



I01-std-fea-017 Audit Trail (Entity Audit)

Feature in Govern and GNA V6

Release 6.0/6.1 Version 1

Last Revision Update: 2016/08/02

Version History

Version	Date	Modify By	Description
1.0	2016/07/27	Olusegun Olaniyan	Create document

Disclaimer

Harris Govern has taken due care in preparing this manual. However, nothing contained herein modifies or alters in any way the standard terms and conditions of the purchase, lease, or license agreement by which the product was acquired, nor increases in any way the liability of MS Govern to the customer.

Table of Contents

Version History.....	2
OVERVIEW.....	8
Audit Trail Reports	8
USER INTERFACE	9
Launching the Audit Report	9
Audit Trail report tabs.....	9
Enter Parameter Values	9
Security Setup	11
Audit Report Security.....	11
Report Viewer Interface.....	11
Rerunning a Report	12
Displaying the Viewer area View... ..	12
CONFIGURATION.....	13
Pre-configuration Steps	13
Audit Flags.....	13
Enabling or Disabling Audit Flags	13
Where to Locate the Report	14
Configuration in the Govern New Administration (GNA)	14
UNC Paths in the Govern System Registry.....	14
Using the Report Parameters Editor.....	15
Configuring with the GNA Profile Editor	16
APPENDIX.....	17
Tables	17
Govern Audit Trail	17
GNA Audit Trail	17
Audit Trail Queries	18
Govern.....	18

GNA	19
-----------	----

OVERVIEW

Govern is an application that manages sensitive data. If access is gained to this data, there can be grave repercussions associated with both authorized, and unauthorized access. As a result of this, it is necessary to have administrative features that will provide a trail of activity within the application. This is the function of the Audit Trail (Entity Audit) feature. With an audit trail report, administrators have a tool that will allow them to review user activity within the Govern application. Upon request an activity report may be generated, one that will provide information such as the following:

- Date of activity
- Username
- The type of action performed, e.g. Create, Update, and Delete.
- Which OpenForm was modified and so on...

Audit Trail Reports

The Audit Trail feature consists of Crystal Reports that can be further modified to suit the customized needs of user. Customization can include modification of the queries or subqueries that are used in populating the report. Further customization can through branding in the form of adding a logo; this can be performed by an administrator with knowledge and access to a licensed package of **Crystal Reports 2011** or greater.

There are currently two standard Audit Reports, one for **Govern** and the other for **GNA**. The difference between these reports is the tables that are queried.

Audit trail reports can be generated that track modifications made in Govern OpenForms, or in the GNA application. The Audit Trail is a standard report that is distributed with Govern. Setting up an audit trail requires granting access to the item feature in the Business Entity Designer (BED).

Audit Trail Report

From: 2016-07-19 To: 2016-07-31
Action: All
User: nana
Form: Bld
Table: All
Column: All

Date	User	Action	Form	IP Address	Computer
19-Jul-2016 10:51 am	Nana Fraga	Update	CAMA - Buildings	192.168.60.144	22QBC21
Attribute	Table	Column	Old Value	New Value	
Inactive Year	PC_LK_PARCEL_BLDG	INACTIVE_YEAR	9999	9999	
Date	User	Action	Form	IP Address	Computer
19-Jul-2016 10:51 am	Nana Fraga	Create	CAMA - Buildings	192.168.60.144	22QBC21
Attribute	Table	Column	Old Value	New Value	
Building ID	PC_LK_PARCEL_BLDG	BLDG_ID		5007983	
Building Sequence	PC_LK_PARCEL_BLDG	BLDG_SEQ		0	
Effective Year	PC_LK_PARCEL_BLDG	EFFECTIVE_YEAR		2017	
Inactive Year	PC_LK_PARCEL_BLDG	INACTIVE_YEAR		9999	
Parcel ID	PC_LK_PARCEL_BLDG	P_ID		2370831	
Date	User	Action	Form	IP Address	Computer
19-Jul-2016 9:24 am	Nana Fraga	Create	CAMA - Buildings	192.168.60.144	22QBC21
Attribute	Table	Column	Old Value	New Value	
Building ID	PC_LK_PARCEL_BLDG	BLDG_ID		5007982	
Building Sequence	PC_LK_PARCEL_BLDG	BLDG_SEQ		0	
Effective Year	PC_LK_PARCEL_BLDG	EFFECTIVE_YEAR		2017	
Inactive Year	PC_LK_PARCEL_BLDG	INACTIVE_YEAR		9999	
Parcel ID	PC_LK_PARCEL_BLDG	P_ID		2370831	
Date	User	Action	Form	IP Address	Computer
19-Jul-2016 9:14 am	Nana Fraga	Delete	CAMA - Buildings	192.168.60.144	22QBC21
Attribute	Table	Column	Old Value	New Value	
Building ID	PC_LK_PARCEL_BLDG	BLDG_ID	5007981		
Building Sequence	PC_LK_PARCEL_BLDG	BLDG_SEQ	0		
Effective Year	PC_LK_PARCEL_BLDG	EFFECTIVE_YEAR	2017		
Inactive Year	PC_LK_PARCEL_BLDG	INACTIVE_YEAR	9999		
Parcel ID	PC_LK_PARCEL_BLDG	P_ID	2370831		

