Boldon James
A QINETIQ company

Classifier Reporting Console Guide

UM642205

October 2019

Gold Microsoft Partner

Contents

1 OVERVIEW

The Boldon James **Classifier Reporting Console** V1.4.0 provides dashboards and reports that enables administrators and managers to see the way that Classifier components are being used in their organisations.

This document describes the **Classifier Reporting Console** that is part of the **Classifier Reporting System**. For more information on the Classifier Reporting System, and its components, refer to the Classifier Reporting System Guide.

2 INSTALLING AND CONFIGURING THE REPORTING CONSOLE

2.1 Installation

The Classifier Reporting Console is installed by running the 'Classifier Reporting Console.exe' executable.

There are three features in the installation:

1. The Reporting console
2. Dashboard designer
3. Report designer

Only the Reporting console will be installed by default. When running the installation from the command line, the designer features can be specified as follows:

Installs the console and the report editor

msiexec /i "Classifier Reporting Console.msi" ADDLOCAL=REP_EDITOR

Installs the console and the dashboard editor

msiexec /i "Classifier Reporting Console.msi" ADDLOCAL=DASH_EDITOR

Installs the console and the both the dashboard and report editors

msiexec /i "Classifier Reporting Console.msi" ADDLOCAL=ALL

2.2 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. This section will explain how the SQL Connection string is configured and how it is stored.

