

OpenText Core Content

Admin Quick Start Guide

Welcome to OpenText Core Content, a SaaS content services platform with industry-leading content management capabilities purpose-built to maximize employee productivity by aligning content to business needs.

This quick start guide overviews how to configure your Core Content subscription as an administrator, including:

- Users
- Categories
- Document types
- Access control lists (ACLs)
- Records management with OpenText Core for Federated Compliance

1 Users

Invite users to join your Core Content subscription to give them access to the application. Each user must register an OpenText OT2 account and join the subscription to access the app.

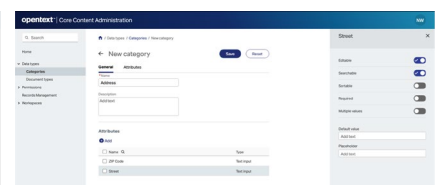
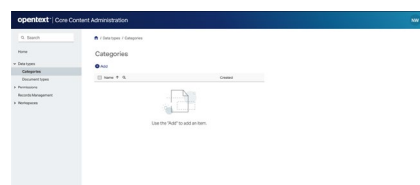
As a tenant admin, you have several options to invite users to Core Content, including sending individual invites or inviting multiple users at the same time using a .csv file to import users. Please reference page 14 and 15 of the [OT2 subscription admin guide](#) for more detail.

2 Categories

Create **Categories** to enable users to apply metadata values to Enterprise volume items. Within each category you create, you must add and configure one or more attributes. Each attribute corresponds to a metadata value that users can apply to items. When you add an attribute to a category, you must specify which type of attribute to add, such as text or number values. When you configure an attribute, you can specify a default value for the attribute and rules for using the attribute.

To create a category:

- On the navigation menu, select **Data Types**, then **Categories** and **Add**.
- Under **General**, add a name for the category and description.
- To add an attribute to the category, under **Attributes**:
 - Select **Add** and select the type of attribute you want to add.
 - Enter a name for the attribute and select **Add** ✓.
 - Select the attribute name configure as needed.
- **Repeat** step 4 to add more attributes to the category as needed and **Save**.



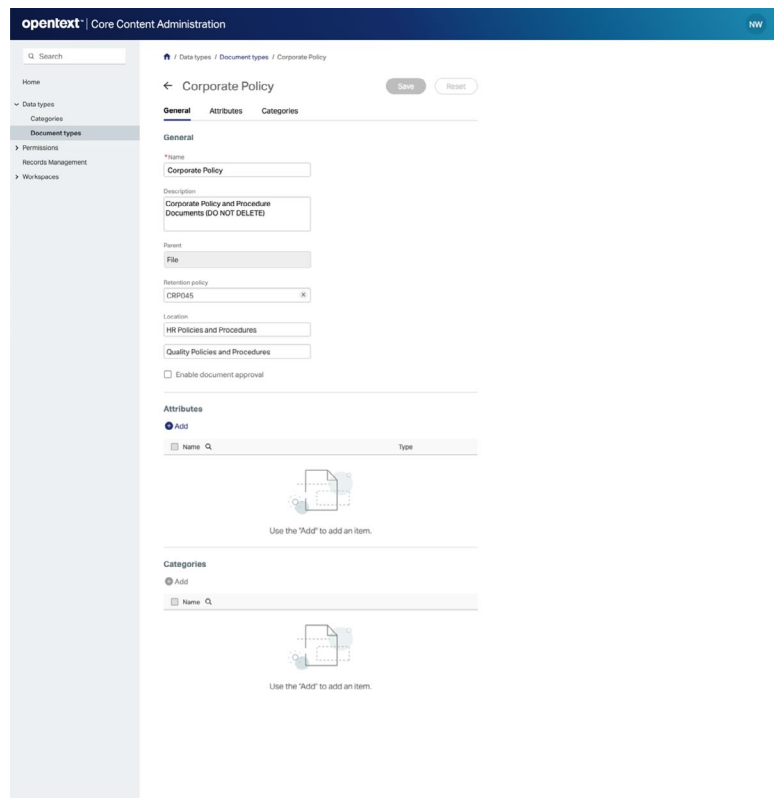
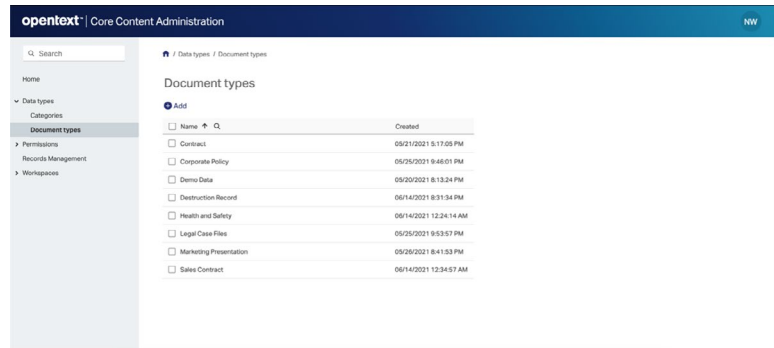
3 Document Types

