Content Manager

Software Version 24.2

Microsoft Teams Integration

Document Release Date: November 2024
Software Release Date: November 2024

Legal notices

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Except as specifically indicated otherwise, this document contains confidential information and a valid license is required for possession, use or copying. If this work is provided to the U.S. Government, consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Documentation updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for updated documentation, visit https://www.microfocus.com/support-and-services/documentation/.

Support

Visit the MySupport portal to access contact information and details about the products, services, and support that OpenText offers.

This portal also provides customer self-solve capabilities. It gives you a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the MySupport portal to:

- View information about all services that Support offers
- Submit and track service requests
- Contact customer support
- Search for knowledge documents of interest
- View software vulnerability alerts
- Enter into discussions with other software customers
- Download software patches
- Manage software licenses, downloads, and support contracts

Many areas of the portal require you to sign in. If you need an account, you can create one when prompted to sign in.

Contents

Introduction

This document provides high level information for you to configure MS Teams integration with Content Manager.

The Content Manager Microsoft Teams (MS Teams) integration enables you to integrate Content Manager with Microsoft Teams.

The integration enables you to:

- Capture conversation of a channel or chat in Content Manager
- Check In posts and files to Content Manager
- Create new Check In Styles
- Access documents in OneDrive

MS Teams integration prerequisites

Before you begin, make sure that the following configurations are complete:

- Content Manager EmailLink is configured with Content Manager (for server side filing of data).
- Service API is configured with HTTPS
- MS Teams integration feature in Content Manager **System Options > Features** tab is enabled
- Content Manager users accessing the integration must have their OpenID Connect details included in their **Location - Network Login** profile

Licensing and payment requirements

There are different licensing models available for Microsoft Teams APIs in Microsoft Graph. Choose the model suitable for your organization. Evaluation model is the default licensing model. If you are using the default licensing model, then there is a limitation on seeded capacity. You can capture 500 chat conversations per month in Content Manager.

For detailed information on licensing and payment requirements, see https://docs.microsoft.com/en-us/graph/teams-licenses.

Configuration overview

This section briefly describes the steps you need to perform to integrate MS Teams with Content Manager.

- **Enable OpenID Connect authentication** - OAuth authentication is managed via OpenID Connect authentication. The authentication is configured in your Identity Provider (e.g. Azure AD) and then the appropriate details are stored in Content Manager in the hptrim.config file.
  - **Create or register an app with your Identity Provider** - the integration requires you to create or register an app with secret IDs generated and set permissions for Microsoft Graph API.
  - **Edit configuration file** - update the configuration file with details that would help your integration work.
- **Configure Content Manager EmailLink** - For server side filing from MS Teams to Content Manager, configure Content Manager EmailLink with the domain details, add app and tenant ID details, choose a licensing model, and set the polling interval.
- **Create manifest file** - based on the template file provided, create a manifest file with specifications as per your requirement and upload it to the Office portal.

For enabling OpenID Connect authentication, see *Content ManagerOpenID Connect authentication* document and for configurations specific to MS Teams integration, see Modes of operation in MS Teams integration.

Configuring for private and shared channels

Content Manager supports capturing content from private and shared channels.

You can add Content Manager app to private and share channels, and perform all the operations you perform on any standard channel.

To add private or shared channel to your existing integration and then to capture content to Content Manager, see Content Manager MS Teams Integration Help.

> **IMPORTANT: For share channels only**,
>
> The existing Content Manager integration with MS Teams will not work with the shared channel.
>
> To integrate the Content Manager app with the shared channel, you need to generate a new manifest file, and then register the Content Manager app along with the newly generated manifest file with your Identity Provider. Once the app is registered, add the new Content Manager app to the MS Teams.
>
> To generate new manifest file for shared channels, execute the **az_install.ps1** script in **Windows PowerShell ISE** available in the following location:

> **https://github.com/content-manager-sdk/Community/blob/master/docs/files/24.1/az_install.ps1**

Modes of operation in MS Teams integration

The MS Teams integration has two modes of operation, Client and Server side. It is possible to use the integration in either one or both of these modes. The Service API and MS Teams application manifest must be installed irrespective of which mode the integration is to be used in. If only the Server side mode is required, then follow the directions below to modify the manifest. If only the Client side integration is required, then EmailLink does not need to be configured.