Page 1 of 2

Audit Trail Report

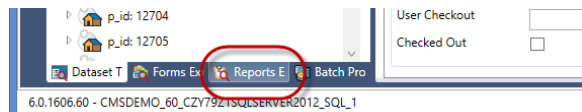
2016-07-19 3:05:54PM

Figure 1 - The Audit Trail Report

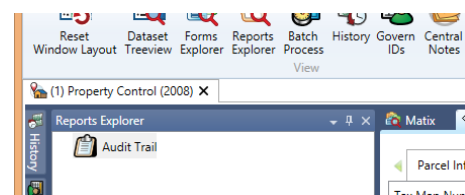
USER INTERFACE

Launching the Audit Report

Reports that have been added to a profile can be launched from the profile that they have been configured with through the Profile Editor in GNA. The Audit report is accessed through the **Reports Explorer** tab. This tab is presented, by default, as a tabbed pane located on the left hand side (LHS) of the Govern interface.



1. In Govern open the profile that has been configured with a report.
2. Select the Reports Explorer tab with a click to reveal the Reports that have been configured with the profile.
3. Click the Audit Trail configured Audit Trail report.



Audit Trail report tabs

When the Audit Trail report is open there will be two tabs displayed, **Parameter** and **Report**.

Parameter tab – Under this tab are any parameters that will need to be configured prior to launching the report. For the audit report there are no additional parameters to enter.

Report tab – This is an embedded viewer to display the pages of the report.

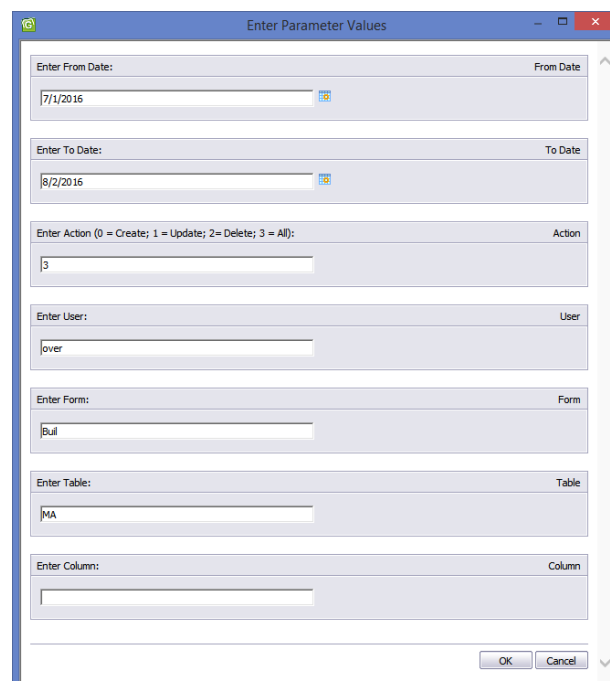
To view the Audit Report results...

1. Return to the Parameter tab, click **Run Report** to start.
2. Click **OK** to launch the Audit Report or **Cancel** to cancel.

Enter Parameter Values

The Enter Parameter Values form is displayed to allow you to enter the criteria for the audit query. Criteria include the following:

- **From Date** (Required) – A click on the icon will display the current date by default, navigate to the date required, or enter the
- **To Date** (Required) – This is a required field and must be entered or an error message is displayed.



The 'Enter Parameter Values' form contains the following fields:

- Enter From Date:** A date field with a calendar icon, showing 7/1/2016.
- Enter To Date:** A date field with a calendar icon, showing 8/2/2016.
- Enter Action (0 = Create; 1 = Update; 2 = Delete; 3 = All):** A dropdown menu with '3' selected.
- Enter User:** A text field with 'lover' entered.
- Enter Form:** A text field with 'Bul' entered.
- Enter Table:** A text field with 'MA' entered.
- Enter Column:** An empty text field.

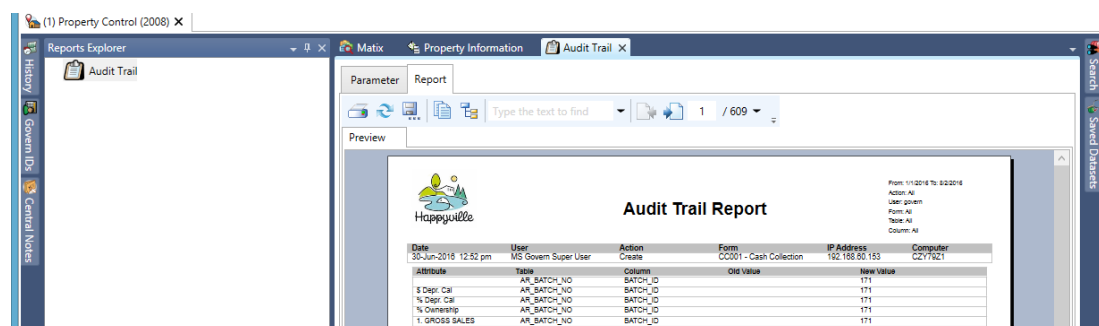
At the bottom right, there are 'OK' and 'Cancel' buttons.

