

# Quick Reference to OFD Security

## Overview

The purpose of this document is to provide an overview of setting up security for the Govern user forms. *Full details are provided in the Govern OpenForms Designer guide.*

## What's New

In previous versions of Govern OpenForms, security permissions were defined in the Govern Security Manager (GSM). In v6, only the initial right to execute the form is defined in the GSM.

After that all permissions are granted in the OpenForms Designer (OFD). These include the view, update, and delete rights for the entities, the tabs, group boxes, and data entry fields. They also include the security settings for both normal and alternative security, all profiles, and all roles and users.

## Prerequisites

A few items required for setting up security on the forms are listed in this section.

### Roles and User Accounts

Ensure that your Roles and user accounts are defined and up-to-date. User accounts are managed in GNA and Roles are managed in the GSM.

### Forms

Ensure that your forms are created in the OpenForms Designer.

### Profiles

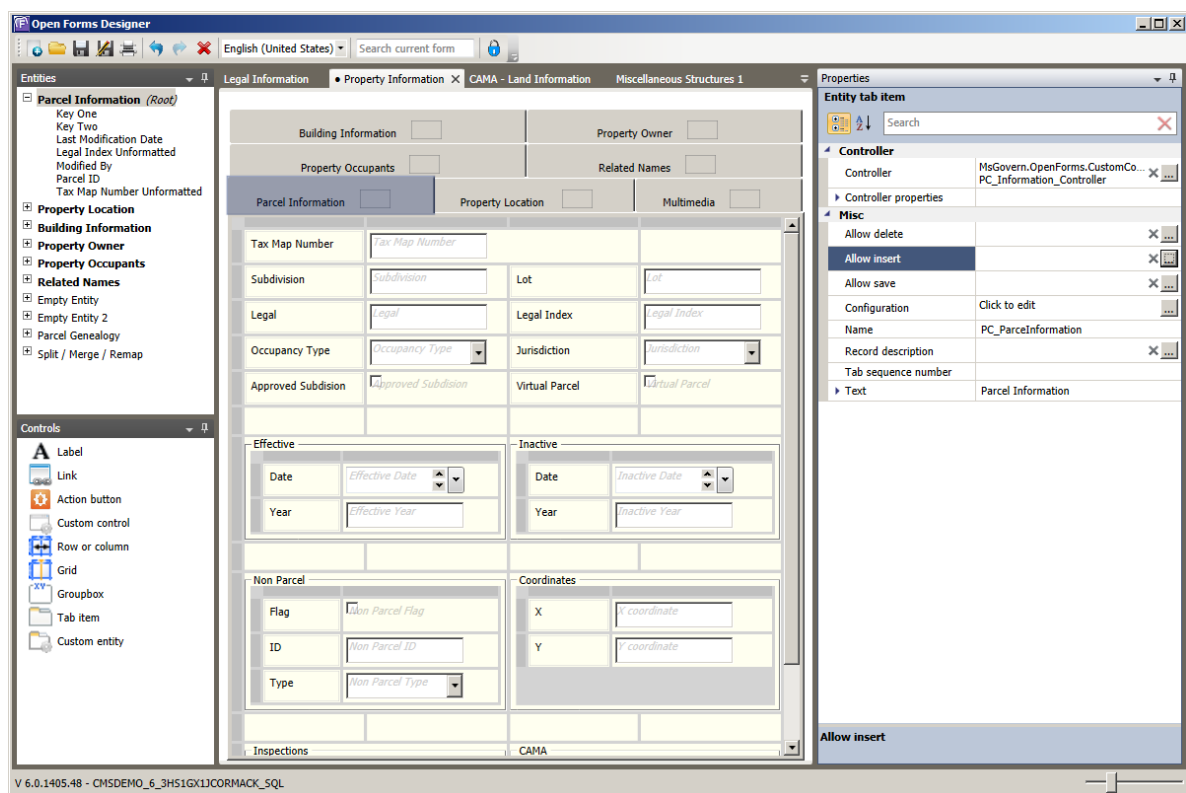
Ensure that your Profiles are created and that the required forms are added to the required Profiles.