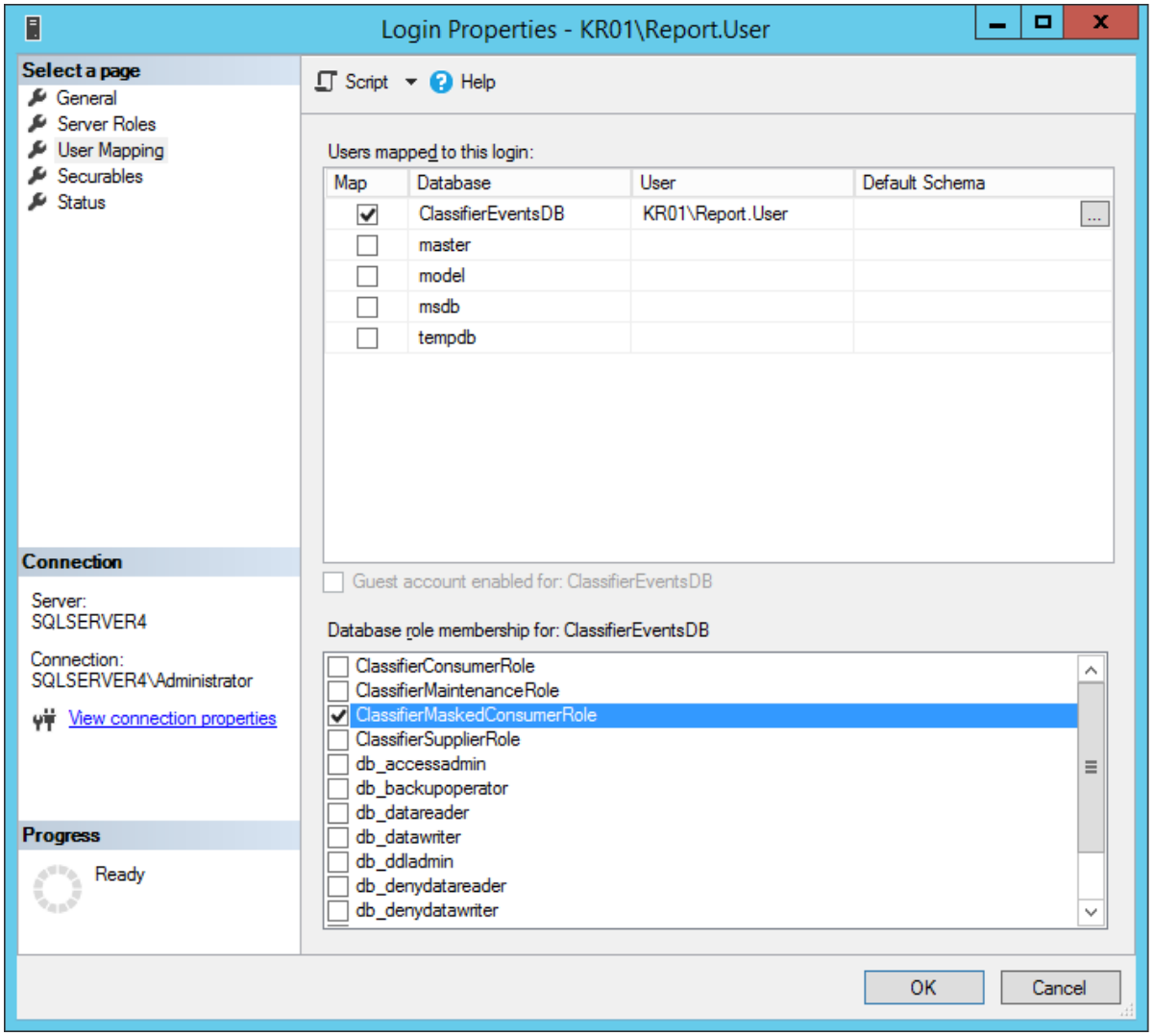
2.2.1 Configuring a Database login

The first step to configure the SQL Connection string is to define a login that has access to the Classifier Reporting Database. The login can be either based on Windows authentication or SQL Server authentication.

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.

1. If you want to use Windows authentication you will need to use a Windows domain account to run the service.

2. First, using **SQL Server Management Studio** create a Security login and either associate the login either with a Windows domain account or configure the login to use SQL Server authentication.
3. Secondly, you have to grant permissions to the login to read data from the database by mapping the account to the ***ClassifierConsumerRole*** role as shown below, map the account to the **ClassifierMaskedConsumerRole**, role as shown below, to restrict access to sensitive data.



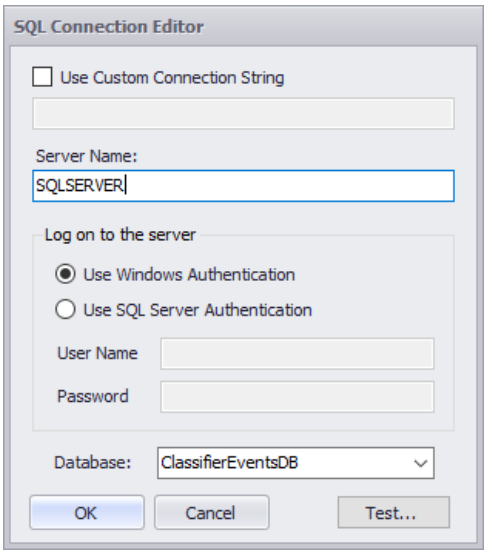
Assign role

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.

2.2.2 Configuring the Console (SQL Connection Editor)

When the Console is started it will look for a SQL connection string in the ***SQLConnectionString*** value in the registry, see the section Configuring the Classifier Reporting Console via the registry for more details. If no SQL connection string is defined in any of the registry keys, which may be the

case the first time that the Console is run, the User will be presented with the SQL Connection Editor to supply the connection needed to construct the SQL connection string.

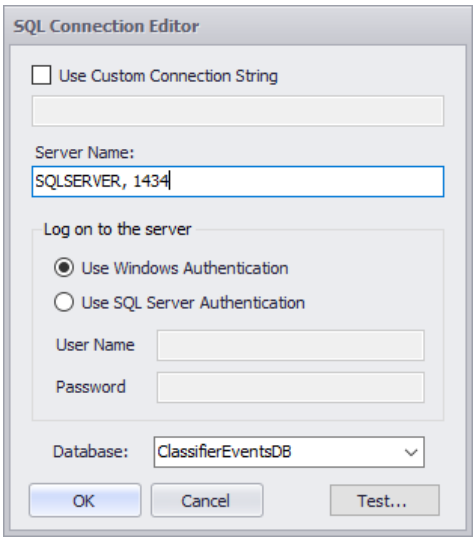


SQL Connection Editor

The fields of the SQL Connection Editor will now be explained.

- The ***Use Custom Connection String*** option allows you to define your own SQL connection string. See the section Defining your own SQL Connection String for more details on how to do this.
- ***Server Name*** is the 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 you will have to add the name of the instance to the server name, for example if your Classifier Reporting database is stored in an instance called Classifier you should define the server name as ***SQLSERVER\Classifier.***

  If your installation of SQL Server is not listening on the default TCP port you will need to add the port number SQL Server is listening on, to the server name. For example if your SQL Server is listening on port 1434 you should define the server name as ***SQLSERVER,1434***. If your Classifier Reporting database is stored in an instance called Classifier you should define the server name as ***SQLSERVER\Classifier,1434*** as shown below.



