boldonjames
by HelpSystems

User Guide
Classifier Reporting Server

June 2021

Copyright Terms and Conditions

202106140903

Table of Contents

Classifier Reporting Server

The Classifier Reporting Server (CRS) is a web-based application providing a centralised reporting and dashboarding solution. It enables organisations to provide their end users with the ability to access, design, and manage dashboards and reports effectively and monitor the data classification activities enforced by the Classifier suite of products.

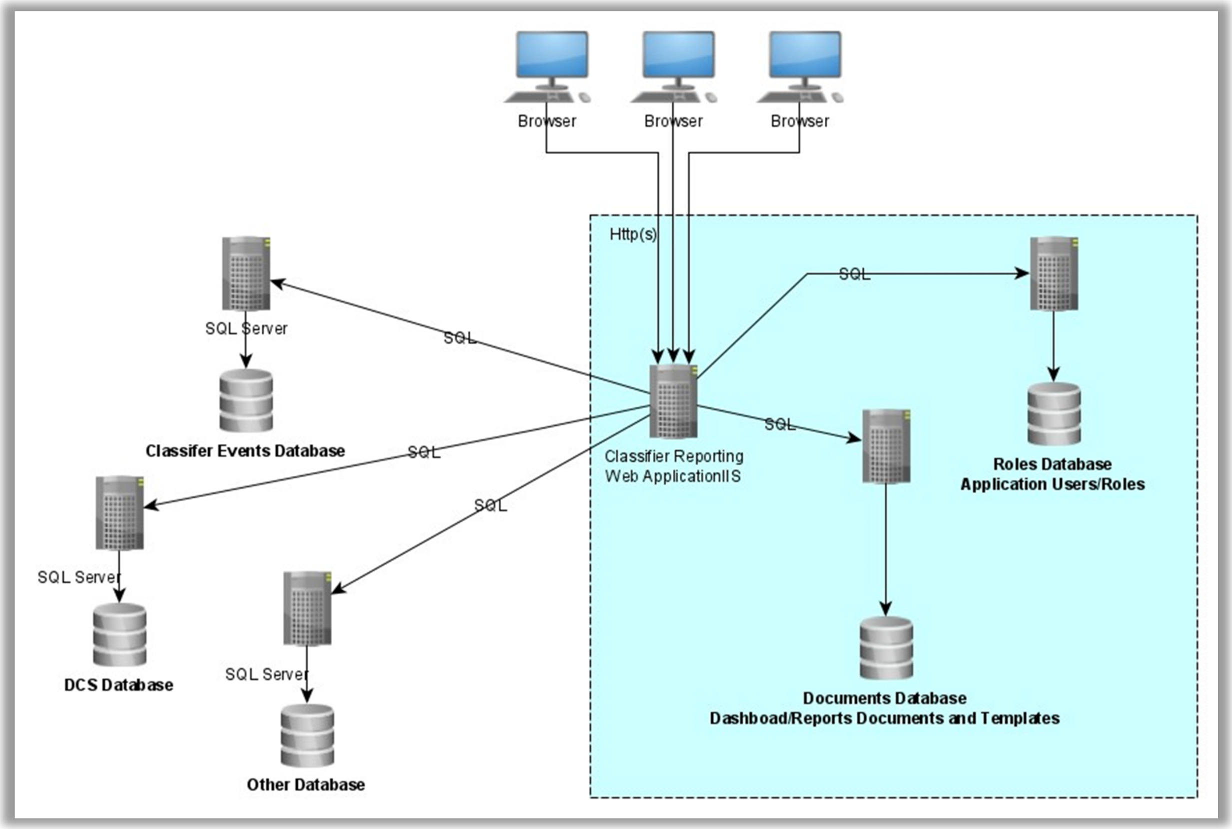
Reporting Server will be deployed by enterprise customers in place of the current Classifier Reporting Console. In conjunction with an access control system it will alleviate the concern of providing end users direct access to SQL server farms.

CRS components

Classifier Reporting Services (CRS) is comprised of:

- a Windows Service that converts Windows Event log entries into SQL tables
- Reporting Server Web Service - an IIS-hosted web service that provides web-based reporting and dashboarding with granular data access control but enforcing a single-entry point to databases.
- SQL databases - Reporting Server requires two internal databases “Reports and Dashboard Storage” and “User Role Storage”. Any number of databases providing data can then be referenced from within the application.