## Tips and Reminders

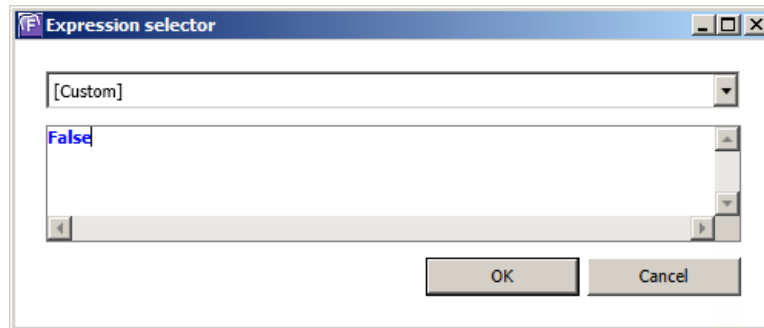
Data entry fields and other controls can be disabled on a form due to any of the following:

- No records are loaded in the tree view.
- No data exist for the selected name or property record.
- A custom control
- A controller
- An expression added to the entity or to any control in the OFD.
- An expression added to an attribute in the BED.

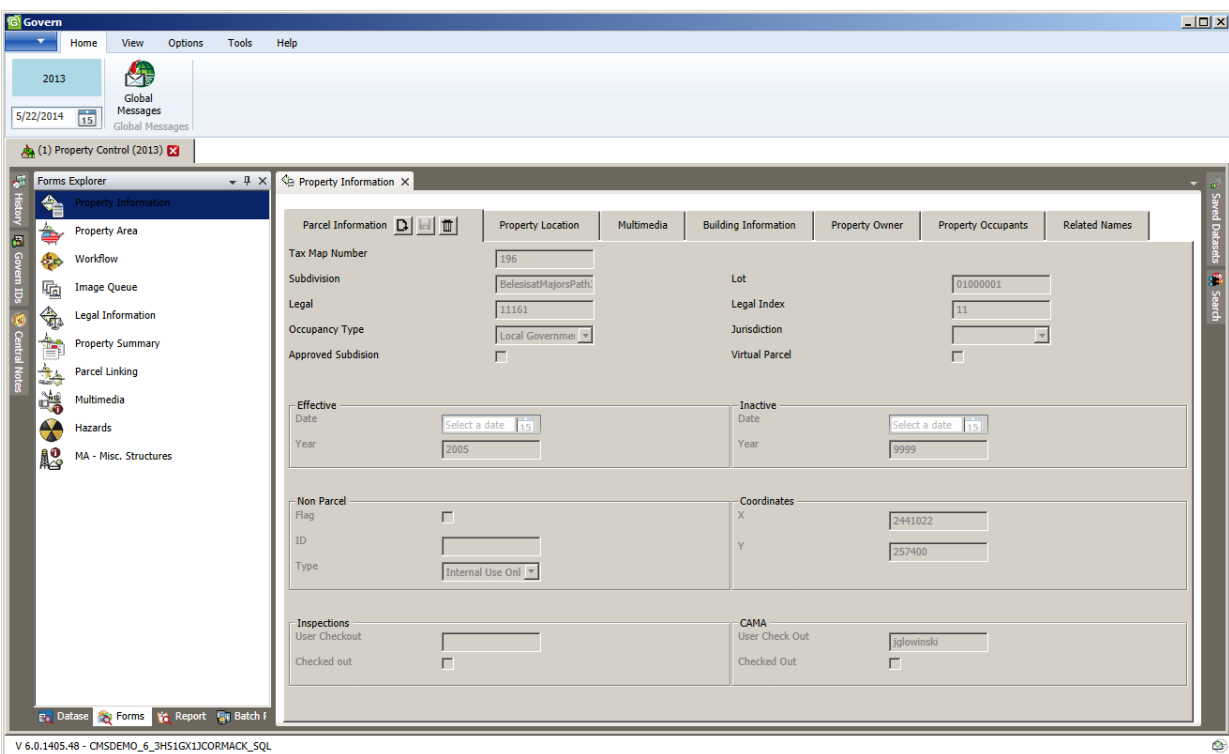
For example, you could write an expression to disable or attach a condition to the save, insert, or delete functionality of a form at the entity level.



If the following expression is added to the **Allow save** property, the **Save** button is disabled on the Govern form and the fields are disabled.



If the form is already open in Govern, click the Refresh button on the Govern ribbon in order to see the results.