Logon to SQLSERVER\Classifier,1434

Note: You will have to open the firewall on the SQL Server to allow SQL connections. For example you will have to open port 1434 to allow access in the above example.

- ***Use Windows Authentication*** – this configures the Console to use the domain account of the user running to authenticate to the Classifier Reporting database. This account should be associated with a role as described in the Configuring a Database login section.
- ***Use SQL Server Authentication*** - this configures the Console to use the SQL Server login and credentials defined in the ***User Name*** and ***Password*** fields. This login should be associated with a role as described in the Configuring a Database login section.

  In the picture above, for example, replace the text ***–REPLACE USERNAME –*** with the SQL Server login name.
- ***Database*** is the name of Classifier Events database and should always be **ClassifierEventsDB**.
- The ***Test*** button attempts a SQL connection to the database using the provided details.
- The ***OK*** button first attempts a SQL connection to the database using the provided details and if the connection is successful, the details are saved and the SQL connection editor is closed.
- The ***Cancel*** button closes the SQL connection editor without saving any configuration details.

2.2.3 Defining your own SQL Connection String

If the ***Use Custom Connection String*** option is selected it is possible to 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 you could add the required keywords to the SQL Connection string.

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

- If Windows Authentication is being used, the format is

  Data Source=<Server name>; Initial Catalog=ClassifierEventsDB;Integrated Security=True

  Where ***<Server name>*** is the name of the server hosting the Classifier Reporting database.

- If SQL Server Authentication is being used, the format is

  Data Source=<Server name>; Initial Catalog=ClassifierEventsDB;Integrated Security=False, User ID=<Login Name>,Password=<Password>

  Where ***<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.

The website https://www.connectionstrings.com/sql-server/ is a good general reference for SQL Connection strings and the website 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 provides 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.

2.3 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 will scan the registry keys in the following order:

1. ***HKCU\SOFTWARE\Policies\Boldon James\Classifier Reporting Console***
2. ***HKLM\SOFTWARE\Policies\Boldon James\Classifier Reporting Console***
3. ***HKCU\SOFTWARE\Boldon James\Classifier Reporting Console***
4. ***HKLM\SOFTWARE\Boldon James\Classifier Reporting Console***

(Use Wow6432Node on 64bit OS e.g. ***HKLM\SOFTWARE\WoW6432Node\Boldon James\Classifier Reporting Console***)

2.3.1 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.

2.3.2 Dashboard and Reports Folders

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

"%ProgramFiles%\Boldon James\Classifier Reporting Console\Dashboards",

And

"%ProgramFiles%\Boldon James\Classifier Reporting Console\Report" Respectively.

In addition, it will record these installation paths to the registry string values “DashboadPath” and “ReportPath” using the registry path.

HKLM\SOFTWARE\Boldon James\Classifier Reporting Console

This setting may be overridden by setting the “DashboadPath” and “ReportPath” values in either

HKCU\SOFTWARE\Policies\Boldon James\Classifier Reporting Console

Or

HKLM\SOFTWARE\Policies\Boldon 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.

2.4 Configuring Classifier Reporting Console via Group Policy

2.4.1 Introduction

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, 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 further 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