The following diagram shows the architecture of the Reporting Server Web Service and SQL databases:



Reporting Server Users

The following users must be identified when deploying the Reporting Server:

User	Description
SQL Database Administrator	The SQL Database Administrator must have permission to create the Reporting Server databases on the specified SQL server however this level of access is temporary. Post-installation actions are required for creating the Reporting Server databases, once these initial configuration stages are complete, the SQL Database administrator credentials are no longer required.
Reporting Server Database User	Reporting Server requires read and write access to the two internal databases created by the SQL Database Administrator. These can be the same or unique users and are configured after installation.
Reporting Server Installer	The Reporting Server Installer is the user that installs the Reporting Server software onto the web server. This user requires permissions to install the product into the local file system and create websites within IIS.

User	Description
Reporting Server Administrator	During installation, the installer delegates a Reporting Server Administrator to run Reporting Server. They will require access to the websites file system folder for reading and writing files from the application. This user will be automatically added to the Reporting Server system with System Manager Role.

Installing and Configuring the Reporting Server

Prerequisites

Requirement	Description
Operating System	• Windows Server 2016 • Windows Server 2019 • Reporting Server must be installed on a machine that is a member of an Active Directory Domain.
SQL server	• SQL Server 2016 • SQL Server 2019
Software	• .NET Framework 4.7.2 or higher. • .Net Core 3.1 Desktop Runtime (v3.1.x) • ASP.NET Core 3.1 Runtime (v3.1.x) - Windows Hosting Bundle **NOTE:** This must be installed after IIS is installed and its features enabled. Ensure the following Web Server (IIS) Roles (under Windows Server Roles) are enabled for the Reporting Server: • IIS Management Console • .NET Extensibility 4.6 • HTTP Errors • ISAPI Extensions • ISAPI Filters • Logging Tools • Request Filtering • Windows Authentication A fully trusted server authentication certificate to use for SSL bindings to the web site is required. This certificate must be trusted on any machine from where the Reporting Server is accessed.

To enable all the pre-requisites for your platform, use the following command in an elevated command prompt/PowerShell session:

```
dism.exe /online /enable-feature /all /featurename:NetFx4

/featurename:IIS-NetFxExtensibility45

/featurename:IIS-WebServerManagementTools

/featurename:IIS-ISAPIExtensions /featurename:IIS-ISAPIFilter

/featurename:IIS-RequestFiltering /featurename:IIS-HttpErrors

/featurename:IIS-LoggingLibraries

/featurename:IIS-WindowsAuthentication

/featurename:IIS-ManagementScriptingTools
```

Installing the Reporting Server

During the installation, a Reporting Server Administrator will be required to act as the account the server should run as within IIS.

The Reporting Server installation package does not open ports in the Windows Firewall for the web service. If users on the local network access the web service, then ensure the required ports are open.

1. Run the Classifier Reporting Server.msi.
2. Read and accept the end-user licence agreement.
3. Choose an installation folder to put your files.
4. Choose an available TCP Port number.
5. Choose a fully trusted certificate to be used by Reporting Server. You can either choose an existing certificate from your certificate store or create a self-signed certificate.
6. Enter the user credentials for the Reporting Server Administrator. In a production environment, consider using a different account than the one needed to install the software; the service account requires fewer permissions.
7. Click **Verify** to confirm the user account exists and the password provided is correct.
8. Click **Next**, then click **Install.**
9. Restart the computer to ensure all pre-requisite and relevant components are fully re-loaded.

Creating and initializing the Reporting Server databases

The Reporting Server requires the following databases:

- the Roles Database for the user and role information
- the Document Database for dashboards and report storage

Use the PrepareDatabase application (installed with the Reporting Server) to create these databases, and to create and secure the connections to these databases.

1. From the Start menu, locate and right-click **PrepareDatabase** and select **Run as Administrator**.
2. In the **Roles Database** tab, enter the name of the SQL Server.
3. Change the name of the database if necessary, but Boldon James recommends leaving the default name.
4. Click **Ensure database Exists** to check if the database exists. If not, then one is created. Once the database has been created, the required schema is applied.

   Select **Use Current User Credentials** and enter the credentials of the user running the application, or specify a SQL account. Close the dialog.
5. Click **Configure Connection** to specify how the service will connect to the database. If the service is to use Windows Authentication (trusted connection), then select the **Use the Service's Windows Account**. If SQL authentication is to be used, then supply the credentials. Click **Set Connection** and close the dialog.

   > **NOTE:** The account credentials specified must have read and write access to the database.

6. Select the **Document Database** tab and repeat steps 1 -5.

   As these connections may contain SQL account details, they are stored as encrypted strings. The Permissions tab shows which accounts have access to the connection storage. This group will, by default, include the user who runs this application and the service account. Users can be added and removed from the list, but it must always contain the service account. Once the connections have been set, only these users will have access to read or modify these settings.
7. Click **Start Web Site**.

