is not automatically displayed by the console. A user name and classification has to be entered before this report can be created. The report can be filtered on the classification value.</p> <p>The time period's initial value is 28 days.</p>
Printed documents over the last 7 and 30 days	<p>This report presents the number of printed documents, grouped by classification, in the last 7 and 30 days.</p>

Machines running classifier over the last 7 and 30 days	<p>This report presents the number of distinct machines that have had classifier running in the last 7 and 30 days.</p> <p>If the Active Directory service is configured the report can also show the number of machines that have no classifier applications running in the last 7 and 30 days.</p>
AD Service Status	<p>This report lists the activity in the Computers and Users containers in Active Directory (AD) that are processed by the AD Service on each timer poll (default every 1 minute). The activity recorded consists of AD objects (Computers and Users) that have been added or deleted.</p> <p>Start and End Date parameters can be set to filter on a date range, defaulting to the last 7 days.</p>
Event Log Service Status	<p>This report lists the Classifier Events processed or skipped by the Event Log Service on each timer poll (default every 10 seconds).</p> <p>Start and End Date parameters can be set to filter on a date range, defaulting to the last 7 days.</p>
Classifier User Deployment	<p>The reports shows the number of users who have started using classifier and the number of machines that classifier has been installed on. It also shows the date that each user started using classifier.</p>
Classifier User Diagnostic	<p>The reports shows the number of users who have had problems running classifier and the number of machines that classifier had problems being started on. It also shows, for each user who has had a problem, the most recent date that a problem occurred and the number of elapsed days since that date plus the most recent date that classifier started without any problem and the number of elapsed days since that date.</p>
Classifier Version Report	<p>This report shows what versions of Classifier are deployed in the organisation. It contains a chart showing the number of computers configured with each deployed version of Classifier and a table showing the computers configured with each version of Classifier.</p> <p>The report can be filtered by the user's computer, the user's name and the application and the time period. The time period's initial value is 28 days.</p>

Extending the Console

The Classifier Reporting Console provides the Dashboard Editor and the Report Editor for creating new dashboards and reports respectively.

Creating Dashboards

To create a dashboard:

1. Consider the elements you want to present on the dashboard.
2. Consider the SQL statement that will provide the relevant data. Use the SQL schema that is documented below.
3. Create a SQL View in the ClassifierReporting schema. See the Classifier Reporting Database Schema Guide for more information on the ClassifierReporting schema.
4. If possible, copy an existing dashboard file, located in your <install directory>/Dashboards directory.
5. Run the Dashboard Editor and then open the dashboard file created in step 4, or select New from the Home tab.
6. Amend (or create) the SQL statement using the Edit Queries button in the Data Source tab.
7. From the Home tab, select the presentational element e.g. Pie Chart, that you would like to add to the dashboard.
8. Drag the elements from the SQL view to the Data Items panel as appropriate.
9. Save the new dashboard.
10. Amend the <install directory>/Dashboards/DashTiles.xml file to include the new dashboard.

Configuring a Connection String in the Simple Report Editor

If you create a new report using the Report Wizard, you must either select a connection from a list, including a default value of LocalSqlServer, or manually enter connection details.