Edit manifest to remove Client side mode

Once the manifest has been either manually created or generated using the script, the Client side integration with Channels and Chats can be remove by removing the contents of the **configurableTabs** property and leaving it as an empty array.

```
"configurableTabs": [ ],
```

Components

The MS Teams integration is made up of three components. You can configure the components depending on the level of functionality required.

The components are:

- Service API
- Teams application manifest
- EmailLink (only required for Server side filing)

Requirements

The components listed above work together to provide the complete MS Teams integration. If you require only the Client side components, then only the Service API and MS Teams manifest are required. EmailLink is required to support scheduled Server side filing of chats, posts and files.

Server side architecture

Check In Styles and Check In Places

The Server side component of the MS Teams integration is managed using Check In Styles and Check In Places. Check In Styles and Places have a one to many parent-child relationship, meaning one Check In Style may have zero or more Check In Places associated with it. The purpose of the Check In Style is to encapsulate a collection of properties required to create a record, the purpose of the Check In Place is to track the connection details and synchronization state for a particular application and user.

For example, there might be one Check In Style that specifies a record type and default settings required for a particular project or customer. This Check In Style may have linked to it many Check In Places for different users, some linked to email folders, some linked to Teams channels and others linked to teams users for filing Teams chats.

Creating the Check In Style and Check In Place for MS Teams

The usual way to create Check In Styles and Places for the teams Server side integration is via the teams Client side app. This will allow you to create a Check In Style, navigate to a channel or a user and create a Check In Place for that channel or a user. Check In Places may be created via the SDK, if there is a need to automate this process, for example, if it is undesirable to install the Client app in Teams.

To create the Check In Place,

1. Find the appropriate Check In Style.
2. Use the Microsoft Graph API to get the details of the desired channel or user.
3. Create the Check In Place using CheckinStyle.FindOrCreatePlace.

NOTE: The place ID must be structured correctly:

Place type	Description	Place ID	Place ID example
ChannelPostsForServerProcessing	All posts for a channel.	{team-id}/channels/{channel-id}	`dd8b1122-13f0-41df-923d-a407637b4047/channels/19:3te1ccfc9b6c4390be34f7b69439f57a@thread.tacv2`
ChannelDocsForServerProcessing	All files for a channel.	{team-id}/channels/{channel-id}	`dd8b1122-13f0-41df-923d-a407637b4047/channels/19:3te1ccfc9b6c4390be34f7b69439f57a@thread.tacv2`
TeamsChatForServerProcessing	All chats involving this user.	users/{id}/chats/getAllMessages	`users/98e82caf-9073-449d-9284-1bfad890e3d5/chats/getAllMessages`
DocsForServerProcessing	All files owned by this user.	users/{id}/drive/root	`users/98e82caf-9073-449d-9284-1bfad890e3d5/drive/root`

Service API

The Service API must be installed and must have a valid HTTPS certificate, any HTTP errors will cause the Teams Integration to fail.

The Service API performs four functions within the integration:

- hosts the web application that is used to administer the Teams integration (at /CMServiceAPI/office/index.html?teamsadmin=1),
- hosts the web application that is embedded in Teams as the posts, chat and files add-ins (at /CMServiceAPI/office/index.html),
- provides the backend services to which the add-on communicates when reading from or writing to Content Manager, and
- provides services that act as a proxy between the add-in and the Microsoft Graph API for reading from and writing to Microsoft Graph API.

Setup script

The simplest way to configure the Microsoft Teams integration is to use the setup script, which will create:

- an Azure App,
- a manifest for Teams, Office and Outlook integrations, and
- sample authentication settings for the **ServiceAPI hptrim.config**.

