opentext™

OpenText™ Documentum™ Content Management for Microsoft® 365™

Deployment and Administration Guide

Deploy and configure OpenText Documentum Content Management (CM) for Microsoft 365.

EEMSODC250400-IGD-EN-01

OpenText™ Documentum™ Content Management for Microsoft® 365™
Deployment and Administration Guide
EEMSODC250400-IGD-EN-01
Rev.: 2025-Oct-31

This documentation has been created for OpenText™ Documentum™ Content Management for Microsoft® 365™ 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 CM for Microsoft 365 is an integration between Microsoft Teams, Microsoft SharePoint, and OpenText Documentum Content Management (CM), that provides seamless access across these platforms. It can be deployed as an app within both Microsoft Teams and Microsoft SharePoint.

This integration enables you to:

- Create or select an existing folder in the OpenText Documentum CM repository for the Microsoft Teams channel.
- Select an existing folder in the OpenText Documentum CM repository for the Microsoft SharePoint.
- Import a file from Microsoft Teams and Microsoft SharePoint to the repository.
- Navigate the repository folder structure.
- Preview the repository files in Microsoft Teams and Microsoft SharePoint.
- Edit Microsoft Word, Microsoft Excel, or Microsoft PowerPoint files from the repository using Microsoft Teams editor and in Microsoft SharePoint.
- Edit file properties.
- Add files and folders to Favorites.
- Convert to a virtual document.
- Send content to a Lifecycle state.

Chapter 2

Deploying OpenText Documentum CM for Microsoft 365

Use the following instructions to deploy OpenText Documentum CM for Microsoft 365.

2.1 Prerequisites

Ensure that your system meets the supported environments and compatibility requirements outlined in the *Release Notes* on My Support (support.opentext.com). You must install or deploy the following prerequisites before deploying OpenText Documentum CM for Microsoft 365:

- Apache® Tomcat™
- Java
- OpenText™ Documentum™ Content Management Client REST API: Ensure the REST API version matches the version of the OpenText™ Documentum™ Content Management client:
  - Make sure OpenText Documentum Content Management (CM) Client REST API is deployed in an environment with internet to communicate with Microsoft Entra ID and is running in HTTPS mode with a trusted certificate issued by CA.
- OpenText™ Documentum™ Content Management client configuration
- OpenText Directory Services (OTDS)
- Documentum Secret Integration Services (DSIS) (optional)
- If you are using OpenText™ Documentum™ Content Management Server 24.4 and later, make sure that you have a valid license associated with the product. For more information, see "Licensing OpenText Documentum CM" on page 19.

2.2 Deploying OpenText Documentum CM for Microsoft 365

Administrators can use the following instructions to deploy the OpenText Documentum CM for Microsoft 365 files on the servers.

Note: OpenText Documentum CM for Microsoft 365 and Online Editing Service (OES Connector) version must be same as OpenText Documentum CM client.

To deploy OpenText Documentum CM for Microsoft 365:

1. Download and extract OpenText Documentum CM - Microsoft Integrations 25.4 from OpenText My Support. Extract the `SmartViewM365_25.4` ZIP file.
2. Use the following files from the extracted folder to deploy OpenText Documentum CM for Microsoft 365:
   - `DAR`
   - `EncryptionUtil.zip`
   - `NotificationService.zip`
   - `SmartviewM365.zip`
   - `TeamsSmartviewCache.dar`
   - `LanguagePack.zip`
   - `xECMUsersProject.dar`

   Note: If you are using OpenText Documentum Content Management (CM) Server 24.4 or 25.2, then deploy the matching Documentum Composer version of the `TeamsSmartviewCache.dar` and `xECMUsersProject.dar` files the *<Extracted zip location>*`\DAR\TeamsSmartviewCache\`*<version>* and *<Extracted zip location>*`\DAR\xECMUsersProject\`*<version>* respectively.
3. Register the OpenText Documentum CM for Microsoft 365 application in Microsoft Entra admin center using the following steps:

   Go to App registrations

   a. Click **New Registration**.

   b. Specify the name of the application.

   c. Click **Register**.

   Go to Manage > Authentication

   a. Select **Accounts in this organizational directory only (Single tenant)**.

b. Go to **Overview** from the pane and copy the `Application (client) ID` and `Directory (tenant) ID`.

c. Go to **Authentication** > **Platform configurations** > **Add a platform** and select a **Single Page Application**.

d. Select **Redirect URIs** and provide the URL

`https://<hostname>:<port>/SmartViewM365/ui`

e. In **Implicit grant and hybrid flows**, select the following check boxes:

- **Access token (used for implicit flows)**
- **ID token (used for implicit and hybrid flows)**

f. Click **Configure**.

Go to Manage > Certificates & secrets

a. Click **New client secret**.

b. Specify the description in the **Description**, and click **Add**.

c. Copy the added value of the secret and save.

Go to Manage > API permissions

a. Click **Add a permission**.

b. Select **Microsoft Graph**.

c. Select **Delegated permissions**, and select the following delegated permissions:

```
Files.Read
Files.Read.All
Files.ReadWrite
Files.ReadWrite.All
Mail.read
offline_access
User.Read
TeamMember.Read.All
```

d. Select **Application permissions**, and select the following application permissions:

```
Directory.Read.All
Directory.ReadWrite.All
GroupMember.Read.All
User.Read.All
User.ReadBasic.All
TeamMember.Read.All
```

e. Select **Microsoft SharePoint**.

f. Select **Delegated permissions**, and select the following delegated permissions:

```
AllSites.Read
AllSites.Write
MyFiles.Read
MyFiles.Write
```

```
User.Read.All
User.ReadWrite.All
```

g. Click **Add permission**.

h. Select **Grant admin consent** to grant all the permissions.

Go to Manage > Expose an API

a. Click **Add** next to the **Application ID URI**.

b. In the **Edit application ID URI** screen, under **Application ID URl**, specify the scope name as illustrated in the following format:

`api://<smartviewM365 server host>:<port>/<auto generated id>`

For example,

```
api://banddqa902.otxlab:8443/
988beae6-8c4b-46ab-9013-22f8e9033355
```

c. Click **Save**.

d. Click **Add a scope**.

e. In the **Add a scope** screen, specify the **Scope name**, **Admin consent display name**, **Admin consent description** and click **Add scope**.

f. Click **Add a client application** section, for **Client ID**, add the following globally unique identifier (GUID):

```
1fec8e78-bce4-4aaf-ab1b-5451cc387264
5e3ce6c0-2b1f-4285-8d4b-75ee78787346
```

4. Deploy `TeamsSmartviewCache.dar` and `xECMUsersProject.dar` in Documentum CM Server.

5. Deploy OpenText Documentum CM for Microsoft 365 in Tomcat using the following steps:

To deploy OpenText Documentum CM for Microsoft 365 for Windows:

a. Extract `SmartviewM365.zip` file downloaded from OpenText My Support. The extracted `SmartviewM365.zip` contains:

- `D2-Config.zip`
- `d2sv-msgrpgh_plugin-<version>.jar`
- `msgraph.properties`
- `SmartViewM365.war`

b. Copy the `SmartViewM365.war` file and perform the following steps:

i. Start Tomcat to extract the `SmartViewM365.war` file content.

ii. Stop the Tomcat application server.

iii. Remove the `SmartViewM365.war` file.

c. Update the following values, which are used to generate the manifest, in the `value.xml` file located in the `<Tomcat>/webapps/SmartViewM365/` file path:

XML file tags	Description
`<appname>`	Name of the app. The default name of the app is `Documentum`.
`<d2rest_url>`	Client REST API URL. For example, `https://myrestserver:8080/D2-Rest`
`<host>`	Domain name of SmartViewM365 server. For example, `mydomain.teams.net:8090`
`<teamsrootpath>`	The Teams home page or mapped folder. Make sure the `<teamsrootpath>` is not blank. By default, the `/TeamsM365` cabinet is created in the Documentum CM Server. Make sure that you provide the `WRITE` permission to `<dm_world>` on the `/TeamsM365` cabinet or the configured path.
`<clientid>`	Provide the client ID that you have copied during app registration in Microsoft Entra admin center.
`<loglevel>`	The log level of the Tomcat server. The recommended value is `ERROR`.
`<window>`	Log files open in a new window if set to `true`. The recommended value is `false`.
`<consoleRe>`	Log files open in the console if set to `true`. The recommended value is `false`.
`<performancetimestamp>`	Provides the detailed time stamp hh:mm:ss in the log file if set to `true`. The recommended value is `false`.
`<timing>`	Provides the time stamp in hh:mm format for the log files if set to `true`. The recommended value is `true`.
`<sharepointdomains>`	Microsoft SharePoint domain name where the app is deployed. **Note:** This configuration is required for the Microsoft SharePoint app only.
`<tenantid>`	Provide the tenant ID of your app that you have copied during app registration in Microsoft Entra admin center.
`<appredirecturi>`	The redirection URI that you configured in the app in Microsoft Entra admin center.

XML file tags	Description
`<importconfig>`	Indicates the configuration for import operation (`move` or `copy` or `both`).
`<defaultconfig>`	The default value is set to `copy`. Based on the requirement for your import operation, your administrator can set the value `move` or `copy` to have the default selected button for import in the dialog box.
`<rootreposelection>`	If you set the value to `true`, the root of the repository is displayed on the configuration page of the app. If you set the value to `false`, you can choose to map any folder or location in the repository. The default value for `rootreposelection` is set to `false`.

d. Run the `setup.bat` file located in the *<Tomcat>*`/webapps/SmartViewM365/` file path in Tomcat. The `SmartViewM365` manifest file is generated for both Microsoft Teams and Microsoft SharePoint in their respective folders.

   Manifest file path for Microsoft Teams: *<Tomcat>*`/webapps/SmartViewM365/manifests/download/teams`

   Manifest file path for Microsoft SharePoint: *<Tomcat>*`/webapps/SmartViewM365/manifests/download/sharepoint`

e. Restart the Tomcat server.

To deploy OpenText Documentum CM for Microsoft 365 for Linux:

a. Extract `SmartviewM365.zip` file downloaded from OpenText My Support. The extracted `SmartviewM365.zip` contains:

   - `D2-Config.zip`
   - `d2sv-msgrpgh_plugin-`*<version>*`.jar`
   - `msgraph.properties`
   - `SmartViewM365.war`

b. Copy the `SmartViewM365.war` file and paste in `<root_path>/ApacheTomcat/webapps` location, and then perform the following steps:

   i. Start Tomcat to extract the `SmartViewM365.war` file content.

   ii. Stop the Tomcat application server.

   iii. Remove the `SmartViewM365.war` file.

c. Update the following values, which are used to generate the manifest, in the `launcher.json` file located in the *<Tomcat>*`/webapps/SmartViewM365/ui/` file path:

XML file tags	Description
<app_server_url>	d2rest_url is OpenText Documentum CM client REST URL. Make sure <app_server_url> is not blank. For example, https://<appserver:<port>/d2rest
<teamsrootpath>	The Teams home page or mapped folder. Make sure the <teamsrootpath> is not blank. By default, the /TeamsM365 cabinet is created in the Documentum CM Server. Make sure that you provide the WRITE permission to <dm_world> on the /TeamsM365 cabinet or the configured path.
<appclientid>	Provide the client ID that you have copied during app registration in Microsoft Entra admin center. For example, 3236905f-eb36-4d13-9530-b5260320
<sharepointdomains>	Microsoft SharePoint domain name where the app is deployed. For example, https://abc.sharepoint.com **Note:** This configuration is required for the Microsoft SharePoint app only.
<tenantid>	Provide the tenant ID of your app that you have copied during app registration in Microsoft Entra admin center.
<appredirecturi>	The redirection URI that you configured in the app in Microsoft Entra admin center. Indicates the configuration for import operation (move or copy or both). For example, https://myrestserver:<port>/SmartViewM365/ui
<importconfig>	Indicates the configuration for import operation (move or copy or both).
<defaultconfig>	The default value is set to copy. Based on the requirement for your import operation, your administrator can set the value move or copy to have the default selected button for import in the dialog box.

XML file tags	Description
<rootreposelection>	If you set the value to true, the root of the repository is displayed on the configuration page of the app. If you set the value to false, you can choose to map any folder or location in the repository. The default value for rootreposelection is set to false.

d. Update the manifest.json file located in SmartViewM365\manifests\manifest\manifest.json path to generate the manifest. Perform the following to update the manifest file:

- Update application name in the following command:

```
"name": {
      "short": "linuxTest2",
      "full": "linuxTest2"
  },
```

- Update appType as teams or sharepoint in the following command:

```
"configurableTabs": [
      {
          "configurationUrl": "https://cs244rhorb141.otxlab.net:8081/
SmartViewM365/ui/?appType=teams#teamsconfig",
          "canUpdateConfiguration": true,
          "scopes": ["team"]
      }
```

- Update the SmartviewM365 server host and port in the following command:

  For example: mydomain.teams.net:8090

```
],
"validDomains": [
      "cs244rhorb141.otxlab.net:8081"
  ],
```

- Provide Azure app registration client ID for id and hostname for resource in the following command:

  For example, mydomain.teams.net:8090.

```
"webApplicationInfo": {
      "id": "c554c07a-67ff-4ae5-b914-0c54256ccb2b",
      "resource": "api://cs244rhorb141.otxlab.net:8081/c554c07a-67ff-4ae5-
b914-0c54256ccb2b"
  },
```

- After the manifest.json file is updated, compress all files into a ZIP archive within the SmartviewM365 folder.

e. Restart the Tomcat server.

6. Configure Client REST API for OpenText Documentum CM for Microsoft 365 using the following steps:

   a. Add the following tags in the rest-api-runtime.properties file located in *<Tomcat>*\webapps\D2REST\WEB-INF\classes\ in Client REST API.

```
rest.cors.enabled=true
rest.cors.allowed.origins=<xECM server: Port>
rest.cors.allowed.methods=GET, POST, PUT, DELETE, OPTIONS, HEAD
rest.cors.allowed.headers=OT-DCTM-PRODUCT-CODE, DOCUMENTUM-CUSTOM-UNAUTH-
SCHEME, Authorization, Content-Type, Accept, X-CLIENT-LOCATION, X-CLIENT-
APPLICATION-NAME, X-D2-CLIENT-TYPE, DOCUMENTUM-CSRF-TOKEN
rest.cors.exposed.headers=Location, Accept-Ranges, Content-Encoding,Content-
Length, Content-Range,Authorization, Content-Disposition, Set-Cookie,
DOCUMENTUM-CSRF-HEADER-NAME, Date, Content-Type, Connection,DOCUMENTUM-CSRF-
QUERY-NAME, X-Allow-Within-IFrame
rest.security.auth.mode=ct-otds_token
rest.security.csrf.enabled=true
rest.security.csrf.http_methods=POST,PUT,DELETE
rest.security.csrf.generation.method=server
rest.security.csrf.header_name=DOCUMENTUM-CSRF-TOKEN
rest.security.csrf.parameter_name=csrf-token
rest.security.csrf.token.length=256
rest.dql.access.mode=group
rest.dql.access.groups=group1,group2,group
rest.security.client.token.cookie.samesite=none
rest.context.config.location=com.emc.d2.rest.context.jc,com.opentext.d2.rest.co
ntext.jc,com.opentext.ls
```

Note: In the `rest-api-runtime.properties` file the `dql.disallowed.types=` attribute should not have the following `dm_formate`, `dm_user`, `dm_subscription`, `dm_relation`, `dm_document`.

b. Configure one of the following authentication in `rest.security.auth.mode` within the `rest-api-runtime.properties` file located in the *<Tomcat>*`\webapps\D2REST\WEB-INF\classes\` file path:

- `basic-ct`: To configure basic authentication
- `ct-otds_token`: To configure OTDS authentication. For more information on OTDS authentication, see *OpenText Documentum Content Management - Client Installation Guide (EDCCL250400-IGD)*.

c. Deploy the `d2sv-msgraph_plugin-`*<version>*`.jar` file extracted from the `SmartviewM365.zip` file in Client REST API at the `<tomcat>\webapps\D2REST\WEB-INF\lib\` file path.