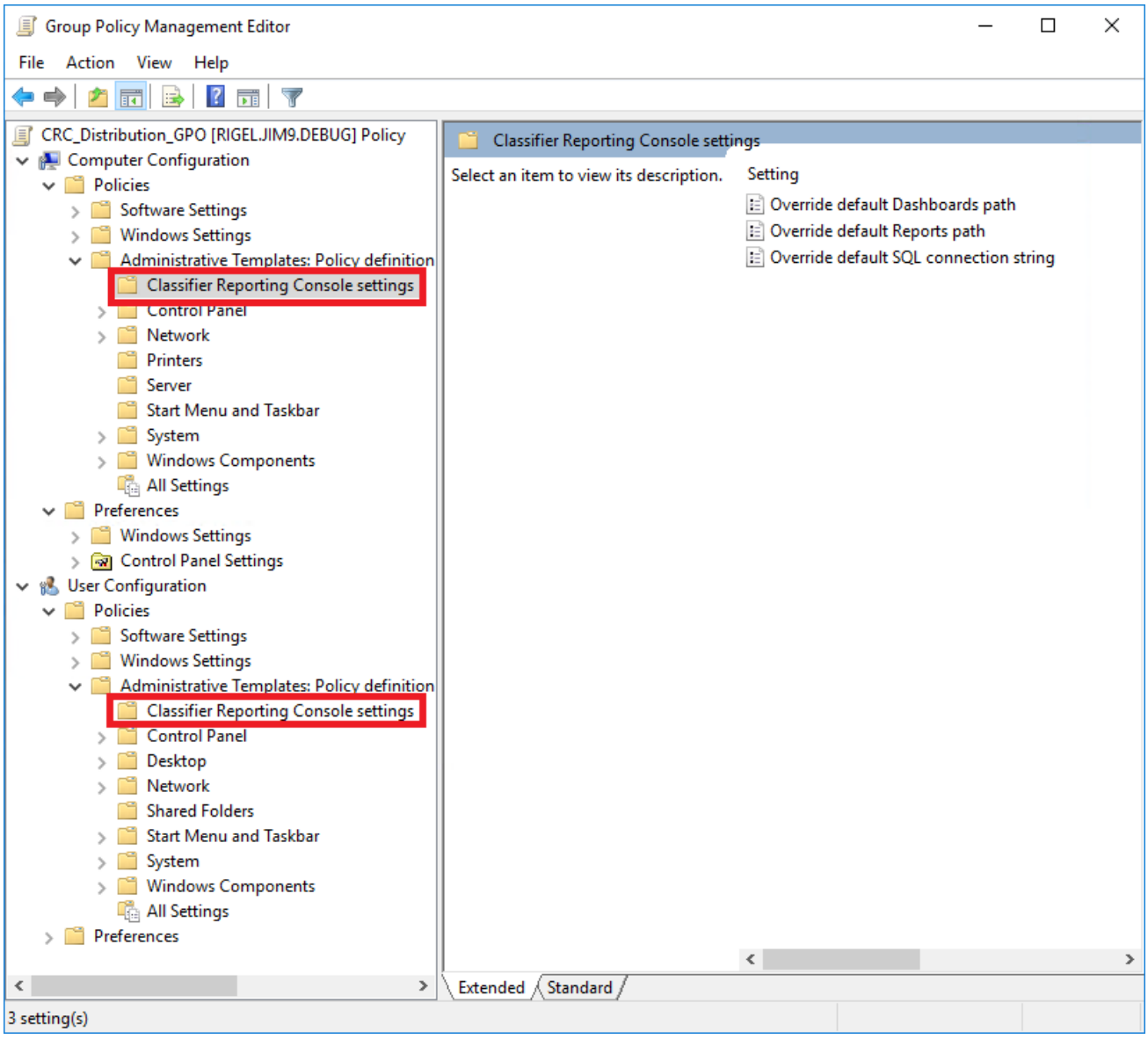
2.4.2 Usage

From the installation media, copy the required ADMX template file(s) and associated ADML resource file(s) 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 template(s) should appear labelled as “Classifier Reporting Console settings” under the “Administratrive Templates: Policy definition” sections of the Computer or Users Configuration, depending upon the copied templates:



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 PC(s).

Three 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.

Similarly on the client PC(s) to immediately pickup Group Policy changes issue the command "`gpupdate /force`". A log out / reboot might be necessary to apply the changes.

2.5 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 which has 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>1</id>
    <icon>1</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.

3 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. This is discussed in the section Extending the Classifier Reporting Console.

3.1 Dashboards

Dashboards are automatically displayed by the Console for a time range of 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 5th of July, selecting this time period would create a dashboard for June.
Last 3 Calendar Months	Displays the activity for the previous 3 month, for example if a dashboard was created on the 5th 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 5th 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 5th of July, selecting this time period would create a dashboard from 28th 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 5th of July, selecting this time period would create a dashboard from 21st 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 5th of July, selecting this time period would create a dashboard from 7th 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 5th of July, selecting this time period would create a dashboard from 5th July in the previous year to the time the report is created..

The following dashboards are available with this release:

Dashboard	Description
Overview	Presents 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. • **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	This dashboard presents 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	This dashboard 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	This dashboard presents 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	This dashboard shows the Classifier policy usage, number of users for each Classifier policy and other enviroment 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 (e.g. audit, warn, prevent etc.) is displayed for each Classifier rule.

Dashboard	Description
Policy checks	This dashboard 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 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).
Policy warning trends	This dashboard 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	Used to show any technical issues reported by Classifier clients and Classifier Management Agent: • 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.

