Content Categories

- Overview
- Category Creation
- Sub Category Creation
    - Publish Access & Approvals
    - Report Version History
    - Content Security Access
        - Primary Org Content Security
- Edit Category/Sub Category
- Delete Category/Sub Category

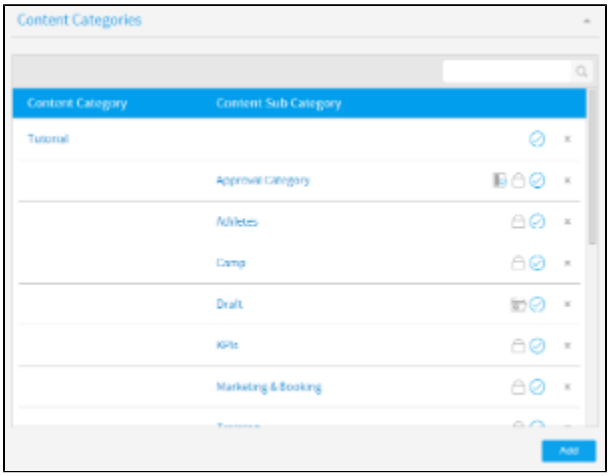
Overview

top
Content is stored within a two tier folder structure of Categories and Sub Categories.

- **Categories** are used to hold and split Sub Categories into grouping. They do not contain content directly.
- **Sub Categories** are located within a defined Category and are used to store content with specified function and access permissions.

The content types that are stored in this structure are Reports, Dashboard Tabs, and Storyboards.

Content Categories are managed through the Admin Console.