To use the script,

1. Install the Azure CLI,
2. Download and run the script,

   > **IMPORTANT: New setup script to create new Azure applications**
   >
   > From 24.3 onwards, as part of Content Manager installation, a new setup script, **az_install.ps1**, is available at the installation location (for example, **C:\Program Files\Micro Focus\ContentManager\Service_API\office\AzureScript**) to create new Azure app for Content Manager MS Teams and ZFP Office/Outlook integrations.
   >
   > The administrator must use/run the setup script, **az_install.ps1**, to create new Azure app.

3. If you wish to use Azure CLI 2.36 then download the old version of the setup script.

Conversation silent interval

The Teams integration groups user chats into conversations so that each conversation can be stored in a separate Record. To achieve this the integration assumes that a period of silence in a group chat indicates that particular conversation has finished. For example, if users A, B and C are chatting in Teams and a period of time elapses with nothing being said the integration will assume that the next thing said is a new conversation and file it in a new Record. When filing chats manually it is possible to choose to file one or more of these contiguous conversations as a single record.

To configure the silent time, navigate to **System Options > Email and chat** in Content Manager Client and set the value for **Wait until the conversation has been silent for the specified time**.

Setup instructions

Service API authentication permissions

The Service API must be configured to use OpenID Connect authentication as described in the *Content Manager OpenID Connect authentication setup* document. New permissions must be assigned to the Azure AD Application to support Teams, these are:

- Delegated:
  - ChannelMessage.Read.All
  - ChannelSettings.Read.All
  - Chat.Read
  - ChatMember.Read
  - email
  - Files.Read
  - Files.Read.All
  - Files.ReadWrite.All
  - GroupMember.Read.All
  - Sites.ReadWrite.All
  - User.Read.All
- Application:
  - ChannelMessage.Read.All
  - ChannelMember.Read.All
  - ChannelSettings.Read.All
  - Chat.Read.All
  - ChatMember.Read.All
  - Files.Read.All
  - Files.ReadWrite.All
  - TeamSettings.Read.All

To assign these permissions,

1. Open the Azure AD application used for authenticating Teams.
2. Go to **API permissions** and Select **Add a permission**.

3. Select **Microsoft Graph API**.
4. Choose either **Delegated** or **Application** permissions.
5. Find the permission and add it.
6. Once you have added all the permissions, select **Grant admin consent** to consent to all permissions.

Service API authentication application ID

The Teams integration requires that the Application ID URI in the Azure AD App include the domain name of your Service API server, this must be adjusted before installing the office integration manifests. To adjust the Application ID URI:

1. Open the Azure App referenced from your **ServiceAPI hptrim.config** file.
2. Go the **Expose an API** page and edit **the Application ID URI** field.

   By default, the Application ID URI will look something like this `api://2d89cb2b-3xx7-4c21-807e-029fdbfe74a7`,
3. Edit the Application ID URI to include the name of your Service API server. For example `api://myserver.com/2d89cb2b-3xx7-4c21-807e-029fdbfe74a7`.
4. Once you have modified this you will need to update the **appIdURI** property (case sensitive) in the **ServiceAPI hptrim.config** file.

Service API authorized client applications

The Teams integration relies on Single Sign On from the Microsoft add-in framework. To allow this to work we need to register our add-in, this is done in the **Expose an API** section of the Azure App created previously.

To register your add-in,

1. Add a Scope.
2. Name it `access_as_teams_user`.
3. Fill in the fields with appropriate values, for example:
   - **Admin consent display name:** CM Teams Tab.
   - **Admin consent description:** Enable Teams to call the add-in's web APIs with the same rights as the current user.
   - **User consent display name:** Teams can act as you.
   - **User consent description:** Enable Teams to call the add-in's web APIs with the same rights that you have.
4. Save the scope.
5. Add two client applications, each time selecting the scope you just added, the Client ID for each of the these are:
   - 1fec8e78-bce4-4aaf-ab1b-5451cc387264
   - 5e3ce6c0-2b1f-4285-8d4b-75ee78787346

Manifest

The purpose of the manifest file is to notify Microsoft Teams of the presence of your add-in. Manifest files must be customized before uploading to your Office 365 Admin.

