



# **Govern Security Manager**

**Release 6.0 Version 1**

Last Revision Update: 3/7/2019

Govern  
Govern Security Manager  
Version: 1.0

March 2019 - Release 6.0  
Copyright © MS Govern 1997 - 2019  
All rights reserved

## 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 *Harris Govern* to the customer.



# Table of Contents

Disclaimer .....	i
<b>Introduction .....</b>	<b>1</b>
What's New .....	2
Change in Hibernate Behavior .....	2
No Inheritance for Top Level Objects .....	2
<b>Security Manager Terms .....</b>	<b>3</b>
Applications .....	3
Permission .....	3
Exclusions .....	3
Menu .....	3
Profiles .....	3
Roles .....	4
Users .....	4
GSM Components, Nodes, and Sub-nodes .....	4
Synchronize .....	4
<b>Starting the Govern Security Manager (GSM) .....</b>	<b>5</b>
Method of Authentication .....	5
<b>The Govern Security Manager (GSM) Interface .....</b>	<b>6</b>
Resizing the Application Window .....	7
The Govern Suite Button .....	8
Exiting from the Govern Security Manager .....	8
<b>The Ribbon .....</b>	<b>9</b>
Minimize the Ribbon .....	9
The Culture group .....	10
<b>Object Explorer Pane.....</b>	<b>11</b>
Components, Nodes, and Sub-nodes .....	11
Sub-nodes .....	12
Applications component and nodes .....	12
Roles component and nodes .....	12
Users component and nodes .....	12
Object Explorer pane - Command Buttons .....	13
Refresh button .....	13
Synchronize All button .....	14
Changes to the Synchronize Feature .....	14
Synchronize All Component and Nodes .....	15
Synchronize a Node or Sub-Node .....	16
When to Synchronize .....	16
Synchronize for the GNA application .....	16
Synchronize for the Govern application .....	17
Synchronizing Profiles / Menus / External Applications /Searches .....	17

Synchronize for Batch Processes .....	17
Synchronize for the Query Tool .....	17
<b>Standard Features .....</b>	<b>18</b>
Floating Menus .....	18
Floating Menus for Components, Nodes, and Sub-nodes .....	18
<b>The Edit form .....</b>	<b>20</b>
Edit form - Command Buttons .....	20
Opening Multiple Edit forms .....	21
Edit form - General tab .....	22
“Main” Type Objects .....	22
Exclusions tab .....	23
Making an Exclusion .....	23
<b>Enabling Security .....</b>	<b>25</b>
Security at the Application Level .....	25
Security at the Roles Level .....	25
Security at the User Level .....	25
Security and the Govern Scheduler (SC) .....	26
<b>Applications .....</b>	<b>27</b>
Menus and Profiles in Govern .....	27
Menu .....	27
Profiles .....	28
<b>Roles .....</b>	<b>30</b>
Roles Command Buttons .....	30
Roles Menu Options .....	31
Importing Govern Roles .....	31
Roles Parameters .....	32
Roles - General tab parameters .....	32
Roles - Permissions tab parameters .....	32
Creating Roles .....	32
Add or Delete Users from a Role .....	33
Modifying Permissions to a Role .....	34
Modify Permissions to a User in a Role (Exclusions) .....	35
Copying a Role .....	37
Deleting a Role .....	38
Rules of Inheritance and Creating Roles .....	39
<b>Users .....</b>	<b>40</b>
Viewing Users .....	40
Editing a User .....	40
Adding a User to a Role .....	41
Removing a User from a Role .....	41
Giving a User Access to a Profile .....	42
Permission Flags .....	43
Setting Permission Flags .....	43
Two (2) State Check Boxes .....	44
Access to Alternate or Historical Data .....	44
Setting or Changing the Alternate Permission flag .....	44

---

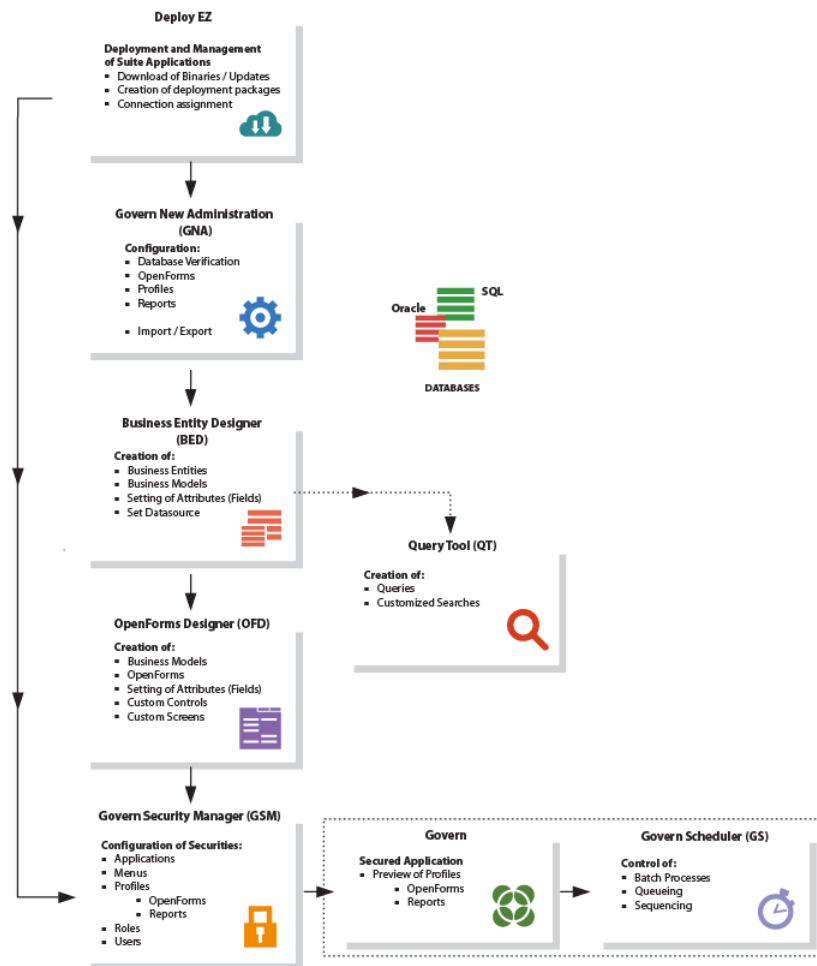
Parent and Child Object Inheritance .....	45
Types of Permission Flags.....	46
Using Permission Flags .....	47
Restricting Access to an Application .....	48
By Role .....	48
By User .....	49
Restrict Access to a Menu .....	49
Restrict Access By Role .....	50
Restrict Access By User .....	50
Restrict Access to a Profile .....	51
Restrict Access By Role .....	51
Restrict Access By User .....	52
Securing Profiles .....	53
Working with Centralized Notes in Govern .....	53
Allow Users to Modify Centralized Notes .....	54
Prevent Modification of Centralized Notes .....	54
Prevent Addition of Centralized Notes .....	55
Prevent Deletion of Centralized Notes .....	55
Hide the Centralized Notes Pane .....	56
Hide the Centralized Notes Management tab .....	57
Working with Global Messages in Govern .....	58
Allow Users to Modify Global or Department Messages .....	58
Prevent Modification of Global Messages .....	59
Prevent Addition of Global Messages .....	59
Prevent Deletion of Global Messages .....	60
Hide the Global Messages Ribbon Option .....	61
Securing the Govern Matix GIS Application.....	62
Restricting Access to Govern Matix User Validation Tables .....	62
Securing the Govern New Administration (GNA).....	63
Restricting Access to a Menu or Sub Menu items .....	63
Hiding the Menu Item... .....	65
<b>Index.....</b>	<b>67</b>

# Introduction

## Overview

The Govern Security Manager (GSM) is responsible for the top-level security management for the Govern Suite of applications.

The GSM manages user access to *Govern* applications such as *Govern*, *Govern Scheduler*, *Govern New Administration (GNA)*, *GIS Application Components and Configuration*, *Query Tool (QT)*, and *Validation Tables*. Depending on the Suite application, the level of user access can be controlled to the . Users that are familiar with earlier versions of the GSM should note that there are changes in the functioning of the release 6.0 application. *Refer to the section called What's New on page 2 for details about changes*





## What's New

This section lists new features, or new ways of performing an old function in the *Govern Security Manager (GSM)*. These new features are indicated by the **NEW!** symbol. Note that release 6.0 was a re-engineering of many of the Govern suite applications, there were changes to the way the GSM effects security from this version onwards.

### Change in Hibernate Behavior

By design the Govern application will not load if the (E)ecute OR (V)iew flags are disabled in the GSM. As of Release 6.0 1509.0038 and Release 6.1 1509.0054

### No Inheritance for Top Level Objects

Users of Release 6.0 and greater of the Govern Security Manager (GSM) should note that when securing objects, the solid blue square that signifies "Inheritance" is no longer available for top level objects.

## Security Manager Terms

Prior to using the *Govern Security Manager (GSM)*, it is recommended to review the terms that are used to describe virtual objects or actions within the context of the *GSM*.

### Applications

These are the applications that can be secured by the *Govern Security Manager (GSM)*. Examples include the *Govern* menus and profiles, *Entities* and *Entity Sets* in the *Query Tool* release 6.0, the *Batch Scheduler* console, *Govern New Administration (GNA)*, and the *Govern GIS Application*. In the future, other applications will be added. See *Applications* on page 27.

### Permission

This is an action or rule that applies to an action that a user can perform. This can be anything from viewing to modifying, or deleting data records. Another name for a permission is an *Access Right*. See *Permission Flags* on page 43.

### Exclusions

These are exceptions to a permission or access right. An exclusion may take the following form: e.g. All users can view the data in field "X", except for user B, who will be excluded from viewing the field. See *Making an Exclusion* on page 23.

### Menu

These refer to the user accessible menus and sub menus for accessing functions and initiating processes within the application. See *Menu* on page 27.

### Profiles

A *Profile* is best described as a *Workspace* or work environment. *Profiles* inform the system that anyone that is in this workspace will have access to these *Openforms*, *Reports*, *fiscal year*, and has a set level of access to private information. For example, a profile for a *Building Department* will specify access to the *OpenForms* and or *Reports*, required for the department to operate. See *Profiles* on page 28.

## Roles

Roles are a collection of users and permissions that give access to *Profiles*. A role is the equivalent of a *Group* in *Govern for Windows*. One can say that within a county office, there are many "roles"; i.e. secretaries, clerks, tax collectors, and assessors, to name a few. In order for a user to work in the office, they must first be assigned or made a member of a *Role*. A user can be assigned to many roles. See *Roles on page 30*.

## Users

In the context of the *Govern Security Manager (GSM)*, a *User* is an individual that requires access to a secured application. Anyone can be a user regardless of their level of access. A user can be part of one or more profiles. For example you can have a user that has access to the *Building* function through several profiles. One assigned profile might be able to insert, update and delete, while another profile will have inquiry access only. See *Users on page 40*.

## GSM Components, Nodes, and Sub-nodes

A *GSM Component* is a top level object that can represent an *Application*, *Object Types*, *Roles*, or *Users*. Under these components are nodes and sub-nodes. See *Components, Nodes, and Sub-nodes on page 11*.

## Synchronize

As changes are made to the security of an application, or changes to a database, the overall system will need to be made aware of these changes. Making these changes known to the system is called synchronizing in the context of Govern. See *Synchronize All button on page 14*.

# Starting the Govern Security Manager (GSM)

## Method of Authentication

Administrators should note that during the setup of the deployment package that will contain the GSM, at the *Deployment Authentication Type* option, *Microsoft Active Directory (MSAD)* is the default. When *MSAD* is the authentication method, the application will verify that the user exists in Govern's *USR\_USERFILE* table. Users that have been logged into windows will have unhindered access to the application.

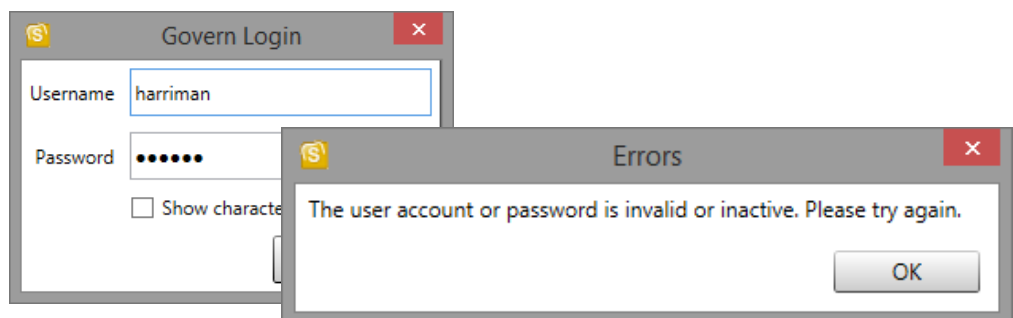
When the *GOVERN* authentication method is selected, users will be presented with a login screen.

**Note:** When the *GOVERN* authentication method is selected, because this option authenticates the user with Govern's user table (Table: *USR\_USERFILE*), administrators should ensure that users are entered as Govern users. *For details about creating a user, see the User Maintenance section of the Super User guide for Govern for Windows. An authentication method of NONE is not recommended.*

Users that are presented with a Log-in screen...

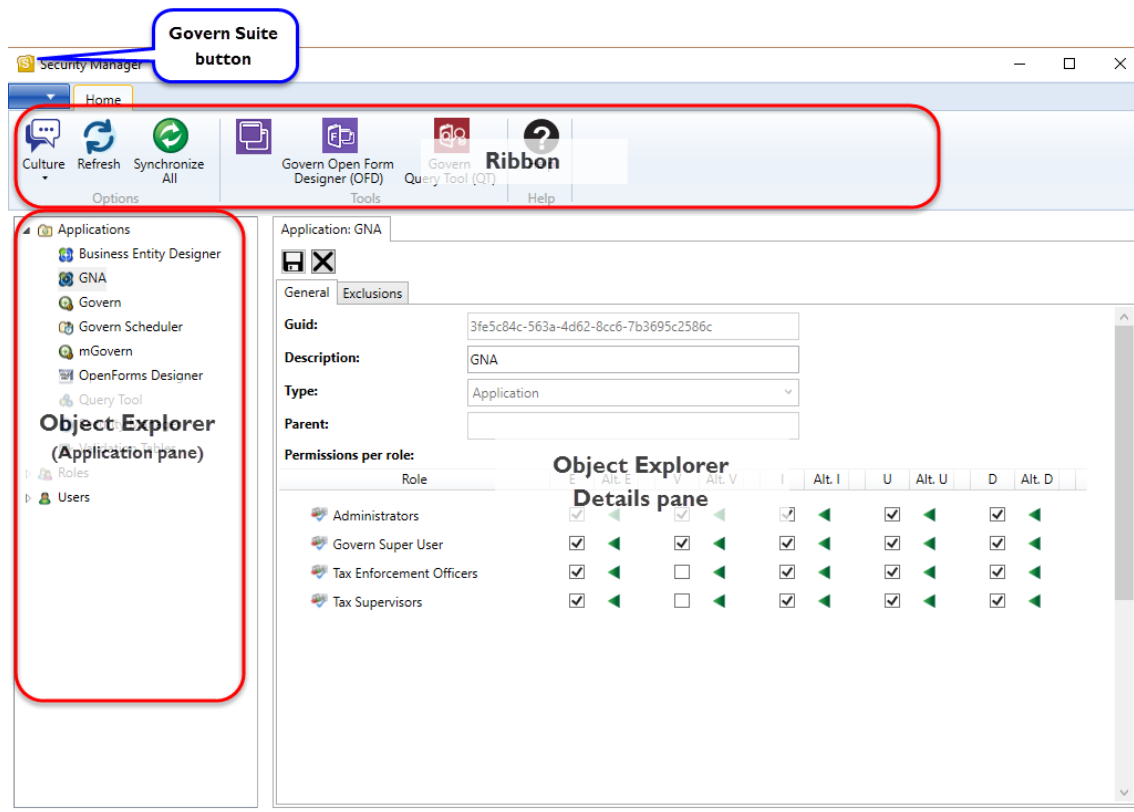
1. Ensure that the correct database connection has been selected; enter a username and password.
2. Click **OK** to start the program.

If an incorrect *Username* and *Password* combination is entered, an error message will be displayed; click **OK**, and make any required corrections.



You have a maximum of three (3) attempts to make a correct entry; three failed entries in a row will result in the application closing down.

# The Govern Security Manager (GSM) Interface



## Overview

The *Govern Security Manager (GSM)* interface is divided into three (3) principal areas.

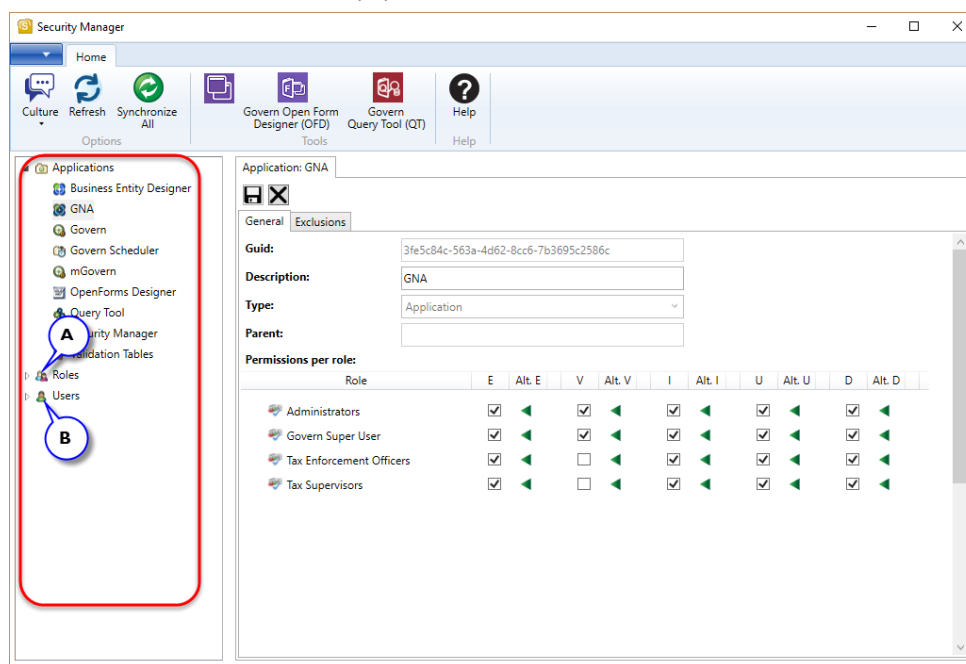
**Ribbon:** This is the location where you can effect quick changes to the Interface.

**Object Explorer Details or Details pane:** Details of the components that are selected in the *Object Explorer* are found in this area.

**Object Explorer:** Application components are displayed in a treeview in this area. The GSM is set up in a hierarchical manner to allow the user to quickly access securable components within an application. Object can be accessed using a "drill down" process. For example, a double-click on the Applications

icon will display any applications that can be secured. When you are able to "drill down" to a new level, the information that appears is displayed in the icon that appears in the Treeview area. This information is also displayed in the *Object Details* pane. A right-click on any object type will display a context-sensitive menu.

When the object icons first appear, you must double click on them to expand their content. After the double click, when there are one or more items within the icon, an arrowhead (A) will be displayed beside the expanded icon. Click on the "turned" arrowhead (B) to collapse the icon.



**Note:** It is only when you click on the icons, do the sub-items load into memory. Depending upon your system configuration, if there are many items to be loaded, there may be a delay during the loading process.

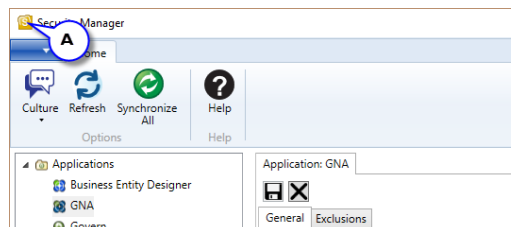
## Resizing the Application Window

As is the standard for Microsoft Windows, the *Govern Security Manager* window can be resized by placing your pointer at any one of eight (8) positions along the windows edge until you see a double sided arrow; click and drag to resize the window (A).

