opentext™

OpenText™ Documentum™ Content Management

Microsoft® Integrations Admin Console Guide

Configure OpenText Documentum Content Management (CM) Microsoft integrations in Admin Console, including sensitivity labels from Microsoft Purview Information Protection and Editing and co-authoring in Microsoft® 365™.

EDCADC250400-AIN-EN-1

OpenText™ Documentum™ Content Management
Microsoft® Integrations Admin Console Guide
EDCADC250400-AIN-EN-1
Rev.: 2025-Nov-12

This documentation has been created for OpenText™ Documentum™ Content Management CE 25.4.
It is also valid for subsequent software releases unless OpenText has made newer documentation available with the product, on an OpenText website, or by any other means.

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Tel: +1-519-888-7111
Toll Free Canada/USA: 1-800-499-6544 International: +800-4996-5440
Fax: +1-519-888-0677
Support: https://support.opentext.com
For more information, visit https://www.opentext.com

Table of Contents

Chapter 1

Overview

OpenText Documentum Content Management (CM) supports integration of several products from Microsoft. This guide provides help on configuring these integrations in Admin Console.

Chapter 2

Editing and co-authoring

Microsoft 365 editing and co-authoring enables the editing of files directly in Microsoft 365 apps. Files do not need to be downloaded, they are checked out automatically when opened and back in when closed. In addition, multiple users can edit the same file simultaneously, seeing each other's changes in real-time. For more information on Microsoft 365 editing and co-authoring, see section 2.6.1 "Edit and co-author in Microsoft 365" in *OpenText Documentum Content Management - Smart View User Help (EDCCL-H-UGD)*.

This chapter provides information on enabling and configuring editing and co-authoring in Microsoft 365 for Smart View.

Notes

- Depending on your licensing and configuration, this option might not be available.

To access Microsoft 365 editing and co-authoring options:

1. Sign in to Admin Console with the proper access rights.

   To configure mandatory online editing service (OEM) options, you must sign in with an OpenText Directory Services enabled account.

2. On the **Home** page, click the **Microsoft** tile, and then the **Editing and co-authoring** tile.

   The **Editing and co-authoring in Microsoft 365 General settings** page opens.

2.1 Configure editing and co-authoring in Microsoft 365

The **Editing and co-authoring in Microsoft 365** page includes a list of requirements to configure and enable Microsoft 365 editing and co-authoring. Fields marked with an asterisk are mandatory.

Prerequisites:

Before you configure Microsoft 365 editing and co-authoring, you must do the following:

1. Install and configure OpenText Documentum CM Online Editing Service (OES): Section 3 "Deploying OpenText Documentum CM Online Editing Service" in *OpenText Documentum Content Management for Microsoft 365 - Deployment and Administration Guide (EEMSODC-IGD)* and Section 4 "Deploying Notification

Service" in *OpenText Documentum Content Management for Microsoft 365 - Deployment and Administration Guide (EEMSODC-IGD)*.

2. Add the following to Admin Console's `rest-api-runtime.properties` file:

```
rest.security.headers.x_frame_options.disabled=false
rest.security.headers.x_frame_options.policy=SAMEORIGIN
```

3. To configure mandatory online editing service (OEM) options, you must sign in with an OpenText Directory Services enabled account.

To configure editing and co-authoring in Microsoft 365

1. Log in to OpenText Admin Center to collect the required configuration information. This includes:
   - Tunnel tenant
   - Tunnel key
2. Gather the remaining required information for setup, provided by OpenText onboarding support.
3. Fill out the fields on the **Editing and co-authoring in Microsoft 365** page. These fields are explained below: "Configuration options" on page 8.
4. Accept the *Online Editing Service Terms of Use*.
5. Click **Save**.

   If there is a problem with your configuration, an error message appears. If you receive an error, ensure that the **OES connector base URL** is correct and valid.
6. Click **Test**. For more information on testing and troubleshooting the connection to the online editing service (OEM), see "Test Microsoft 365 OES connection" on page 11.

Click **Reset** at any time to revert any changes made before saving your configuration.