- **Action** – Enter the type of action effected on the form that you are looking for...
 - **0** – Create
 - **1** – Update
 - **2** – Delete
 - **3** – All; i.e. all three above actions. This is the default setting.
- **User** – User Name; even a partial name will suffice as the report will look for even a portion of the name that was entered; e.g. entering “red” will bring up **Fred**, **Frederick**, **Mildred**, and so on.
- **Form** – Provide a partial or complete name of the form that you are interested in. An empty parameter will result in querying all forms.
- **Table** – Enter a partial or complete name of the table that you are interested in. An empty parameter will result in querying all tables.
- **Column** – Type in a partial or complete name of the column that you are interested in. An empty parameter will result in querying all columns in the tables.

Fields that are Audited

Audit Report results display the following fields:

- **Date** – This is date that the actions were performed.
- **User** – Display of the username.
- **Action** – This is the action performed through the form. Actions include:
 - *Create (C)*
 - *Update (U)*
 - *Delete (D)*
- **Form** – The form name, e.g. CAMA – Buildings.
- **IP Address** – Address that the actions were performed from, e.g. 192.168.220.155
- **Computer** – This is the network name of the computer that the action was performed from; e.g. BIG_DADDY24
- **Attribute** – Name of the attribute affected, e.g. Building ID.
- **Table** – The name of the table that was affected, e.g. PC_LK_PARCEL_BLDG
- **Column** – This is the column name affected, e.g. BLDG_ID
- **Old Value** – The previously existing value; this may be empty is new data was entered.
- **New Value** – This is the new value that was entered.



Date	User	Action	Form	IP Address	Computer
30-Jun-2016 12:52 pm	MS Govern Super User	Create	CC001 - Cash Collection	192.168.85.163	CE77621

Attribute	Table	Column	Old Value	New Value
3 Dep: Cst	AK_BATCH_NO	BATCH_ID		171
% Dep: Cst	AK_BATCH_NO	BATCH_ID		171
% Ownership	AK_BATCH_NO	BATCH_ID		171
1. GROSS SALES	AK_BATCH_NO	BATCH_ID		171
10. Total Amount Due	AK_BATCH_NO	BATCH_ID		171

Security Setup

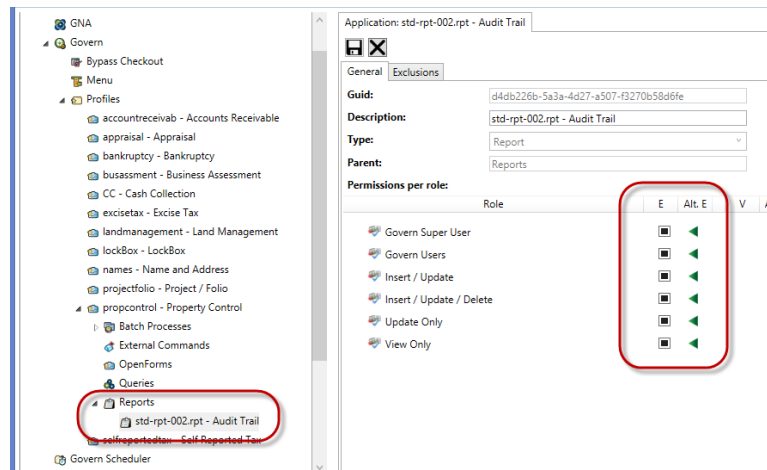
Audit Report Security

As always security concerns will exist as to who has access to the information that is displayed by the Audit Report. The Report Explorer is a securable component that can be restricted through the Govern Security Manager (SM) application.

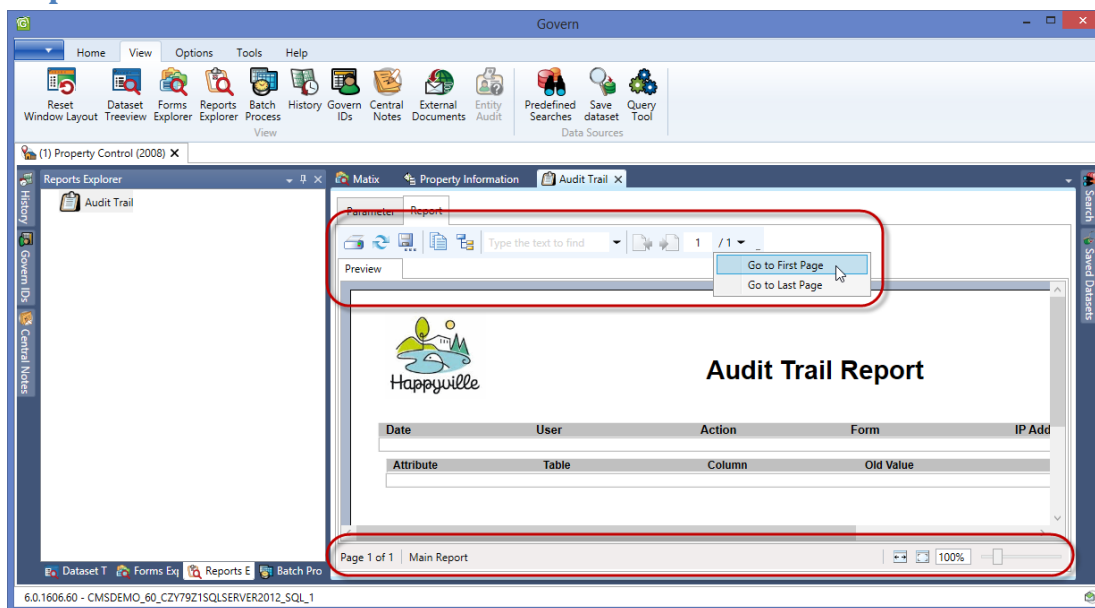
The path to the securable node is the SM is the following...