## The Govern Suite Button

The *Govern Suite* button (A) contains the *Close* option (Alt + F4) used in the application.

**Close:** To close the application, select **Close**.



**Note:** You may exit the application with a double-click on the Govern Suite Button.

## Exiting from the Govern Security Manager

Before you exit from the *Govern Security Manager*, always ensure that all changes have been saved. There are different areas where you can exit from the *Govern Security Manager*.

To exit from the *GSM*...

1. Double click on the Govern Suite button.

**OR**

2. Click the *Govern Suite* button and select **Close**.

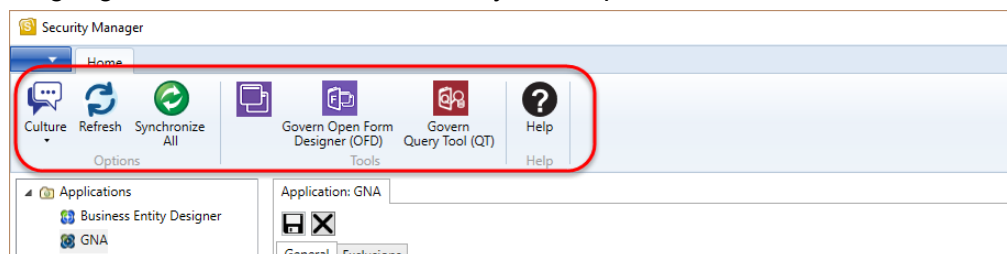
**OR**

3. Click the application close button (*Upper right hand corner*).

## The Ribbon

### Overview

The GSM *Ribbon* gives access to controls that allow users to change the language of the interface. In addition you can perform a screen Refresh.

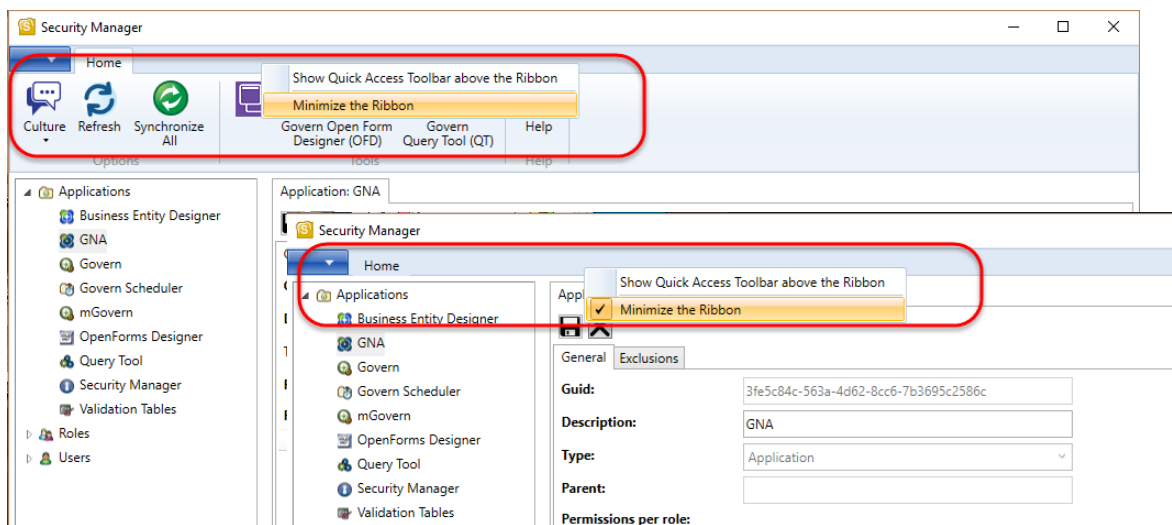


To access the Ribbon menu, right-click anywhere in the area of the toolbar. The floating menu will present you with the option to **Minimize Ribbon**.

**Note:** The options that are greyed out in menus are not available for selection.

### Minimize the Ribbon

To obtain more space on your desktop, you can minimize, i.e. hide, the Ribbon.



To **Minimize or Maximize** the Ribbon...



1. Right-click on an area of the ribbon with text on it.
2. Select **Minimize the Ribbon (A)**.

When selected, this menu option will have a “check mark” beside it. To turn off the option, right-click to display the floating menu and reselect the same menu option.

The *GSM Ribbon* consists of a *Tools* tab that is divided into two sections. These section are *Options*, *Ribbon Color Theme*, and *Culture*.

### The Culture group



Click **Culture (C)** to change the language of the interface. Currently there are two (2) languages supported:

**en-ca (English):** When selected this option will change the interface language to *Canadian* english.

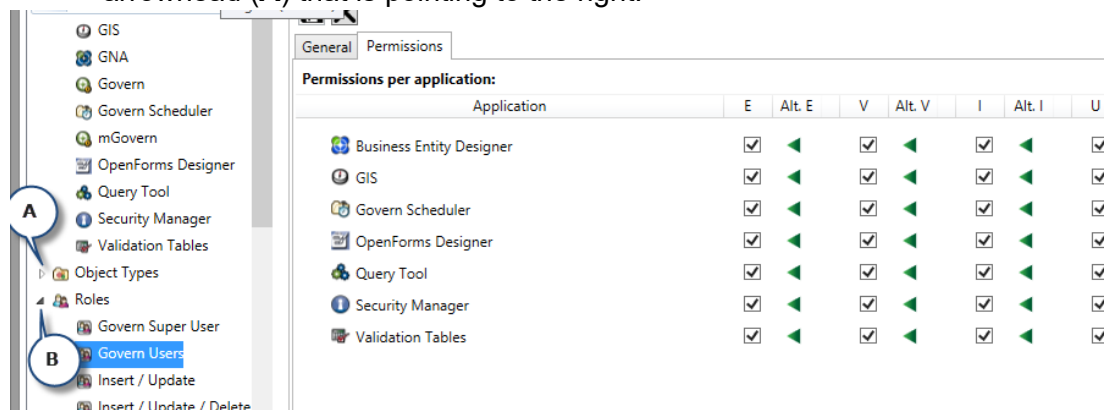
**fr-ca (French):** Select this to change the interface language to French.

**Note:** The default language and Theme of the GSM is determined by the administrator when the deployment is set up in the *ClickOnce™ Publisher*.

# Object Explorer Pane

## Overview

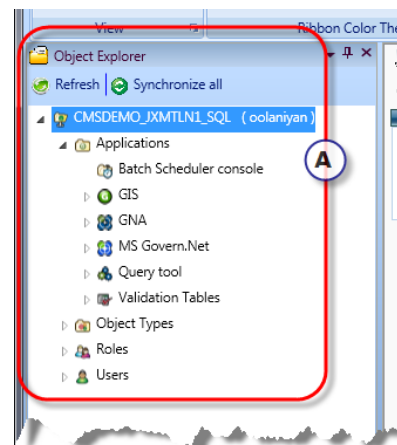
Components that appear in the *GSM* are presented in a treeview interface. With a treeview interface, you are able to “drill down” into the component icon. Double-click on an icon to, when available, expand it. An expanded icon will be preceded with a turned down arrowhead (**B**), to collapse the tree, click the arrowhead again. When collapsed the icon will be preceded with a white arrowhead (**A**) that is pointing to the right.



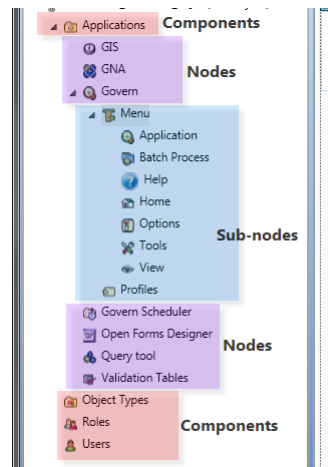
## Components, Nodes, and Sub-nodes

In the *Object Explorer* pane you are presented, by default, with the database connection icon and three (3) component icons.

A double click on the **Applications** icon collapses or expands the icon to reveal the areas that can be secured (**A**). The double-click action to access a node or sub-node is referred to as a “**drill-down**”, or a “**drilling down**” process..



The following are the *Components* that the *Govern Security Manager (GSM)* is able to secure. These components are, *Applications*, *Object Types*, *Roles*, and *Users*. Within the different components are nodes, and sub-nodes.



### Sub-nodes

You can **drill-down** into the main components to view sub levels. The sub-level of a component is referred to as a node. Sub-levels or *Sub-nodes* can be seen, when available, with a drill-down on any of the node icons.

### Applications component and nodes

The *Applications* that are secured for use within the *GSM* can be found under this icon. See *Applications* on page 27 for details.

### Roles component and nodes

This node is where user roles are configured. Roles are a collection of permissions that give users access to *Applications*, *Profiles*, and *Objects*. See *Roles* on page 30 for details.

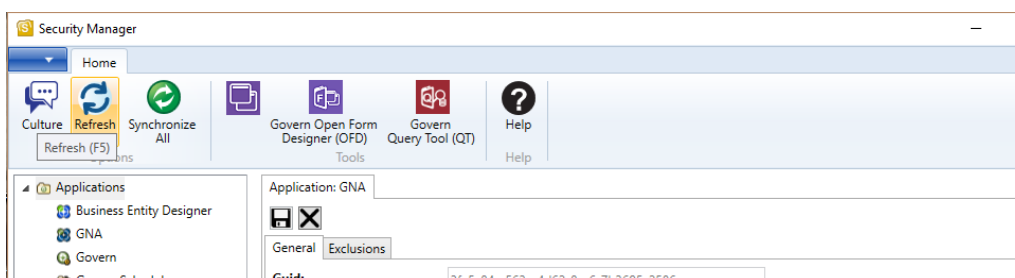
### Users component and nodes

This a list of all users with accounts that are registered in the system. See *Users* on page 40 for details.

## Object Explorer pane - Command Buttons

The Object Explorer pane has two (2) principal command buttons; the *Refresh* button, and the *Synchronize All* button. The functioning of the *Synchronize All* button was changed in release 4.7, see *Changes to the Synchronize Feature on page 14 for details*.

### Refresh button

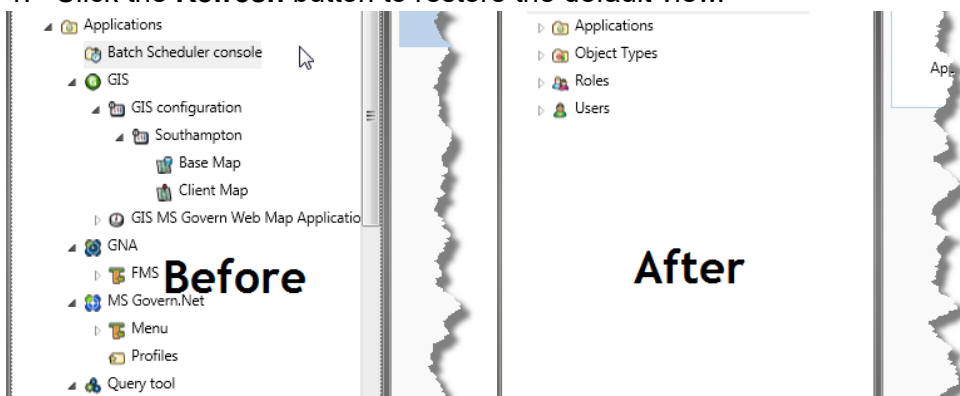


During the course of working in the *Object Explorer* pane, it will be necessary to expand the various nodes, i.e. *Applications*, *Roles and Users Types*, *Roles*, and *Users*. *Refresh* is used to clear cached levels when an icon has been expanded to a sub-node. At a certain point the treeview area can become cluttered with the expanded nodes and sub-nodes. For a quick reset to the default treeview displaying the database and the three (3) principal nodes, click **Refresh (F5)**.

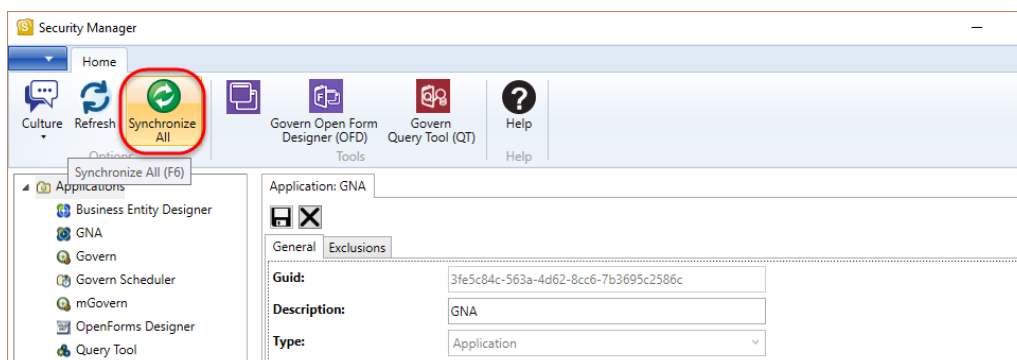
**Note:** Response time for a refresh may vary due to hardware restrictions such as slower CPU's or system RAM. In addition network lag due to connection speed or an older generation ethernet card.

To reset the Treeview to the default view when nodes and sub-nodes have been expanded...

1. Click the **Refresh** button to restore the default view.



## Synchronize All button



The **Synchronize All** button (B) is used when modifications have been made to the settings of any of the *Govern* applications, or changes affecting the database. For example, in *Govern*, when changes are made to a *Profile*, *Menu*, *External Application*, or *Search* objects, the synchronize process would be required. Another instance is when newly created searches are added to *Predefined Searches*, they will not be acknowledged by the system until a *Synchronization* has been performed. Other changes that would warrant a synchronization are the adding of new reports, fields, or *Business Models* to an *OpenForm function*, or changing access to the *Query Tool*.

## Changes to the Synchronize Feature

In previous releases of the *Govern Security Manager (GSM)*, the *Synchronize All* option could be found as a floating menu option with a right-click. To streamline the interface the function has been localized to a single **Synchronize All** button. When no nodes are selected, a click on **Synchronize All** will perform a complete synchronization with the database.

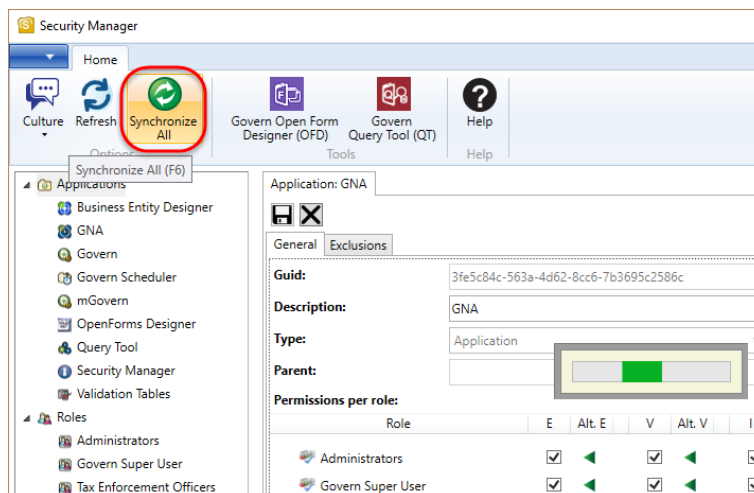
To perform a synchronization of the element of a single node, select the node and right-click. When available, select **Synchronize** from the floating menu.

## Synchronize All Component and Nodes

An overall synchronization, i.e. a complete synchronization of all components nodes, should be performed when development changes have been made to one or more *Govern* applications or modules..

**Note:** The Synchronization process is non-destructive, therefore it can be repeatedly performed for any type of update. One factor that may deter a user from choosing to perform the *Synchronize All* process is time due to connection speeds and complexity of database changes.

To synchronize all nodes...

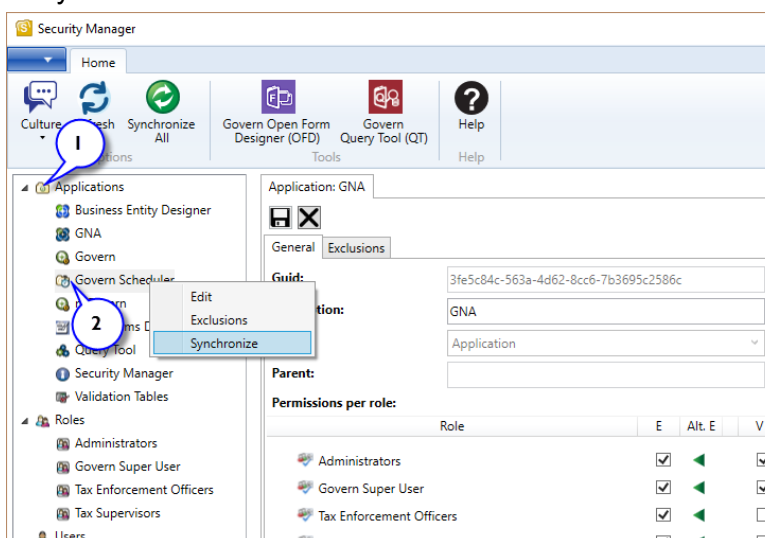


1. Click **Synchronize All** on the Ribbon.

A complete synchronization for all nodes and sub-nodes with the database will occur.

## Synchronize a Node or Sub-Node

To synchronize an individual node or sub-node...



1. Click to select the required node or sub-node (1).
2. Right-click to display the floating menu; select **Synchronize** (2).

Note the progress bar; when the bar disappears, the process is complete. The selected node and all sub-nodes will be synchronized with the database.

## When to Synchronize

**Note:** The length of any of the following processes is dependent upon the conditions for synchronizing, i.e. number of nodes and sub-nodes, network traffic, or connection speed.

The following are specific conditions that can warrant a synchronization at a specific component node, as opposed to an overall synchronization.

### Synchronize for the GNA application

Perform a synchronization when development changes have been made to the *Govern New Administration* application.

### Synchronize for the Govern application

Use this option to perform an overall refresh of the application when changes have been made to various areas like Profiles, Menus, etc. this is an alternative to synchronizing each individual component.

### Synchronizing Profiles / Menus / External Applications / Searches

When an addition or deletion has been made to any of the *Profiles*, *Menus*, *External Applications*, or *Searches*, select the appropriate node and right-click; select *Synchronize* from the floating menu. The update will correspond to the area of change.

### Synchronize for Batch Processes

Perform a synchronization at this level when development changes have been made to *Batch Processes* through the *Govern New Administration* application.

### Synchronize for the Query Tool

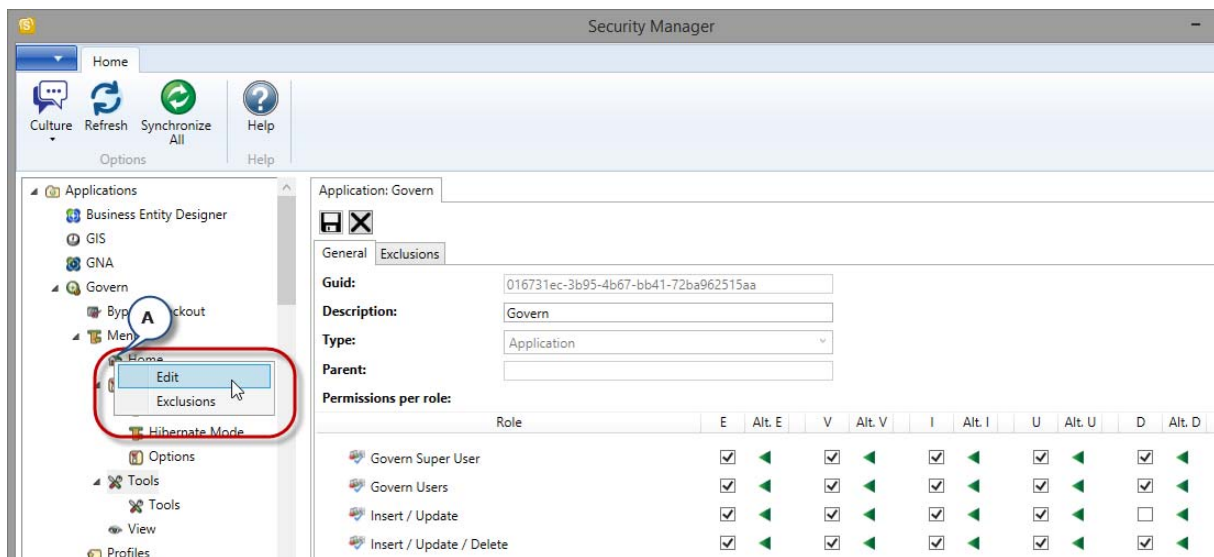
Synchronize the *Query Tool* node or sub-nodes when *Business Entities (BE's)* or *Business Models (BM's)* have been made available to the *Govern Query Tool* application.