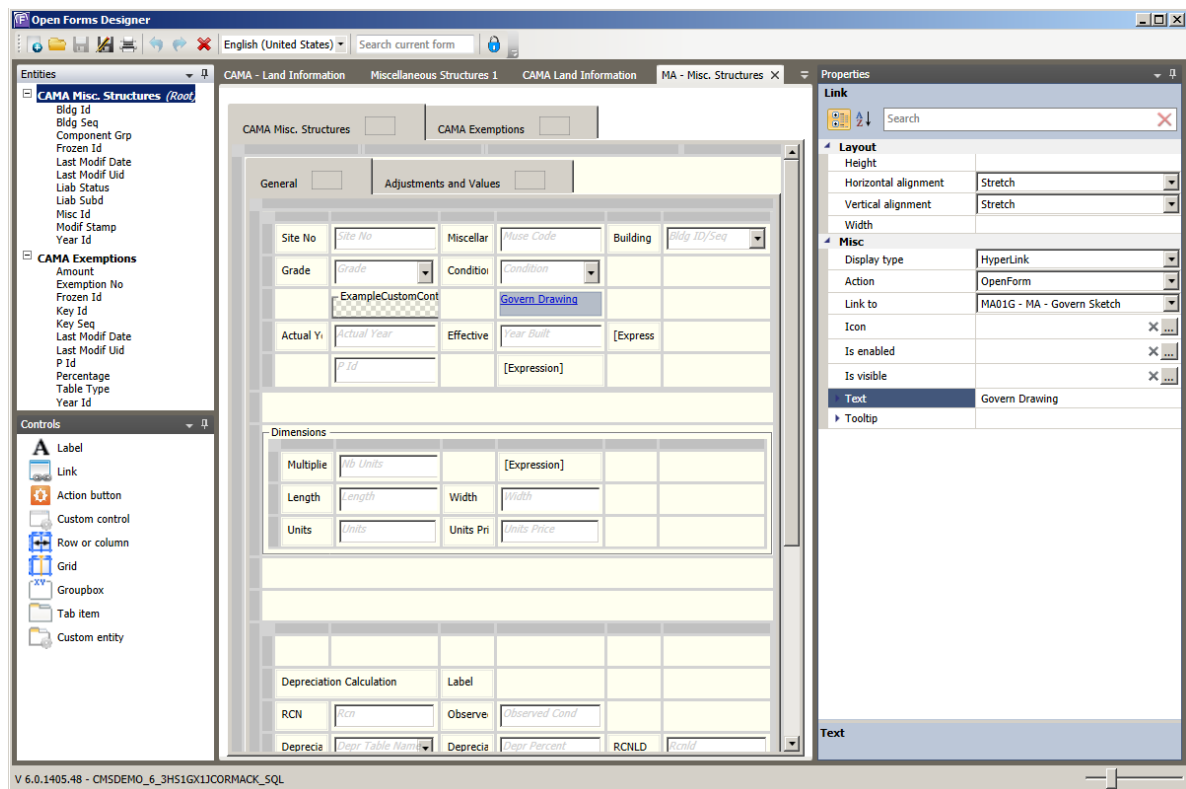


Add this expression to the **Allow insert** property to disable the **New** button in Govern.

Add it to the **Allow delete** button to disable the **Delete** button.

You could add the same expression to the **Is enabled** or **Is visible** properties which are available in the OFD for:

- Attributes
- Labels
- Links
- Custom controls
- Tab items
- Tab Controls



These properties are not available for:

- Grids
- Rows
- Columns
- Custom Entities

The **Action** button has the **Is Enabled** property but not the **Is Visible**.

You could write an expression that attaches a condition to a functionality. for example, add `IsNull(@attrAPPRAISED_VALUE,0) = 5` to the Save button to disable the save unless the property value is equal to 5.

**Rule:** For expressions, the most restrictive definition applies.

For example, the following expression, can be added to the **Is Visible** property of a tab in the CAMA Land entity.

```
IsNull(@attrFINAL_ADJ_PERCENT,0) = 5
```

This would make the tab invisible unless the final percent were equal to five. You could then have other labels and attributes inside the tab. These would only need to be configured if the condition were met.