Applications > Govern > Profiles > profileName > Reports > Audit_Trail_ReportName

NOTE: Refer to the Govern Security Manual user guide for details about securing nodes.



Report Viewer Interface



As indicated earlier, the report viewer is an embedded Crystal Report viewer with controls that allow the user to perform the following on report results.

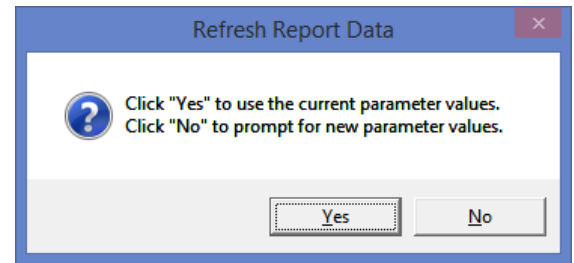
Print – Click Print to display the Windows dialog to print the report to a configured device.

Regenerating a Report

Refresh – To **Refresh**, i.e. rerun the report, click Refresh. This will provide to option to rerun the audit query with the same parameters entered, or provide new parameters.

Export Report – Click **Export** to export the report to Adobe (c) .PDF format.

- **Copy** – Click to copy to the Windows *Clipboard*.
- **Toggle Side Panel** – This will display the
- **Go to Previous / Next Page** – When you need to navigate to the previous page of the reports, click **Go to Previous Page**.
- **Go to page** – Highlight the current page number and enter a specific page to jump to.



Displaying the Viewer area View...

Fit to Width – Click to display the report in full width of the viewer.

Full Page – This option will display the full width and height of the report in the current viewer area

Magnification (parameter and slider) – Manually enter a magnification value in the parameter, or use the slider on the immediate right of the parameter to adjust the size of the report.



CONFIGURATION

NOTE: Due to the similarity in the procedures for the Audit Trail (Entity Audit) feature for Govern and the Govern New Administration (GNA), the following configuration steps are used for both types of Audit Reports.

Pre-configuration Steps

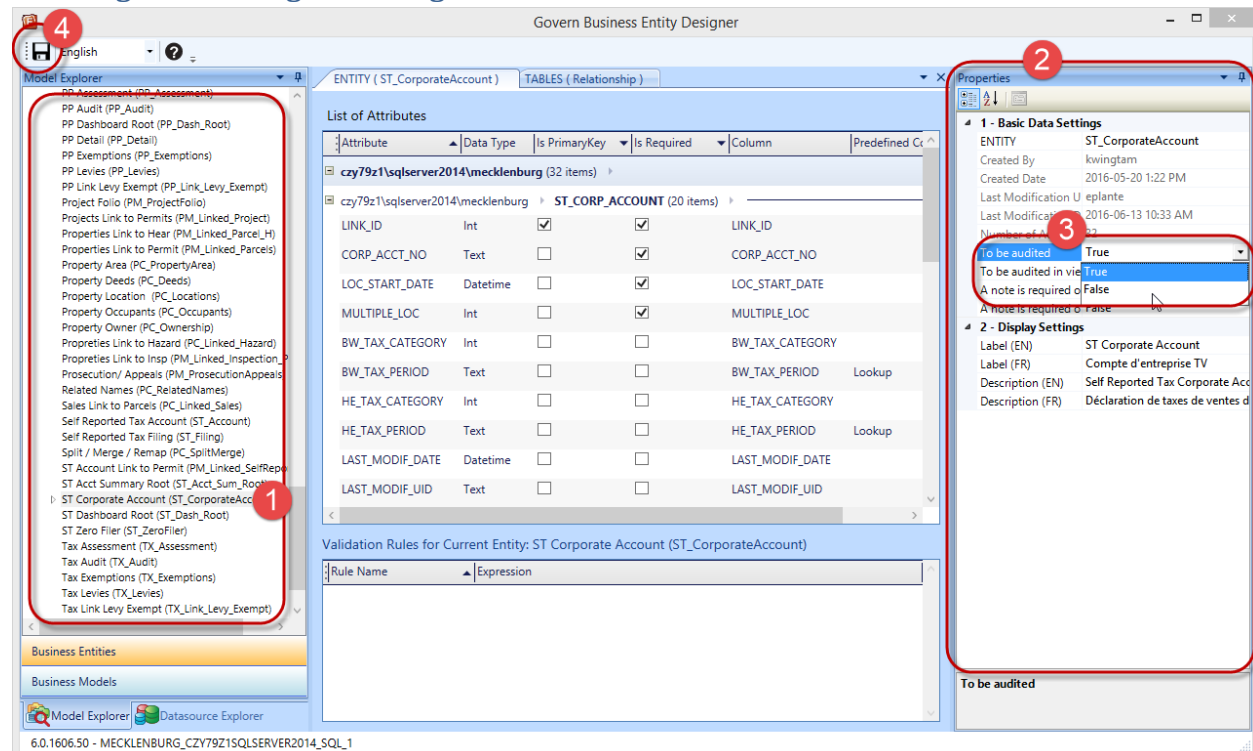
In order retrieve audit information on specific entity, said entity must be enabled. Enabling an entity is performed by setting a flag in the *Business Entity Designer (BED)*. In the BED there are two flags that are associated with the audit feature.