# Standard Features

The following display features can be seen at all levels of the GSM.

## Floating Menus



## Floating Menus for Components, Nodes, and Sub-nodes

Floating menus are contextual in the sense that the type of component icon that is selected will determine the menu options that are displayed.

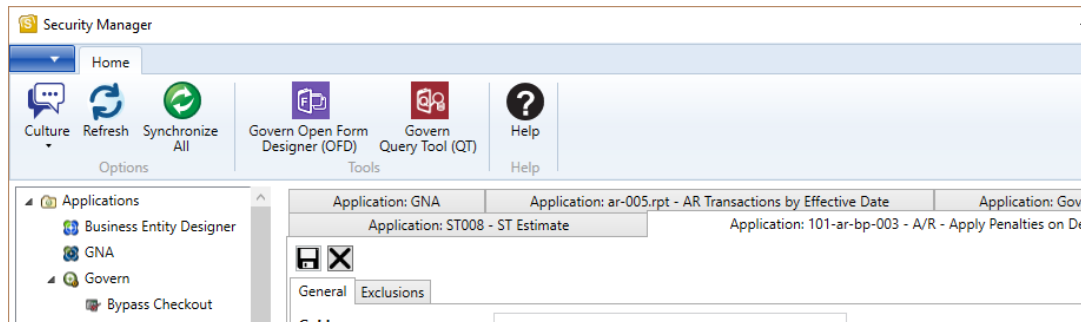
Component	Component Menu	Node Menu	Sub-Node Menu
<b>Applications</b>	- no options -	<i>Edit</i>	<i>Edit</i>
		<i>Exclusions</i>	<i>Exclusions</i>
		<i>Synchronize</i>	
<b>Roles</b>	New	<i>Edit</i>	- N/A -
	Refresh	<i>Permissions</i>	- N/A -
	Import Govern roles	<i>New Role</i>	- N/A -
		<i>Delete</i>	- N/A -
		<i>Copy</i>	- N/A -

---

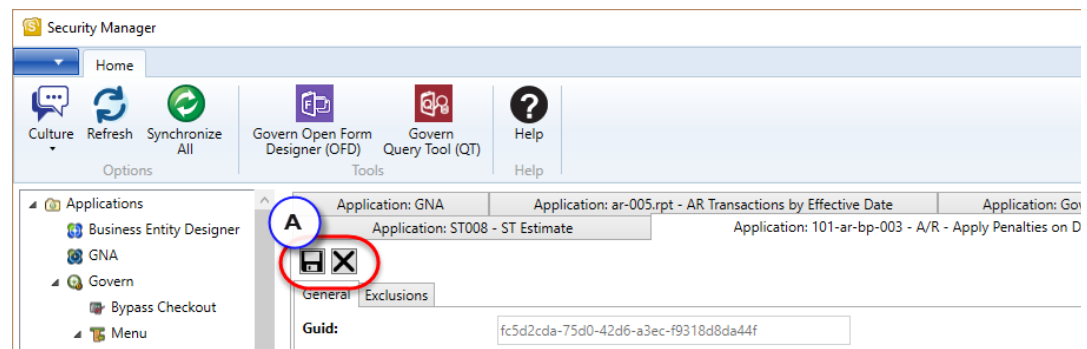
Component	Component Menu	Node Menu	Sub-Node Menu
<b>Users</b>	- no options -	<i>Edit</i>	- N/A -
		<i>Permissions</i>	- N/A -

## The Edit form

When the *Edit* option is selected from the floating menu, a form is displayed in the *Object Explorer Details* pane. This form displays the details of the settings of the component or node. This is also the interface that will be used to make modifications to the settings.



## Edit form - Command Buttons



The standard command buttons for an *Edit* form are:

**Save:** After entering or modifying any of the parameters, click the **Save** icon to save your changes (A).

**Note:** This **Save** button is not available for selection unless a change has been made to the form.

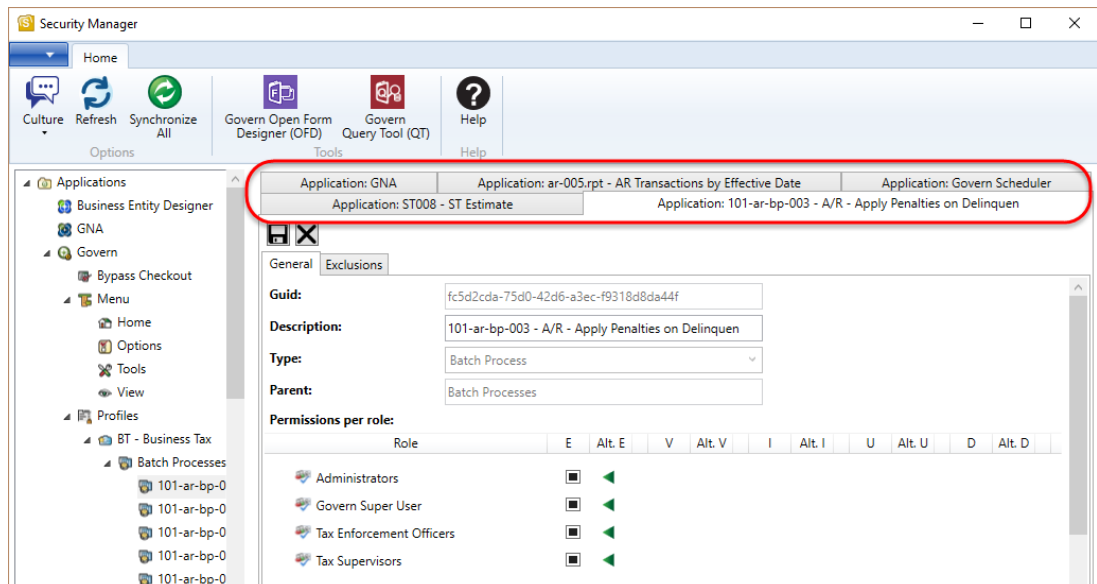
**Refresh:** Click Refresh to update the interface with any new information that may have been updated in the database (**A**).

**Note:** The Refresh button at this level is not the same as the one on the main ribbon.

**Close:** Click **Close** to exit from the *Edit* form (**A**).

## Opening Multiple Edit forms

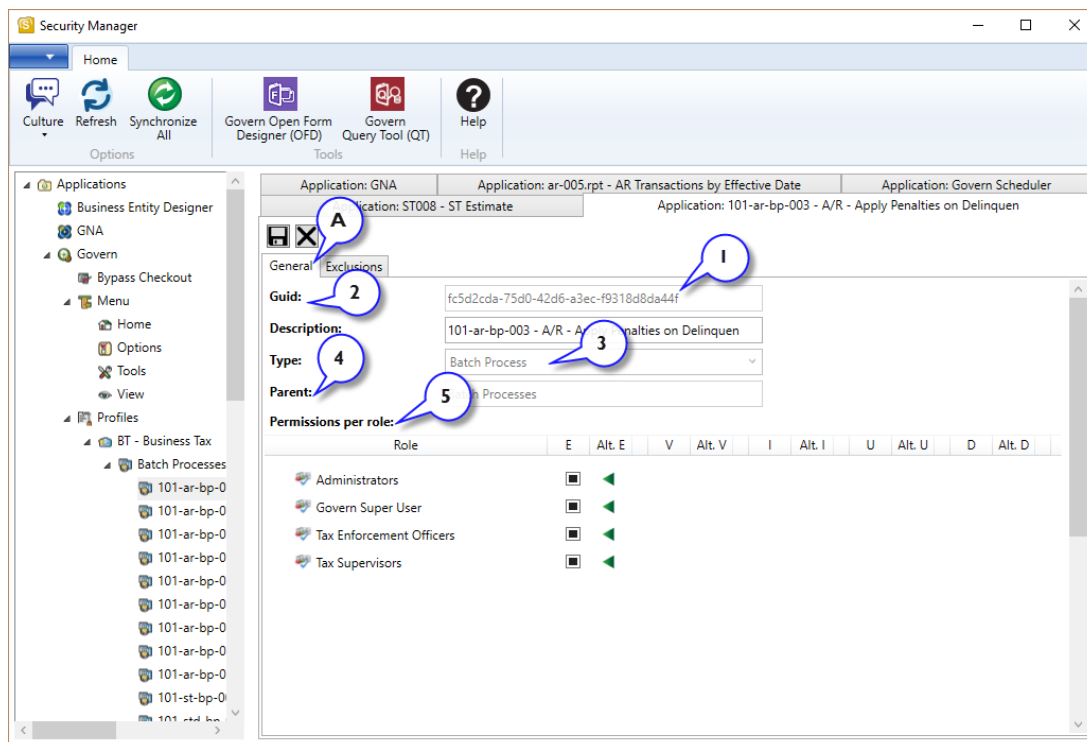
When you have finished working on an *Edit* form, it is recommended that you immediately close the form. If the Edit form is not closed, selecting another object type or a different part of the interface, will force the *Edit* form to be displayed as a tab in the *Object Explorer Details pane*. This can result in multiple *Edit forms* being open. Multiple open Edit forms can be confusing during configuration, in addition they can take up valuable system resources, and affect the performance of the *Govern Security Manager (GSM)*.



When multiple *Edit* forms are opened, they will be accessible through tabs appearing in the *Details pane*.

## Edit form - General tab

The General tab contains the main configuration parameters of an object type that is being secured (A).



The screenshot shows the 'Security Manager' application window. The 'General' tab is selected, displaying configuration parameters for an application. The parameters are as follows:

Parameter	Value
Guid	fc5d2cda-75d0-42d6-a3ec-f9318d8da44f
Description	101-ar-bp-003 - A/R - Apply Penalties on Delinquen
Type	Batch Process
Parent	Processes

Below the parameters is a table for 'Permissions per role'.

Role	E	Alt. E	V	Alt. V	I	Alt. I	U	Alt. U	D	Alt. D
Administrators	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Govern Super User	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Tax Enforcement Officers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Tax Supervisors	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Guid:** This is a system generated ID that cannot be modified by the user (1).

**Description:** Displays the description of the object, i.e. the name of the application (limit 116 characters) (2).

### “Main” Type Objects

Main type objects, i.e. *Main OpenForms*, *Main Profile*, and *Main Report*, are “containers” that exist within the *GSM* security structure. These containers are used to pass on inheritances from nodes to sub-nodes. **Main** type objects are used within the *GSM* and cannot be accessed within the *Govern* application. See *Parent and Child Object Inheritance* on page 45 for details about inheritance.

- **Profile** - This is the security container used for profiles.
- **OpenForms** - This is the security container that is used for *OpenForms*.

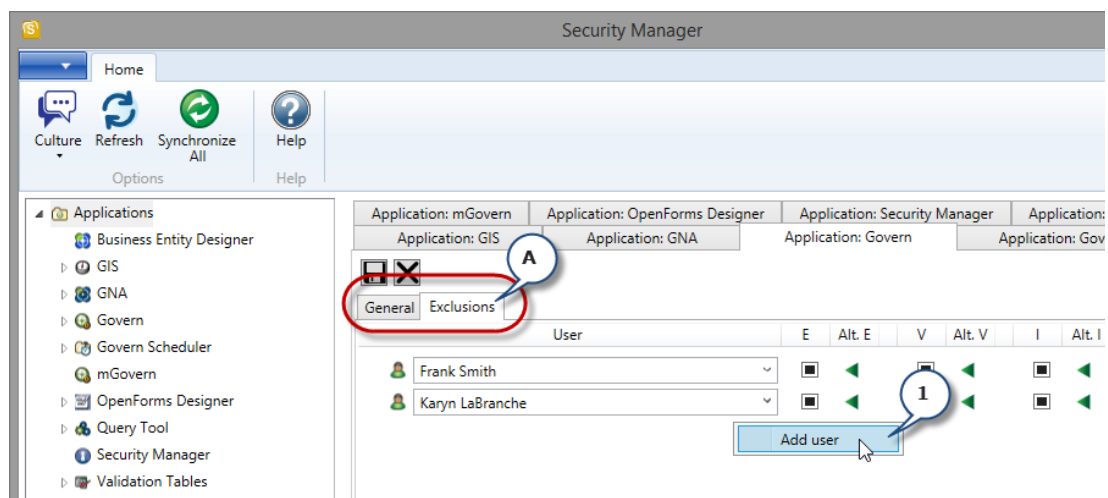
- **Reports** - This is used for passing inheritance to Reports.

**Parent:** This parameter will indicate, when applicable, the GUID of the parent that the object inherited permissions from. This parameter cannot be modified.

**Permissions per role:** This is the area where you can add a role and specify its permissions. See *Applications on page 27 for details about setting permissions*.

## Exclusions tab

The *Exclusions* tab (A) allows you to create exceptions to permissions that have been set in the **Permission per role:** section of the General tab.



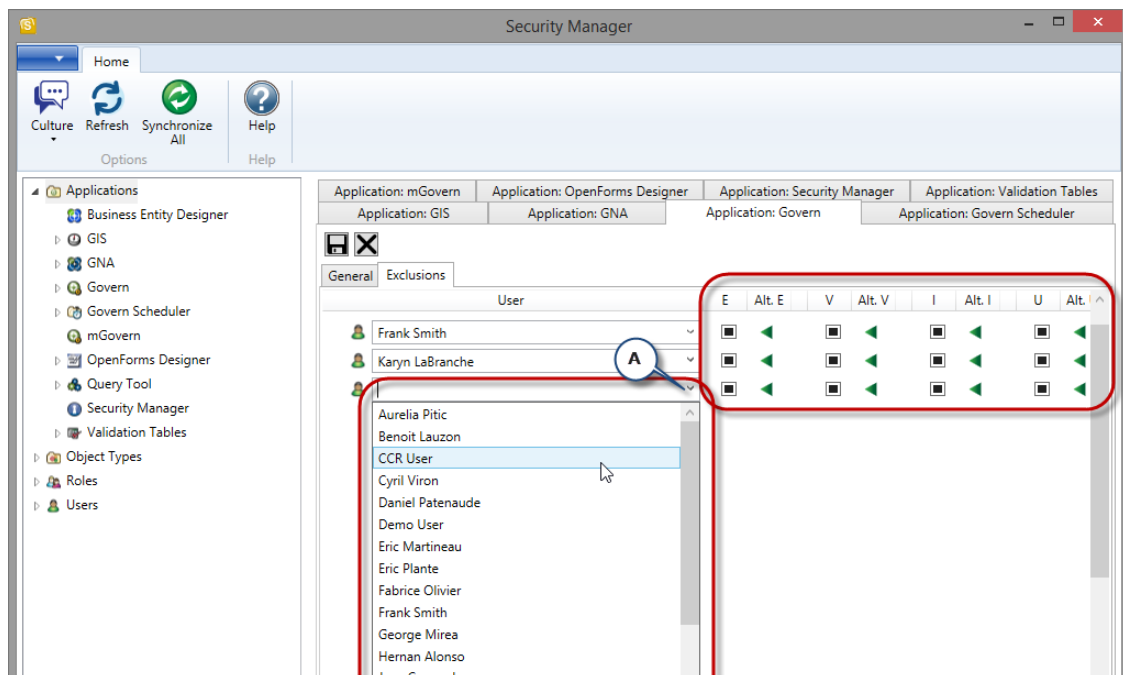
For example if you were to create a *Role* called **All Users (1)**, it could be given all permissions within the application, i.e. *Delete, Execute, Insert, Update, and View*. For a new employee you may want to make an exception or **Exclusion** to their permission, one that would only allow them to view data.

## Making an Exclusion

To make an Exclusion...

1. Select the *Exclusions* tab.
2. Right-click below the *User* column heading; in the floating menu, select **Add User**.

3. A new user will appear under the **User** column.



4. Click the drop-down menu list to select a user from the list (A).
5. Select the permissions that are to be exceptions for this user (B). See *Applications on page 27 for details about setting permissions.*

**Note:** The permissions check boxes, or *flags* that are associated with the user, will appear as solid blue squares. Click on these flags to change the permissions settings..

**Note:** The presentation of the solid blue square is a function of the Windows Theme that the computer is set to. For example, when the Windows theme is set to Windows Classic, the solid square is presented as a check mark that is colored a lighter shade of grey.

6. Click **Save**.

# Enabling Security

## Overview

The *Govern Security Manager (GSM)* allows you to secure applications in the Govern suite at three locations, through the *Applications* component, the *Roles* components, and the *Users* components. The area that you choose to apply the security will depend upon your requirements.

### Security at the Application Level

It is at the application level that *Exclusions*, i.e. exceptions, to granted permissions are made to individual users. Granting permissions at this level is still the same as going to the user and granting access to the application, it is merely looking at it from a different point of view. For example, when you need to secure one or more users, or exclude individuals within roles, you could also apply your security at the level of the application. This can be useful in situations where an individual may be a member of multiple *Roles* and exceptions need to be made to apply to the individual for all of them.

### Security at the Roles Level

Granting Permissions at the Roles level lets you provide access to all areas of the application. Any settings are applied to the Role, and all members. At this level, when individual users are added to the Role, they are granted the access rights of that Role.

**Note:** When a user is a member of multiple Roles, they will inherit the rights of the role with the highest access rights. For example a user is a member of two (2) roles with the following rights, a **View Only** role, and an **Insert / Update / Delete** role. As the Insert / Update / Delete role has higher access rights, This will be the rights given to the user regardless of whether they are a member of a role with **View Only** rights.

### Security at the User Level

Securities set at the *User* level, will allow you to add the user to specific Roles, or deactivate the user. In addition, permissions to any component within the application can be disabled for that user. Note that this is the same as creating an *Exclusion* within a *Role*.



---

## **Security and the Govern Scheduler (SC)**

Administrators should note that when security is enabled for *Govern Scheduler (SC)* users, those users with full administrator rights will be able to see and modify all batch processes, i.e. start, pause, restart, or delete processes for themselves as well as for all other users. A standard user will only be able to view and modify the processes that they started.

# Applications

## Overview

The *Applications* node icon, when expanded, displays the applications that can be secured by the GSM. Double-click the Applications node icon to expand it; select an application icon. Right-click on an application icon and select **Edit**. See *The Edit form on page 20 for details*. For demonstration purposes, and because of the level of granularity that can be achieved in the security, *Govern* will be used for examples.

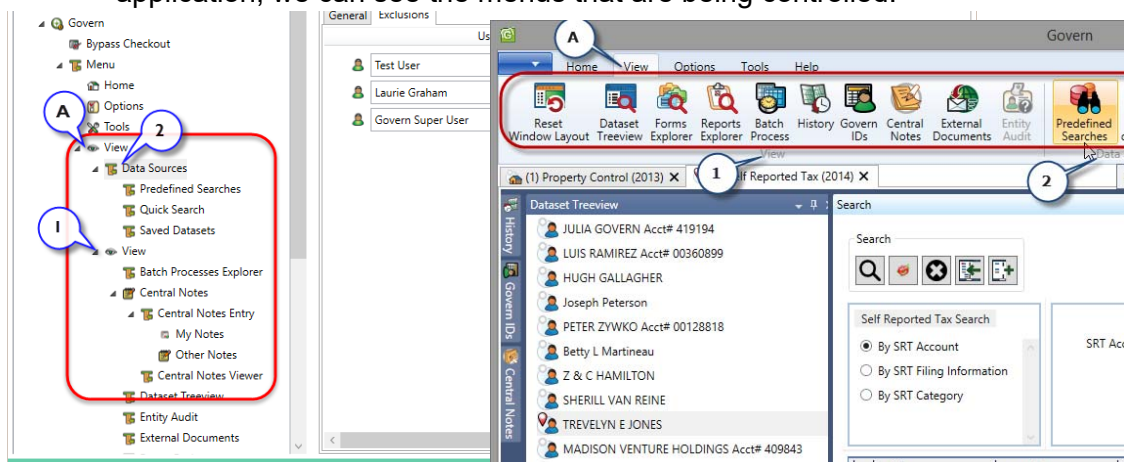
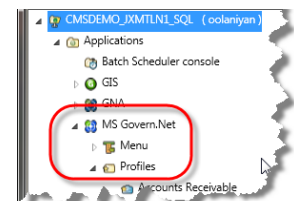
Application components can be secured by *Role* and *User*. See *Restricting Access to an Application on page 48 for details*.