If you want to enable the `move` operation from Microsoft Teams and Microsoft SharePoint to OpenText Documentum CM, make sure you enable *Checksum* in Documentum CM Server.

d. Copy the `msgraph.properties` file downloaded from the OpenText My Support in step 3 to the Client REST API deployment path such as, *<Tomcat>*`\webapps\D2REST\WEB-INF\classes\`:

Update the following content in the `msgraph.properties` file:

```
app.client.id=<client_id>
app.client.secret=<client_secret>
app.tenant.id=<tenant_id>
app.scope = Mail.read offline_access
app.config.proxy.config.host=<hostname/IP_address>
app.config.proxy.config.port=<Port_number>
```

where:

- *<client_id>* is the Microsoft Graph registration client ID.

- *<client_secret>* is the Microsoft Graph registration client secret value.
- *<tenant_id>* is the Microsoft Graph tenant ID.

  If you are using a proxy server, provide the hostname or IP address and port number of the proxy server.

e. Restart Tomcat.

7. Configure OpenText Documentum Content Management (CM) client configuration for OpenText Documentum CM for Microsoft 365 using the following steps:

   a. Extract the `D2-config.zip` file downloaded in step 3 on page 41. This contains the `Teams-config.zip` file.

   b. In client configuration, import the `Teams-config.zip` file and select the following options:

      - **FOLDER** and **xecmdms_teams_Acl** for the security configuration element
      - **xecmdms_channel** and **xecmdms_teams** for the context

      Note: The configuration elements and contexts should be mapped to the respective application.

   c. Configure the following security configuration elements in the client configuration:

      - For the **xecmdms_channel** context, enable the **FOLDER** security configuration element.
      - For the **xecmdms_teams** context, enable the **xecmdms_teams_Acl** security configuration element.

   d. Refresh the client configuration cache.

   Configure the Tile View for the OpenText Documentum CM for Microsoft 365 app to be used in Microsoft SharePoint, in client configuration. For more information, see the *OpenText Documentum Content Management - Client Configuration Guide (EDCCL250400-AGD)*.

The Microsoft Teams administrator must upload the generated manifest file for all users in Microsoft Teams admin center to make the app available in Microsoft Teams.

Note: When you upload the manifest file, make sure the file is in a ZIP format.

2.3 Configuring OTDS account for OpenText Documentum CM for Microsoft 365

Prerequisite

- Ensure that the OTDS service is deployed and working properly.

To create a system account user in OTDS for OpenText Documentum CM for Microsoft 365:

1. Create a separate OTDS resources for each OpenText Documentum CM repository. For more information, see, *OpenText Directory Services - Installation and Administration Guide (OTDS250400-IWC)*.
2. Create an individual OTDS partitions corresponding to each repository. For more information, see, *OpenText Directory Services - Installation and Administration Guide (OTDS250400-IWC)*.
3. Upload the license to OTDS and apply it to all repositories on the OpenText Documentum CM. For more information, see *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.
4. Create a dedicated partition named `M365SystemPartition` in OTDS for OpenText Documentum CM for Microsoft 365.

   Note: You can use same partition created for OpenText Documentum CM Online Editing Service.
5. Configure OTDS authentication:
   - Create a user in OTDS with the username `M365_SERVICE` and password `Xecmserviceuser@123` (password is case sensitive).
   - In the **Password Options** area:
     - Select **Do not require password change on reset**.
     - Clear the **User cannot change password** check box.
     - Select the **Password never expires** check box.
   - Create the user `M365_SERVICE` in the `M365SystemPartition`.
   - Allocate the license for your product. For more information, see *OpenText Directory Services - Installation and Administration Guide (OTDS250400-IWC)*.

   Note: Since `M365_SERVICE` is a service account, its password is automatically updated by the system after the service starts.
6. Consolidate the `M365_SERVICE` user to all required repositories. Ensure that the `M365_SERVICE` user is synced to each consolidated repositories.
7. Create an OTDS Client ID, for example, `d2_oauth_client`.

- Ensure the **Confidential** option is not selected.
- In the **Redirect URLs** tab, add the following:
  - `https://<D2_REST hostname>:port/D2REST`

2.4 Uploading manifest file for Microsoft Teams and Microsoft SharePoint

To upload the manifest file in Microsoft Teams:

1. Log in to the Microsoft 365 Admin Center with your administrator credentials.
2. In **Admin centers**, select **Teams**.
3. Go to **Teams apps**, and select **Manage apps**.
4. On the **Manage apps** page, under **Actions**, select **Upload new app**.
5. Click **Upload** and select the .zip file.

   The Microsoft Teams owner can now add the app to the required channel.
6. Select one of the following options for uploading:
   - **For your organization**: Upload apps that are available for the entire organization.
   - **For specific users or teams**: Upload apps just for specific users or teams.

To upload the manifest file in Microsoft SharePoint:

1. Log in to the Microsoft 365 Admin Center with your administrator credentials.
2. Select **Admin centers** and click **SharePoint** to open the SharePoint Admin Center.
3. In Microsoft SharePoint Admin Center, in the **More features** section, go to **Apps**, and click **Open**.
4. On the **Manage apps** page, click **Upload** and select the app.

   Browse for the .zip file that contains the custom SharePoint app package.
5. In the **Enable app** panel, select the **Enable this app and add it to all sites** option, and then click **Enable app** button.

   Anyone with the appropriate permissions can now add the app, which is available for all sites, to the page.

2.5 Configuring Documentum Secret Integration Service

To configure the Documentum Secret Integration Service (DSIS) for use with the OpenText Documentum CM for Microsoft 365, follow these steps:

- Set up Documentum Secret Integration Service (DSIS) as described in the *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.
- In the `<dsis>/application.properties` file, add the `vaultEnabled=true` attribute.
- In the HashiCorp Vault server, create the following secret name and key pairs for the OpenText Documentum CM for Microsoft 365:
  - For Database Password (encrypted):
    - Secret_Name: `M365NS_DBPASSWORD`
    - Key_Name: `dbpassword`
  - For Database Password (unencrypted):
    - Secret_Name: `M365NS_DBPASSWORD`
    - Key_Name: `unencrypteddbpassword`
- Define the system environment variable `%VAULT_HOME%` and set its location. For example, `C:/Program Files/`.

Note: Use the same database and the `M365_SERVICE` user account for both `SmartviewM365-Teams` and the `OES Connector`, as the Notification Service is shared between them.

2.6 Post-deployment task

2.6.1 Licensing OpenText Documentum CM

OpenText Documentum CM uses OpenText Directory Services (OTDS) to apply licenses for all OpenText Documentum CM components. For more information about procuring the license file and configuring OTDS and license, see *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

Chapter 3

Deploying OpenText Documentum CM Online Editing Service

To use Microsoft 365 online editing feature, you must deploy OpenText Documentum CM Online Editing Service (OES Connector) which enables the editing of files directly in the browser while within OpenText Documentum CM client.

Use the following instructions to deploy OES Connector.