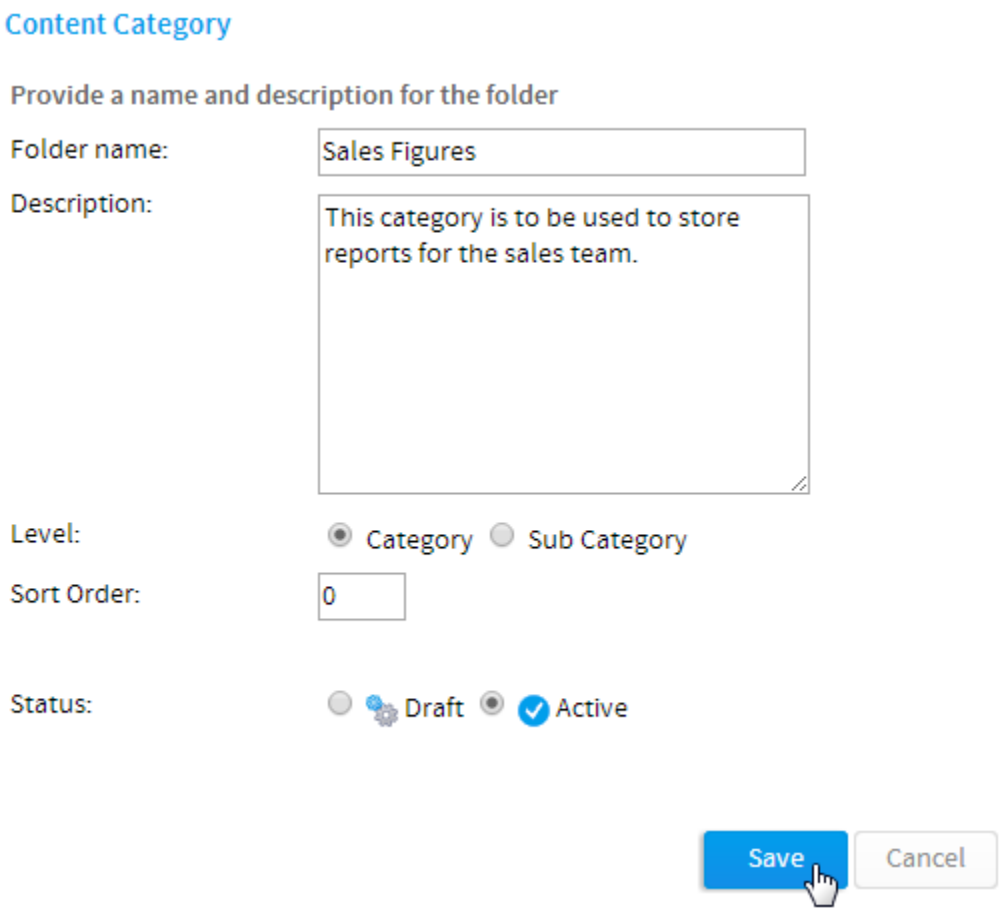


Category Creation

top
To create a Content Category, click the **Add** button under the Content Categories list in the Admin Console. You will now be taken to the Category setup page, where you will need to define the following:

1. **Folder Name:** this will be the name of the folder displayed in various parts of the system when saving and viewing content.
2. **Description:** this will be the description of the folder, used to define its intended purpose and audience.
3. **Level:** leave this with **Category** selected. The Category level needs to be created before any Sub Categories can be defined.
4. **Sort Order:** defaults to zero, provide a numeric sort order if you do not wish the categories to be sorted alphabetically.
5. **Status:** when the Category is ready to be seen by users set the status to **Active**. When **Draft** only administrators will be able to view and edit it, and it can't be used for storage.

Click **Save** to complete the Category.

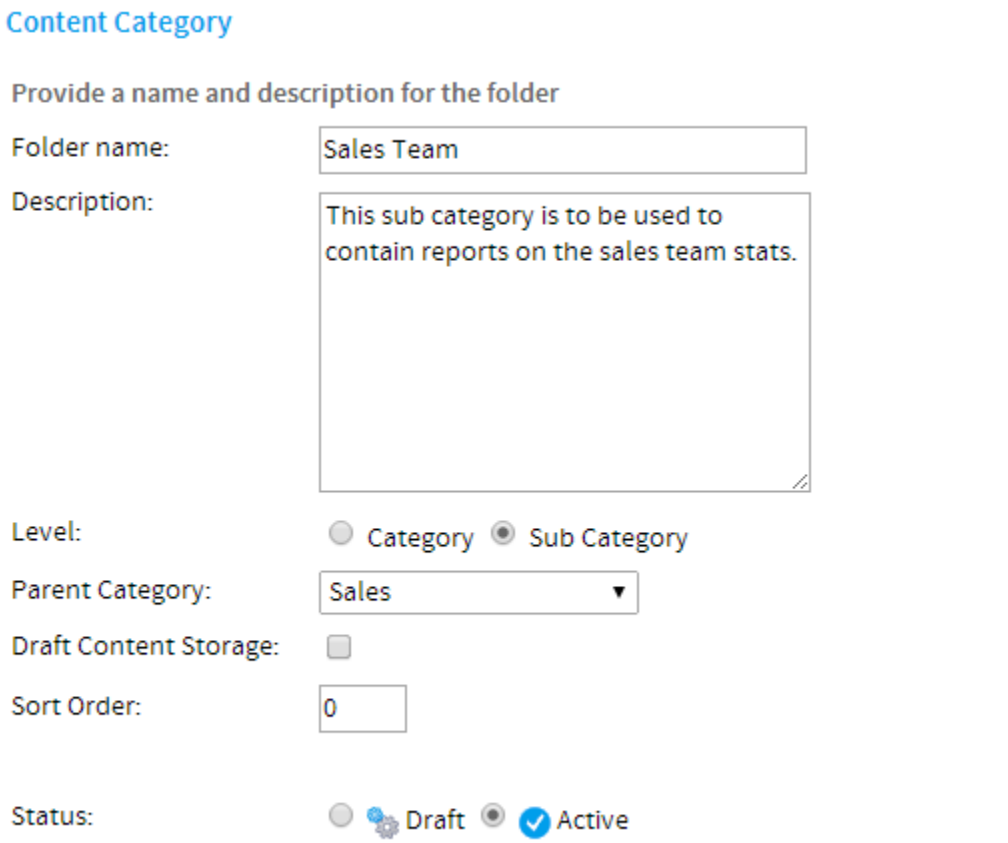


Sub Category Creation

top

Once at least one Category has been created, click the **Add** button under the Content Categories list in the Admin Console to start defining Sub Categories. You will now be taken to the same Category setup page, where you will need to define the following:

1. **Folder Name:** this will be the name of the folder displayed in various parts of the system when saving and viewing content.
2. **Description:** this will be the description of the folder, used to define its intended purpose and audience.
3. **Level:** select the **Sub Category** option. Once changed, a range of different options will become available.
4. **Parent Category:** select the **Category** this Sub Category will be stored within.
5. **Draft Content Storage**: there can be one default Draft sub category in the system, which will contain all draft content until a different sub category has been selected by the content writer. This is used to keep all draft content in one place, making it easier to keep the system organised.
   Note: enabling this option means that any content that is not activated is automatically stored in this Sub Category. There can only be **one** Draft Storage category.
6. **Sort Order:** defaults to zero, provide a numeric sort order if you do not wish the categories to be sorted alphabetically.
7. **Status:** when the Sub Category is ready to be seen by users set the status to **Active**. When **Draft** only administrators will be able to view and edit it, and it can't be used for storage.

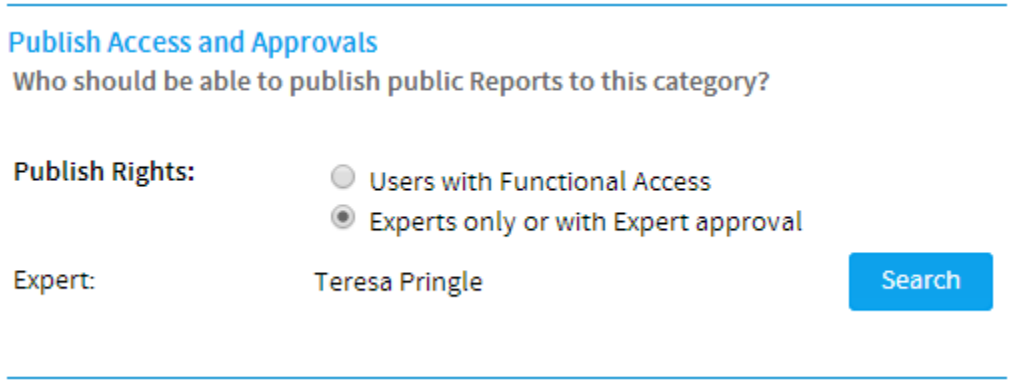


Now that the **Level** has been set to **Sub Category** the following sections will need to be defined. These relate to content settings and as such only correspond to the sub category level, as the category level can't directly contain content.

Publish Access & Approvals

This section allows you to determine which users can publish public reports to the folder.

- If you select **Users with Functional Access** then all users with the public report function can write to this folder
- If you select **Experts only or with Expert Approval** then only specified users can publish reports into that folder. If a user does not have access to publish to that folder the report will be routed to an Expert for approval. This allows administrators and advanced users to approve all reports stored into the folder before they are activated for public consumption, ensuring they are correct and the data can be trusted.