## Menus and Profiles in Govern

*Menus* and *Profiles* are the sub-nodes that immediately follow the securable *Govern* application node.

### Menu

At the menu level, we see the menus that are available in the application. For the *Govern* application, when we drill-down into the *Menu*, we can see two (2) menu groups, *Data Sources*, and *View* in the *Object Explorer*. When we drill down further, we can see the sub menu's within these menus. In the application, we can see the menus that are being controlled.



- The View tab (**A**)
- View group (**1**)
- Data Sources group (**2**)

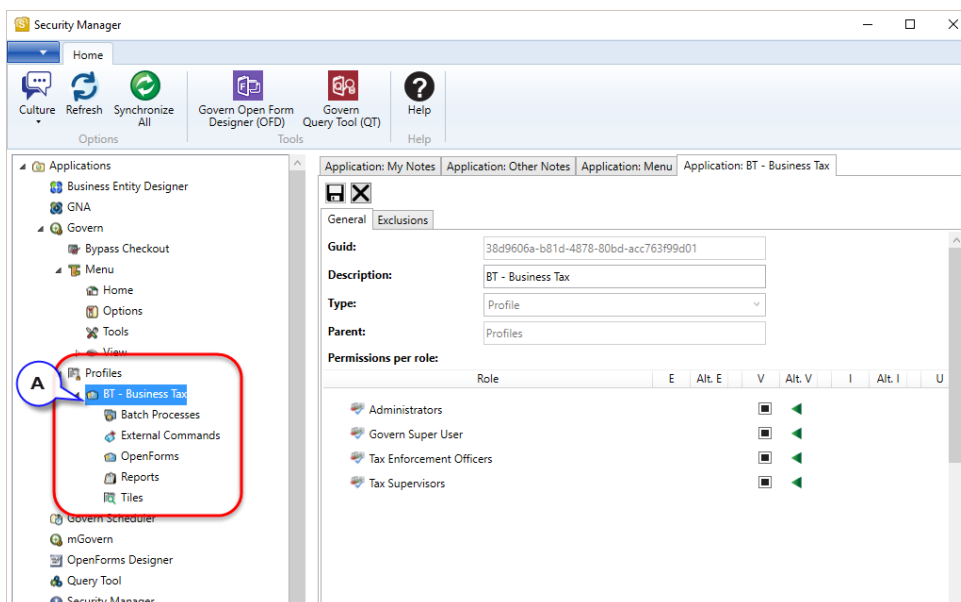
A further “drill down” will reveal that every level of the menu can be secured by **Role** or by individual **User**.

See *Restrict Access to a Menu* on page 49 for details.

## Profiles

A profile can be considered as a department, or a work environment. Profiles are a collection of *OpenForms* and *Reports*. Users of *Govern for Windows* could look at an *OpenForm* as a *Function*. For example, in a municipality with a Property Control department, our profile could be called **Property Control**. This profile would then contain the *OpenForms* (formerly called *Functions*) that would be used by the department, as well as any *Reports* that they would need to run. This setup is performed in the *Govern New Administration (GNA)*.

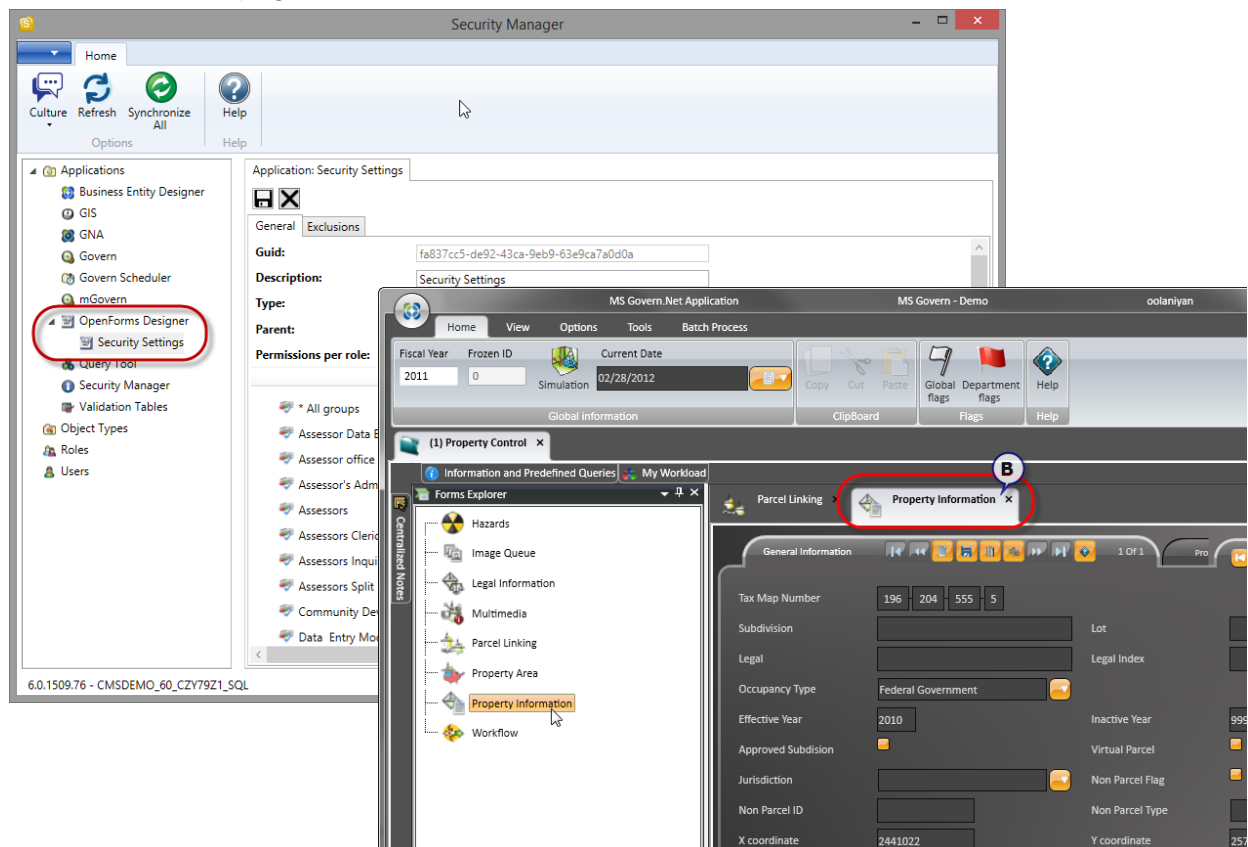
**Reports:** These are the *Govern* reports that were specified as being required by the department. As with the *OpenForms* objects, these reports can also be secured by **Role** or by **User** through the *OpenForms Designer (OFD)*.



**OpenForms:** For our Property Control Department, the *OpenForms* required are *Hazards*, *Image Queue*, *Legal information*, *Multimedia*, *Parcel Linking*,

*Decisions, Property Area, Property Information, and Workflow.* In the *GSM* when we drill down into the *OpenForms* icon, the setup that was made in *GNA* is seen. Each *OpenForm* can now be secured by **Role** or by **User**.

Below we see the *OpenForms* object in the *GSM* on the left, and its appearance in *Govern* on the right. Note that the list of *OpenForms* are displayed in *Govern* inside the *Forms Explorer*, and the *Property Information* object (**B**) appears as a tab. As we drill down further, we are able to isolate each individual object type and secure it. We are able to give a *Role* or a *User* access to one or more Profiles. See *Giving a User Access to a Profile* on page 42.

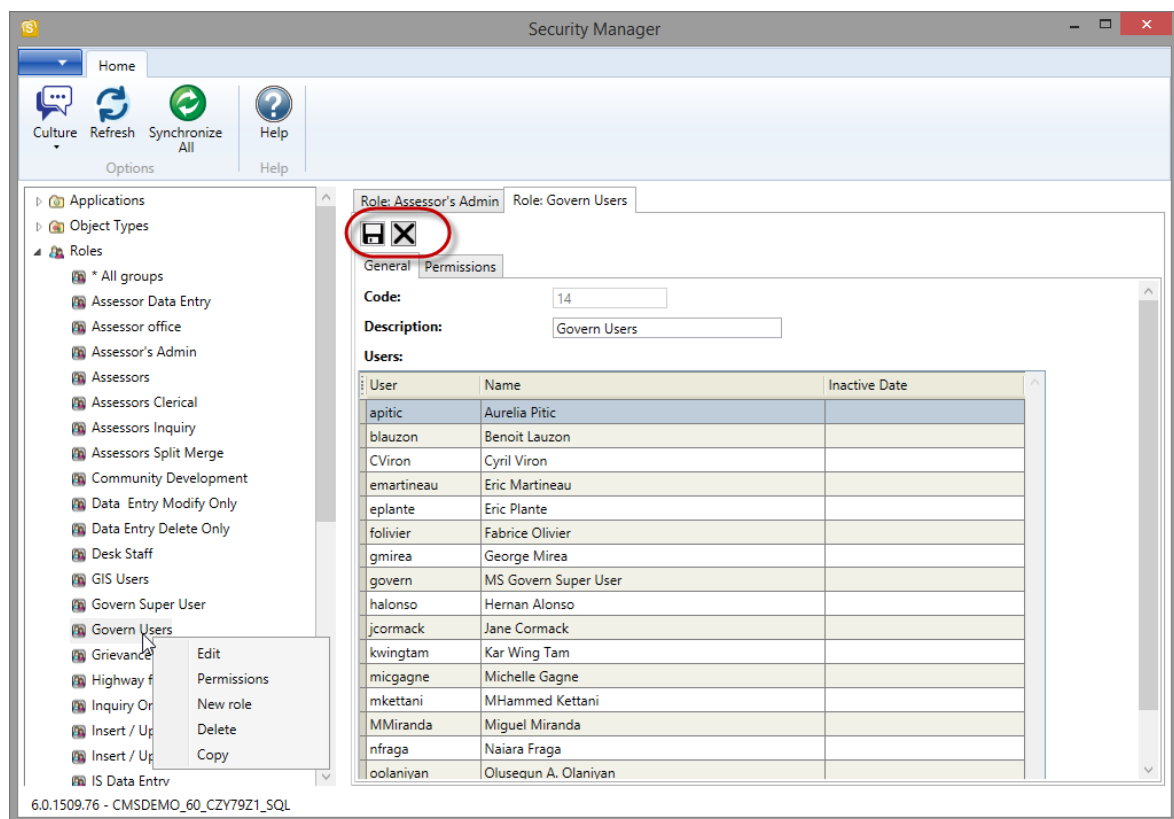


# Roles

## Overview

As stated earlier, *Roles* are best described as a collection of users and permissions. *Roles* are the equivalent of *Groups* in *Govern for Windows*. In fact during conversion of *Govern for Windows* data to *Govern* format, the groups can be set to be directly converted into *Roles*. From a municipal management standpoint, in an office there are many roles including Secretaries, Clerks, Tax Collectors, and Assessors; therefore when you have a user, they will need to be told what their functions are within the office. In addition, as in a municipal office, an employee can have multiple functions. This is also true in the *GSM*, i.e. a user can have multiple roles.

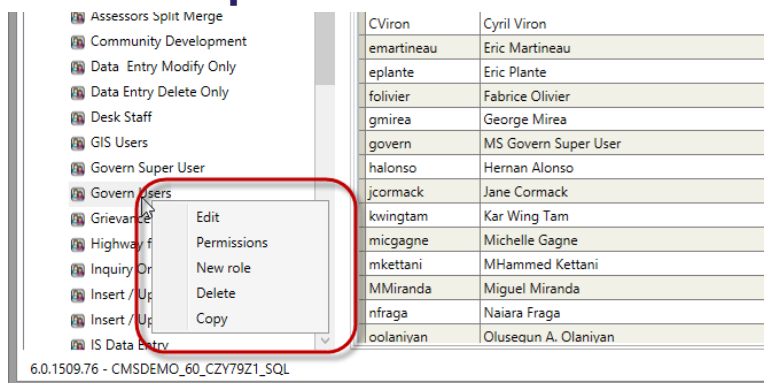
## Roles Command Buttons



**Save:** After entering or modifying any of the parameters, click **Save** to save your changes.

**Close:** Click **Close** to close the current Roles details tab.

## Roles Menu Options



When you right-click on the *Roles* object in the *Object Explorer*, you have the following menu options:

**New:** Select this menu option to create a new role.

**Refresh:** The refresh option will refresh all *Roles* object types with information from the database.

**Import Govern Roles:** This option will import any existing “Groups” from *Govern for Windows*. These groups will be imported and converted into Roles.

## Importing Govern Roles

As a time saver, *Govern for Windows* groups can be imported into the *Govern Security Manager (GSM)*. *Govern for Window* groups will be converted into Roles and any users that were in the groups will be imported into the *Roles Users* list.

**Note:** Although users are imported into their associated Roles, due to the incompatibility with the security structure of Govern and Govern for Windows, permissions will have to be re-established manually.

---

## Roles Parameters

### Roles - General tab parameters

Under the general tab you will find the parameters applicable to the Role.

**Code:** This parameter contains a system generated number identifying the role. This parameter cannot be modified.

**Description:** Enter a short, descriptive name for the Role.

**Users:** This is the list of users that are currently assigned to this Role.

### Roles - Permissions tab parameters

There are three command icons in the *Roles* object type details form. These icons are related to the creation and modification of roles.

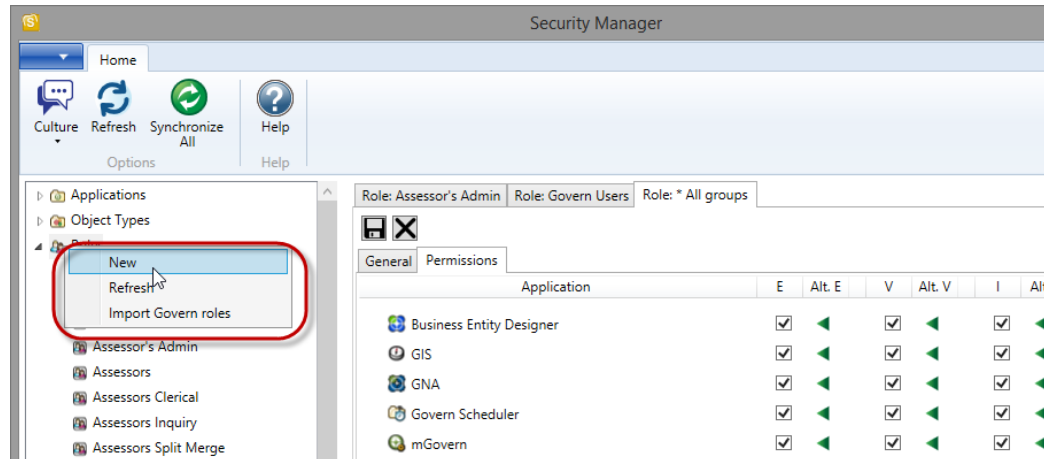
**Application:** Under the Application column is a drop-down menu list that is used to select the application that permissions will be set for. Permissions are as follows:

- **E** - Execute
- **V** - View
- **I** - Insert
- **U** - Update
- **D** - Delete

## Creating Roles

To create a new *Role*...

1. To create a new *Role*, right-click the *Roles* object type in the treeview and select New from the floating menu.



- Parameters will be presented in the *Object Details* pane on the right hand side.
- The default name is *New Role*, this will change after the *Role* has been saved.

There are two (2) tabs that are used to configure the role, General, and Permissions.

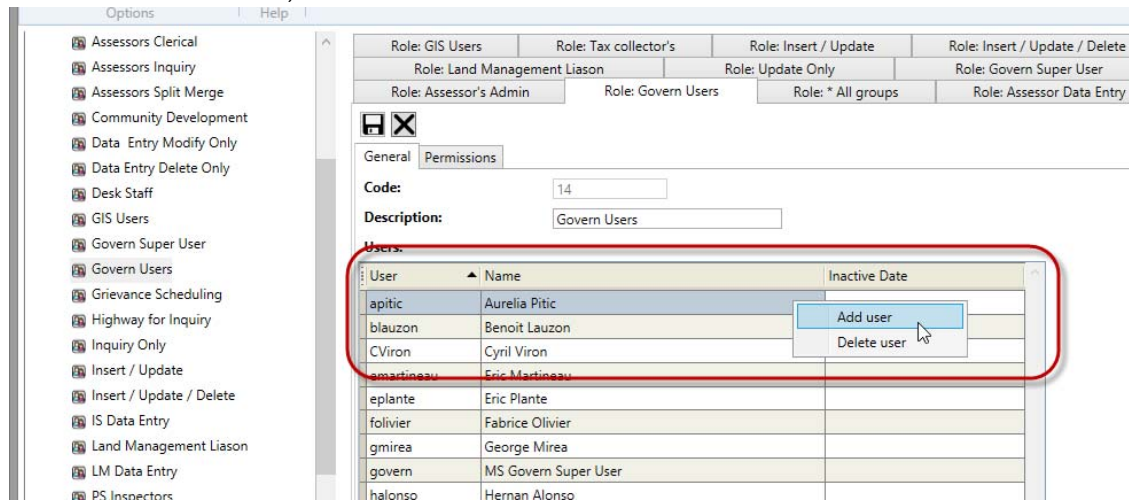
## Add or Delete Users from a Role

To Add or Delete a user...

- Click to select the *Role* that you would like to add a user to, or delete a user from.
- Right-click on the *Role*; select **Edit** from the floating menu.
- In the *Details* pane, click to select the name that you would like to delete.

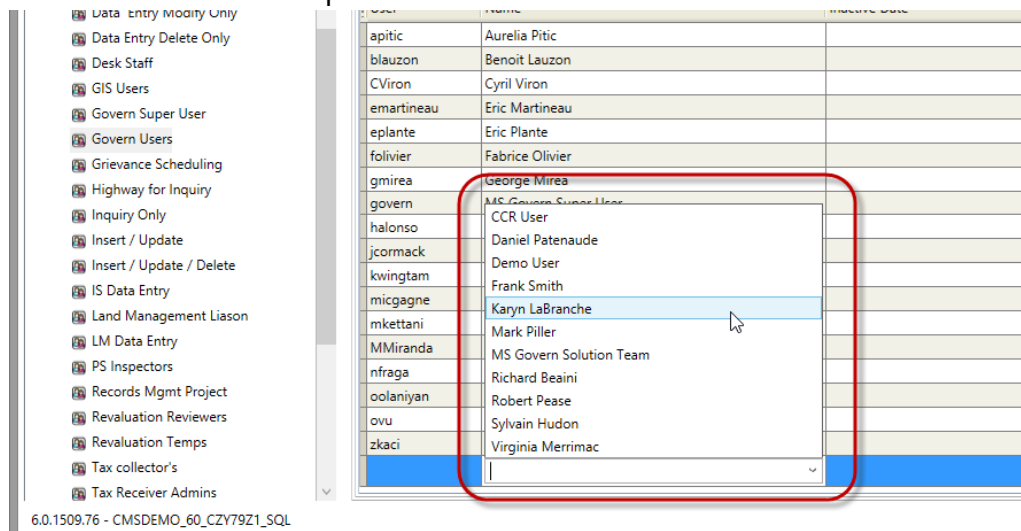


4. Right-click on the name; on the floating menu, select Add user, to add a new user, or select Delete user to delete the selected user.