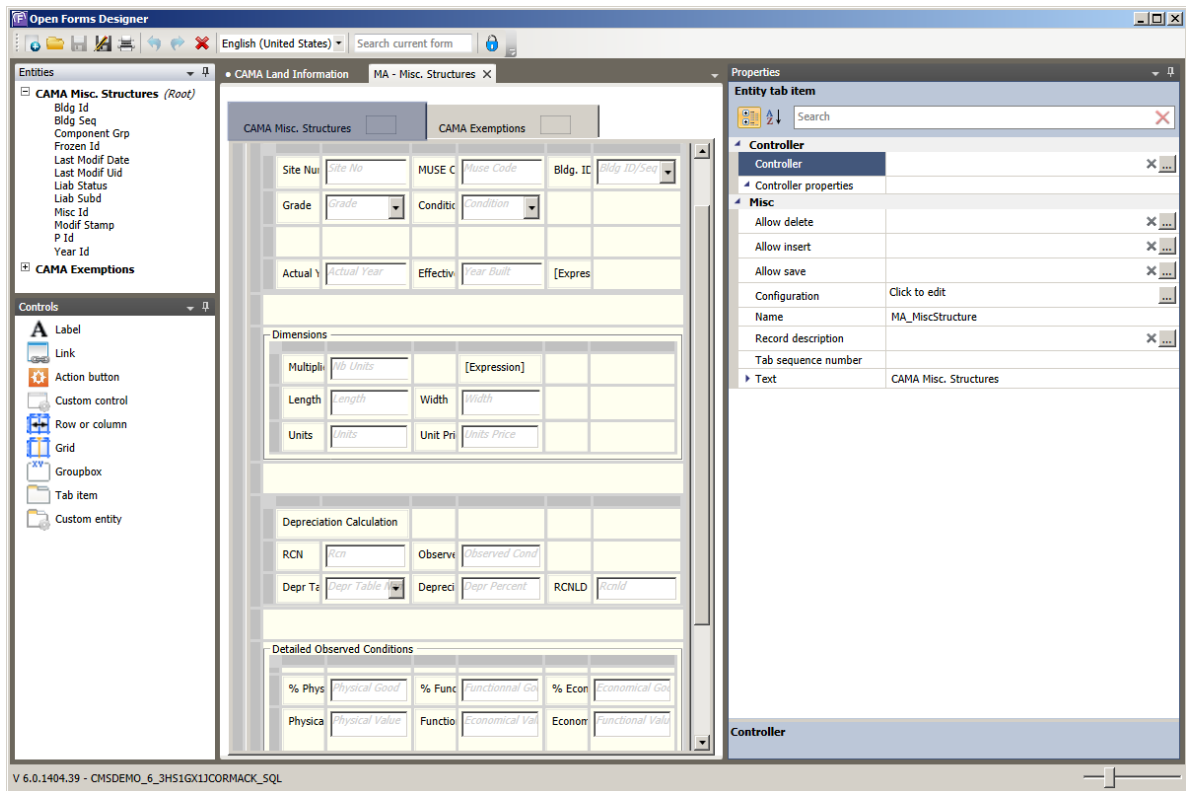
If the view permissions for the tab were removed in the security settings, then these would override the expression. Not being able to view a tab is more restrictive than being able to view it under a specific condition.


An expression can also be added to an attribute in the Business Entity Designer (BED), for Calculated Values.