Opening the UI

Documents

When you open the Reporting Server UI, the Home page opens to show the currently logged in user and any recently opened documents. Depending on your access to the document, you may see different items in the navigation menu.

Access	Description
Reader	Users with access to one or more documents can access the “Dashboards” and “Reports” buttons on the Navigation menu. You can filter the main view through Tags applied to the documents. Users can select one or more tags from the drop-down panel to filter the contents. Each document is represented by a box which contains the documents title and description as a quick reference. Clicking this box will navigate to the document in read-only mode. Additionally, each document box contains a small “…” icon which allows you to navigate to a specific page specific in this document.
Author	Document Authors have the same access as readers, but they can also create new documents from scratch or to use pre-installed templates (if configured). Using the “…” icon, authors can edit the title and description and add or remove “Tags”. Click an action menu to access the documents designer, to make changes, to apply permissions applied, and to delete the document from the application. **NOTE:** If a document requires access control, this must be applied after the document has been created. By default no access control is applied.
Designer	The Document Designer is the tool used by Authors to create and modify the rendering of the dashboards and reports. For further information, contact Boldon James support.

Document Contents

Content	Description
Templates	Document templates provide pre-defined dashboards and reports that can be used by document authors. They must be enabled before being accessible. See *Intelligence Packs* for more information. Once enabled, templates are found when a user is a member of “Document Author Role”. Clicking the “From Template” action button on the main document panel will display a list of available templates grouped by the parent pack and version. Selecting a template allows you to create a page where the name and description of the template can be changed. It’s critical that the connections are correctly configured. Failure to choose the correct connection may result in the dashboard or report failing to render correctly. Multiple copies of the same template can be created, but we strongly suggest re-naming and adding an appropriate description for users to easily identify its purpose.
Tags	Document tags are words or phrases that can be associated with a given document. By using the same tag on multiple documents, they can then be grouped and filtered by users. Only Document Authors are able to add and remove tags; readers will only see tags which appear in documents they have access to; however, we strongly recommend not using sensitive information within tags.
Permissions	Document permissions can only be changed by document owners or users within author roles. Permissions are accessed from the “...” page of a document and then selecting the Permissions buttons from the Action menu. You can select another user to be the owner of the document. There’s a list of all roles available allowing role-based access to this document. Selecting the “Read” checkbox will give users of that role the ability to see and open the document. Selecting the “Update” will give members the ability to modify the document. An “Owner” setting is available under the “Permissions” page of a document. This allows a user to be given update permissions on the document outside of their role membership. There can be only one document owner and by default the owner will be the original author of the document.

Creating a Document from a Template

Documents can be created by members of the “Document Author Role”, “System Document Manager Role”, or “System Manager Role”. They can be created from scratch using the designer or imported from a template pre-installed from an intelligence pack. Documents created from templates can be modified using the designer as a user with the appropriate permissions.

1. Log onto Reporting Server with a member of “Document Author Role” or equivalent
2. Click **Dashboards**, and choose **From Template**.
3. Click the template you wish to create.
4. Select the connection that is to be used by this template from the list provided under the “Template Connection <…>”.
5. Click **Save**.

Changing Permissions on a Document

The ability to control who has visibility of a document is done through the enabling and disabling of roles on a document.

1. Log onto Reporting Server with a member of “Document Author Role” or equivalent
2. Click **Dashboards**.
3. Click the “…” icon.
4. Click **Action** menu and choose **Permissions**.
5. Select the **Read** checkbox alongside the appropriate role and click **Save.**

Roles

Reporting Server is a role-based access-controlled application. Roles are applied to documents and access to the document is then driven by adding and removing users or groups to roles. Role configuration is only available to users within the “System Role Manager Role” or “System Manager Role”. They can access the configuration page through an additional “Roles” button on the navigation bar. This will not be visible to users who do not have access.

You should find what access a specific user or group has; this is provided through the User view within the role’s configuration. Find the user in the list and the “Roles” column will show the what the user or group is a member of. Clicking the user will allow the user to be added or removed from roles using the appropriate checkbox. Using the “+” button allows new user to be added and assigned to a role in one operation.

A number of predefined system roles exist within Reporting Server and users can be added and removed from the system roles as appropriate, however system roles names, descriptions and permissions cannot be modified.

Active Directory Users and Groups are added using a name resolver querying Active Directory. Any user or group resolvable in this tool can be added to the system. This means existing active directory groups can be added to a role as a single entity without the need to add individual users. The same permissions will be applied to all users within that active directory group driven from the permissions of the role within Reporting Server.