**Note:** In order to be able to add a user, they must be in (Table: **USR\_USERFILE**) in *Govern Admin*.

5. Select a name from the drop-down menu list (1); click **Save** (2). Repeat as needed to add multiple names.



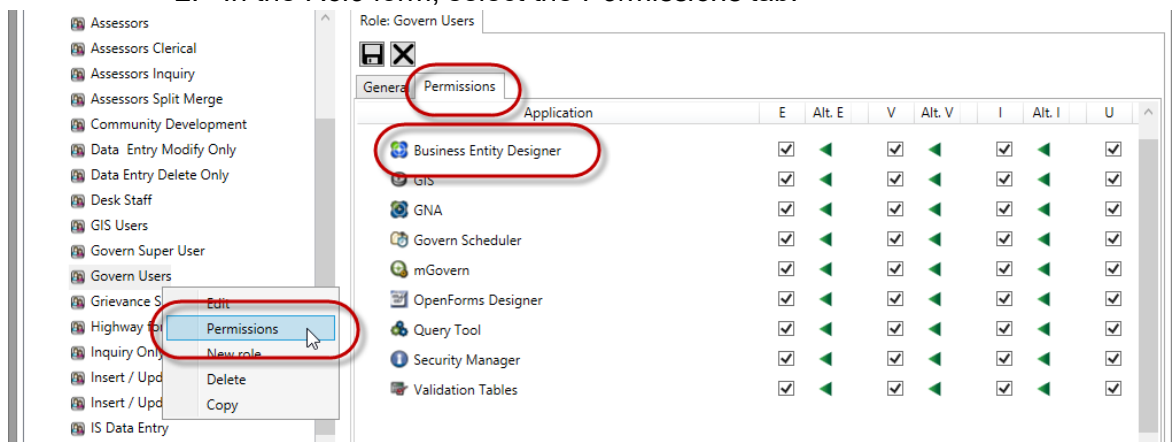
## Modifying Permissions to a Role

In the *Roles* object type, we are able to modify permissions. These permissions can apply to the *User*, the *Application*, its nodes and subnodes.

Permissions are modified through the *Permissions* tab. Under the *General* tab of the *Roles* object type, we have the list of users that are part of the role; under the *Permissions* tab, we can see and modify how users are able to access the application.

To modify user permissions in a Role...

1. Select a *Role* object type, right-click and select Edit from the floating menu.
2. In the *Role* form, select the *Permissions* tab.



3. Under the *Permission* tab, we see the application at the top level; double-click on the application to drill down.
4. When you have reached the level of the application that you want to modify, click to select the Permissions Flag to modify it.

Modifications that are made at the level that has the application name or the node or sub-node of the application will be applied to all members of the *Role*. When you want to modify permissions to an individual, then you will have to add an **Exclusion**.

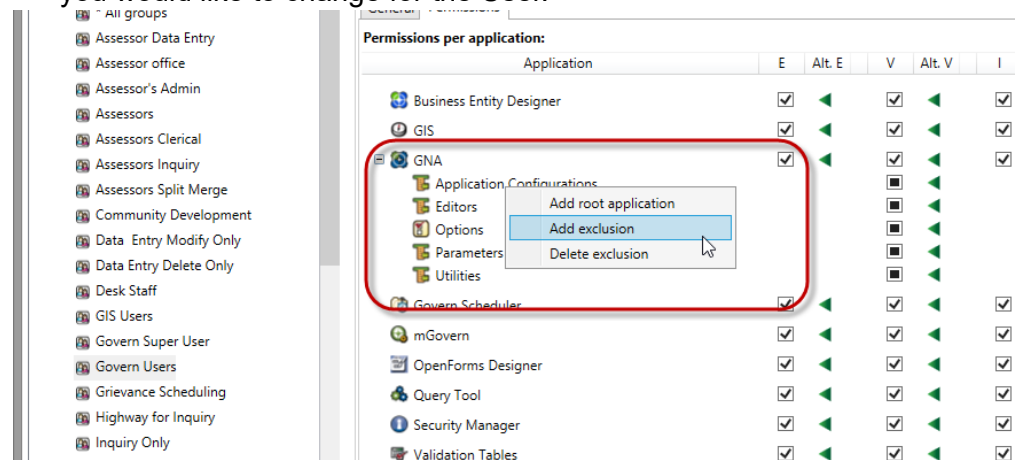
## Modify Permissions to a User in a Role (Exclusions)

Permissions to individual users within a role are modified through **Exclusions**. With an exclusion, a user that has permissions as part of a *Role*, can have those permissions removed.

**Note:** When you expand the application object type under the permissions tab, you will observe permission flags that are set to solid blue. This is an indication that the permissions have either not been set, or are inherited from the *Role*.

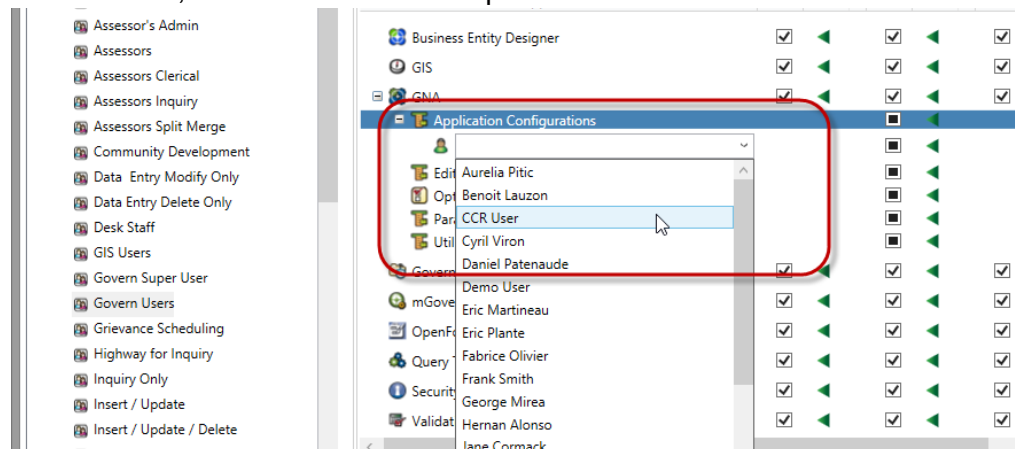
To remove permissions from a User in a Role...

1. Under the Permissions tab, drill down to the level of the application that you would like to change for the User.

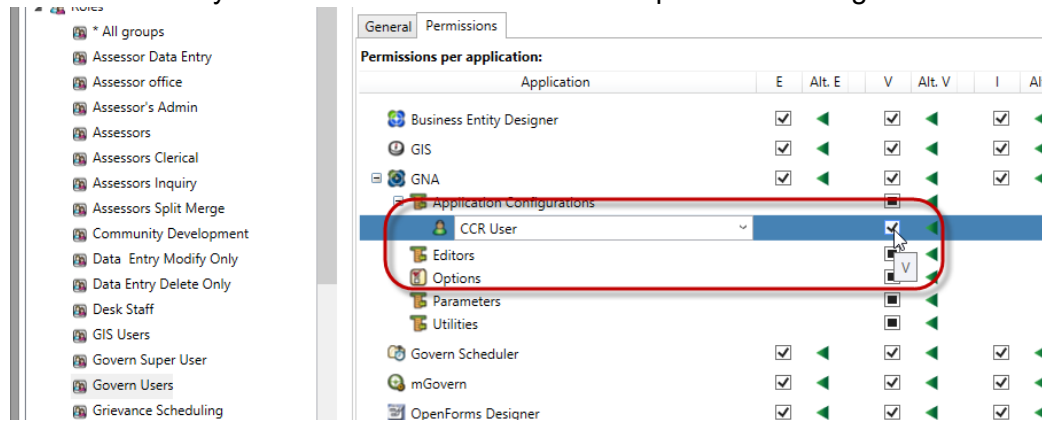


For this example we are creating an exclusion for the **Application** menu in *Govern*. If we clear the flags at this level, all members of the Role will be excluded from this menu. Since this will be for one or more individuals, we will create an exclusion.

2. Right-click on the application menu item; in the floating menu, select **Add exclusion (1)**.
3. In the user icon that appears, click to select the drop-down menu list.
4. In the list, select the user whose permissions are to be modified.



5. Individually clear the check boxes to set the permissions flags.



6. Click **Save** to save the settings.

The permissions have now been set for the individual without affecting all members of the *Role*.

## Copying a Role

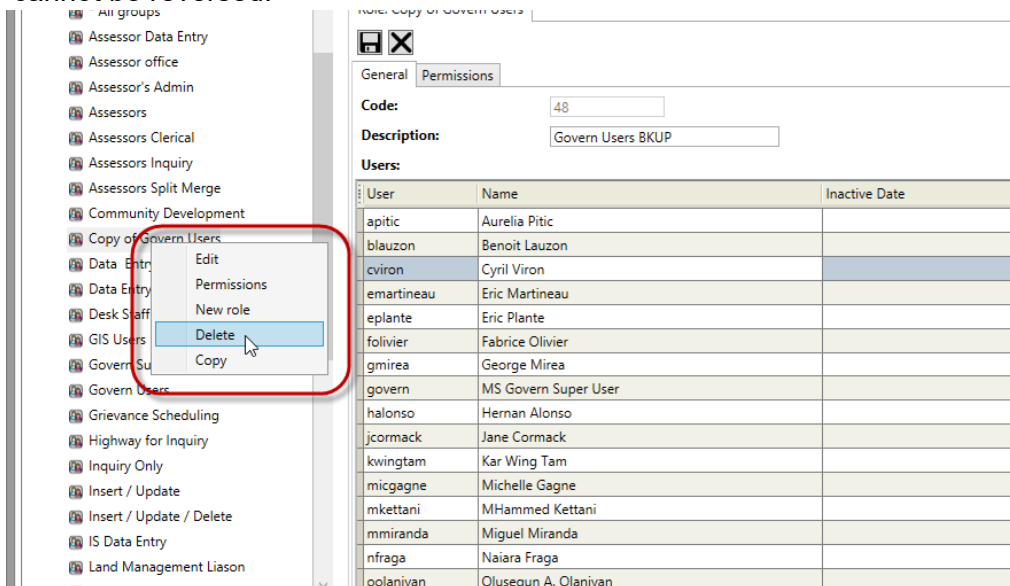
*Roles* object types can be copied. When copied, the *Role* will have the same rights of the parent role, i.e. the role that it was copied from.

To copy a *Role*...

1. Right-click on an existing *Roles* object type (**A**), (**1**), that you would like to copy.
2. In the floating menu, select **Copy** (**2**).
3. A copy of the Role is now displayed; "Copy of" is appended at the beginning of the name.

## Deleting a Role

The process of deleting a *Roles* object type is similar to that of creating; this is a permanent process and should be carried out with caution; this action cannot be reversed.



To delete a *Role*...

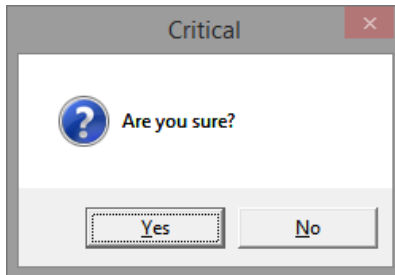
**WARNING:** All **Deletion** actions should be performed with caution; this action is not reversible

1. Right-click on an existing *Roles* object type, that you would like to delete in the *Object Explorer*.

**Note:** If displayed, this action may also be performed in the *object Explorer Details* pane.

2. In the floating menu, select **Delete** (2).
3. You will be presented with a confirmation window.

4. Click **Yes** to confirm the deletion.



## Rules of Inheritance and Creating Roles

When you are creating roles, a simple rule to follow is to create roles with the least amount of permissions at the top of your hierarchy. This means that sub roles that are created can then have their permissions increased. For example, we want two types of assessors, regular assessors, and the ones that will have added permissions, e.g. a supervisor.

In this situation, it is recommended to create a role for the regular assessors first. The logic behind this is that until permissions are manually set, a role that is created as a sub role will inherit the permissions of the parent. Therefore if you start by creating an assessor with supervisor permissions, those permissions will be inherited by a sub role. Whenever changes are made to the "parent", they will be inherited by the "child". In the end, it is better to have users that inherit a minimum of permissions than to risk creating a series of Super Users. The worst case scenario is that you will have to add permissions to a sub-role, rather than having to individually manage users that have all permissions.

The above rule applies to all cases where inheritance of permissions are involved, e.g. *Users* and *Roles*.

# Users

## Overview

A *User* is the individual that requires access to the application. This access can be managed by the *Govern Security Manager (GSM)* on an individual user basis, or by the roles that they are members of. In order for a user to be managed by the *GSM*, they must be in (Table: USR\_USERFILE) in the *Govern* database.

## Viewing Users

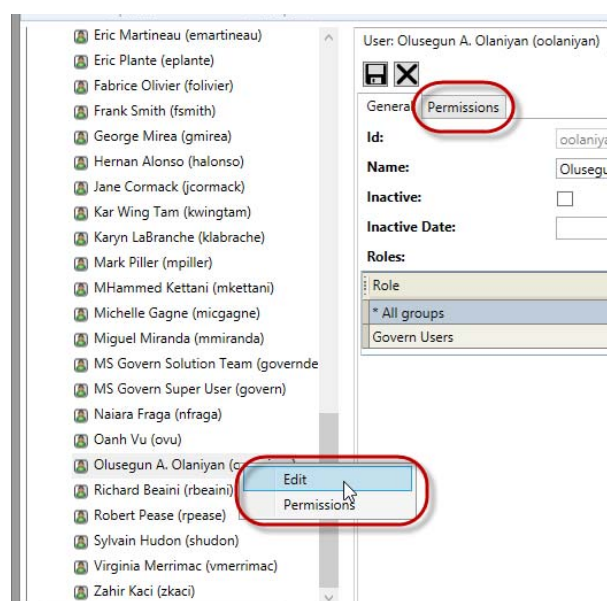
To view users that are currently in the USR\_USERFILE table in the database...

1. In the *Object Explorer*, double-click on the **Users** icon.
2. When the *User* icon expands, a list of the user ID's are displayed. Users will also be displayed in the *Details pane* on the right hand side.

## Editing a User

When we refer to editing the properties of an existing user, we can edit the following:

- **Name** - This is the username, and should not be confused with the ID; the user ID cannot be modified.
- **Inactive / Inactive Date** - These parameters are used to display the status of the user. When the *Inactive Date* that is selected in the **Inactive Date** parameter has been reached, a check mark will be displayed to indicate that the user does not have access.



- **Roles** - The role(s) that the user is a part of (4).
- **Permissions** (tab) - Select this tab to display the access rights that this user has to the application.

To edit the properties of an existing user...

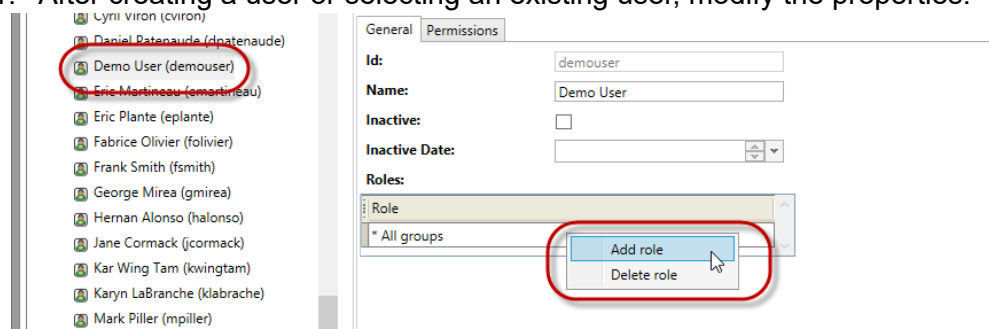
1. Right-click on the icon for the user in the *Object Explorer* or the *Details* pane.
2. In the floating menu, select *Edit*, *Permissions*, or *Copy*

## Adding a User to a Role

A single user can have one or more roles. A user can be added to a Role under the *General* tab of the *User* edit form.

To add a *User* to a *Role*...

1. After creating a user or selecting an existing user, modify the properties.



2. Under the **General** tab, locate the **Roles:** parameter.
3. Right-click inside the *Roles* parameter and select **Add role**.
4. Click **Save** to save your changes.

This process can be repeated if it is required for a user to have several roles.

## Removing a User from a Role

A user can be removed from a role under the *General* tab of the *User* edit form.

To add a *User* to a *Role*...

1. After creating a user or selecting an existing user, modify the properties.



2. Under the **General** tab, locate the **Role:** parameter.
3. Click to select an existing Role.
4. Right-click inside the *Roles* parameter and select **Delete role**.
5. Click **Save** to save your changes.

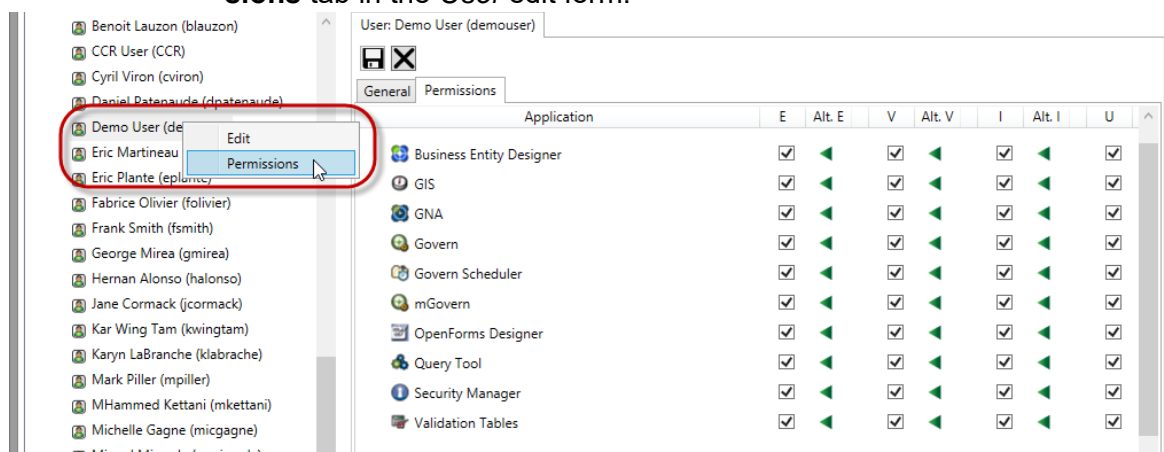
Once completed, the user will no longer be part of the deleted role, nor will they have any of the permissions associated with the role.

## Giving a User Access to a Profile

It is sometimes required for a User to have access to one or more departments. In the GSM, this would be the equivalent of a user being able to access multiple profiles. This can be done through permissions. When a user is given access in this manner, an exclusion is automatically created under the profile.

To give a user access to a *Profile*...

1. Select a user; right-click on the user and select *Edit*; click the **Permissions** tab in the *User edit* form.



2. With a new user, if no application has been added, right-click in the area under *Application* and select **Add Root Application** from the floating menu.
3. Double-click on the root application until you reach *Profiles*.

4. Under the Permissions column select the checkbox and click until the check mark appears.

**Note:** When you click on a Permissions flag, the check box will appear in three (3) possible states, a solid or filled state indicating inheritance, a checked state that indicates selected, and clear state that indicates deselected. See *Permission Flags* on page 43 for details.

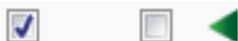
Setting the permissions at this level will give the user access to all profiles. If it is only specific profiles that you would like to limit access to, then double click to drill down to the next level which will list the individual profiles. Repeat this process for each profile required.

## Permission Flags




In an application, it is necessary to control which areas users are permitted to access. Likewise when dealing with sensitive information, it is important to be able to determine who can and cannot modify this information. In the GSM this level of control is achieved through the *Permissions* form. In the Permission form, check boxes or “Flags”, can be set for Roles and / or Users.

### Setting Permission Flags

In the GSM, the check box for the permissions can appear in three (3) possible states.




User of previous, i.e. pre Release 6.0 versions of the GSM will notice the absence of the “Solid Blue” state that indicates that the parameter has “inherited” the setting of the parent that it was copied from.

-  **Solid (inheritance)** - This indicates that this permission will be inherited from the role.
-  **Cleared (disabled)** - An indication that the permission has not been selected and access has not been granted.
-  **Checked** - The check mark indicates that the permission is selected, i.e access is granted.

## Two (2) State Check Boxes

In release 6.0 and higher, only two (2) state Check Boxes are used for Top Level items in the GSM.

-  **Like...** - The green “**Like...**” arrow indicates that permission to access alternate, e.g. historical data, will be “like” the setting that the arrow is pointing to. This means that the flag will be set to be the same as the one on the immediate left of the green arrow. See *Access to Alternate or Historical Data* below.