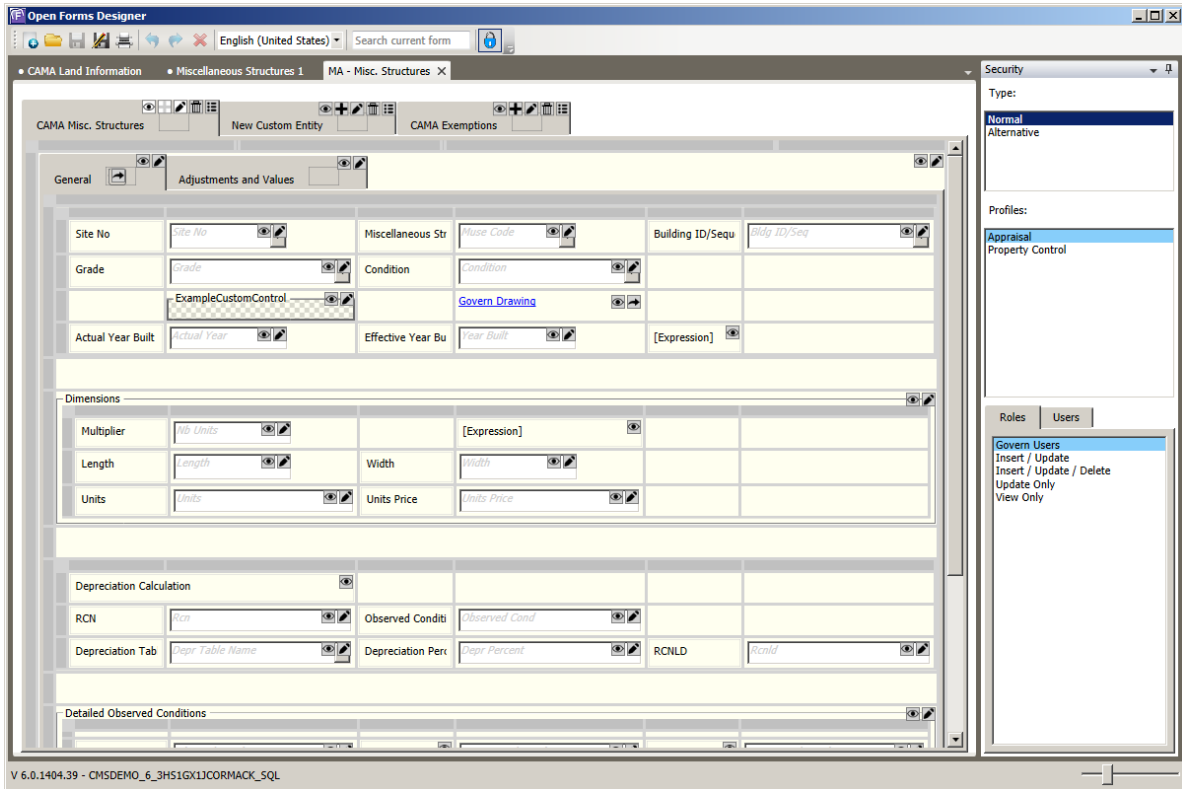
## Recommended Procedure

To access the OFD security settings:

1. Launch the OFD
2. Open the form and the entity in the OFD editor.



- Click the **Security** icon  in the title bar.  
This opens the form in Security mode.



The screenshot shows the Open Forms Designer (OFD) Security Explorer interface. The main window displays a form for 'Miscellaneous Structures' with various fields like Site No, Grade, Condition, etc. On the right, the Security Explorer is open, showing three sections: Type (Normal, Alternative), Profiles (Appraisal, Property Control), and Roles/Users (Govern Users, Insert / Update, Insert / Update / Delete, Update Only, View Only).

When you are in Security mode, the Security Explorer is displayed on the right. This explorer has three lists boxes for the following options:

- **Type:** Normal or Alternative
- **Profile:** the groups under which the forms are located, such as Appraisal, Property Control, Accounts Receivable, etc.
- **Roles and Users:** User groups and individual user accounts

4. Select a Security **Type: Normal** or **Alternative**.

It is recommended to set up the Normal security first. By default, the security permissions defined for Normal security apply to the Alternative security.

5. Select a profile under **Profile** if the form is added to multiple profiles.

6. Do one of the following:

- Click **Roles** and select the role for which you want to define security.
- Select **Users** and select the user account for which you want to define security.

**Note:** It is recommended to define security for the role, then define the exceptions for the individual user.

Once you select an item in each list box, the security icons are displayed. These are displayed at the entity level and for each control. They are displayed at the top right of the control or item.

7. Select the icon corresponding to the security that you want to set for the control or item.
8. Click **Save**.
9. Continue to define the security for each item on which you want to set explicit permissions. If a security permission is not explicitly set for an item, the Default security is applied. *See Default Normal Security on page 159.*
10. Repeat steps 7 to 9 in order to define the security for each role or user.
11. Select **Alternative** under **Type** and repeat steps 7 to 9 where applicable.

The default permissions for the alternative security is applied if the security permissions are not explicitly set. *See Default Alternative Security on page 160.*
12. Repeat the procedure for each Profile.
13. Repeat the procedure for each role and user under each Profile and type.









---

# Using the Security Icons

## Overview

The security icons are used to define permissions for the actions that users can perform. They can be defined at the entity level and on most controls, such as a tab, groupbox, label, or attribute.


The actions include View:  Insert:  Update:  Delete:  Browse:  and Link: . Each one has to be defined separately on each control. The actions that they perform on each control are *described under Defining Security on the Entity and the Controls on page 162*.