3.1 Prerequisites

Ensure that your system meets the supported environments and compatibility requirements outlined in the *Release Notes* on My Support (support.opentext.com). Perform the following prerequisites before deploying Online Editing Service:

- Apache® Tomcat™
- Java
- OpenText™ Documentum™ Content Management Client REST API: Ensure the REST API version matches the version of the OpenText™ Documentum™ Content Management client
- Database: Supported database include PostgreSQL, Microsoft SQL Server, and Oracle

  Note: Before deployment, select the database type and create the database to set up the required tables. For MSSQL, you must create the database name as `OES_CONNECTOR`.
- OpenText™ Documentum™ Content Management client configuration
- OpenText Directory Services (OTDS)
- Documentum Secret Integration Services (DSIS) (optional)

3.2 Deploying Online Editing Service

Administrators can deploy the OES Connector files on the servers using following procedures.

Note: Ensure that the version of OpenText Documentum CM for Microsoft 365, which contains Online Editing Service and Notification Service, is the same as the version of OpenText Documentum CM client.

To deploy OpenText Documentum CM Online Editing Services:

1. Download and extract OpenText Documentum CM - Microsoft Integrations 25.4 from OpenText My Support. Extract the `SmartViewM365_25.4` ZIP file.
2. Use the following files from the extracted folder to deploy OpenText Documentum CM Online Editing Services:
   - `dbutil`
   - `EncryptionUtil.zip`
   - `NotificationService.zip`
   - `oes_setup.bat`
   - `OESConnector.zip`
   - `OESConnectorDAR.dar`
3. For Windows: When you run the `oes_setup.bat` file, it prompts you to enter values for each parameter interactively. Perform the following:
   a. Open a command prompt and run the `oes_setup.bat` file. The following options appear in the command prompt:

```
1.Fresh Install
2.Update Current Installation
3.STOP OES Connector
4.STOP Notification Service
5.Start OES Connector
6.Start Notification Service
7.Start/Stop Notification Service as Windows Service
8.Exit
```

   b. Type `1` to deploy the Online Editing Service. During the new deployment, the OES Connector Service and Notification Service starts automatically.
   c. Enter the Tomcat installation directory path when prompted.
   d. Provide notification service port number. Press Enter to use the default port.
   e. Select the required database type from the following option.

```
1.Oracle
2.MSSQL
3.PostgreSQL
```

   The administrator must create the database name prior to allow table creation.

f. Specify whether the selected database uses SSL or non-SSL.

g. Enter values for the following variables when prompted:

Variables	Description
<Is vault enabled?>	Type y if the HashiCorp Vault is enabled. Type n if the HashiCorp Vault is disabled.
<jdbc_username>	JDBC username. For example, jdbcusername.
<jdbc_password>	JDBC encrypted password. Use the encrypt_your_password command file to encrypt the password. After the password is encrypted, update the value in the parameter. **Note:** If VaultEnabled is set to true, leave this field blank.
<jdbc_url>	JDBC URL. It will be prompted when database is SSL. For example, jdbc:postgresql://mydatabaseserver:5432/notificDB.
<hostname>	Hostname of the database server. For example, localhost.
<port>	Database server port number. For example, 5432. Default values: • PostgreSQL: 5432 • Oracle: 1521 • MSSQL: 1433
<dbname>	Database name. For example, my12database123.
<proxy_host>	Proxy host (if applicable).
<proxy_port>	Proxy port (if applicable).
<http-go-server-port>	Port number of the go server. Default port number is 8888 and keep this port open.

h. Select the required option to deploy Notification Service.

```
1.Run in Console Mode
2.Install as Windows service
```

Note: You can also run the oes_setup.bat file to:

- Update Current Installation
- STOP OES Connector

- STOP Notification Service
- Start OES Connector
- Start Notification service
- Start/Stop Notification Service as Windows Service
- Exit

i. Deploy the OESConnectorDAR.dar and OESConnectorDAR.installparam files from the OESConnector folder to the Documentum CM Server. During deployment, specify OESConnectorDAR.installparam as **Input File**.

Note: Use the latest version of Documentum Composer to deploy the OESConnectorDAR.dar file.

4. For Linux: Perform the following:

a. Extract OESConnector.zip file downloaded from OpenText My Support. The extracted folder contains the following files:

- DAR
- deployment
- oes-connector.war
- OESConnectorDAR.dar
- OESConnectorDAR.installparam
- xECMUsersProject.dar

b. Deploy the OESConnectorDAR.dar and OESConnectorDAR.installparam files from the OESConnector folder to the Documentum CM Server. During deployment, specify OESConnectorDAR.installparam as **Input File**.

Note: Use the latest version of Documentum Composer to deploy the OESConnectorDAR.dar file.

c. Copy oes-connector.war file and paste in <root_path>/ApacheTomcat/webapps location. For example, /root/ApacheTomcat/apache-tomcat-10.1.46/webapps/

d. Start Tomcat to extract the content from oes-connector.war file.

e. Stop the Tomcat application server.

f. Remove the oes-connector.war file.

g. The following table lists the parameters and their descriptions. Manually update the values for following variables in the database.properties file located in oes-connector\WEB-INF\classes\config:

Parameter / XML Tag	Description
<jdbc_username>	JDBC username. For example, jdbcusername.

Parameter / XML Tag	Description
<jdbc_password>	JDBC encrypted password. Use the encrypt_your_password command file to encrypt the password. After the password is encrypted, update the value in the parameter. **Note:** If VaultEnabled is set to true, leave this field blank.
<jdbc_dbSchemaName>	The SchemaName of the JDBC database. For example, public.
<jdbc_driverClassName>	The className of the JDBC driver. • For PostgreSQL: org.postgresql.Driver • For Oracle: oracle.jdbc.driver.OracleDriver. • For MSSQL: jdbc.driverClassName =com.microsoft.sqlserver.jdbc.SQLServerDriver.
<jdbc_url>	JDBC URL. For example, jdbc:postgresql://mydatabaseserver:5432/notificDB.
<quartz.dbDelegateClass>	Delegate class of the database.
<databaseSecretKeyName>	Secret key name of the database. **Note:** Do not change this value if VaultEnabled is set to true.

h. Update the values for following variables in the setup.properties file located in oes-connector\WEB-INF\classes\config:

Parameter / XML Tag	Description
<notificationserviceHost>	Hostname of the Notification Service.
<notificationservicePort>	Notification Service port number.

5. Configure Client REST API for OpenText Documentum CM Online Editing Service using the following steps:

a. Add the following tags in the rest-api-runtime.properties file located in *<Tomcat>*\webapps\D2REST\WEB-INF\classes\ in Client REST API.

```
rest.cors.enabled=true
rest.cors.allowed.origins=<xECM server: Port>
rest.cors.allowed.methods=GET, POST, PUT, DELETE, OPTIONS, HEAD
rest.cors.allowed.headers=OT-DCTM-PRODUCT-CODE, DOCUMENTUM-CUSTOM-UNAUTH-
SCHEME, Authorization, Content-Type, Accept, X-CLIENT-LOCATION, X-CLIENT-
APPLICATION-NAME, X-D2-CLIENT-TYPE, DOCUMENTUM-CSRF-TOKEN
rest.cors.exposed.headers=Location, Accept-Ranges, Content-Encoding,Content-
Length, Content-Range,Authorization, Content-Disposition, Set-Cookie,
DOCUMENTUM-CSRF-HEADER-NAME, Date, Content-Type, Connection,DOCUMENTUM-CSRF-
QUERY-NAME, X-Allow-Within-IFrame
```

```
rest.security.auth.mode=ct-otds_token
rest.security.csrf.enabled=true
rest.security.csrf.http_methods=POST,PUT,DELETE
rest.security.csrf.generation.method=server
rest.security.csrf.header_name=DOCUMENTUM-CSRF-TOKEN
rest.security.csrf.parameter_name=csrf-token
rest.security.csrf.token.length=256
rest.dql.access.mode=group
rest.dql.access.groups=group1,group2,group
rest.security.client.token.cookie.samesite=none
rest.context.config.location=com.emc.d2.rest.context.jc,com.opentext.d2.rest.co
ntext.jc,com.opentext.ls
```

Note: In the `rest-api-runtime.properties` file the `dql.disallowed.types=` attribute should not have the following `dm_formate`, `dm_user`, `dm_subscription`, `dm_relation`, `dm_document`.

b. Configure the following authentication in `rest.security.auth.mode` within the `rest-api-runtime.properties` file located in the *<Tomcat>*`\webapps\D2REST\WEB-INF\classes\` file path:

- `ct-otds_token`: For OTDS authentication. For more information on OTDS authentication, see *OpenText Documentum Content Management - Client Installation Guide (EDCCL250400-IGD)*.

c. Restart Tomcat to apply the changes.