Audit Flags

To be audited – Set this flag to generate a log entry if any one of the three following actions is performed by the user, **EDIT**, **INSERT**, or **DELETE**. *This flag is by default set to TRUE.*

To be audited in view mode – When a log is requested to determine if the selected entity is viewed by a user. *Typically this flag is set to FALSE.*

Enabling or Disabling Audit Flags



The screenshot shows the Govern Business Entity Designer (BED) interface. The left pane (Model Explorer) lists various entities, with 'ST_CorporateAccount' selected (indicated by a red circle 1). The main pane displays the 'List of Attributes' for 'ST_CorporateAccount', showing columns like LINK_ID, CORP_ACCT_NO, LOC_START_DATE, etc. The right pane (Properties) shows the 'Basic Data Settings' for the selected entity. A red circle 2 highlights the 'To be audited' property, which is currently set to 'True'. A red circle 3 highlights the 'To be audited in view mode' property, which is currently set to 'False'. The status bar at the bottom indicates the current entity is 'ST_CorporateAccount'.

To enable or disable audit flags in the BED...

1. Launch the BED.

2. In the Model Explorer pane on *Left Hand Side* (LHS), click to select the entity that you would like enable or disable the audit trail entry for.
3. Locate the **Properties** pane on the *Right Hand Side* (RHS).
4. Under “**1 – Basic Data Settings**” group, click on the **To be audited** flag and set it to **TRUE** to enable auditing, or **FALSE** to disable auditing.
5. Click **Save** to save the setting.

Once the flag has been set to Enabled (TRUE) or Disabled (FALSE), log entries

Where to Locate the Report

The Audit Trail report is a standard report, and as such can be located in the Reports folder of the deployment. With a standard installation the path is the following:

`\\appServerName\[DeploymentRoot]\Deployments\Reports`

Administrators should ensure that they are up to date with the latest version of the Govern OpenForm reference file. This file “**DynamicSearchReference.XML**”. This file can be updated in *Govern New Administration* (GNA) with the **Import Data From File** utility.

Audit Report Configuration in GNA

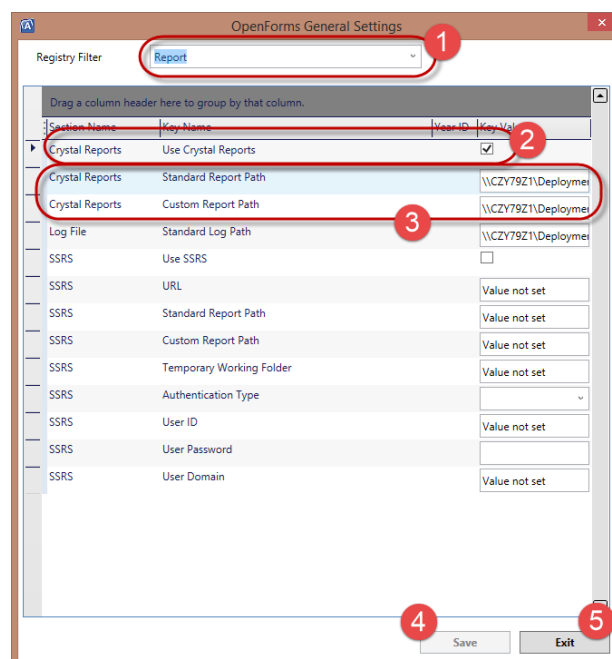
As with other Govern integrations, the Audit Trail Report can be configured through the Reports Editor in GNA. The Report Editor form is used to configure reports on an individual basis. These reports display query results found in the fields of tables within the data source. Reports are given access through the default connection key. If required, they may also be configured using an alternate connection key. As long as the alternate connection key has been defined in the Connection Key Management form, it will be available in the Alternate Connection Key list.

UNC Paths in the Govern System Registry

Prior to configuring the report, ensure that a UNC path has been set in the **OpenForms General Settings** form. It is in this form that a system option to use Crystal Reports is specified. In addition the UNC paths to Standard, and Custom report paths are specified. To verify your settings in the OpenForms General Settings form...

In the GNA Ribbon...

