# Security & Governance



## Overview

top

Security of your Public information is critical. When deploying Yellowfin an analysis of the security needs of your business should be undertaken. Yellowfin has a number of security features that you can use to ensure the security of your Public information. These can be applied is a mix of ways depending upon the level of security that you require. The security features available include:


- Roles & Functions
- Content Folders
- Data Source Access Management
- View Access Management
- Column Access & Restrictions
- Access / Value Based Filters


This section describes the security framework available to you through Yellowfin. It has been set out so that the highest level security features are described first. For instance Access Roles are the highest and easiest to administer form of security whilst column level security is the most granular and by default the most complex to administer over a large user base deployment.

## Roles & Functions

top

Yellowfin user management is designed around the concept of user roles. This means that multiple users share a commonly defined role for access to the application. Individual users do not have a unique security profile.

A role is a collection of available security functions. Each user will have a role associated with them. As the Yellowfin report writers you can either:

1. Change a person's role – and thus the type of access they have to the application or
2. Change a role definition by adding or removing functions and thereby updating all users' access to the system that share that role.

When a user is logged in the system checks that they are still registered in the application and if so what role they should have. Based on the role access the users interface will be dynamically built – only showing them links and functions that their role has access to.

> *See **Roles** for more information.*

If a user's role does not have access to the dashboard when they login they will be taken to the report list page. A user with dashboard will be taken in to the dashboard page.

| | |
|---|---|
| **When to use** | Use if you wish to limit access to certain functions – such as the ability to write reports |
| **When not to use** | Roles cannot be used effectively to limit access to information and data. |
| **Benefits** | Easy to maintain for all users. |
| **Tips** | Limit the number of roles created at your organization. By increasing the number of roles the level of effort required to manage access increases. Generally only permit a single role per user. Although Yellowfin does support multiple roles it can lead to confusion in a business user. |

## Content Folders

top
All content is managed through a similar security and categorisation infrastructure which is managed through the Content Folders.

The security of your reports is managed at the folder and sub folder level, not at the individual item level. The purpose of this is to simplify the creation of reports in the system.

> *See Content Folders for more information.*

Rather than having to specify who is allowed to see a specific report, each time you create a new report, the security for the report is inherited from the sub folder of the item that is created.

| | |
|---|---|
| **When to use** | Use folders to create meaningful business groupings for reports.<br>If your views are 'write' secured then providing access securities to folders allows a user to publish sensitive reports into secure folders for wider but secure read only distribution. |
| **When not to use** | Folder security is meaningless if users can write reports against a specific view (i.e. it is unsecure) but cannot see a folder in which that view logically fits.<br>For example the Folder may be HR reports and the view is a view to the HR database.<br>If a user can write reports and the view is not secure then whether there is security on the folder is largely irrelevant since the user will have access to the base data through report builder.<br>If all your sensitive views have READ level access defined – applying security to your folder is not required. |
| **Benefits** | Folder Security is excellent for locking read only users out of specific subject domains. |
| **Tips** | Create Subject domains that are intuitive for users to understand.<br>For example Executive HR – this folder can then be made exclusively available to Senior Management for HR reports.<br>Users publishing reports into folders must be aware of the security attached. |

## Data Source Access Management

top
When setting up a source system in Yellowfin you can define which users have the rights to create views against the source as well as write SQL queries against the source.

The general rule for source system security is that it is used for controlling Yellowfin report writers that wish to create views against the source. It is through this process that a user could write reports against the source system and thereby gain unauthorised access to data.

> *See Managing a Data Source for more information.*

If the HR system is to be setup as the source system any user with View Definition access will be able to view all tables including payroll data if the source is unsecure. By securing the source to only HR view builders, only those authorised users will be able to define and manage the HR related views.

| | |
|---|---|
| **When to use** | Use if you have multiple view administrators – each of whom require access to specific source databases only.<br>Use if some users have free hand SQL access to write reports and the data in the data source is sensitive. |
| **When not to use** | Do not set security on the source in an attempt to limit access to drag and drop report writer users. |
| **Benefits** | It is easy to maintain for a select number of users. |
| **Tips** | Limit the number of users that have administration access to views. Especially if they wish to edit the same source system.<br>Multiple administrators can lead to contention issues when managing views. |

**Note:** If there is only 1 Yellowfin report writer of your Yellowfin deployment, and no additional users writing SQL reports, then you may consider leaving your source systems unsecure.