6. Deploy Notification Service for OES Connector. For more information, see "Deploying Notification Service for OES Connector" on page 34.

Notes

- After deployment, configure the OES Connector in the Admin Console. For more information, see *OpenText Documentum Content Management - Microsoft Integrations Admin Console Guide (EDCADC-AIN)*.
- To verify that the OES Connector Service is running:
  - For health: `https:<host>:<port>/oes-connector/health`
  - For version: `https:<host>:<port>/oes-connector/version`

3.3 Configuring OTDS account for OES Connector

Prerequisite

- Ensure that the OTDS service is deployed and working properly.

To create a system account user in OTDS for OES connector:

1. Create a separate OTDS resources for each OpenText Documentum CM repository. For more information, see, *OpenText Directory Services - Installation and Administration Guide (OTDS250400-IWC)*.
2. Create an individual OTDS partitions corresponding to each repository. For more information, see, *OpenText Directory Services - Installation and Administration Guide (OTDS250400-IWC)*.

3. Upload the license to OTDS and apply it to all repositories on the OpenText Documentum CM. For more information, see *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.
4. Create a dedicated partition named `M365SystemPartition` in OTDS for the `OES connector service`.

   Note: You can use same partition created for OpenText Documentum CM for Microsoft 365.
5. Configure OTDS authentication:
   - Create a user in OTDS with the username `M365_SERVICE` and password `Xecmserviceuser@123` (password is case sensitive).
   - In the **Password Options** area:
     - Select **Do not require password change on reset**.
     - Clear the **User cannot change password** check box.
     - Select the **Password never expires** check box.
   - Create the user `M365_SERVICE` in the `M365SystemPartition`.
   - Allocate the license for your product. For more information, see *OpenText Directory Services - Installation and Administration Guide (OTDS250400-IWC)*.

   Note: Since `M365_SERVICE` is a service account, its password is automatically updated by the system after the service starts.
6. Consolidate the `M365_SERVICE` user to all required repositories. Ensure that the `M365_SERVICE` user is synced to each consolidated repositories.
7. Grant superuser privileges to the `M365_SERVICE` user in all available repositories.
8. Create an OTDS Client ID, for example, `oes_oauth_client`.
   - Ensure the **Confidential** option is not selected.
   - In the **Redirect URLs** tab, add the following:
     - `https://<oes-connector hostname>:port`
9. Select **Trusted Sites**.
10. Click **Add** and then provide `https://<Admin console>:<port>` URL.

3.4 Configuring Documentum Secret Integration Service for OES Connector

To configure the Documentum Secret Integration Service (DSIS) for use with the OES Connector, follow these steps:

- Set up Documentum Secret Integration Service (DSIS) as described in the *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.
- In the `<dsis>/application.properties` file, add the `vaultEnabled=true` attribute.
- In the HashiCorp Vault server, create the following secret name and key pairs for the OES Connector:
  - For Database Password:
    - Secret_Name: `OES_DATABASE_PASSWORD`
    - Key_Name: `oesConnector`
  - For OES Client Secret:
    - Secret_Name: `OES_CLIENT_SECRET`
    - Key_Name: `oesConnector`

    Note: Ensure that the password and client secret are encrypted.
- Define the system environment variable `%VAULT_HOME%` and set its location. For example, `C:/Program Files/`.

Note: Use the same database and the `M365_SERVICE` user account for both `SmartviewM365-Teams` and the `OES Connector`, as the Notification Service is shared between them.

3.5 Post-deployment task

3.5.1 Licensing OpenText Documentum CM

OpenText Documentum CM uses OpenText Directory Services (OTDS) to apply licenses for all OpenText Documentum CM components. For more information about procuring the license file and configuring OTDS and license, see *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

Chapter 4

Deploying Notification Service

The Notification Service is used for user synchronization between Microsoft Teams and Documentum CM Server and between Online Editing Service (OES) and OES Connector Service.

4.1 Prerequisites

- Java
- Client REST API
- Database configuration
  - Oracle
  - PostgreSQL
  - MSSQL
- Create or have access to database with necessary permissions to create table in the database, in Oracle or PostgreSQL or MSSQL.
- Add the following **Application Permissions** during app registration for OpenText Documentum CM for Microsoft 365 in Microsoft Entra admin center, refer section step 3:

```
Directory.Read.All
Directory.ReadWrite.All
GroupMember.Read.All
User.Read.All
User.ReadBasic.All
TeamMember.Read.All
```

- For OTDS authentication: Administrator must create the user in OTDS with the user name as `M365_SERVICE` and password as `Xecmserviceuser@123` (password is case sensitive). In the **Password Options** area, select **Do not require password change on reset** from the list and do the following:
  - Clear the **User cannot change password** check box.
  - Select the **Password never expires** check box.

  Allocate the license to the `M365_SERVICE` user for your product. For more information, see *OpenText Directory Services - Installation and Administration Guide (OTDS250400-IWC)*.

  Note: Since `M365_SERVICE` is a service account, its password will be automatically updated by the system after the service starts.

4.2 Deploying Notification Service for OpenText Documentum CM for Microsoft 365

1. Extract the `NotificationService.zip` file downloaded from OpenText My Support.
2. If you are using `Basic` authentication, deploy the `xECMUsersProject.dar` file in the Documentum CM Server.
3. You must create the database manually, based on the created database, edit and run the respective script in Query tool to create DB schema:
   - **For Oracle**:
     1. Open the `\NotificationService\deployment\oracle\teams_notifications_oracle.sql` file.
     2. Run the `teams_notifications_oracle.sql` file.
   - **For PostgreSQL**:
     1. Open the `\NotificationService\deployment\postgres\teams_notifications_postgres.sql` file.
     2. Run the `teams_notifications_postgres.sql` file.
   - **For MSSQL**:
     1. Open the `\NotificationService\deployment\sqlserver\teams_notifications_mssql.sql` file.
     2. Run the `teams_notifications_mssql.sql` file.
4. Run the `encrypt_your_password.cmd` script from `NotificationService\encrypt_your_password.cmd` location to encrypt the given database password. Specify a password and press enter to get an encrypted password and save it for future.
5. For Windows:
   - Update the values for following variables in the `values.xml` file:

Parameter / XML Tag	Description
`<hostname>`	Hostname of the database server. For example, `mydomain.teams.net`.
`<port>`	Database server port number. For example, `5432`. Default values: – PostgreSQL: `5432` – Oracle: `1521` – MSSQL: `1433`

Parameter / XML Tag	Description
<dbname>	Database name. For example, my12database123.
<jdbc_username>	JDBC username. For example, jdbcusername.
<vaultEnabled>	Set the value to true to enable the Vault and set the value to false to disable the Vault. For more information on configuring Vault, see "Configuring Documentum Secret Integration Service" on page 19.
<jdbc_password>	JDBC encrypted password. Use the encrypt_your_password command file to encrypt the password. After the password is encrypted, update the value in the parameter. **Note:** If VaultEnabled is set to true, leave this field blank.
<jdbc_dbSchemaName>	The SchemaName of the JDBC database. For example, public.
<jdbc_driverClassName>	The className of the JDBC driver. – For PostgreSQL: org.postgresql.Driver – For Oracle: oracle.jdbc.driver.OracleDriver. – For MSSQL: jdbc.driverClassName =com.microsoft.sqlserver.jdbc.SQLServerDriver.
<jdbc_url>	JDBC URL. For example, jdbc:postgresql://mydatabaseserver:5432/notificDB.
<ms_tenant_id>	The tenant ID that is obtained during the app registration in Microsoft Entra admin center.
<ms_client_id>	The client ID that is obtained during the app registration in Microsoft Entra admin center.
<ms_secret>	The secret that is obtained during the app registration in Microsoft Entra admin center.
<proxy_host>	Proxy host (if applicable).
<proxy_port>	Proxy port (if applicable).