1. Click *Parameters (tab)* > **General Settings Editor**;
2. In the **OpenForms General Settings** form, Change the Registry Filter to **Reports**.
3. Click to select the **Use Crystal Reports** option.

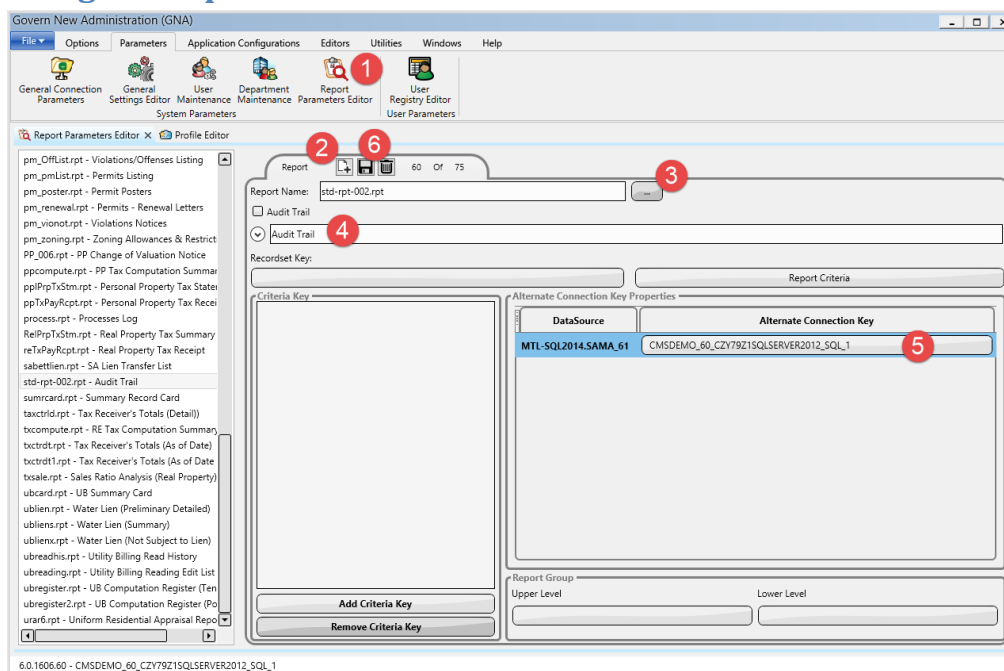


The screenshot shows the 'OpenForms General Settings' window. The 'Registry Filter' dropdown is set to 'Report' (1). The 'Use Crystal Reports' checkbox is checked (2). The 'Standard Report Path' and 'Custom Report Path' are both set to '\\CZY79Z1\Deployme...' (3). The 'Save' button is at the bottom left (4) and the 'Exit' button is at the bottom right (5).

Section Name	Key Name	Value
Crystal Reports	Use Crystal Reports	<input checked="" type="checkbox"/>
Crystal Reports	Standard Report Path	\\CZY79Z1\Deployme...
Crystal Reports	Custom Report Path	\\CZY79Z1\Deployme...
Log File	Standard Log Path	\\CZY79Z1\Deployme...
SSRS	Use SSRS	<input type="checkbox"/>
SSRS	URL	Value not set
SSRS	Standard Report Path	Value not set
SSRS	Custom Report Path	Value not set
SSRS	Temporary Working Folder	Value not set
SSRS	Authentication Type	Value not set
SSRS	User ID	Value not set
SSRS	User Password	Value not set
SSRS	User Domain	Value not set

4. Complete the UNC paths for the following parameters; **Standard Report Path**, and **Custom Report Path**.
5. Click **Save** to save your paths and **Exit** to close and exit from the form.

Using the Report Parameters Editor



Next it will be necessary to configure the report in the **Report Parameters Editor**.

In the GNA ribbon...

1. Click *Parameters (tab)* > **Report Parameters Editor**;

NOTE: All available reports are read and will be scanned. Connection options to the database are by default specified as the current connection. During the initial scanning phase, if a report is determined to be invalid, i.e. incompatible, a warning is displayed in the form of a window with a list of the offending reports.

2. To create a new report setting, click the **Create a new item** icon.
3. Click the Ellipsis button to display the Report Selector; locate Audit Trail report (std-rpt-002.rpt)
4. Enter a name for the report, e.g. Audit Trail.
5. Next in the Alternate Connection Key (CK) Properties group, ensure that there is a connection specified for the database that the report will be querying. Although database connection parameters are set in the Govern DeployEZ™, they can be overridden on a report by report basis. If required, use the alternate connection key parameter to specify the Connection Key
6. To save the settings, on the Report tab, click **Save the current item**.