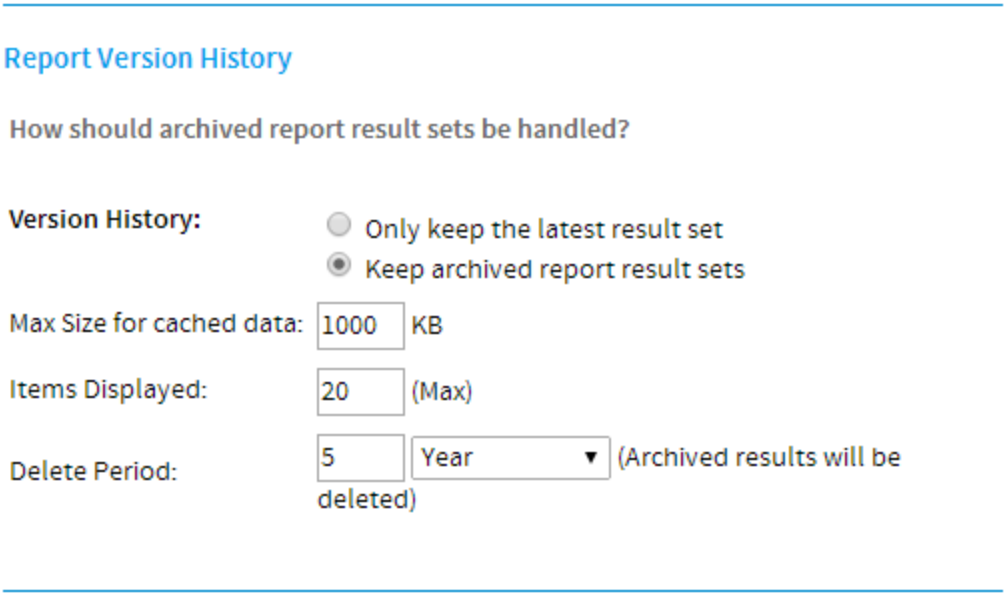


Report Version History

The system has the ability to maintain historical result sets for reports. When a user selects this option not only is the report definition saved but the data as well. This allows users to view previous versions of the report and compare result sets.

All versions of the report data are stored in the Yellowfin Database. As the administrator you can determine how much history and the maximum size of reports you wish to save. This is an application management process that permits you to control the use of your infrastructure.

Version History	The version history allows you to store the data returned in a report. If version history is set to **Only keep the latest result set** then no historical results will be kept. If the **Keep archived report result sets** option is selected then all historical versions of the reports will be kept. **Note:** It's important to remember that this option can quickly build up quite a large amount of data, so use this option sparingly.
Max Size	The maximum size for data to be saved in cache or in the database where version history is required.
Max Items Displayed	The maximum number of items to be displayed on the history drop down list for management information reports.
Delete Period	After what period of time should archived reports be deleted.



Content Security Access

Sub Categories can be secured to restrict access to the content they contain based on specified permissions. The options for setting the security are as follows:

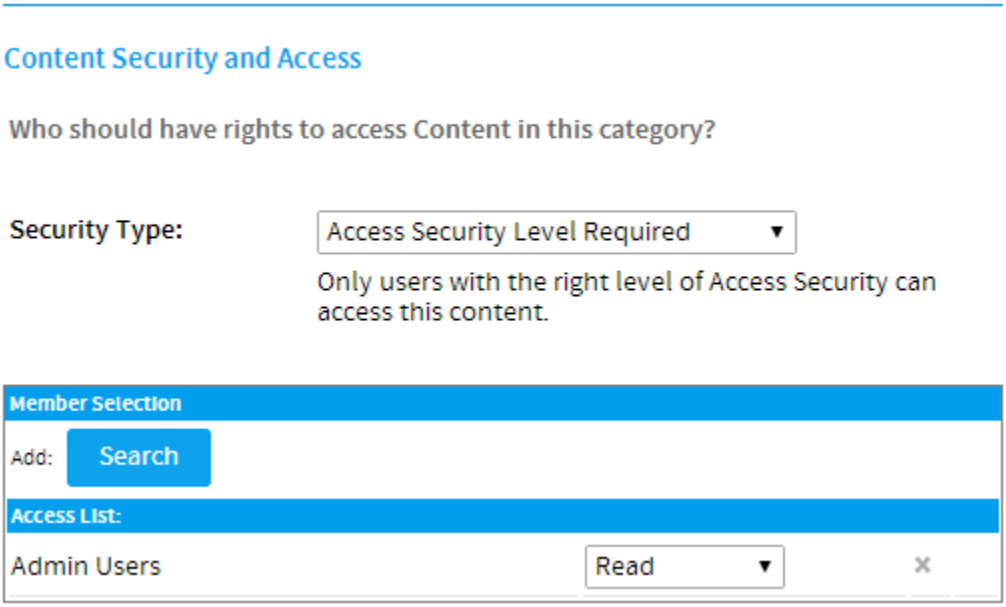
1. **Unsecure Content:** people can access this without logging on.
2. **Secure:** users will have to logon before being able to view the content, but all users of the system will be able to view it.
3. **Access Security Level Required:** only selected users will be able to access this content.