To prepare your manifest,

1. Download the sample manifest.
2. Generate a new Guid and replace [MANIFESTGUID] with this new Guid.
3. Replace [SERVICEAPIURL] with your Service API URL.
4. If you want to include a link to the Content Manager Web Client replace [WEBSITEURLATTR] with `"websiteUrl": "[YOUR WEB CLIENT URL]",`
5. If you do not wish to include a link to the Content Manger Web Client remove [WEBSITEURLATTR],

   > **IMPORTANT:** Replace [VALIDDOMAINSATTR] with "validDomains": ["[DOMAIN FROM SERVICEAPIULR]", "[IF DIFFENT THE DOMAIN FROM YOUR WEB CLIENT URL]"]. For example: "validDomains": ["mydev.dev", "mycorp.com"].

6. Replace [APPCLIENTID] with the client ID from the Azure AD App.
7. Replace [APPIDURI] with the Application ID URI from the Azure AD App.
8. Create a zip file called content-manager-teams.zip which contains the following:
   - Your manifest renamed to manifest.json
   - The image files color.png and outline.png
9. Upload the manifest from the Microsoft Teams Admin center.

Browser Cookies

It may be that the MS Teams integration add-in does not display after it has been uploaded. To resolve this, ensure that all cookie blocking is disabled in your web browser.

EmailLink

EmailLink serves two purposes in the Teams integration:

1. File all posts and/or files in selected Channels, and
2. File all chats for selected users.

EmailLink should be installed and there must be a Microsoft authentication configuration for your Office 365 domain that is of type **OAuth** and has **Teams** selected.

Configuring Content Manager EmailLink

To capture server side data from MS Teams to Content Manager, you need additional configurations in Content Manager EmailLink.

To configure Content Manager EmailLink, perform the following steps:

1. In EmailLink, navigate to **Preference > Configuration > Authentication**.
   a. Select the provider as **Microsoft**.
   b. Enter the domain name for Domain.
   c. Select Authentication Type as **OAuth**.
   d. Enter the details for Application / Client ID, Directory / Tenant ID, and Client Secret.
   e. Select **Teams** as supported services.
   f. Click **Add** and save the details.
2. In the System settings, choose appropriate Microsoft Teams licensing model. For details, see Licensing and payment requirements , on page 4.
3. To set the polling frequency to check for new messages in MS Teams, set the **Time to check for new Social Media / Teams posts** parameter.

Adding Content Manager app

You can add the Content Manager app to top level to capture server side data or you can add the app at channel or individual chat level to capture client side data.

Adding Content Manager app to capture client side data

To capture client side data, there are two ways of adding the Content Manager app. Perform one of the following:

Adding from Apps or More option

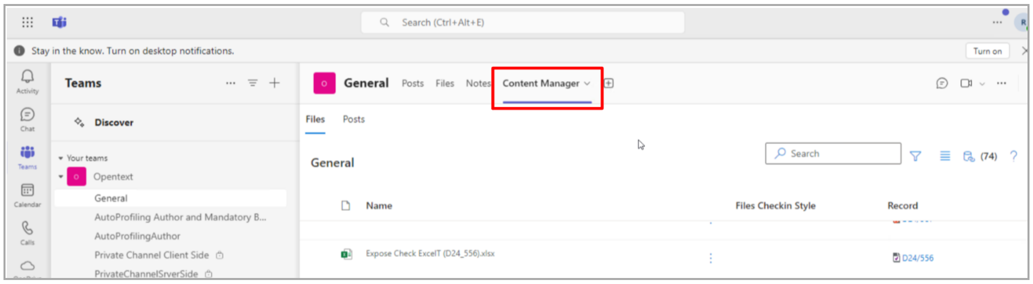
1. In Teams, click **Apps** on left pane or (three dots) More option.
2. Search for Content Manager.
3. Click **Content Manager** app.
4. In the dialog displayed, click the drop down and select either **Add to a team** or **Add to a chat**.
5. In the next dialog, search for the channel or chat and select the required channel or chat from the list displayed.
6. Click **Set up**.