Role	**Description**
System Manager Role	System Managers have control (create, edit, read, and delete) over all roles, connections, templates, and documents of the application.
System Role Manager Role	System Role Managers create, edit, read, and delete roles. They also manage role membership.
System Document Manager Role	System Document Managers can create, edit, read and delete all templates, dashboards, and reports in the application. They can also manage dashboard and report access.
System Document Reader Role	System Document Readers can read any dashboard or report in the application.
Document Author Role	Document Authors can create new dashboards and reports. They can also read, edit, delete, and assign roles to read any dashboard or report that they own.
<Custom Role>	Creating custom roles allows for grouping of access to documents. By applying a role to a specific group of documents and then adding users to that role, you ensure only role members have access to that document. Modifying access is then as easy as changing the user within the role, without having to worry about specific documents. Creating a custom role is done through the “Roles” view and clicking the “+” action menu. A basic form is filled in and require both a name and description. We strongly recommend spending some time to ensure these names and descriptions are useful as they are used throughout the application for reference. Once the new role is created, it will now appear in the main role list window. Select it from the list and add users using the name resolver tool as appropriate.

Adding members to the System Manager Role

You must add members to the System Manager Role so a user has full control over Reporting Server. By default, the account defined during the installation is delegated as the system manager and they have full administrative rights over Reporting Server.

1. Log into Reporting Server using the same account as the user defined during Reporting Server installation
2. Click **Roles**.
3. Click **System Manager Role**.
4. Select the **Add User or Group** dropdown and enter the display name of the user you wish to make a system manager.
5. Click the appropriate user or group and they will be added to the “System Manager Role”.

Creating a Custom Role

You can create custom roles to allow users or groups to be added and removed without having to directly manage individual documents. Role creation and membership can be performed by any members of the “System Role Manager Role”.

1. Log onto Reporting Server as a member of the “System Role Manager Role” or “System Manager Role”.
2. Click **Roles**.
3. Click the “Plus” icon.
4. Enter a Name and Description. Ensure you describe exactly who or what type of user will be included in this role.
5. Click **Save**.
6. Click the newly added role.
7. Click the **Add User or Group** dropdown and enter a user or group. Typically, domain users are already grouped through common properties such as department or office site; choosing an existing group can allow many users to be added in a single operation.

   Clicking the user or group from the drop-down list will add them to the role.

   Users currently logged on to Reporting Server will be required to log off and close their browser to see permissions changed through role access.

Connections

Connections provide customisable levels of access to the data within a database. Due to the sensitive nature of information, they can only be created and modified by members of the “System Manager Role”. An additional “Connections” button will be added to the navigation menu on the left for users with the appropriate role membership.

Connections are created using the “+” button.

> **NOTE:** The credentials require only read-access to just the tables, views, and stored procedures enabled on the connection. Details about required tables, views, and stored procedures for templates will be provided alongside the relevant “Intelligence Pack”.

You can apply roles to the connections using the Permissions tab. Roles can then be given read and/or update abilities on those connections.

Connections allow control over what is exposed from a database to a given connection. The Data tab will list all available “Tables”, “Views” and “Procedures” accessible by the credentials provided for this connection. All data can be exposed using the “All” checkbox and “Save” icon on each tab.

> **NOTE:** When a new connection is created, no tables, views, or stored procedures are exposed.

Creating Database Connections

Only the System Manager can create a database connection. This database must correlate with data as referenced in the documents for the dashboards and reports to render correctly.

1. Log onto Reporting Server as a member of the “System Manager Role”.
2. Click **Connections**.
3. Click the “Plus” icon.
4. Enter a Name field ensuring it is relevant to the database context so document authors can identify this connection when choosing from a list.
5. Enter the Server and Database names.
6. If your credentials should be the same as the Reporting Server credentials configured during install, then you should select the “Use Server Credentials”; otherwise clear this checkbox and enter the username and password as provided by your database administrator.
7. Click the newly created connection.
8. Click the Data tab, and for each tab, click the “All” checkbox above its child list and click **Save**.

Intelligence Packs

Intelligence Packs are collections of documents that allow the visualisation of information contained within databases populated by other Boldon James products. The documents are also referred to as templates within Reporting Server as these can either be used as is by customers or modified to suit.

You can configure an Intelligence Pack using the “Pack” button. This is only visible to users belonging to the “System Manager Role”. You can see all currently installed packs with a collapsible list of each template contained within the pack.

You can view a list of templates contained within the pack. Alongside each template, a checkbox indicates whether the template is visible to document authors. Changing the checkbox will not remove existing documents that have been created using the template, but the template will no longer be usable by authors.