## Access to Alternate or Historical Data

When permissions are granted to a user, role, or application, it is granted for access to data for the current fiscal year. Conditions may require that access to alternate or historical data should not be given to users. When this is the case, there is an **Alternate** column in the *Details* pane of the *Object Explorer*. The function of the *Alternate* column is to grant access to *Alternate* data. For example, you may want to grant a user or role access to, Execute (E), View (V), and Insert (I) data for their current year, but they cannot View (V) historical data.

**Note:** When viewing alternate data records in Govern, the OpenForm entity tab will display a Yellow dot. This is an indication that the data is subject to Alternate Permission settings.

## Setting or Changing the Alternate Permission flag

By default the setting for the *Alternate security* is to be the same state as that of the regular security. This means that the alternate or historical data can be accessed with the same permission settings as the check box on the immediate left.

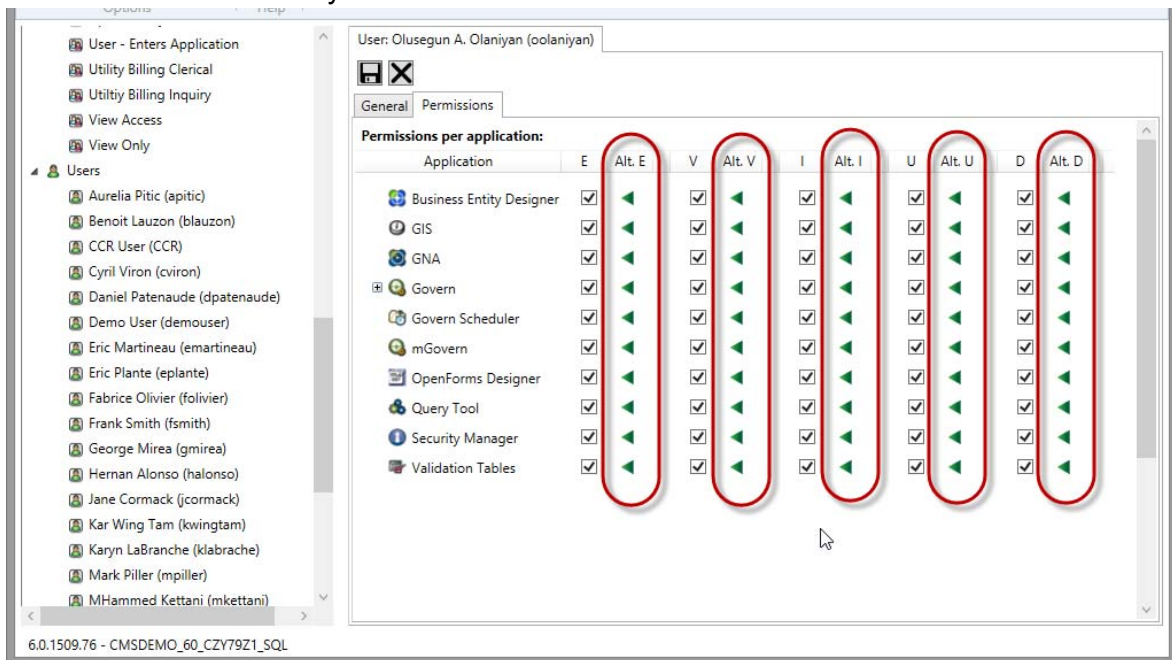
An easy way to tell what access is given to alternate/historical data is to look at the icon that represents the state. If the **Like...** arrow is visible, then the permission is the same or “like” that of the current year.

To change the Alternate permission flag...

1. Locate the Alternate column in the Details pane.
2. Click the **Like...** arrow to change the *Alternate* permission setting.

Multiple clicks under the column will cycle through the three (3) standard state, *Cleared*, *Checked*, and *Solid*.

3. In order to set the flag back to the **Like...** state, you must hold down the **Shift** key and then **Click**.



**Note:** The click on the **Like...** alternate flag will clear the setting, i.e. the user has no access to alternate/historical data. To re-establish the **Like...** flag, hold down the **Shift** key then click the flag.

## Parent and Child Object Inheritance

One rule that the GSM follows is that of *Parent /Child Inheritance*. This means, when a sub object type is created or found underneath an object type at a higher level, the sub object type will “inherit” the properties of the parent. This inheritance can be seen in areas of the GSM. For example, when a sub Role is created from a Role, or when we see a menu and sub menu items, or Profiles and their sub items.

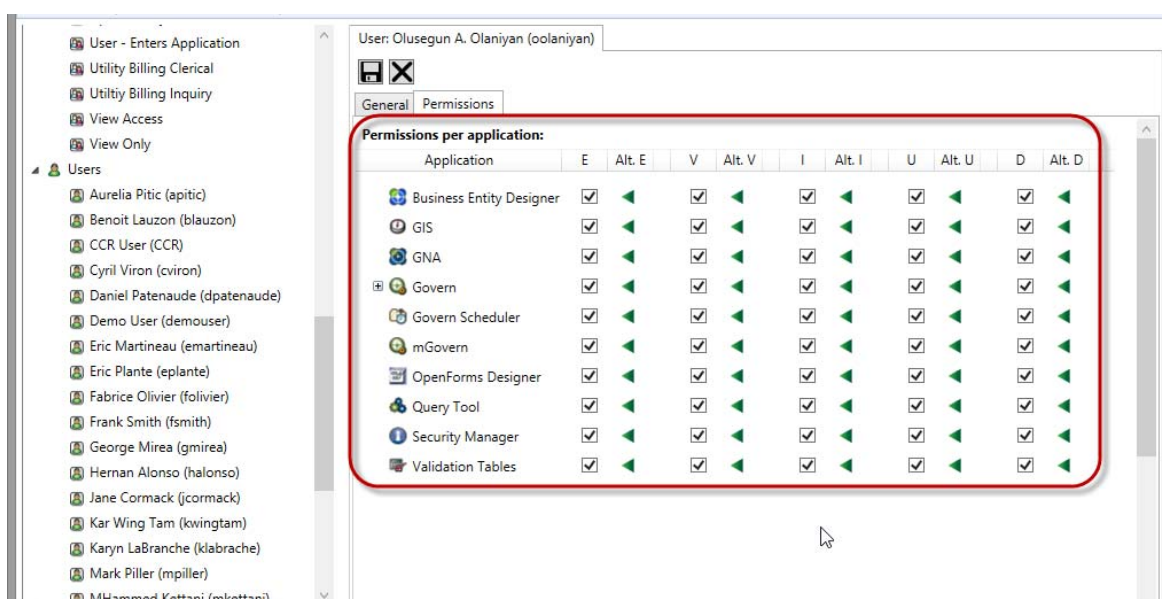
When a child object inherits the permissions of a parent object, Each child object gains the base permissions of the parent, and will remain in that state until those permissions are overwritten. This also means that if permissions are changed in the parent, any child that inherits those permissions will also assume the new settings of the parent. This can be a time saver when setting up users, but can also have a drawback in that you may not necessarily want

the child permissions to change. See *Rules of Inheritance and Creating Roles* on page 39 to see how this can relate to Roles.

## Types of Permission Flags

The Flags (**A**) that can be set are as follows:

- **E** - *Execute* allows the user to run or execute something like a query.
- **Alt. E/V/I/U/D** - The Alt. (alternate) column allows you to set the flag for user access to alternate or historical datatypes. Refer to *Setting or Changing the Alternate Permission flag* on page 44 for details.
- **V** - *Visible* - The area will be visible to the user
- **I** - *Insert* - The parameter will allow users to insert a record into the database.
- **U** - Set the *Update* a record flag to allow the user to update records.
- **D** - Set the *Delete* flag to allow the user to delete a record.



User: Olusegun A. Olaniyan (oolaniyan)

General Permissions

Permissions per application:

Application	E	Alt. E	V	Alt. V	I	Alt. I	U	Alt. U	D	Alt. D
Business Entity Designer	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
GIS	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
GNA	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Govern	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Govern Scheduler	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
mGovern	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
OpenForms Designer	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Query Tool	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Security Manager	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Validation Tables	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

**Note:** Not all flags will apply to all object types or sections within the application. For example a menu item like **Paste**, would only have two permissions to set, (**E**)xecute and (**V**)isible. Permissions like (**D**)elete or (**I**)nsert, would not apply.

## Using Permission Flags

The user permission flags are the key to restricting access to an application or the object types within the application.

The following grid will serve as a guide to which permissions you should disable, in order to restrict access to an object type.

Object Type (Description)	Permission Flag(s) to Disable				
	(E)xecute	(V)iew	(I)nsert	(U)pdate	(D)elete
Applications	x	<b>X</b>	x	x	x
Govern Scheduler	<b>X</b>				
GIS App Items		<b>X</b>			
GIS Base Map		<b>X</b>			
GIS Client Map		<b>X</b>			
GIS Configuration		<b>X</b>			
Main Open Forms	<b>X</b>				
Main Profile	<b>X</b>				
Main Reports	<b>X</b>				
Menu	x	<b>X</b>			
Open Forms Designer	<b>X</b>				
Open Form	<b>X</b>				
Profile		<b>X</b>			
Query Tool		<b>X</b>			
Query Tool Entity		<b>X</b>			
Query Tool Entity Set		<b>X</b>			
Report	<b>X</b>				
Validation Tables		<b>X</b>	x	x	x
System Validation Tables		<b>X</b>	x	x	x
User Validation Tables		<b>X</b>	x	x	x
List of Users		<b>X</b>	x	x	x

Object Type (Description)	Permission Flag(s) to Disable				
	(E)xecute	(V)iew	(I)nsert	(U)pdate	(D)elete
Matix		<b>X</b>	x	x	x
Matix Base Map		<b>X</b>	x	x	x
Matix Theme Map		<b>X</b>	x	x	x

**Note:** The “X” under the permission is an indication that the Flag should be cleared (disabled). When a permission flag has an “X” in bold, it means that although all the recommended flags should be cleared, the Permission with the bold “X” is the only one required.

## Restricting Access to an Application

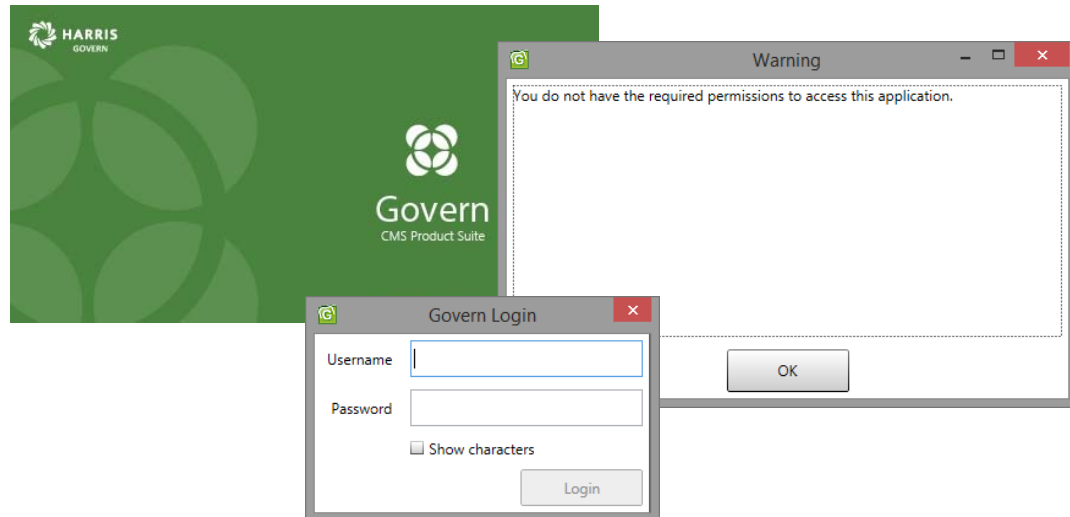
To remove user access to an application, looking at the above grid, you would need to be at the *Applications* level. The access right that is to be removed is the ability to **Execute** the application; note that securities can be effected by *Role* or by *User*.

### By Role

To restrict access to an application by *Role*...

1. Locate the Applications icon in the *Object Explorer*.
2. Right-click on the application icon select **Edit**.
3. In the *Details* pane, click to select the **General** tab.
4. Under *Permissions per role*:, click to select the role that the access is to be removed from.
5. Click under the **E** column to clear the *Execute* flag; Click **Save** to save the settings.

The next time the users that are members of the modified roles attempt to access the application, they will be denied access.



If it is required to restrict access on an individual basis, i.e. by User, then the following can be used.

## By User

To restrict access to an application by *User*...

1. In the *Details* pane, click to select the **Exclusions** tab.
2. Under the *User* list, click to select the User that the access is to be removed from.
3. Click under the **E** column to clear the *Execute* flag; Click **Save** to save the settings.

## Restrict Access to a Menu

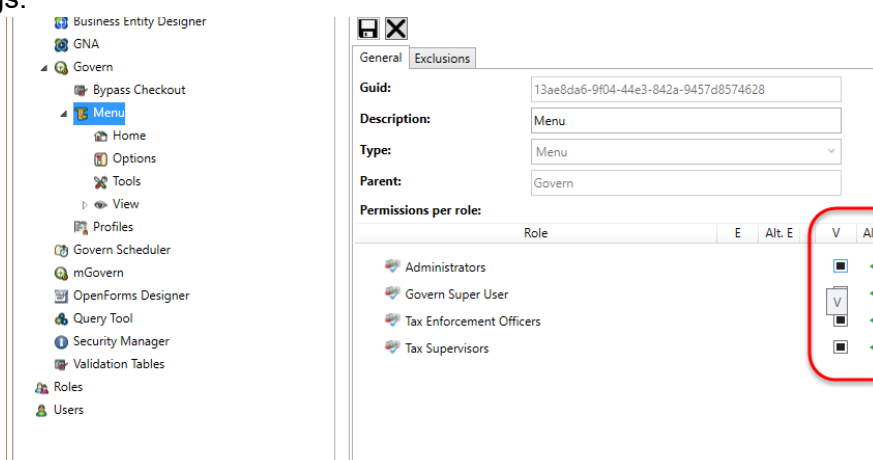
To remove user access to a menu, you would need to be at the *Applications* level. Restricting access to a menu can be carried out in two (2) ways. Looking at the *Permissions Flag* grid, see *Using Permission Flags* on page 47, we see that we can remove the ability to **Execute** the menu, or hide the menu, i.e. disabling the **View** flag. Recommendation is to hide the menu; if a user cannot see the menu, they cannot attempt to gain access to it.



## Restrict Access By Role

To restrict access to a menu by *Role*...

1. Locate the Applications icon in the *Object Explorer*.
2. Double click to “drill down” to the **Menu** or **Sub menu** level.
3. Right-click on the Menu and select **Edit** from the floating menu.
4. In the *Details* pane, click to select the **General** tab.
5. Under *Permissions per role*:, click to select the role that access is to be removed from.
6. Click under the **V** column to clear the View flag; Click **Save** to save the settings.



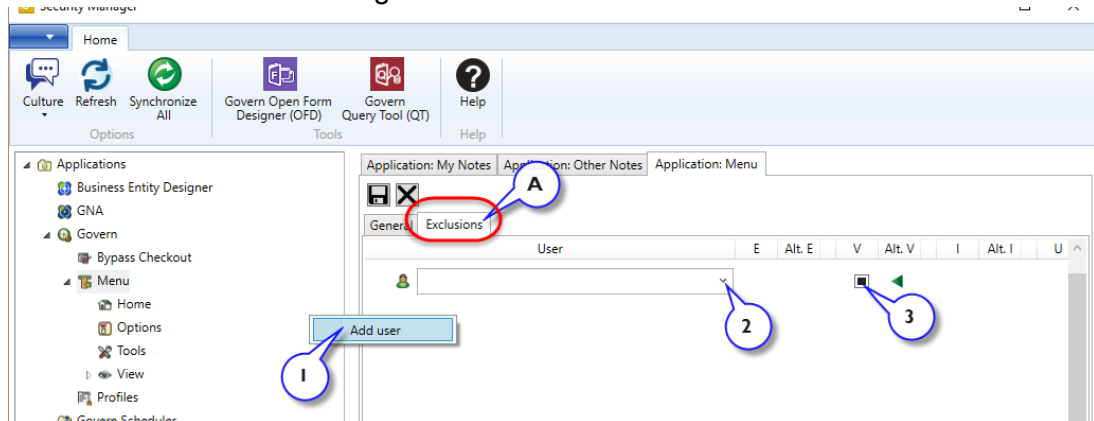
All members of this *Role* will now be restricted from accessing the application.

## Restrict Access By User

To restrict access to a menu by *User*...

1. In the *Details* pane, click to select the **Exclusions** tab.
2. Under the *User* list, right-click and select **Add user** to add a new User.
3. Click the drop-down menu list and select a user.

## 4. Clear the *View* flags to remove access.



## 5. Click **Save**.

The user will now be restricted from accessing the application, but other members of the *Role* will not.

## Restrict Access to a Profile

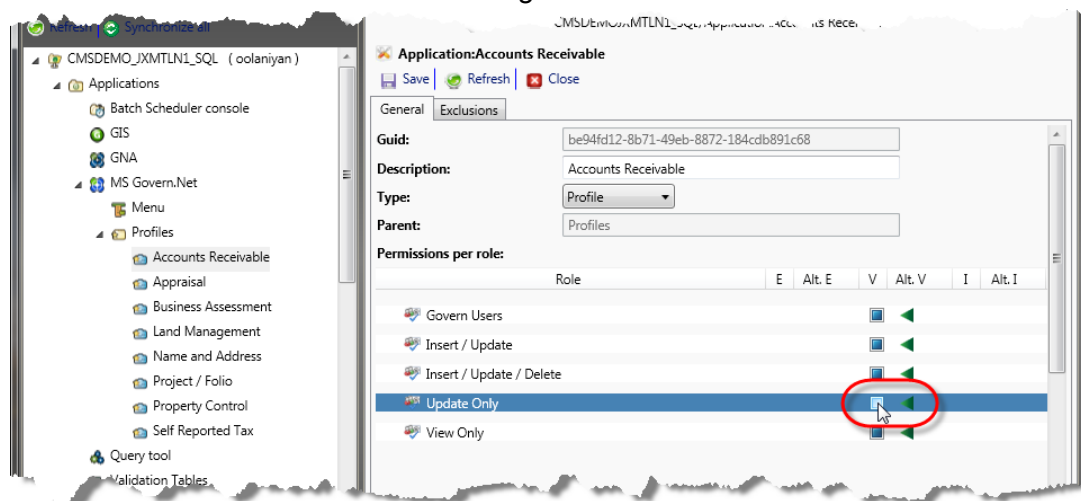
The methodology for restricting user access to a profile is the same as that used for restricting access to an application or a menu. Restricting access to a profile can be carried out in two (2) ways. Looking at the *Permissions Flag* grid, see, *Using Permission Flags on page 47*, we see that we can remove the ability to **View** the profile, i.e. disabling the **View** flag; if the user *cannot see it*, they *cannot use it*.

## Restrict Access By Role

To restrict access to a profile by *Role*...

1. Under the Applications component, drill down to the Govern component in the *Object Explorer*.
2. Double click to “drill down” to the **Profiles** node; double-click to access the sub-node.
3. Right-click on the specific *Profile* and select **Edit** from the floating menu.
4. In the *Details* pane, click to select the **General** tab.
5. Under *Permissions per role*:, click to select the role that access is to be removed from.
6. Click under the **V** column to clear the *View* flag.

7. Click **Save** to save the settings.

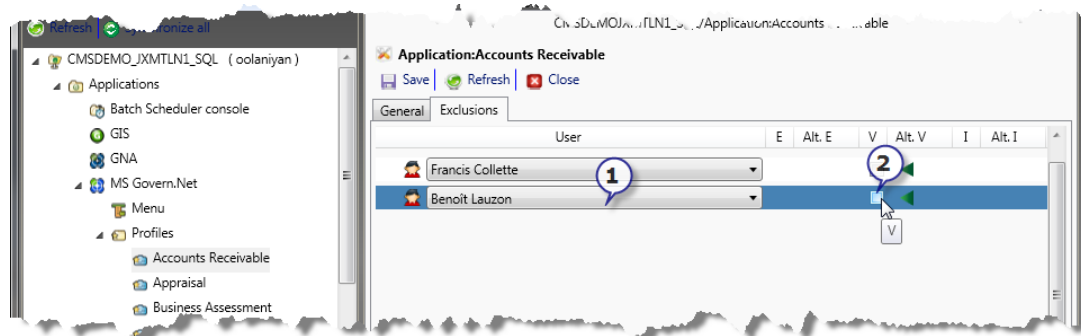


All members of this *Role* will now be restricted from accessing the profile.  
Repeat the above procedure for each profile required.