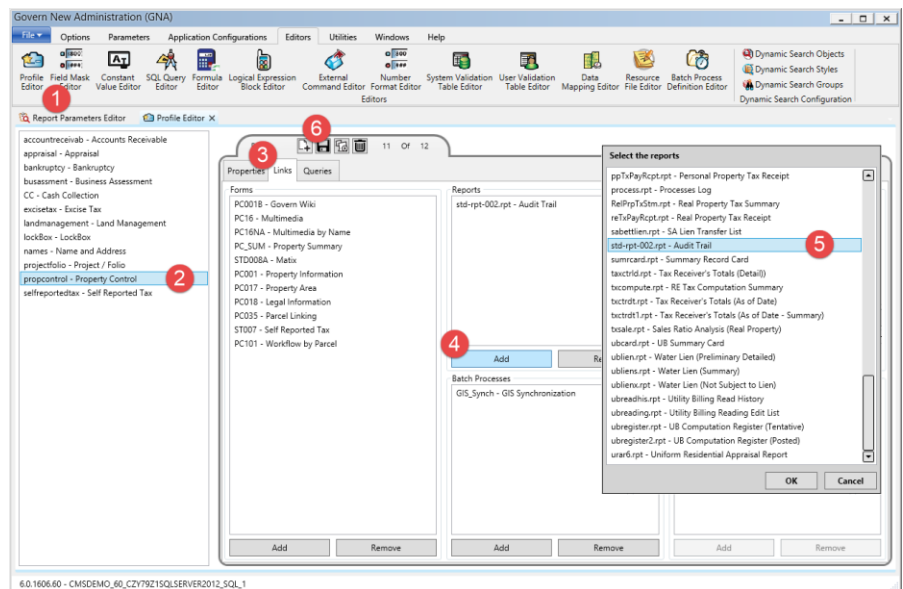
Refer to the GNA user guide for additional details on the topic of configuring reports.

Configuring with the GNA Profile Editor

After the previous step of creating your report in the Report Parameters Editor, you can now add the report to a profile that can be accessed in Govern. Reports can be added to an OpenForms profile through the Profile Editor for access in Govern.

To add the report to a profile in the *Govern New Administration (GNA)*...

1. On the GNA ribbon click *Editors (tab) > Profile Editor*.
2. Select the profile through which users can access the report.
3. In the Profile Editor, click *Links (tab)*.
4. In the Reports group, click **Add** to display the **Select the reports** list of system reports.
5. Click to select the Audit Trail report and click OK.
6. Save the changes to the form; click the **Save the current item** icon on the tab.



After this step the Audit Trail Report is ready to be launched in the OpenForm.

APPENDIX

Tables

As there are two Audit Trail reports, Govern, and GNA, there are two sets of tables that are used to store the information related to their activity.

Govern Audit Trail

The following tables are queried for Govern:

- **USR_AUDIT_OPENFORMS**
 - AUDIT_ID
 - AUDIT_ACTION
 - ENTITY_ID
 - FORM_CODE
 - USER_ID
 - AUDIT_DATE
 - IP_ADDRESS
 - SOURCE_COMPUTER_NAME
 - REMOTE_COMPUTER_NAME
- **USR_AUDIT_OPENFORMS_CHANGE**
 - AUDIT_ID
 - ATTRIBUTE_ID
 - TABLE_NAME
 - COLUMN_NAME
 - OLD_VALUE
 - NEW_VALUE
- **USR_AUDIT_OPENFORMS_KEY**
 - AUDIT_ID
 - ATTRIBUTE_ID
 - KEY_NAME
 - KEY_VALUE
 - IS_PRIMARY_KEY

GNA Audit Trail

The following tables are queried for the Govern New Administration (GNA)

- **USR_ADM_AUDIT_TRANS** – *One record for each save*
 - AUDIT_TRANS_ID
 - LAST_MODIF_UID
 - LAST_MODIF_DATE
 - IP_ADDRESS
 - SOURCE_COMPUTER_NAME

- REMOTE_COMPUTER_NAME
- **USR_ADM_AUDIT_RECORD** – *One record for each table included in a save*
 - AUDIT_RECORD_ID
 - AUDIT_TRANS_ID
 - TABLE_NAME
 - RECORD_ID
 - MODIF_TYPE
 - RECORD_DESCRIPTION
- **USR_ADM_AUDIT_FIELD** – *One record for each field, only when a modification*
 - AUDIT_FIELD_ID
 - AUDIT_RECORD_ID
 - FIELD_NAME
 - OLD_VALUE
 - NEW_VALUE

Audit Trail Queries

The following are the queries that are used for populating the Audit Trail report for Govern and GNA. Note the columns that are referenced, e.g. NAME, AUDIT_ACTION, IP_ADDRESS, COLUMN_NAME, TABLE_NAME, and so on.