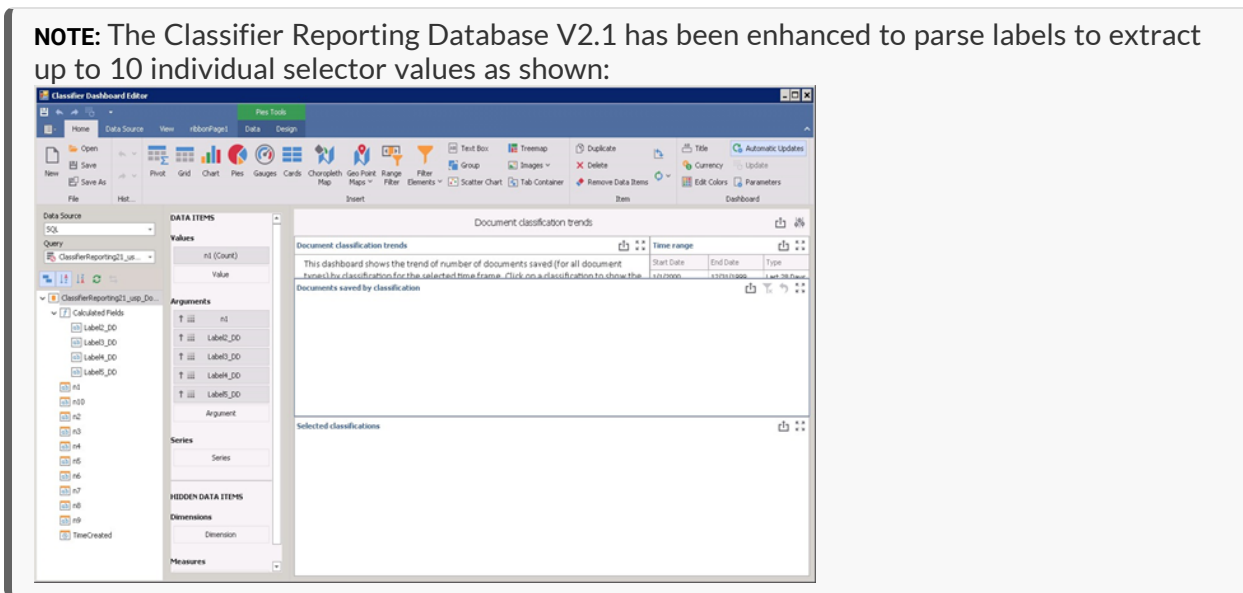
You can add another connection to the list by defining a SQL connection string by editing the SimpleDashBoardDesigner.exe.config file stored in the Classifier Reporting Console installation directory. To add another connection string, add the following between the <connectionStrings>:

```
</startup>  
  <connectionStrings>  
    <add name="BJConnection" connectionString="your connection string"/>  
  </connectionStrings>  
</configuration>
```

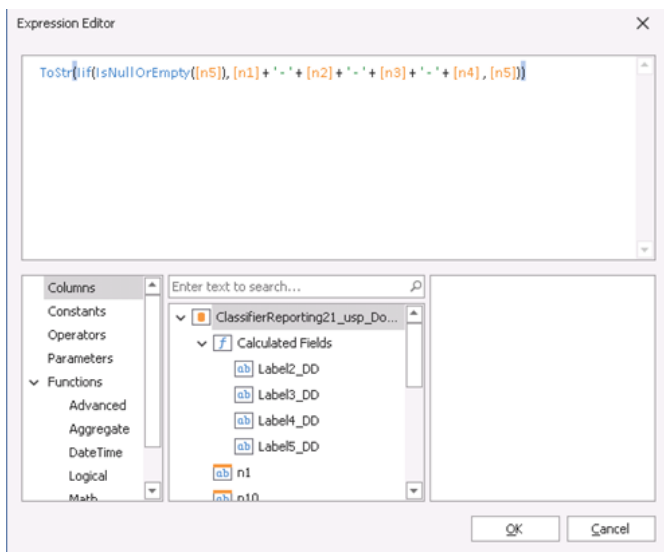
Extending the “drill-down” level in Dashboards

Dashboards provide the ability to drill-down into the individual selector values in labels. For example, if a classification had a value of CONFIDENTIAL SALES PRODUCT JANUARY, a pie or bar chart would show the value of CONFIDENTIAL. If the user clicked the chart, the next value SALES would be displayed. Clicking the SALES value will cause PRODUCT to be displayed.

NOTE: The Classifier Reporting Database V2.1 has been enhanced to parse labels to extract up to 10 individual selector values as shown:



1. Open the Classifier Dashboard Editor, and open the dashboard you wish to extend. The values n1, ..., n10 shown in the list on the left in the image above represent the parsed selector values on the label.
2. From the Data Source tab, select Add Calculated Field.



3. Name the field, for example, Label6_DD.

4. Move the newly created calculated field to the Arguments component of the DATA ITEMS panel.