Parameter / XML Tag	Description
<d2rest_url>	Client REST API URL. This is a mandatory field. The Client REST API URL is same as the value in the values.xml file that is available in the SmartViewM365 folder located in <tomcat>/webapps/SmartViewM365/ file path. By default, the value is https://myrestserver:8080/D2-Rest.
<otds_server_url>	Applicable for OTDS authentication. The OTDS Server URL. For example, https://myotdsserver:8090/otdsws.
<otds_client_id>	Applicable for OTDS authentication. The OTDS client ID.
<smartviewhome>	Your Smart View home folder location where the Notification Service is deployed. For example, C:\myfolder\smartviewm365_home.
<loglevel>	Log level for the notification service. Allowed values are debug, info, warn, error, fatal, trace. By default, the value is set to warn.

- Run the setup.bat file as administrator. The following options appear in the command prompt:

```
1.Deployment
2.Start Notification service
3.Exit
```

  a. Type 1 to deploy Notification Service.

  b. Type 2 to start the Notification Service.

  c. Type 3 to exit.

6. For Linux: Perform the following:

- Update the values for following variables in the database.properties file located in NotificationService\config:

Parameter / XML Tag	Description
<jdbc_username>	JDBC username. For example, jdbcusername.

Parameter / XML Tag	Description
<jdbc_password>	JDBC encrypted password. Use the encrypt_your_password command file to encrypt the password. After the password is encrypted, update the value in the parameter. **Note:** If VaultEnabled is set to true, leave this field blank.
<jdbc_dbSchemaName>	The SchemaName of the JDBC database. For example, public.
<jdbc_driverClassName>	The className of the JDBC driver. – For PostgreSQL: org.postgresql.Driver – For Oracle: oracle.jdbc.driver.OracleDriver. – For MSSQL: jdbc.driverClassName =com.microsoft.sqlserver.jdbc.SQLServerDriver.
<jdbc_url>	JDBC URL. For example, jdbc:postgresql://mydatabaseserver:5432/notificDB.
<quartz.dbDelegateClass>	The delegate class of the database.
<databaseSecretKeyName>	Secret key name of the database. **Note:** Do not change this value if VaultEnabled is set to true.

- Update the values for following variables in the ExtApi.config file:

Parameter / XML Tag	Description
service_port	Provide the Notification Service port number.
teams-ns-enabled	Set the teams-ns-enabled value to true.
ms-client-id	Provide the client ID that you have copied during app registration in Microsoft Entra admin center. Applicable if teams-ns-enabled is enabled.
ms-tenant-id	Provide the tenant ID of your app that you have copied during app registration in Microsoft Entra admin center. Applicable if teams-ns-enabled is enabled.
ms-secret	The secret that is obtained during the app registration in Microsoft Entra admin center. Applicable if teams-ns-enabled is enabled.
proxy-host	Proxy host (if applicable).
proxy-port	Proxy port (if applicable).

Parameter / XML Tag	Description
D2DocumentumRestURL	Provide the OpenText Documentum CM client REST URL.
otdsUrl	Applicable for OTDS authentication. The OTDS Server URL. For example, https://myotdsserver:8090/otdsws.
otdsClientId	Applicable for OTDS authentication. The OTDS client ID.

- Go to <root_path>/NotificationService folder located in /root/Documentum/M365 path and run the following command to start the Notification Service:

```
java -jar NotificationService.jar
```

4.3 Deploying Notification Service for OES Connector

Note: For Windows, the Notification Service for OES Connector is deployed as part of OES Connector deployment.

To deploy Notification Service for OES Connector for Linux, perform the following steps:

1. Extract the NotificationService.zip file downloaded from OpenText My Support.
2. If you are using Basic authentication, deploy the xECMUsersProject.dar file in the Documentum CM Server.
3. Run the encrypt_your_password.cmd script from NotificationService\encrypt_your_password.cmd location to encrypt the given database password. Specify a password and press enter to get an encrypted password and save it for future.
4. You must create the database manually, based on the created database, edit and run the respective script in Query tool to create DB schema:
   - **For Oracle**:
     1. Open the \NotificationService\deployment\oracle\oes_file_notifications_oracle.sql file.
     2. Run the oes_file_notifications_oracle.sql file.
   - **For PostgreSQL**:
     1. Open the \NotificationService\deployment\postgres\oes_file_notifications_postgres.sql file.

2. Run the `oes_file_notifications_postgres.sql` file.

- **For MSSQL**:

  1. Open the `\NotificationService\deployment\sqlserver\oes_file_notifications_mssql.sql` file.
  2. Run the `oes_file_notifications_mssql.sql` file.

5. Update the values for following variables in the `database.properties` file located in `NotificationService\config`:

Parameter / XML Tag	Description
`<jdbc_username>`	The JDBC username. For example, `jdbcusername`.
`<jdbc_password>`	The JDBC encrypted password. Encrypt the password by running the `encrypt_your_password` command file. After the password is encrypted, update the value in the parameter. **Note:** If `VaultEnabled` is set to true, the `jdbc_password` field must be null.
`<jdbc_dbSchemaName>`	The SchemaName of the JDBC database. For example, `public`.
`<jdbc_driverClassName>`	The className of the JDBC driver. • For PostgreSQL: `org.postgresql.Driver` • For Oracle: `oracle.jdbc.driver.OracleDriver`. • For MSSQL: `jdbc.driverClassName =com.microsoft.sqlserver.jdbc.SQLServerDriver`.
`<jdbc_url>`	The JDBC URL. For example, `jdbc:postgresql://mydatabaseserver:5432/notificDB`.
`<vaultEnabled>`	To enable the HashiCorp Vault set `vaultEnabled` to `true`.
`<database.secretkey_vault>`	Vault secret and key details. This is mandatory when vault is enabled.

6. Update the values for following variables in the `ExtApi.config` file located in `NotificationService\config`:

Parameter / XML Tag	Description
`service_port`	Provide the Notification Service port number.
`max_notification_limit`	Provide the maximum number of notification that need to be fetched from each request.

Parameter / XML Tag	Description
oes-ns-enabled	Set the oes-ns-enabled value to true.
D2DocumentumRestURL	Provide the OpenText Documentum CM client REST URL.
otdsUrl	Applicable for OTDS authentication. The OTDS Server URL. For example, https://myotdsserver:8090/otdsws.
otdsClientId	Applicable for OTDS authentication. The OTDS client ID.
<proxy_host>	Proxy host (if applicable).
<proxy_port>	Proxy port (if applicable).
http-go-server-port	Provide the port number of the go server. Default port number is 8888 and keep this port open.