Configuration options

General settings

Enable Editing and co-authoring in Microsoft 365
Controls whether editing with Microsoft 365 is enabled in OpenText Documentum CM. If this check box is cleared, the Microsoft 365 feature is not available, and users cannot edit or co-author with Microsoft 365. Enabling or disabling co-authoring in Microsoft 365 takes approximately 10 minutes to affectOpenText Documentum CM Smart View.

OES connector base URL
The URL of the online editing service connector deployment.

OES file size limit [MB]
Enter the size threshold (in MBs) of a document. When users open documents over this threshold, a message appears warning that the document exceeds the size limit editing might not work as expected. Enter `0` to disable this warning.

Default: `50`

Connector configuration

Customer name
Enter a name for the configuration's customer.

D2 rest endpoint
The URL of the D2–REST API. For example: `http://20.194.100.205:8181/d2-rest`

Tunnel tenant
The tenant's name, as listed in Admin Center.

Tunnel key
The **Connection name**, as listed in Admin Center

OTDS URL
The URL for the OTDS API. For example: `http://20.194.100.205:8080/otdsws`

OTDS client ID
The OTDS authorization client ID. For example: `oes-connector`

CORS
Enable or disable cross origin resource sharing (CORS) support.

CORS allowed origins
Specifies the origins that can be shared. If entering more than one, separate with a comma (`,`). For example, `http://opentext.com,https://test.com:8443`

CORS allowed methods
Specifies the HTTP methods allowed for CORS. The following are the supported methods:

- GET
- POST
- PUT
- DELETE
- OPTIONS
- HEAD

If entering more than one, separate with a comma (`,`). For example: `GET, POST, PUT, DELETE`

CORS allowed headers
Specifies the HTTP headers allowed to be sent. If entering more than one, separate with a comma (,).

For example: `Authorization, Content-Type,ot-dctm-product-code, DOCUMENTUM-CUSTOM-UNAUTH-SCHEME, Authorization, Content-Type, Accept, X-CLIENT-LOCATION, X-CLIENT-APPLICATION-NAME, x-sw-no-cache, x-d2-client-type, Location,x-d2-timezone,documentum-csrf-token`

OES subscriptions

Location
Select your region, which automatically populates some URL data. Select between **US**, **CA**, **AU**, or **Other**. If you select **Other**, you must define **OES endpoint URL**, **Webhooks auth URL**, and **Web socket URL**.

OES endpoint URL
The endpoint URL of the online editing service (OEM). For example: `https://officeonline.dev.com.dctm.com/hub`

Only required if you select **Other** for **Location**. URL provided by OpenText onboarding support.

Webhooks auth URL
The OT2 authentication server for your region. For example: `https://otdsauth.com.dctm.com/oauth2/token`

Only required if you select **Other** for **Location**. URL provided by OpenText onboarding support.

Web socket URL
Where to send events. Must be a valid public URL. For example: `wss://outposts.com.dctm.com/tunnel`

Only required if you select **Other** for **Location**. URL provided by OpenText onboarding support.

OES tenant ID
The tenant ID for your online editing service subscription.

OES client ID
The client ID for your online editing service subscription.

Vault
Enable or disable usage of Vault.

Vault key
Enter the vault key where the client secret is stored.

Does not appear if **Vault** is disabled.

Client secret
Enter the client secret code generated when you registered the online editing service (OES) application.

Does not appear if **Vault** is enabled.

2.2 Test Microsoft 365 OES connection

After filling out the fields on the **Editing and co-authoring in Microsoft 365** page and clicking **Save**, click **Test** to confirm OpenText Documentum CM can connect to the Microsoft 365 OES.

If the connection and your configuration works, a message appears that the test was successful.

If there is a problem with your connection or configuration, a message appears to describe the problem. The following are the possible error messages and recommended solutions:

- **Failed to validate the connection**: Ensure that the **OES connector base URL** is correct and valid.
- **Error in Obtaining Information from OES**: Ensure the **Tunnel tenant**, **Tunnel key**, and **OES endpoint URL** are valid and correct.
- **Failed to Test OES connector configuration**: Ensure the **OES tenant ID** in valid and correct.
- **Authentication to OES failed because an invalid credential is provided**: Ensure the **OES client ID** and **Client secret** are valid and correct.