   The Content Manager app is displayed as a new tab in the channel or chat.

Adding directly from channel or chat

1. Navigate to channel or chat where you want to add the Content Manager app.
2. Click **+**.
3. In the **Add a tab** dialog, search for the Content Manager app.
4. Click **Content Manager** app.
5. In the dialog displayed, click **Save**.

   The Content Manager app is displayed as a new tab in the channel or chat.



Stay in the know. Turn on desktop notifications.

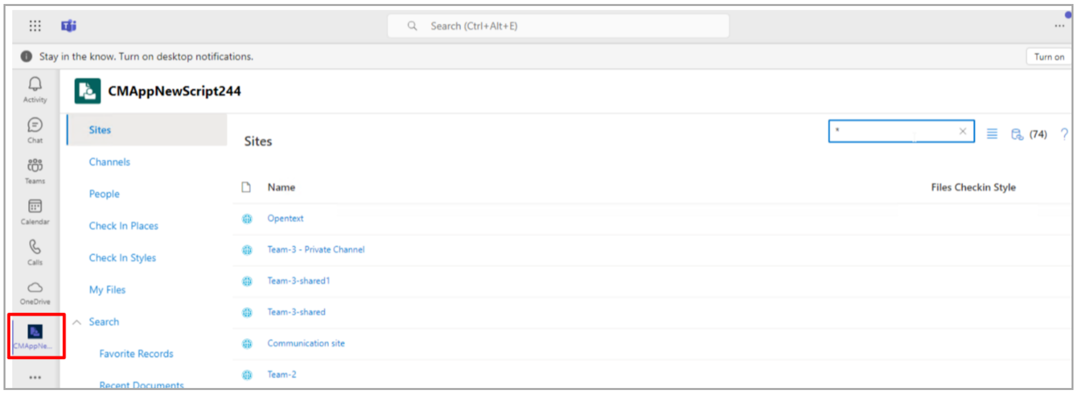
Name	Files Checkin Style	Record
Expose Check ExcelT (D24_556).xlsx		D24/556

Adding Content Manager app to capture server side data

To capture server side data in Content Manager, perform the following steps:

1. In Teams, click **Apps** on left pane or (three dots) More option.
2. Search for Content Manager.
3. Click **Content Manager** app.
4. In the dialog displayed, click **Add**.

   The Content Manager app is displayed on the left pane of MS Teams.



Name	Files Checkin Style
Opentext	
Team-3 - Private Channel	
Team-3-shared1	
Team-3-shared	
Communication site	
Team-2	

Troubleshooting

This section describes the following troubleshooting scenarios.

Login pop-up error

Issue

Login pop-up is displayed while accessing the Content Manager app from MS Teams.

Solution

To resolve this issue, make sure that authentication for service API is enabled as anonymous in IIS.

To enable anonymous authentication, perform the following steps:

1. Open IIS manager.
2. Navigate to **Default Web Site > CMServiceAPI**. CMServiceAPI home is displayed.
3. Double-click **Authentication** available user IIS.
4. Click **Anonymous Authentication** and select **Enable** from the **Action** panel or right-click and select **Enable**.

Protected API access error

Issue

The following log text in the EmailLink logs:

```
Invoked API requires Protected API access in application-only context when not using
Resource Specific Consent.
```

Solution

If you come across the above log message in the EmailLink logs, make sure that your request to access the protected MS Teams API is granted. Otherwise, it is recommended to get in touch with the MS Teams support.