7. Update the proxy values in the outpost-agent.ini file located in NotificationService\outpost-agent\.

   For example,

```
#Specify all the JVM OPTS here
 -Xms64m
 -Xmx256m
 -XX:+UseG1GC
 -Dhttp.proxyHost=ban-prox01-l001.otxlab.net
 -Dhttp.proxyPort=3128
 -Dhttps.proxyHost=ban-prox01-l001.otxlab.net
 -Dhttps.proxyPort=3128
```

8. To set the system environment variable, run following command:

```
sudo nano /etc/environment
```

   - Add the following environment variables:
     - `HTTP_GO_SERVER_HOME=<root_path>/NotificationService/http-go-server/`

       For example, /root/Documentum/OES/NotificationService/http-go-server/
     - `OT2_AGENT_HOME=<root_path>/NotificationService/outpost-agent/`

       For example, /root/Documentum/OES/NotificationService/outpost-agent/
     - Press enter and save the environment variables.

9. Go to <root_path>/NotificationService folder located in /root/Documentum/OES path and run the following command to start the Notification Service:

```
java -jar NotificationService.jar
```

Note: To run multiple instances of the Notification Service on the same machine, such as one instance for Microsoft 365 and another for the OES Connector, configure each instance with a unique `service_port` value in its respective `ExtApi.config` file. All other configuration parameters can be defined as needed for each instance.

4.4 Background services in Notification Service

The Notification Service automatically initiates and manages two background services:

- Outpost Agent
- HTTP Go Server

The following are log locations for these services:

- Outpost Logs: Location: `/outpost-agent/logs`
- HTTP Go Server Logs: Location: Same directory as the Notification Service logs

4.5 Running Notification Service as a Windows service

1. Launch the command prompt with Administrator privileges, navigate to the build location `Installed directory\WindowsService`.
2. Run the `TeamsNotificationServiceInstaller.bat` file. The following options appear in the command prompt:

```
1.Install service
2.Delete service
3.Exit
```

   a. Type `1` to deploy the service and service starts automatically.
   b. Type `2` to delete the service.
   c. Type `3` to exit.

Notes

- To manage the service, double click on `TeamsNotificationServicew.exe` in the build location `directory\WindowsService`.
- From the service manager window, you can change or modify all the options for the service. Also, you can shutdown or restart the service.
- The service can be managed using Windows service manager.

Log files

The service creates two following folders in `SMARTVIEWM365_HOME` directory:

- service_logs: This folder contains the service related logs, such as service startup, shutdown logs or any service failure logs.
- teams_logs: This folder contains the application generated logs.

4.6 Post-deployment task

4.6.1 Licensing OpenText Documentum CM

OpenText Documentum CM uses OpenText Directory Services (OTDS) to apply licenses for all OpenText Documentum CM components. For more information about procuring the license file and configuring OTDS and license, see *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

Chapter 5

Configuring preferred language

OpenText Documentum CM for Microsoft 365 supports the following languages: Arabic, German, Spanish, French, Italian, Japanese, Korean, Dutch, Swedish, Simplified Chinese, Brazilian Portuguese, and Hebrew.

To configure the preferred language:

1. Extract the `LanguagePack.zip` file downloaded in step 3 on page 41 to a temporary location. This file contains the supported language packs.
2. Extract the content of `D2-Smartview_LanguagePack_xx.zip` to the following Tomcat folders:

   Note: `xx` in the filename `D2-Smartview_LanguagePack_xx.zip` indicates the languages supported as mentioned in step 3. Based on your language preference, choose the relevant language pack to extract.

   - `<tomcat>/webapps/D2REST`
   - `<tomcat>/webapps/SmartViewM365`
3. Add the `rest.error.message.supported.locales=en,<locale id>` property to the Client REST API `rest-api-runtime.properties` file. The administrator can add multiple locale IDs as comma-separated values. You can use any of the following *<locale id>*:

   - Arabic: ar
   - German: de
   - Spanish: es
   - French: fr
   - Italian: it
   - Japanese: ja
   - Korean: ko
   - Dutch: nl
   - Swedish: sv
   - Simplified Chinese: zh
   - Brazilian Portuguese: pt_BR
   - Hebrew: he
4. Restart the Tomcat server.

Microsoft Teams user must select the preferred language in Microsoft Teams settings. You should also select the same preferred language for Browser language settings.

To set the preferred language in Microsoft SharePoint:

1. Go to your Site in Microsoft SharePoint and click **Settings** on the header menu.
2. In the **Language and time zone** section, click **Change your language** hyperlink.
3. Provide your Microsoft credentials to sign in to your account.
4. On the **Settings and Privacy** page, go to **Languages & Region** > **Languages** and select **Preferred languages**.
5. Click **Add a language** and select your preferred language.

Chapter 6

Upgrading OpenText Documentum CM for Microsoft 365

Note: The Microsoft SharePoint integration with OpenText Documentum CM is introduced in the 24.4 release. The upgrade steps mentioned in this section are specific to upgrading an existing Microsoft Teams integration and adding the new Microsoft SharePoint configuration.

To upgrade OpenText Documentum CM for Microsoft 365 from version 24.4 or 25.2 to 25.4:

1. Stop the `SmartviewM365` server.
2. Take the backup of the *<Tomcat>*`/webapps/SmartViewM365/values.xml` file.
3. Download and extract OpenText Documentum CM for Microsoft 365 from OpenText My Support. The extracted folder contains the following files:
   - `DAR`
   - `NotificationService.zip`
   - `SmartviewM365.zip`
   - `TeamsSmartviewCache.dar`
   - `xECMUsersProject.dar`

   Note: If you are using Documentum CM Server 24.4 or 25.2, then deploy the `TeamsSmartviewCache.dar` and `xECMUsersProject.dar` files from the *<Extracted zip location>*`\DAR\TeamsSmartviewCache\`*<version>* and *<Extracted zip location>*`\DAR\xECMUsersProject\`*<version>* respectively.
4. Deploy `TeamsSmartviewCache.dar` in Documentum CM Server.
5. Deploy OpenText Documentum CM for Microsoft 365 in Tomcat using the following steps:
   a. Extract `SmartviewM365.zip` file downloaded from OpenText My Support in step 3, in Tomcat.
   b. Copy the values from the `values.xml` backup taken in step 2, and provide those values in the `values.xml` file located in the *<Tomcat>*`/webapps/SmartViewM365/` file path.

      If you are performing a fresh deployment of Microsoft SharePoint along with Microsoft Teams specific upgrade, ensure to update the following variables with your values in the `values.xml` file:

- *<sharepointdomains>*
- *<tenantid>*
- *<appredirecturi>*
- *<importconfig>*
- *<defaultconfig>*
- *<rootreposelection>*

Note: While updating the values in the `values.xml` file to be used for upgrade, change the Client REST API URL to the 25.4-specific URL.

c. Run the `setup.bat` file located in the `<Tomcat>/webapps/SmartViewM365/` file path in Tomcat. The `SmartViewM365` manifest file is generated in the `<Tomcat>/webapps/SmartViewM365/manifests/download/teams` file path.

d. Restart the `SmartviewM365` server.

6. Configure Client REST API for OpenText Documentum CM for Microsoft 365 using the following steps:

Note: If you are upgrading Client REST API, taking the backup of the `rest-api-runtime.properties` and `msgraph.properties` files is necessary as you need to provide the same values from the backup files to configure Client REST API. This helps you to set the relevant properties as configured earlier.

a. Stop the Client REST API server.

b. Take the backup of the `rest-api-runtime.properties` and `msgraph.properties` files from the `<Tomcat>\webapps\D2REST\WEB-INF\classes\` location in Client REST API.

c. Configure one of the following authentication in `rest.security.auth.mode` within the `rest-api-runtime.properties` file by providing the values from the backup file (`rest-api-runtime.properties`) taken in step 6b.

- `basic-ct`: To configure basic authentication
- `ct-otds_token`: To configure OTDS authentication. For more information on OTDS authentication see, *OpenText Documentum Content Management - Client Installation Guide (EDCCL250400-IGD)*.

d. When upgrading from 25.2 to 25.4, add the header `OT-DCTM-PRODUCT-CODE` in `rest.cors.allowed.headers`.

e. Deploy the `d2sv-msgraph_plugin-<version>.jar` file extracted from the `SmartviewM365.zip` file in Client REST API at the `<tomcat>\webapps\D2REST\WEB-INF\lib\` file path.