There are three permissions for the security settings:

- **Granted:** Permission is given
- **Not Granted:** Permission is denied.
- **Undefined / Not explicitly set:** No permission is defined. When new permission is explicitly set, the default permission is granted.

These are applied as described in the following sections:

## Undefined Not Explicitly Set

 When you open a new form in the OFD and switch to Security Mode, all the security icons: View, Insert, Update, Delete, Browse, and Link, are displayed on a gray background. The icons are clearly visible.

At this point, no security is explicitly set. The default security is applied.







## Default Normal Security

In Normal Security, the **Is Granted** permission is the default. At this point the Not Explicitly Set permission is the same as the Is Granted permission.

## Default Alternative Security

By default, the Alternative Security for each item is the same as the Normal Security. For example, if permission to view an attribute is denied in Normal Security, it is also denied in Alternative Security.

When you switch to Alternative Security, the permissions are Not Explicitly Set for Alternative Security. The icons are clearly visible on a gray background. However, security is applied as follows:

Normal Security Setting		Default Alternative Setting	
Icon	Permission	Icon	Permission
	Granted		Granted
	Not Granted		Not Granted
	Not Explicitly Set (Is Granted)		Is Granted


## Recommended Procedure

It is recommended to define your security settings for Normal Security. Then, switch to Alternative Security and define the permissions that are different.

Typically, more permissions would be Granted in Normal Security and Not Granted in Alternative Security. For example, users could have the permission to view, update, and delete records under Normal Security, but only the right to view records under Alternative Security.

## Granting Permission


If you want to grant permission to an item, you can use the default setting or double-click on the icon, under Normal Security.

When security is explicitly set to Is Granted, the background is white but the icon is clearly visible .

For a description of how each permission is applied when granted, see *Defining Security on the Entity and the Controls on page 162*.

## Denying Permission

To deny a permission on an item, click on the security icon.

When permission is Not Granted (denied), the icons are not clearly visible and the background is white 

For a description of how each permission is applied when it is not granted, see *Defining Security on the Entity and the Controls on page 162*.

## Setting Security Permissions by Profile

When you are setting up security permissions, you need to select the Profile.

If the form is added to multiple Profiles, you need to define the security on each Profile separately.

## Setting Security by Role or User

A user can belong to multiple roles.

If different security settings are defined for each role, the settings that give the highest permissions are applied. For example, a user could belong to both an Administrators Role and a Users Role. The administrators could be granted the permission to delete records while the users are not granted this permission. The user, who belongs to both roles, would be able to delete records.

Even if a permission is specifically set to Not Granted for a user, as long as the user is a member of a Role where the permission is Granted, the user is Granted the permission.

The setting that gives the most permission is used.

# Defining Security on the Entity and the Controls

## Overview

This section describes the security icons and settings at each level. In the OFD, security permissions can be defined for View, Insert, Edit, Delete, and Browse permissions.

**Note:** Tooltips for the icons will be added in a future release.

Before defining security permissions, it is important to consider the following:.

**Note:** Entities or fields are always disabled in Govern when:

- No records are loaded to the Dataset tree view
- No data exist for the selected name or property record.

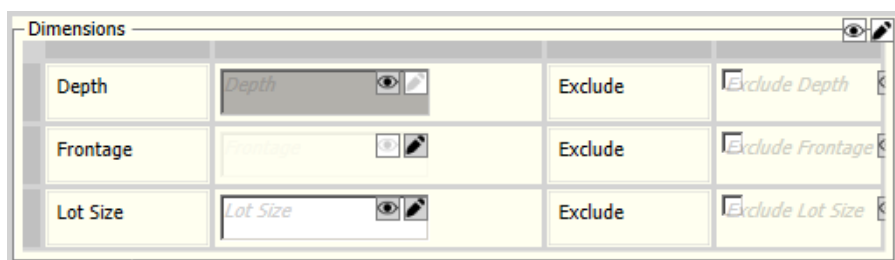
They can also be disabled by any of the following:

- Custom controls
- Controllers
- Expressions
- Security definitions

## Using the Icons to Define Security Permissions

When you define a security permission in the OFD, you have a preview of the result.










For example, in the following screen shot, the Update icon is disabled for the Depth attribute. In the preview, it appears in gray. The View icon for the Frontage attribute is disabled. The attribute is not visible in the Preview.