## View Access Management

top
The main form of security for users creating reports and having access to views which allows them to write any report is through the VIEW security.

When a report is written or edited a user must connect to the view record to determine what fields are available to them. At this stage, security check is made to determine if the view that is being accessed is secure, and if so, does the user have the authority to access it.

The security on your view is the most rigorous in terms of managing access to the data that is stored in it. Not only can you control edit access but you can also control which users are permitted to read reports created from the specified view.

> *See View Options for more information.*

The Finance view is created. Only the finance department is permitted to write finance view reports. In this case the view would be defined as secure and the finance users would be added into the access list with edit access.

| | |
|---|---|
| **When to use** | Use if you wish to limit users that have access to the report writing function using the specified view.<br>Use if you wish to be specific in defining which users can read reports created by a specified view but are not permitted to write reports. |
| **When not to use** | If reports in the view are to be written by a handful of users and then published to a wider community it is preferable not to use READ level security. Use category access for this.<br>For example even though the HR view contains sensitive data the HR report writers must write and distribute many reports from this view – most of which do not contain sensitive data.<br>Simplify security of the view by having secure categories into which the report is saved rather than managing security in both the categories and the view.<br>If the data contained in the view is not sensitive then do not apply security to it. |
| **Benefits** | Easy to maintain for EDIT level security – can become complicated if using READ level security in conjunction with category security. |
| **Tips** | If the view is sensitive determine who the users writing reports against the view are and for whom they are writing reports. Use this to determine the best security strategy for the view. If the reports are for a wide distribution view security for read access might not be appropriate. |

## Column Access & Restrictions

top
In some cases a view might be created that is designed for general use but some columns within that view are highly sensitive. For example the salary column in the human resources view holds data that is not for general consumption.

In this case you have two options.

1. Create a copy of the view and exclude the salary column from this instance. Save the view with a new name to indicate that the view is free of sensitive data.
2. Alternatively Yellowfin provides you with the opportunity to define the columns as restricted columns. Once this has been done an additional layer of security needs to be defined, which allows certain users access to the restricted columns of the selected view.
   **Note:** security to restricted columns is globally defined. You cannot specify different users for separate restricted columns within the view.
   Only users with restricted access will be able to see the item when creating reports. When an active report is run, restricted columns will be displayed to all users who have access to the report.

> *See Field Settings for more information.*

| | |
|---|---|
| **When to use** | Use if you wish to create a general view available to many users but restrict access to sensitive data to only a few users. |

| | |
|---|---|
| **When not to use** | Do not use if the view in general and the columns all have the same users that can access them. |
| **Benefits** | Can be used to secure specific columns within a view. |
| **Tips** | This is a difficult security option to maintain from an administration point of view. Consider alternatives first.<br>Only users with access to the view will be able to have column level access. |

## Access / Value Based Filters

top

In some cases a view might be created that is designed for general use but you only wish report consumers to access data from the view that is relevant for their position in the organisation – such as cost centre manager. In this case you would create an Access or Value based filter.

This is achieved by updating the source connection wizard to specify the available filters – such as cost centre and your users' relationship to that source. You then specify the specific columns on the view that related to that source filter – e.g. you must indicate which column in the view is the cost centre column.

When writing a report you would specify that the cost centre filter must be used as the access filter. In this case the cost centre that the report reader owns will be passed in as a filter on the query. Only users with access filters defined will be able to see the data in their reports.

> *See Restricting Data with Access Filters for more information.*

| | |
|---|---|
| **When to use** | Use if you wish to create a general view available to many users but restrict access to data based on a users relationship to the data – e.g. cost centre managers.<br>This mechanism is very good for creating Privatised reports. By using value based filters you can create a single report which is distributes to many users. Each user will however, only see their specific / Privatised data. |
| **When not to use** | Do not use if the view in general and the columns all have the same users that can access them. |
| **Benefits** | Can be used to secure data within a view to only display relevant data. |
| **Tips** | This is an easy option to maintain from an administration point of view.<br>This mechanism allows you to provide access to all data within a view to all your users with the security of knowing that they will only see their specific data. |

top