Create **Document types** to store collections of metadata and settings that are relevant to specific types of documents. When documents are added to Core Content, they are assigned a document type and inherit metadata and settings from that document type.

When **Enable Document approval** is enabled, users can initiate approval workflows on documents uploaded with this type.

To create a document type:

- On the navigation menu, select **Data Types**, then **Document types** and **Add**.
- Under **General**, enter a name and description for the document type.
- For **Parent**, select a document type to be the parent of the document type you are creating. You cannot change the **Parent** selection once you have saved the document type.
- Select a **Retention policy**.
- Select the **Browse** icon  in the **Location** box to select the folder where the document type will be available.
 - To add more locations, click the **Add new field icon** .
 - Select the **Enable document approval** check box to enable the document approval workflow for the document type.
- To add an **Attribute**, select **Add** and choose the attribute you want to add.
 - **Enter an attribute name** and select **Add** .
 - Select the attribute name and configure the attribute.
 - Repeat to add more attributes to the document type as needed.
- To add a **Category**, select **Add**, choose the category and select **Add**. Repeat this step to add more categories to the document type as needed and then **Save**.



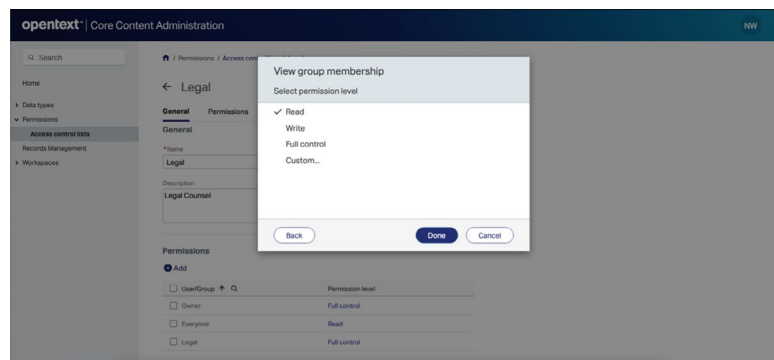
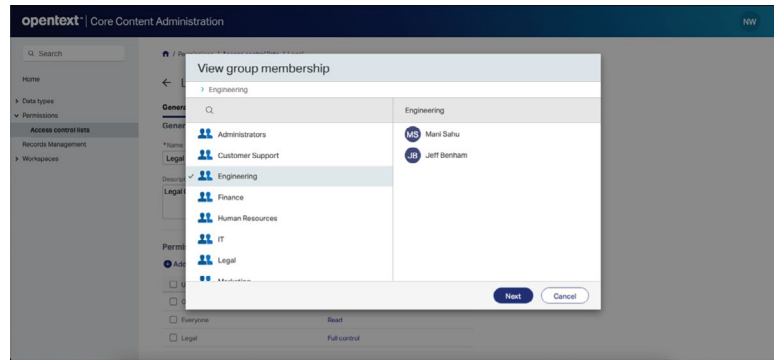
4 Access control lists

Create **Access control lists (ACLs)** for documents, folders, and workspaces to determine who has permissions for the items. ACLs store a list of specific permissions that are associated with a set of selected users and groups. When users manage permissions for items, they can select ACLs instead of manually assigning permissions to each item. ACLs enable admin to better organize permissions and centralize control of different items in the system.