## Restrict Access By User

To restrict access to a profile by *User*...

1. In the *Details* pane, click to select the **Exclusions** tab.
2. Under the *User* list, right-click and select **Add user** to add a new User.
3. Click the drop-down menu list and select a user (1).
4. Clear the *View* flag to remove access (2).



5. Click **Save**.

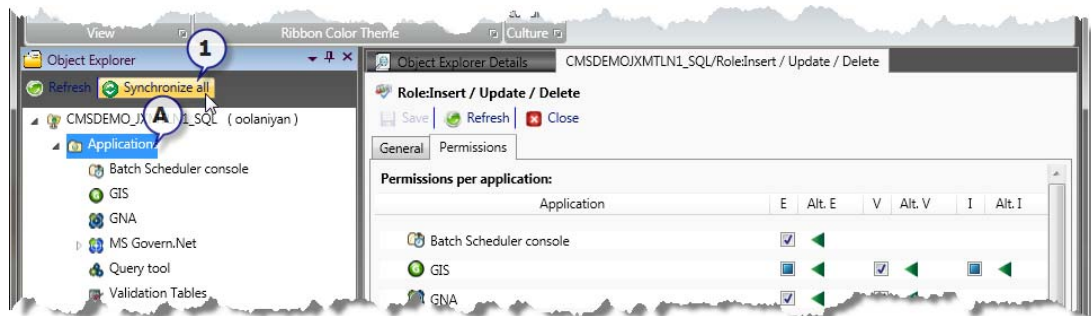
The user will now be restricted from accessing the profile, but other members of the *Role* will not.

## Securing Profiles

When *Profiles* are created in the *Govern New Administration (GNA)*, before a user is able to access it, the securities must be set. This process will require a synchronization.

To secure an application...

1. Create the profile using the *Profile Editor* in *GNA*. For details on creating a new *Profile*, refer to the *Govern New Administration Release 6.0* guide.
2. In the *Govern Security Manager (GSM)*, go to the Application level (**A**) in the *Object Explorer*, pane and click to select the *Applications Component*, click *Synchronize All* (**1**).



3. When the *refresh* process is complete, verify that the securities for the specific profiles is set.

*Profiles* can be secured by *User* or by *Role*. Refer to *Restrict Access to a Profile* on page 51 for details.

## Working with Centralized Notes in Govern

The *Centralized Notes* system in *Govern 4.7* and greater, is designed to allow users to enter and store notes in a centralized storage location. When enabled in the *Business Entity Designer (BED)*, the *Centralized Notes System* enables users to be able to review and edit notes made by other authors. See *Centralized Notes in the Govern user guide*.

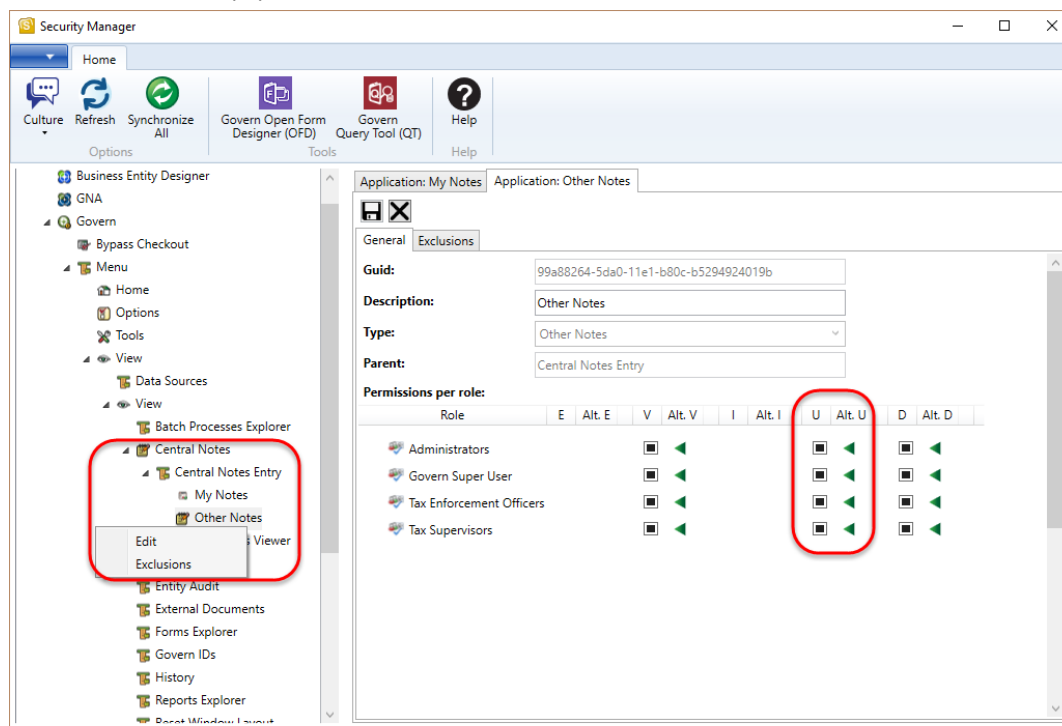
By default, only the notes that have been entered by the author can be modified. When the correct flags have been set in the *BED*, and the following

security settings have been made, users will then be able to edit notes entered by other users.

## Allow Users to Modify Centralized Notes

To ensure that a user is able to modify all Centralized Notes entries...

1. In the Govern Security Manager (**GSM**), in the left hand *Object Explorer* pane, “drill down” *Applications > Govern > Menu > View > Central Notes > Central Notes Entry and Central Notes Management*.
2. Right-click on each of these icons and select **Edit**.
3. In the *Object Explorer* details pane, ensure that the permissions flag for Update (**U**) has been set.



After completing the above process the users will be able to modify all *Centralized Notes* entries.

## Prevent Modification of Centralized Notes

To prevent user modification of *Centralized Notes*...

1. In the Govern Security Manager (**GSM**), in the left hand *Object Explorer* pane, “drill down” *Applications > Govern > Menu > View > View > Central Notes > Central Notes Entry > My Notes* or **Other Notes**.
2. Right-click on the *My Notes* icon, s and select **Edit**.
3. Click to ensure that the permissions flag for *Update (U)* is cleared.

## Prevent Addition of Centralized Notes

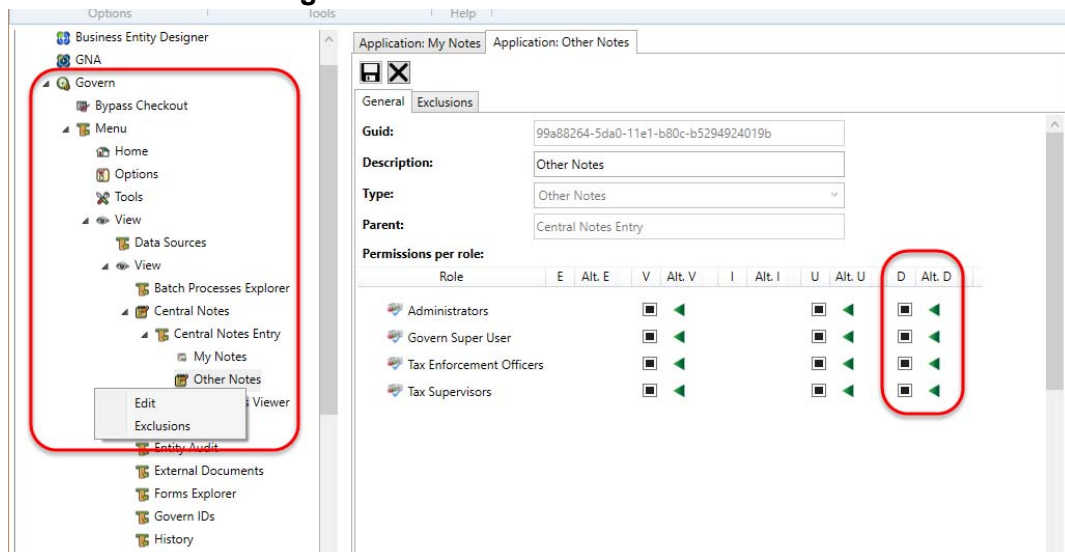
There are scenarios wherein the user can only view notes, but cannot actively add notes. To prevent user addition of *Centralized Notes*...

1. In the *Govern Security Manager (GSM)*, in the left hand *Object Explorer* pane, “drill down” *Applications > Govern > Menu > View > Central Notes > Central Notes Entry* and **Central Notes Management**.
2. Right-click on the *Central Notes Entry* icons and select **Edit**.
3. Click to ensure that the permissions flag for *Insert (I)* is cleared.

## Prevent Deletion of Centralized Notes

When it is required that a user **not** to be permitted to delete entered notes...

1. Open the *Govern Security Manager (GSM)*; in the left hand *Object Explorer* pane, “drill down” to *Applications > Govern > Menu > View > Data Sources > View > Central Notes > Central Notes Entry* and **Central Notes Management**.

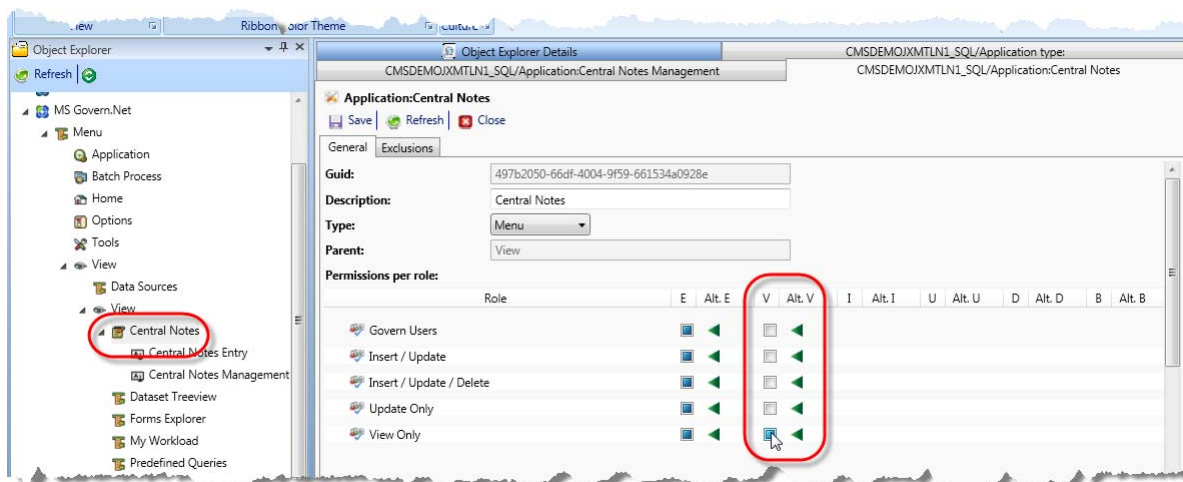


2. Right-click on the icons and select **Edit**.
3. In the *Object Explorer* details pane, ensure that the permissions flag for Delete (**D**) has been cleared.

## Hide the Centralized Notes Pane

When it is not required for the user to view *Centralized Notes*, i.e. hide the pane and all tabs, configure security flags in the *GSM* as follows...

1. In the *GSM* drill down to the *Central Notes* level in the *Object Explorer* pane; use the following path *Applications > Govern > Menu > View > View > Central Notes*
2. Right-click on the *Central Notes* icon; select **Edit** from the floating menu.
3. In the *Object Explorer Details* pane, if not selected, click to select the **General** tab.
4. Under the *View (V)* column, click to clear all flags for all roles that are not required to view the *Centralized Notes*.
5. Under the **Alt. V** column, ensure that the green arrowhead is present for all required roles.



**Note:** No Synchronization process is required when modifying security for Centralized Notes.

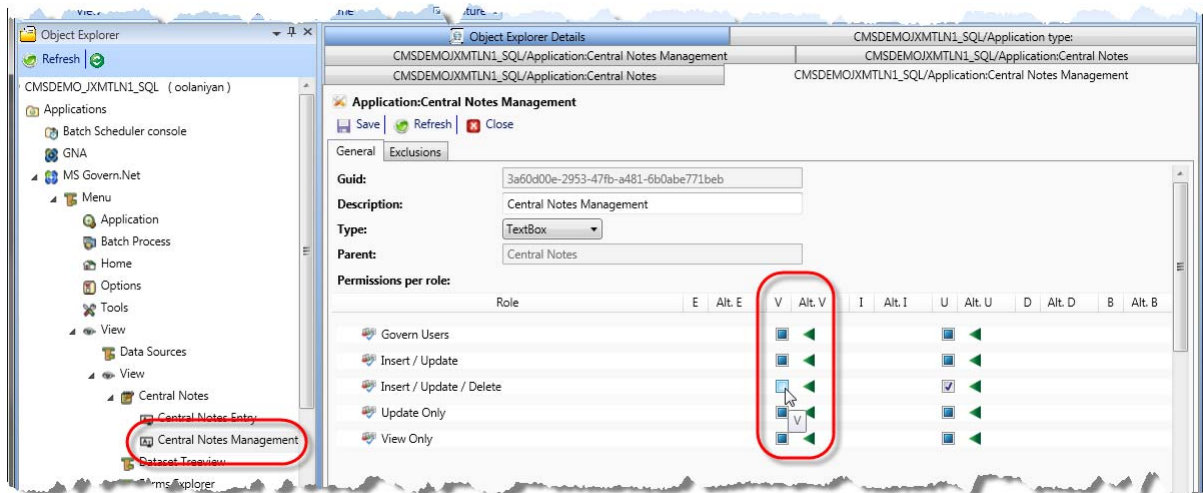
When completed, the user will not see the *Centralized Notes* pane, or the button in the *Govern* ribbon.



## Hide the Centralized Notes Management tab

Users that are required to enter *Centralized Notes*, but do not need to have access to the filters in the *Centralized Notes Management* tab, should configure security as follows...

1. In the *GSM* drill down to the *Central Notes* level in the *Object Explorer* pane.
2. Double click on the *Central Notes* icon to display the two nodes that represent the entry tab and the management tab.
3. Right-click on the *Central Notes Management* icon; select **Edit** from the floating menu.
4. In the *Object Explorer Details* pane, if not selected, click to select the **General** tab.
5. Under the **View (V)** column, click to clear flags for all roles that are not required to view the *Centralized Notes Management* tab.
6. Under the **Alt. V** column, ensure that the green arrowhead is present for all required roles.



**Note:** No *Synchronization* process is required when modifying security for Centralized Notes.

When completed users will view the *Centralized Notes Entry* tab, but they will not have access to the *Management* tab in *Govern*.



---

## Working with Global Messages in Govern

The *Global Messages* system introduced in *Govern 5.1* and greater, is designed to allow users to associate messages to a record or recordset. These records will be linked via one of several primary keys, e.g. *Parcel ID*, *Name ID*, *Building ID*, etc. When enabled in the *Govern Security Manager (GSM)*, messages created, reviewed, edited, and deleted by other users, based upon permissions. See *Global Messages in the Govern 5.1 user guide* for full details.

**Note:** Users that do not see securable nodes for Global Messages under the Applications column in the GSM should verify the version of their version of the GSM, i.e. release.5.1 or greater, then perform a **Synchronize All** action followed by a **Refresh**.

When the security has been set, users may be allowed to create messages that are viewed by all users. i.e. Global, or ones that are restricted to members that are in the same department as the message author.

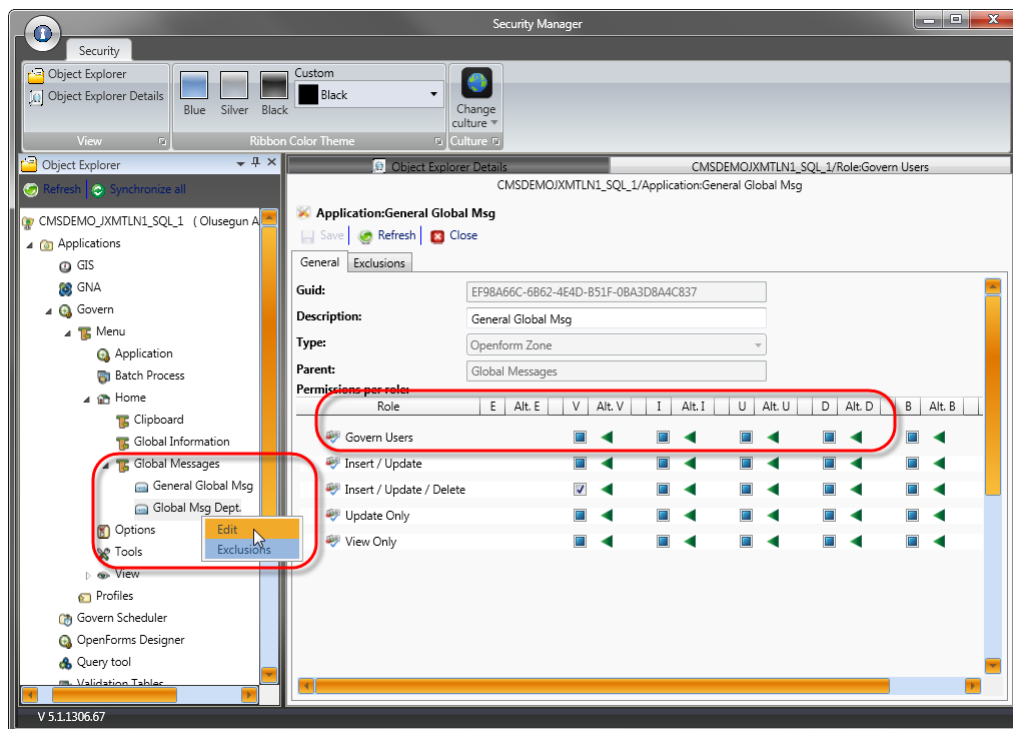
### Allow Users to Modify Global or Department Messages

**Note:** The following example is given with the understanding that the user has been granted prior **View | Alt V**, permissions for **General Global Msg** and **Global Msg Dept**. In all instances the permissions will be granted for both global and department messages. If this is not desired, simply select the icon that corresponds to the type of message that is required.

To ensure that a user is able to see all *Global/Department Messages*...

1. In the Govern Security Manager (**GSM**), in the left hand *Object Explorer* pane, “drill down” *Applications > Govern > Menu > Home > Global Messages > General Global Msg* and **Global Msg Dept**.
2. Right-click on each of these icons and select **Edit**.

3. In the *Object Explorer* details pane, ensure that the permissions flag for Update (U) has been set for the role.



After completing the above process the users will be able to modify all *Global Messages* entries.

## Prevent Modification of Global Messages

To prevent user modification of *Global Messages*...

1. In the Govern Security Manager (**GSM**), in the left hand *Object Explorer* pane, "drill down" *Applications > Govern > Menu > Home > Global Messages > General Global Msg* and *Global Msg Dept.*
2. Right-click on each of these icons and select **Edit**.
3. Click to ensure that the permissions flag for *Update (U)* is cleared.