Installing a new pack is done using the file picker presented after clicking the “Install” button. Intelligence Packs will be provided by Boldon James separate to Reporting Server. For further information, contact Boldon James support.

Deleting packs from the system is done using the “Trash” icon. Deleting a pack will remove all templates from authors, but will not remove any documents created using those documents. Packs can be re-installed if needed.

Installing an Intelligence Pack

Intelligence packs allow document authors to quickly create documents based on pre-existing templates. They can only be installed by members of the “System Manager Role” or “System Document Manager Role”.

1. Log onto Reporting Server as a member of the “System Manager Role” or “System Document Manager Role”.
2. Click **Packs > Manage**.
3. Click **Install**, then select the intelligence pack distribution file you wish to install.
4. Click the expand arrow on the left of the intelligence pack name to show all document templates contained within the pack.
5. Select the checkbox against all the document templates listed and then click **Save**.

Further Information

Configure diagnostic logging

Diagnostic logging for the Reporting Server is provided using Serilog. A comprehensive guide to Serilog can be found at https://github.com/serilog/serilog/wiki

Diagnostic Logging for Reporting Server

Serilog Logging is configured through the appsettings.json file within the Reporting Server installation folder of the installation directory. The default settings are shown below:

```
{
"Serilog": {
"Using": [ "Serilog.Sinks.BJLoggr", "Serilog.Sinks.File" ], "MinimumLevel": {
"Default": "Information", "Override": {
"Microsoft": "Information", "System": "Information", "Reporting Server": "Information"
}
},
"WriteTo": [
{
"Name": "BJLoggr", "Args": {
"componentId": "Reporting Server", "restrictedToMinimumLevel": "Information"
}
},
{
"Name": "File", "Args": {
"path":“%TEMP%\\Logs\\BoldonJamesReportingServer.txt", "rollingInterval": "Day",
"restrictedToMinimumLevel": "Information"
}
}
```

]

}

This configuration provides two sinks, one for the Boldon James Trace Utility BJLogger and one for file. All levels are set to 'Information'

Formatting Diagnostic Output

When writing to the file sink, the diagnostic output can be formatted. For example, you can include the thread identifier to logging by adding a 'ThreadId' property in the Serilog section of appsettings.json:

"outputTemplate": "{Timestamp:yyyy-MM-dd HH:mm:ss.fff zzz} Thread:

<{ThreadId}> [{Level:u3}] {Message:lj}{NewLine}"

An explanation of formatting options for Serilog can be found at https://github.com/serilog/serilog/wiki/Formatting-Output

> **NOTE:** Changes to appsettings.json will have no effect until the service has been restarted.

Reporting Server auditing information

This section lists the various auditing messages created by Reporting Server in the Windows event log.

Audit events

The DCS Data Access Service auditing messages are written to the following channel: Boldon James Auditing/Classifier/Reporting Server/Admin

ID	Text	Task	Level
1000	Classifier Reporting Server Web Site Starting	WebSiteStarted	Informational
1001	Classifier Reporting Server Web Site Stopping	WebSiteStopping	Informational
1002	Classifier Reporting Server Web Site Exception	WebSiteException	Informational
2000	Role Added	RoleAdded	Informational
2001	Role Removed	RoleRemoved	Informational

2002	User added to role	UserAddedToRole	Informational
2003	User removed from role	UserRemovedFromRole	Informational
2004	Permission Group Added To Role	PGAddedToRole	Informational
2005	Permission Group Removed From Role	PGRemovedFromRole	Informational
3000	Intelligence Pack Imported	PackAdded	Informational
3001	Intelligence Pack Created	PackCreated	Informational
4000	Document Added	RSDocAdded	Informational
4001	Document Removed	RSDocRemoved	Informational
4002	Document Read Request	RSDocReadRequest	Informational
4003	Document Read	RSDocRead	Informational
4004	Document Changed	RSDocChanged	Informational
5000	Connection Added	RsConnectionAdded	Informational
5001	Connection Removed	RsConnectionRemoved	Informational
5002	Connection Read	RsConnectionRead	Informational
5003	Connection Changed	RsConnectionChanged	Informational
6000	User Authenticated OK	UserAuthOK	Informational
6001	User has No Claims	UserAuthFailed	Informational

Connection validation

When editing a connection, the “Connection” tab may present an “!”. This is an indication that an attempt to connect using the configured details has failed. This can be the result of environment but should act as a prompt to ensure the server name is still valid and pointing at an existing database, also that the

credentials have permissions to access the defined database. It may also be an indication that the SQL Server is not contactable because of network connectivity problems or system maintenance downtime.