Note: If there is an existing version of the `d2sv-msgraph_plugin-<version>.jar` file available already in the location `<tomcat>\webapps\D2REST\WEB-INF\lib\`, replace it with the latest version. Having both the files at the location breaks Client REST API.

f. Copy the `msgraph.properties` file downloaded from the OpenText My Support in step 3 and paste in the Client REST API deployment path such as, `<Tomcat>\webapps\D2REST\WEB-INF\classes\`.

Update the content in the `msgraph.properties` file using the backup taken previously.

g. Only while upgrading from 24.2 to latest, update the additional permissions required to configure Microsoft SharePoint integration for OpenText Documentum CM for Microsoft 365:

i. Go to the Microsoft Entra admin center.

ii. Go to **API Permissions**.

iii. Select **Microsoft SharePoint**.

iv. Select **Delegated permissions**, and select the following delegated permissions:

```
AllSites.Read
AllSites.Write
MyFiles.Read
MyFiles.Write
User.Read.All
User.ReadWrite.All
```

For more information about app registration in Microsoft Entra admin center, see step 3.

h. Restart the Client REST API server.

7. Configure client configuration for the OpenText Documentum CM for Microsoft 365 using the following steps:

a. Extract the `D2-config.zip` file downloaded in step 3 on page 41. This contains the `Teams-config.zip` file.

b. In client configuration, import the `Teams-config.zip` file and select the following options:

- **FOLDER** and **xecmdms_teams_Acl** for the security configuration element
- **xecmdms_channel** and **xecmdms_teams** for the context

Note: The configuration elements and contexts must be mapped to the respective application.

c. Configure the following security configuration elements in the client configuration:

- For the **xecmdms_channel** context, enable the **FOLDER** security configuration element.
- For the **xecmdms_teams** context, enable the **xecmdms_teams_Acl** security configuration element.

d. Refresh the client configuration cache.

The Microsoft Teams administrator must upload the generated manifest file for all users in Microsoft Teams admin center to make the app available in Teams.

Note: When you upload the manifest file, make sure the file is in a ZIP format and you use the latest manifest file.

To upload manifest file in Microsoft Teams:

1. In Microsoft Teams admin center, click **Teams apps** > **Manage apps**.
2. Go to **App details** and locate the OpenText Documentum CM for Microsoft 365 app.
3. Under **New version**, select **Upload file**.
4. Select the manifest file and upload it.

   The app is now available for the Microsoft Teams owner to add to the required channel.

6.1 Upgrading Notification Service

Use the following steps to upgrade the Notification Service from a previous version.

To upgrade Notification Service:

1. Extract the `NotificationService.zip` file on the existing Notification Service.
2. Copy the values taken from the backup of the `values.xml` to the latest `values.xml` file.
3. Deploy the `xECMUsersProject.dar` file in the Documentum CM Server.
4. To upgrade the database, run the corresponding upgrade script located in `<Extracted Zip Location>\NotificationService\deployment\`.
   - For Oracle database: run the `upgrade_teams_notifications_oracle.sql` script in `oracle` folder.
   - For Postgres database: run the `upgrade_teams_notifications_postgres.sql` script in `postgres` folder.
5. Run the `setup.bat` file as administrator. The following options appear in the command prompt:

```
1.Deployment
2.Start Notification service
3.Exit
```

a. Type 1 to deploy Notification Service.
b. Type 2 to start the Notification Service.
c. Type 3 to exit.

For more information about deploying and starting the Notification Service, see "Deploying Notification Service" on page 29.

6.2 Post-upgrade task

6.2.1 Licensing OpenText Documentum CM

OpenText Documentum CM uses OpenText Directory Services (OTDS) to apply licenses for all OpenText Documentum CM components. For more information about procuring the license file and configuring OTDS and license, see *OpenText Documentum Content Management - On-Premises Upgrade and Migration Guide (EDCCS250400-UMD)*.

Chapter 7

Troubleshooting

The following table lists the common issues that you may encounter and how to resolve them:

Issue	Resolution
Unable to import large files.	Update the parameters, `max-file-size` and `max-request-size` with a higher value in the `web.xml` file in Tomcat. If you are still unable to import the file, make sure you set the `maxUploadFileSize` property in the `D2FS.properties` file available in the `D2REST\WEB-INF\classes\` file path with an appropriate value.
Unable to add the app and there are no error details in the UI.	**Cause**: Issue with app registration and configuration in Microsoft Entra admin center. **Resolution**: To view the error, open the **Console** tab in the Developer tool of the browser. To troubleshoot the issue the detailed information is available in the token call in the **Network** tab.
Unable to import an item using O2 profile.	Make sure O2-related plug-ins are available in the `D2REST\WEB-INF\lib\` file path.
When using the desktop version of Microsoft Teams, there are errors.	You can troubleshoot the issue using the console logs. To view the console logs: 1. On the taskbar, in the notification area, click **Show hidden icons**  . 2. Right-click the **Microsoft Teams** icon. 3. Click **Open DevTools**.

User is unable to access the mapped folder for a channel with the “Internal Server Error.”	Clear the stored preferences for the current user in d2c_preferences and x3_preferences. Run the following DQL statements in iDQL editor in Documentum CM Server:
	`delete d2c_preferences objects where owner_name='<user name>'`
	`delete x3_preferences objects where owner_name='<user name>'`

If users are not synched with the Documentum CM Server in OTDS Authentication.	Make sure you synch the OTDS user `M365_SERVICE` with the Documentum CM Server.

Issue	Resolution
If users are not synched with the Documentum CM Server with Basic Authentication.	Make sure that the `xECMUsersProject.dar` is deployed successfully in the Documentum CM Server.
If appropriate groups are not created for mapped folder in Teams channel.	Make sure you restart the Java Method Server in the Documentum CM Server, client configuration, and Client REST API.
If Microsoft Teams doesn't load	Include the third-party cookies for the Microsoft sites in browser settings if the third-party cookies are blocked while using Microsoft Teams in a web browser. In the Google Chrome browser settings, include the third-party cookies for the following sites: • [*.]microsoft.com • [*.]microsoftonline.com • [*.]teams.skype.com • [*.]teams.microsoft.com • [*.]sfbassets.com • [*.]skypeforbusiness.com For Edge browser, see the article, *Teams doesn't load* in the *Microsoft* documentation.

When using Microsoft SQL Server (MSSQL) as the database for OES Connector, users may encounter the following error messages:
• In OpenText Documentum CM client UI: "`1 item Failed to Collaborate`".
• In OpenText Documentum CM client logs: "`Invalid column name`".
	Update the OES Connector service database collation to `SQL_Latin1_General_CP1_CI_AS` and perform the following:
	1. Connect to the MSSQL Server.
	2. Run the following commands:
	a. `USE master;`
	`ALTER DATABASE <OES_DB_Name>`
	`SET SINGLE_USER WITH ROLLBACK IMMEDIATE;`
	b. `ALTER DATABASE <OES_DB_Name>`
	`COLLATE`
	`SQL_Latin1_General_CP1_CI_AS;`
	c. `ALTER DATABASE <OES_DB_Name>`
	`SET MULTI_USER;`
	
	For example,
	• `USE master;`
	`ALTER DATABASE OES_CONNECTOR`
	`SET SINGLE_USER WITH ROLLBACK IMMEDIATE;`
	• `ALTER DATABASE OES_CONNECTOR`
	`COLLATE`
	`SQL_Latin1_General_CP1_CI_AS;`
	• `ALTER DATABASE OES_CONNECTOR`
	`SET MULTI_USER;`
	3. Restart the OES Connector service.