### Security by Item





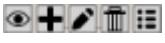
The table in this section provides a description of the security icons for each item:

- Entity
- Tab Control (a group of tabs)
- Tab Item (an individual tab)
- Grid
- Groupbox
- Label
- Link
- Action button
- Custom control
- Custom entity

Level	Icon	Description
<b>Entity</b>  <b>Or Custom Entity</b>		<b>View, Insert, Edit, Delete, and Browse</b> security permissions can be defined at the Entity level.  The icons for the entity are located on the tab at the top of the form.
		<b>View:</b> When the <b>View</b> icon is set to <b>Granted</b> , the entity is visible.  When it is set to <b>Not Granted</b> , the entity is not visible.
		<b>Insert:</b> When the Insert icon is set to <b>Not Granted</b> for the entity, the <b>New</b> icon  is disabled in Govern.  The user cannot create a new record.
		<b>Update:</b> When the <b>Update</b> icon is set to <b>Not Granted</b> for the entity, the <b>Save</b>  and <b>Cancel</b> icons  are disabled on the Govern form.  The Govern fields are visible but cannot be edited.
		<b>Delete:</b> When the <b>Delete</b> icon is set to <b>Not Granted</b> for the entity, the <b>Delete</b> icon  is disabled on the Govern form.  The user cannot delete a record from Govern.

Level	Icon	Description
		<p><b>Browse:</b> When the Browse icon is set to <b>Not Granted</b> for the entity, the <b>Browse</b> icon is disabled on the Govern form.</p> <p>The secondary Browse window is not available.</p>
<b>OFD Controls</b>		The icons for the OFD Controls are located in the top right corner of the control. View and Update permissions can be defined for most controls.
<b>Tab Control (a group of tabs)</b>		<b>View:</b> When the <b>View</b> icon is set to <b>Not Granted</b> for the Tab Control, the tab, or tabs within a group of tabs, are not visible in Govern.
		<b>Update:</b> When the Update icon is set to <b>Not Granted</b> for the Tab Control, the fields within the tab, or tabs, are visible but they are disabled and cannot be updated.
<b>Tab Item (an individual tab)</b>		<b>View:</b> When the <b>View</b> icon is set to <b>Not Granted</b> for a Tab Item, the tab is not visible in Govern.
		<b>Update:</b> When the <b>Update</b> icon is set to <b>Not Granted</b> for a Tab Item, the fields on the tab are visible but they are disabled and cannot be updated.
<b>Grid</b>	N/A	<b>Note:</b> No security permissions can be applied at the grid level.
<b>Groupbox</b>		<b>View:</b> When the <b>View</b> icon is set to <b>Not Granted</b> for the groupbox, the groupbox is not visible on the Govern form.
		<b>Update:</b> When the <b>Update</b> icon is disabled for the groupbox in the OFD, the groupbox is visible but the fields are disabled on the Govern form.
<b>Label</b>		<p>Only the <b>View</b> permission can be set for the Label, if the label is added independently to the form.</p> <p>If the <b>View</b> icon is set to <b>Not Granted</b> for the label, the label is not visible on the Govern form.</p>
<b>Attribute</b>		<p><b>View:</b> When the <b>View</b> icon is set to <b>Not Granted</b> for the attribute, the attribute is not visible on the Govern form.</p> <p>If a label is connected to the Attribute, the label is hidden as well.</p>
		<b>Update:</b> When the <b>Update</b> icon is set to <b>Not Granted</b> for the attribute, the attribute is visible but cannot be edited in Govern.
<b>Link</b>		<b>View:</b> When the <b>View</b> icon is set to <b>Not Granted</b> for the link, the link is not visible on the Govern form.

## Defining Security on the Entity and the Controls

Level	Icon	Description
		<b>Action:</b> When the <b>Action</b> icon is set to <b>Not Granted</b> for the link, the link is visible but it is disabled in Govern.
<b>Action button</b>		<b>Action:</b> When the <b>Action</b> icon is set to <b>Not Granted</b> for the Action button, the action button is visible but it is disabled in Govern.
<b>Custom control</b>		<b>View:</b> When the <b>View</b> icon is set to <b>Not Granted</b> for the Custom control, the Custom Control is not visible on the Govern form.
		<b>Update:</b> When the <b>Update</b> icon is set to <b>Not Granted</b> for the Custom control, the Custom Control is visible but cannot be edited on the Govern form.
<b>Custom entity</b>		The security permissions for the Custom Entity are the same as for the Entity.