If you choose to secure the sub category then you must select a person or group and then the level of access that they are permitted. Three types of access exist:

Read	Users will only be able to read the content but not create new items of this type of content.
Edit & Update	If a content item exists a user will be able to edit and update an existing piece of content but not create new or delete items in this category. They will also be able to read all content in this category.
Delete	Users with delete access will be able to read, edit, create and delete content of this type. **You must have at least one person with delete access.**

Note: if you want all your users to be able to read the item make sure you have a group created with all your users. Use this group for read access.

When you have selected a person and/or a group click add to append them to the access list. You can have as many groups and people in the list as you wish. You cannot finish the process if you do not have at least one person or group with delete access. Select a person with delete access to finish.

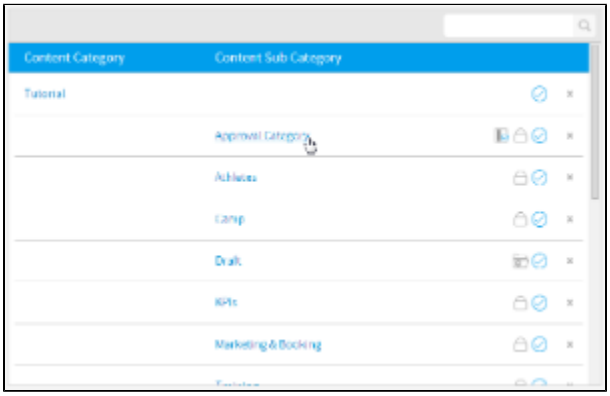


Primary Org Content Security

When using Client Org functionality you are able to secure Content Sub Categories at the Primary Org by assigning access to User Groups created at the Client Org level. This will allow Administrators to restrict Primary Org content to specified users in each Client Org, rather than all Primary Content being available to all Client Org users.

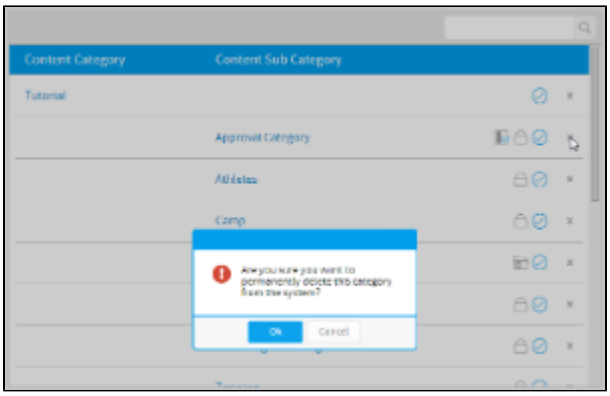
Edit Category/Sub Category

top
To make changes to a Category or Sub Category simply locate it on the Admin Console page and click on its name.



Delete Category/Sub Category

top
To delete a Category or Sub Category simply locate it on the Admin Console page and click on the **x** next to it in the list. From here you will be required to confirm the deletion. If, however, the folder contains content you will be informed that this content must be moved or deleted before the folder can be.


Content Category
Content Sub Category
Tutorial
Approval Category
Camp
OK
Cancel

top