3.2 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 wildcard 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 %** will data for users with the first name **Francis**.

When a report's parameters are selected, the report is displayed by invoking the **Submit** button. The **Reset** button can be used to undo any parameter changes.

The following reports are provided by this release.

Report	Description
Classification activity summary	This report presents, 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	This report presents 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	This report presents 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	This report presents 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. 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. This report requires the Active Directory service to add details of classifier users to the database. The report can be filtered on the user's department.
Classifier checks applied by each user	This report presents, 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. The time period's initial value is 28 days.
User responses to Classifier challenges	This report presents, for a configurable time period, users and their responses to classifier check challenges. The user must enter a User Name before the report can be created. The time period's initial value is 28 days.
Total emails by domains	This report presents, 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. 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. This report requires the Active Directory service to add details of classifier users to the database. The report can be filtered by the classification applied to the email and the user's department.

Report	Description
Sent emails by classification and domain	This report presents, 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. The time period's initial value is 28 days.
Emails sent by user and domains	This report presents, 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. This report requires the Active Directory service to add details of classifier users to the database. The report can be filtered by the classification applied to the email and the user's department. The time period's initial value is 28 days.
Sent emails by classification and username	This report presents, for a configurable time period a breakdown of emails, by classification and by user. The user must enter a user name before the report can be created. The report can be filtered on the classification. The time period's initial value is 28 days.
Email classification changes	This report presents, 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. 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. The time period's initial value is 28 days.
Downgraded emails	This reports presents, 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). This report requires the Active Directory service to add details of classifier users to the database. This report is not automatically displayed by the console. An original classification has to be selected before this report can be created. The report can be filtered by the original classification applied to the email and the user's department. The time period's initial value is 28 days.
Emails sent with unclassified attachments	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

Report	Description
	after the start date. The report also shows the totals for the previous quarter. This report is not automatically displayed by the console. 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. This report requires the Active Directory service to add details of classifier users to the database. The report can be filtered on the user's department and the message's classification.
Saved documents by classification and username	This report presents, for a configurable time period, a list of classifications and the number of documents the users saved with each classification. The user must enter a user name before the report can be created. The report can be filtered on the classification. The time period's initial value is 28 days.
Saved documents by username, classification and filename	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. The time period's initial value is 28 days.
Classifier checks applied to each document	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. The time period's initial value is 28 days.
Document classification changes	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. 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. The time period's initial value is 28 days.
Downgraded documents	This report is not automatically displayed by the console. An original classification has to be selected before this report can be created. This reports presents, 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). This report requires the Active Directory service to add details of classifier users to the database. The report can be filtered by the original classification applied to the documents and the user's department.

Report	Description
	The time period's initial value is 28 days.
Downgraded documents over the last 7 and 30 days	This report presents the number of downgraded documents, grouped by their original classification, in the last 7 and 30 days.
File Classifier labelled documents	This report presents documents labelled by the File Classifier, grouped by user and classification. 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. The time period's initial value is 28 days.
Printed documents over the last 7 and 30 days	This report presents the number of printed documents, grouped by classification, in the last 7 and 30 days.
Machines running classifier over the last 7 and 30 days	This report presents the number of distinct machines that have had classifier running in the last 7 and 30 days. 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.
AD Service Status	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. Start and End Date parameters can be set to filter on a date range, defaulting to the last 7 days.
Event Log Service Status	This report lists the Classifier Events *processed* or *skipped* by the Event Log Service on each timer poll (default every 10 seconds). Start and End Date parameters can be set to filter on a date range, defaulting to the last 7 days.
Classifier User Deployment	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.
Classifier User Diagnostic	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.

3.3 Reports from earlier versions of the Console

Version 1.3 of the Classifier Reporting Console contains a set of new reports and the visual presentation of reports included in previous versions of the console, have also been changed. The changes include branding, colours and the use of images. Reports from earlier versions of console

are still included but not displayed by the V1.3 Console. The console can be configured to display these reports by setting the <hide> XML element to false or by removing the element.

4 EXTENDING THE CLASSIFIER REPORTING CONSOLE

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

4.1 Creating New Dashboards

Follow these steps to create a new dashboard:

1. Consider the presentational elements you want 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. Refer to the CreateViews.sql file (see Section 4.1.2) for guidance on setting up new Views.
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.

The Classifier Reporting Database schema is described in the document Classifier Reporting Database Schema (UM6434).