To create an ACL:

- On the navigation menu, select **Permissions**, then **Access control lists** and **Add**.
- Under **General**, type a name and description.
- To add a user or group to the ACL, under **Permissions**, select **Add** and select **User**, **Group**, or **Everyone**.
 - a. In **View group membership**, select the user or group you want to add, and then **Next**.

Tip: Use **Search**  to find a specific user or group by name.
 - b. For **Select permission level** box, choose the permission you want to assign to the user. If you choose **Custom**, select the check boxes next to the specific permissions you want to assign. Repeat this step to add more users or groups to the ACL as needed and **Save**.



5 Records Management with OpenText Core for Federated Compliance

Your tenancy includes a subscription to [OpenText™ Core for Federated Compliance](#), which provides records management functionality for Core Content. You can use records management to define retention policies and disposition schedules for items stored in Core Content.

To enable Federated Compliance records management, you will need to **configure users and scheduled jobs**.

Configure users

- Core Content administrators must be assigned as users in Federated Compliance in order to access the **Records management admin page** in Core Content.
- Assign yourself and additional users to Federated Compliance on the **User and Role management > Users** page in the subscription administration. Once a user has been added, use the **Roles** administration page in Federated Compliance to add them to the **records_management app role** if you want them to be able to administer records management without giving them access to the Core Content administration pages.

Configure scheduled jobs

- On the tenant **Connections** page, configure a general **OTFCCConnectionType** connection.
- On the Federated Compliance subscription **Jobs > Job list** page, create **Disposition** and **Qualification** jobs.

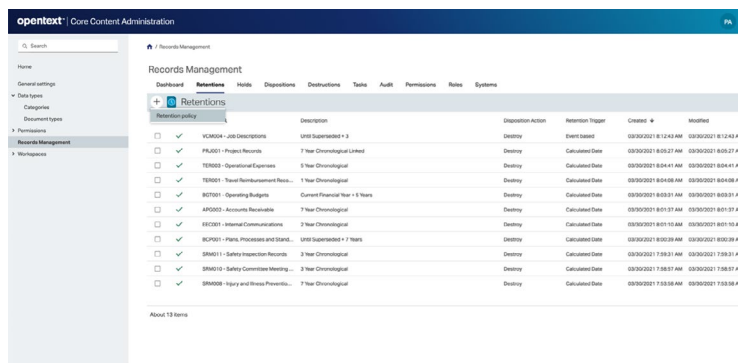
Creating retention policies

Retention policies specify the criteria that are used to calculate retention periods for objects and what happens when the retention criteria are met (i.e. objects are deleted or exported).

Create and configure master retention policy objects on the **Retentions** page. You must add Core Content to a master retention policy to create a retention policy in Core Content.

To create a master retention policy object:

- On the **Retentions** page, select **Add** , and then select **Retention policy**.



- Add a **name** for the master retention policy object and an optional **description**.
 - **OPTIONAL** Add a description to specify the **mandate** of the retention policies created by the master retention policy object. This value will be applied to each retention policy that the master retention policy object creates on the connected systems.
 - **OPTIONAL** Specify the scope of the retention policies created by the master retention policy object under **Scope Notes** box. This value will be applied to each retention policy that the master retention policy object creates on the connected systems.
 - Ensure that the **Enabled** switch is turned on and **Submit**.
- To add the system instance to a master retention policy object:**
- On the **Retentions** page, select the name of a **master retention policy object** you created.
 - Select **Add** , and then **System Type**.
 - In the **Target systems** list, select the Core Content system. This is the same name that is displayed on the **Systems** page.
 - In the **Number of phases** list, click **1** and **Submit**.
 - Configure the values you want to apply to the retention policy.

For more information, use the **Federated Compliance Administration Guide** accessible directly in the Core for Federated Compliance app.

Need more help?

- OT2 Subscription Admin Guide
- Core Content how-to videos
- Core Content Community Forum