## Prevent Addition of Global Messages

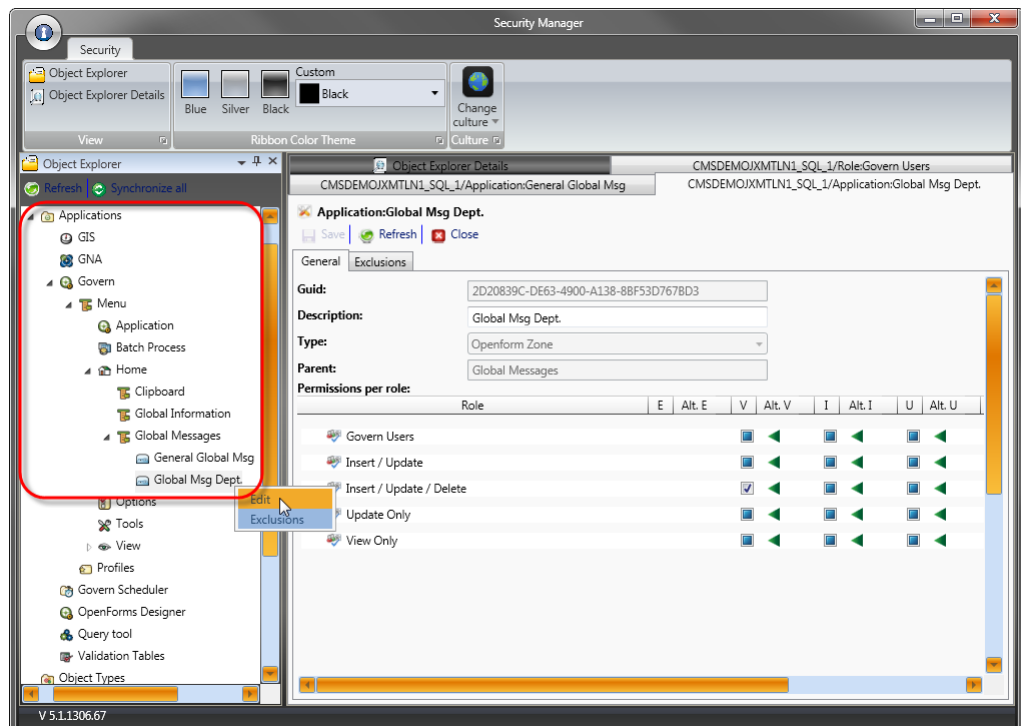
There are scenarios wherein the user can only view *Global Messages*, but cannot add messages. To prevent user addition of *Global Messages*...

1. In the Govern Security Manager (**GSM**), in the left hand *Object Explorer* pane, “drill down” *Applications > Govern > Menu > Home > Global Messages > General Global Msg and Global Msg Dept.*
2. Right-click on each of these icons and select **Edit**.
3. Right-click on the *Global Message* icons and select **Edit**.
4. Click to ensure that the permissions flag for *Insert (I)* is cleared.

## Prevent Deletion of Global Messages

When it is required that a user **not** be permitted to delete *Global Messages*...

1. In the Govern Security Manager (**GSM**), in the left hand *Object Explorer* pane, “drill down” *Applications > Govern > Menu > Home > Global Messages*.
2. Right-click on the icon and select **Edit**.

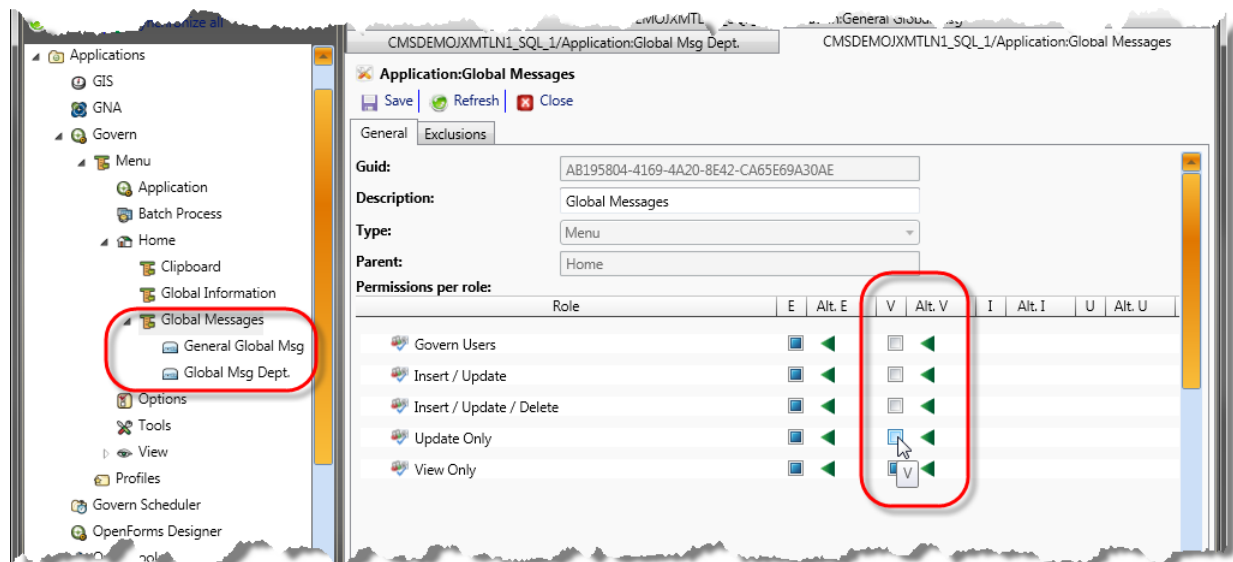


3. In the *Object Explorer* details pane, ensure that the permissions flag for *Delete (D)* has been cleared.

## Hide the Global Messages Ribbon Option

When it is not required for the user to view *Global Messages*, i.e. hide the pane and all tabs, configure security flags in the *GSM* as follows...

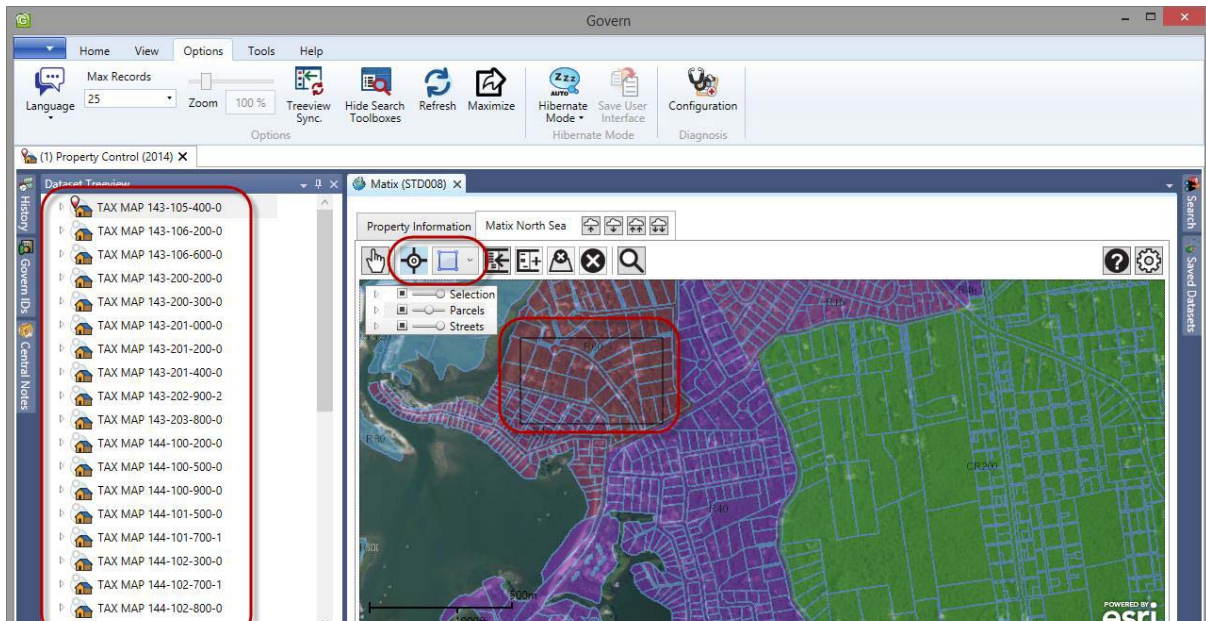
1. In the Govern Security Manager (**GSM**), in the left hand *Object Explorer* pane, “drill down” *Applications > Govern > Menu > Home > Global Messages*.
2. Right-click on the icon; select **Edit** from the floating menu.
3. In the *Object Explorer Details* pane, if not selected, click to select the **General** tab.
4. Under the *View (V)* column, click to clear all flags for all roles that are not required to view *Global Messages*.
5. Under the **Alt. V** column, ensure that the green arrowhead is present for all required roles.



**Note:** After the initial synchronization, when it is in fact required, no Synchronization process is required when modifying security for Global Messages.

When completed users will view *Global Messages*, but they will not have access to editing features in *Govern*.

## Securing the Govern Matix GIS Application



As a custom entity, security is configured directly in the OpenForms Designer (OFD) in Security mode.

### Restricting Access to Govern Matix User Validation Tables

To restrict access to the *Matix* user validation tables...

#### By User...

1. In the *GSM* locate the **Applications** component.
2. Double click to drill down to the *Validation Table* node.
3. Right click on the *GIS Settings* node icon, select **Edit** from the floating menu.
4. On the right hand side in the *Object Explorer Details* pane, click to select the *Exclusions* tab.
5. Right click below the user column; select Add user.
6. From the drop down menu, select the user that is to be restricted.
7. With the user selected, remove the users **View** and **Execute** rights, i.e. click to clear the flags.

Referring to the permissions grid in *Using Permission Flags on page 47*, we see that simply removing the **(V)**iews flag will suffice, the removal of **(E)**xecute rights further reinforces the restriction.

### By Role...

Restrictions by role will also restrict the user, but it will do so at the expense of all other members in the role. Unless this is required, it is not recommended.

## Securing the Govern New Administration (GNA)

Administrators can secure access to critical menu functions within release 5.1 and greater of the *Govern New Administration (GNA)* application. In the *GNA*, the sensitive areas of the application are utilities, forms and tools that access the following:

- Application Configurations
- Editors
- Options
- Parameters
- Utilities

The GSM will allow administrators to lock out entire menu selections, or individual submenu items. As is standard for GSM objects, security can be by *Role* or by *User*. For example, within the *Application Configurations* menu,

User access can be restricted to any of the forms that are accessible through the menu, or the entire menu itself can be locked out.

### Restricting Access to a Menu or Sub Menu items

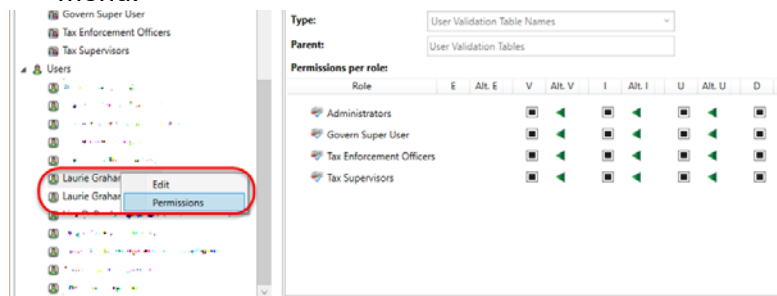
The following is the structure of the menu for a user with the Matix GIS module installed. The current structure for the GIS Configuration under the Application Configuration menu is as follows:

- Application Configurations (*Top Level Menu*)
  - Matix
    - Configuration (*Submenu*)

In the following example, the *Matix* submenu item will be removed for an individual user.

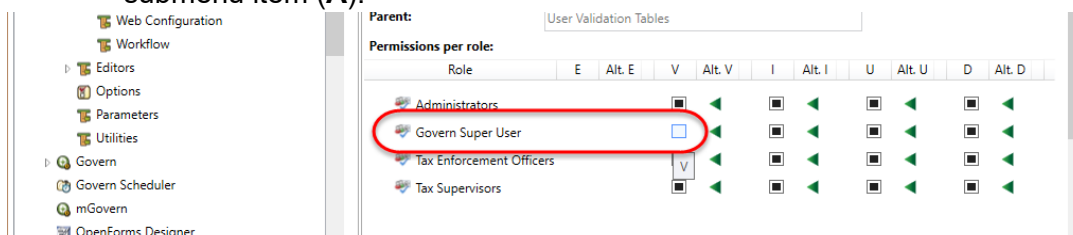
To restrict *User* access to the **Matix** menu item...

1. In the *GSM Object Explorer* pane, double click to expand the **Users** icon.
2. Right click on the user icon and select **Permissions** from the floating menu.



To hide the **Matix** configuration menu, we will need to hide the **View**, i.e. disable the *View* (V) flag.

3. In the Object Explorer Details pane, locate the *GNA* application icon and expand it to the level of the **Configuration** submenu item.
4. Under the **V** column, clear the checkbox to disable the viewing of the submenu item (**A**).



**TIP:** For Administrators, the quickest way to secure an item by *User* or *Role* is to disable the ability to *View* (V) the item.

5. Click **Save** to save the change.
6. Click **Synchronize All**.

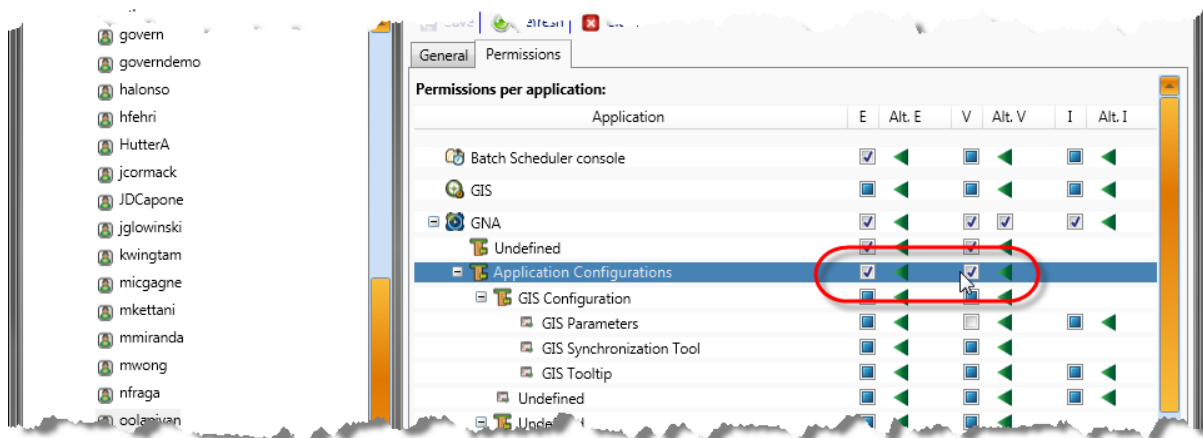
In the *Govern New Administration (GNA)*, when the user enters the application and selects *Application Configurations > Matix*, the icon will be present without a sub-item; the *Matix Parameters* menu has been hidden.

**TIP:** Ideally, for the above example, it is better to remove the *View* flag, one level above. If a menu has only one sub-item, the menu itself should be hidden.

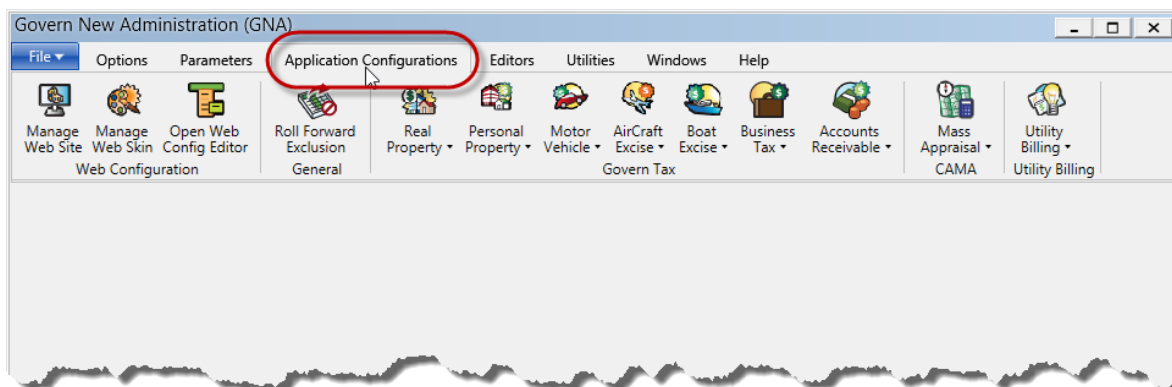


## Hiding the Menu Item...

To hide the entire menu item, i.e. the *Application Configurations* menu and all submenu items, repeat the same procedure as above, but when “drilling down” at the *Application Configurations* level, right-click and disable the *View (V)* Permission flag.



In the *Govern New Administration (GNA)*, the user will see a menu without the *Application Configurations* option visible.







# Index

## A

- Access to Alternate or Historical Data 44
- Add a User to a Role 41
- Add or Delete Users from a Role 33
- Allow Users to Modify Centralized Notes 54
- Allow Users to Modify Global or Department Messages 58
- Alternate or Historical Data 44
- Alternate Permission
  - Changing the flag* 44
- Application Level
  - Security* 25
- Applications 3, 27
- Applications component and nodes 12

## C

- Centralized Notes
  - Allow Users to Modify* 54
  - Hide the Pane* 56, 57
  - Prevent Addition of* 55
  - Prevent Deletion of* 55
  - Prevent Modification of* 54
  - Working with in Govern.NET* 53
- Changing the Alternate Permission flag 44
- Command Buttons
  - Edit* 20
- Component
  - Applications* 12
  - Roles* 12
  - Users* 12
- Components 11
  - Synchronize All* 15
- Copying a Role 37
- Creating Roles 32
- Culture group 10

## D

- Deleting a Role 38

## E

- Edit
  - Form Tabs* 21
- Edit Command Buttons 20

- Editing a User 40
- Enabling Security 25
- Exclusions 3
  - Making* 23
- Exclusions tab 23
- Exit the Govern Security Manager 8

## F

- Floating Menus 18
- Form Tabs
  - Editing* 21

## G

- General tab 22
- GIS Application
  - Restrict Access to* 62
  - Securing* 62
- Giving a User Access to a Profile 42
- Global Messages
  - Allow Users to Modify* 58
  - Hide the Button* 61
  - Prevent Addition of* 59
  - Prevent Deletion of* 60
  - Prevent Modification of* 59
- Govern Groups
  - Importing* 31
- Govern Security Manager Interface 6
- Govern Suite Button 8

## H

- Hide the Centralized Notes Pane 56, 57
- Hide the Global Messages Button 61

## I

- Importing Govern Groups 31
- Inheritance
  - Parent and Child Object* 45

## M

- Main Type Objects 22
- Making an Exclusion 23
- Menu 3, 27
- Menus and Profiles 27
- Minimize or Maximize the Ribbon 9
- Modify Permissions to User in Role (Exclusions) 35

Modifying Permissions to a Role 34

## **N**

Nodes 11

*Synchronize All* 15

## **O**

Object Explorer

*Components* 11

*Nodes* 11

*Sub-nodes* 11

Object Explorer Command Buttons 13

Object Explorer Pane 11

Object Types 30

Objects

*Main Type* 22

## **P**

Parent and Child Object Inheritance 45

Permission 3

Permission Flags 27, 43

*Types of* 46

*Using* 47

Permissions 27

Permissions Flags

*Setting* 43

Prevent Addition of Centralized Notes 55

Prevent Addition of Global Messages 59

Prevent Deletion of Centralized Notes 55

Prevent Deletion of Global Messages 60

Prevent Modification of Centralized Notes 54

Prevent Modification of Global Messages 59

Profile

*User Access to* 42

Profiles 3, 28

*Securing* 53

## **R**

Refresh button 13

Remove a User from a Role 41

Resizing the Application Window 7

Restrict Access By Role 50, 51

Restrict Access By User 50, 52

Restrict Access to an Application 48

Restrict Access to MS Govern GIS Application 62

Role

*Restrict Access By* 50, 51

Roles 4

*Add a User* 41

*Copying* 37

*Deleting* 38

*General tab parameters* 32

*Permissions tab parameters* 32

*Remove a User* 41

Roles Command Buttons 30

Roles component and nodes 12

Roles Level

*Security at the* 25

Roles Menu Options 31

Roles Parameters 32

## **S**

Securing Profiles 53

Securing the MS Govern GIS Application 62

Security 25

Security at the Application Level 25

Security at the Roles Level 25

Security at the User Level 25

Setting Permissions Flags 43

Standard Features 18

Starting the Govern Security Manager 5

Sub-nodes 11

Synchronize

*When to* 16

Synchronize a Node or Sub-Node 16

Synchronize All Components and Nodes 15

Synchronize button 14

## **T**

The Ribbon 9

Types of Permission Flags 46

## **U**

User

*Restrict Access By* 50, 52

User Access to a Profile 42

User Level

*Security at the* 25

Users 4, 40

Users component and nodes 12

Using Permission Flags 47

**V**

Viewing Users 40

**W**

When to Synchronize 16

Working with Centralized Notes in Govern.NET 53