Govern

MTL-SQL2014

```
SELECT DISTINCT "USR_AUDIT_OPENFORMS"."AUDIT_DATE", "USR_USERFILE"."NAME",
"USR_AUDIT_OPENFORMS"."AUDIT_ACTION", "USR_AUDIT_OPENFORMS"."IP_ADDRESS",
"USR_AUDIT_OPENFORMS"."SOURCE_COMPUTER_NAME", "USR_AUDIT_OPENFORMS"."AUDIT_ID",
"V_VT_USER_FORM"."SHORT_DESC_EN", "USR_AUDIT_OPENFORMS_CHANGE"."TABLE_NAME",
"USR_AUDIT_OPENFORMS_CHANGE"."COLUMN_NAME",
"USR_AUDIT_OPENFORMS_CHANGE"."ATTRIBUTE_ID", "USR_AUDIT_OPENFORMS_CHANGE"."OLD_VALUE",
"USR_AUDIT_OPENFORMS_CHANGE"."NEW_VALUE"
FROM    (("SAMA_61"."dbo"."USR_AUDIT_OPENFORMS" "USR_AUDIT_OPENFORMS" INNER JOIN
"SAMA_61"."dbo"."USR_USERFILE" "USR_USERFILE" ON
"USR_AUDIT_OPENFORMS"."USER_ID"="USR_USERFILE"."USER_ID") INNER JOIN
"SAMA_61"."dbo"."USR_AUDIT_OPENFORMS_CHANGE" "USR_AUDIT_OPENFORMS_CHANGE" ON
"USR_AUDIT_OPENFORMS"."AUDIT_ID"="USR_AUDIT_OPENFORMS_CHANGE"."AUDIT_ID") INNER JOIN
"SAMA_61"."dbo"."V_VT_USER_FORM" "V_VT_USER_FORM" ON
"USR_AUDIT_OPENFORMS"."FORM_CODE"="V_VT_USER_FORM"."CODE"
WHERE   "USR_AUDIT_OPENFORMS"."AUDIT_ACTION">=0 AND
("USR_AUDIT_OPENFORMS"."AUDIT_DATE">={ts '2015-07-19 00:00:00'} AND
"USR_AUDIT_OPENFORMS"."AUDIT_DATE"<{ts '2016-08-01 00:00:00'}) AND
"V_VT_USER_FORM"."SHORT_DESC_EN" LIKE '%%' AND "USR_USERFILE"."NAME" LIKE '%g%' AND
"USR_AUDIT_OPENFORMS_CHANGE"."TABLE_NAME" LIKE '%ma%' AND
"USR_AUDIT_OPENFORMS_CHANGE"."COLUMN_NAME" LIKE '%%'
ORDER BY "USR_AUDIT_OPENFORMS"."AUDIT_ID" DESC
```

MTL-SQL2014

```
SELECT DISTINCT "V_VT_USER_BE_ATTRIBUTE"."SHORT_DESC_EN",
"V_VT_USER_BE_ATTRIBUTE"."CODE"
FROM    "SAMA_61"."dbo"."V_VT_USER_BE_ATTRIBUTE" "V_VT_USER_BE_ATTRIBUTE"
```

GNA

```
SELECT DISTINCT "USR_USERFILE"."NAME", "USR_ADM_AUDIT_TRANS"."LAST_MODIF_DATE",
"USR_ADM_AUDIT_TRANS"."SOURCE_COMPUTER_NAME", "USR_ADM_AUDIT_TRANS"."AUDIT_TRANS_ID",
"USR_ADM_AUDIT_RECORD"."AUDIT_TRANS_ID", "USR_ADM_AUDIT_TRANS"."IP_ADDRESS",
"USR_ADM_AUDIT_RECORD"."TABLE_NAME", "USR_ADM_AUDIT_RECORD"."MODIF_TYPE",
"USR_ADM_AUDIT_FIELD"."FIELD_NAME", "USR_ADM_AUDIT_FIELD"."OLD_VALUE",
"USR_ADM_AUDIT_FIELD"."NEW_VALUE"
FROM      (("SAMA_61"."dbo"."USR_ADM_AUDIT_FIELD" "USR_ADM_AUDIT_FIELD" INNER JOIN
"SAMA_61"."dbo"."USR_ADM_AUDIT_RECORD" "USR_ADM_AUDIT_RECORD" ON
"USR_ADM_AUDIT_FIELD"."AUDIT_RECORD_ID"="USR_ADM_AUDIT_RECORD"."AUDIT_RECORD_ID")
INNER JOIN "SAMA_61"."dbo"."USR_ADM_AUDIT_TRANS" "USR_ADM_AUDIT_TRANS" ON
"USR_ADM_AUDIT_RECORD"."AUDIT_TRANS_ID"="USR_ADM_AUDIT_TRANS"."AUDIT_TRANS_ID") INNER
JOIN "SAMA_61"."dbo"."USR_USERFILE" "USR_USERFILE" ON
"USR_ADM_AUDIT_TRANS"."LAST_MODIF_UID"="USR_USERFILE"."USR_ID"
WHERE     "USR_ADM_AUDIT_RECORD"."MODIF_TYPE">=0 AND
("USR_ADM_AUDIT_TRANS"."LAST_MODIF_DATE">={ts '2016-07-21 00:00:00'} AND
"USR_ADM_AUDIT_TRANS"."LAST_MODIF_DATE"<{ts '2016-07-23 00:00:00'}) AND
"USR_USERFILE"."NAME" LIKE '%na%' AND "USR_ADM_AUDIT_RECORD"."TABLE_NAME" LIKE '%%'
AND "USR_ADM_AUDIT_FIELD"."FIELD_NAME" LIKE '%%'
ORDER BY "USR_ADM_AUDIT_RECORD"."AUDIT_TRANS_ID" DESC,
"USR_ADM_AUDIT_TRANS"."AUDIT_TRANS_ID" DESC
```