Chapter 3

Sensitivity labels

Sensitivity labels from Microsoft Purview Information Protection allow organizations to classify and protect Microsoft 365 documents across devices, apps, and services. Sensitivity labels control access to content and can be applied with and without protection. Examples of sensitivity labels are *Public*, *Confidential*, and *Highly Confidential*.

Support for sensitivity labels allows OpenText Documentum Content Management (CM) to store and process documents with sensitivity labels while preserving the protection defined by those labels.

Support for sensitivity labels includes the following:

- **Protected storage:** Enables users to store labeled content with label information stored and visible.
- **Protected content processing:** Provides full-text indexing and thumbnail generation for content specified with sensitivity labels.
- **Protected transformation:** Enables PDF renditions of labeled content to be protected with the same sensitivity label as in the original document.

The following document types are supported:

- Microsoft Word (.doc, .docx, .docm)
- Microsoft PowerPoint (.ppt, .pptx)
- Microsoft Excel (.xls, .xlsx)
- Email (.msg)
- Adobe® Acrobat® (.pdf)

When sensitivity labels are available

Sensitivity labels are turned on and supported when each of the following is completed:

1. An administrator has turned sensitivity labels on in Admin Console. See "Turn sensitivity labels on" on page 14.
2. An administrator has selected the processes and sensitivity labels to be supported in the Smart View environment. See "Specify processes and sensitivity labels" on page 15.
3. An administrator has configured sensitivity labels in client configuration. See Section 24 "Microsoft Sensitivity Labels" in *OpenText Documentum Content Management - Client Configuration Guide (EDCCL-AGD)*.

For more information about sensitivity labels and their behavior, see Section 7 "Sensitivity labels" in *OpenText Documentum Content Management - Smart View User Help (EDCCL-H-UGD)*.

3.1 Configure sensitivity labels

Configure and set up sensitivity labels for your Smart View environment by following these procedures:

1. Register the sensitivity labels application in Microsoft Entra admin center.
2. Turn sensitivity labels on in Admin Console.
3. Optional Specify processes and sensitivity labels in Admin Console.
4. Configure sensitivity labels in client configuration. See Section 24 "Microsoft Sensitivity Labels" in *OpenText Documentum Content Management - Client Configuration Help (EDCCL-H-AGD)*.

Turn sensitivity labels on

The first step in configuration is to turn sensitivity labels on in your environment and provide the credentials you obtained when you registered the sensitivity labels as an application in the Microsoft Entra admin center (see "Register the sensitivity labels application" on page 16). This registration allows Smart View to capture the labels defined by your organization in the Microsoft Purview portal.

Enable sensitivity labels:

1. Sign in to Admin Console with the required access rights.
2. On the **Home** page, click the **Integrations** tile, click the **Microsoft** tile, and then click the **Microsoft Purview sensitivity labels** tile.
3. On the **Microsoft Purview Information Protection configuration** page, do the following:
   a. Turn the **Enable MIP** switch on.
   b. Enter the **Tenant ID**, **Client ID**, and **Client Secret** obtained when you registered sensitivity labels as an application in the Microsoft Entra admin center. For more information, see "Register the sensitivity labels application" on page 16.
4. Click **Test connection & Save**.

   If the test connection fails, you are notified that your entries are invalid. Click **Reset** at the top of the page and re-enter the information.

   If the connection test is successful, the information is saved, the page is refreshed, and an **Optional MIP processing** area appears below.
5. Optional Follow the steps in "Specify processes and sensitivity labels" on page 15.

Specify processes and sensitivity labels

The second step in configuration is to specify the processes and sensitivity labels that you want supported in Smart View. This step is optional.

Unlike other processes, such as transformation, full-text search indexing and thumbnail generation require explicit and more granular configuration because, based on permissions, they might expose content through search summaries and thumbnail views regardless of the protection applied.

Use the settings in the **Optional MIP processing** area of the **Microsoft Purview Information Protection configuration** page to apply this configuration by explicitly enabling search indexing and thumbnail creation.

To apply even more granular controls, include and exclude content from these processes by selecting the applicable sensitivity labels. Only content with a selected label is subject to search indexing or thumbnail creation.

Specify processes and sensitivity labels:

1. Ensure that you have tested and saved your sensitivity labels application credentials (see "Turn sensitivity labels on" on page 14) and that the **Optional MIP processing** area of the **Microsoft Purview Information Protection configuration** page is visible.
2. To turn on full-text search indexing of labeled content, select the **Search** check box.
3. To turn on thumbnail creation for labeled content, select the **Thumbnails** check box.
4. To update and synchronize the list of available labels with the Microsoft Purview portal, click the **Sync labels** button.

   Note: You can synchronize the list even if sensitivity labels are turned off (see "Turn sensitivity labels on" on page 14).
5. In the **Labels** list, select the applicable sensitivity labels to include/exclude content from the enabled processes.

   The selected labels appear in a box below. To remove a label, click the × button next to its name. Any labels that are no longer valid since the last synchronization (**Last synced**) appear in red.

   Note: Adding a label to the **Labels** box means that content with that label will have search indexing and/or thumbnail creation applied to it. To exclude content from these processes, ensure that the applicable labels do not appear in the box.
6. When you are done with your selection, click the **Save** button at the top of the page.

Important

- If you do not see an expected label in the **Labels** list, click the **Sync labels** button. You should now see the label in the list so you can select it.
- If you make a change in your Microsoft tenant settings (see "Turn sensitivity labels on" on page 14), your label selections are deleted and you need to make your selections again.
- If a change is made to a sensitivity label name, the new name appears in the **Labels** list but is not applied to any document that already has the label. The label name on existing documents is updated only when they are checked in and out or when a new version is uploaded. The name change also applies to newly imported documents.
- Changes made to your sensitivity label selections do not apply to labeled documents already in the repository. They do apply to newly imported documents and to existing documents when they are checked in and out or when a new version is added.

3.1.1 Register the sensitivity labels application

To turn sensitivity labels on in Admin Console, you must first register an application and add the required permissions in the Microsoft Entra admin center. Follow all the steps below:

1. Register the application:

1. Log in to the Microsoft Entra admin center with administrator privileges.
2. Select **App registrations** and then click **New registration**.
3. Enter a **Name** for the application.
4. Under **Supported account types**, select **Accounts in this organizational directory only (Single tenant)**.
5. Leave the **Redirect URI (optional)** fields empty.
6. Click **Register**.

2. Obtain the application credentials:

1. Select **Overview**.
2. Copy the **Application (client) ID** and **Directory (tenant) ID**.

   You will enter these credentials as **Client ID** and **Tenant ID**, respectively, when you enable sensitivity labels in Smart View (see "Turn sensitivity labels on" on page 14).

3. Create a client secret:

1. Select **Certificates & secrets** and then click **New client secret**.

2. Enter a **Description** and select a validity period in the **Expires** list.
3. Copy the client secret immediately. It will not be visible later.

   You will enter the client secret as **Client Secret** when you enable sensitivity labels in Smart View (see "Turn sensitivity labels on" on page 14).

4. Add permissions:

1. Select **API permissions**.
2. Click **Add a permission**.
3. On the **Request API permissions** page, select the **Microsoft APIs** tab.
4. Select **Azure Rights Management Services** as the Microsoft API.
5. Select **Application permissions** as the permission type.
6. In the **Select permissions** list, select **Content.SuperUser** and click **Add permission**.
7. Click **Grant admin consent** and then click **Yes**.
8. Repeat steps 2 to 7 to add the remaining permissions, following the table below:

API	Permission type	Permission name	Admin consent required
Azure Rights Management Services	Application	Content.DelegatedWriter	Yes
Azure Rights Management Services	Application	Content.Writer	Yes
Azure Rights Management Services	Delegated	user_impersonation	Yes
Microsoft Graph	Delegated	User.Read	Yes
Microsoft Information Protection (API)	Application	InformationProtectionPolicy.Read.All	Yes
Microsoft Information Protection Sync Service	Application	UnifiedPolicy.Tenant.Read	Yes