Content Manager

Software Version 24.4

Mobile App Setup

opentext™

Legal notices

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 includes high level configuration and setup details required by your organization to allow users to access and use the Content Manager Mobile app.

The Content Manager Mobile app is available as a native application and depending on your device operating system, it can be downloaded from the Google Play Store for Android devices or Apple App Store for Apple devices.

The Content Manager Mobile app allows you to:

- Search for records

- View electronic documents and record properties

- Create new records

- Check Out existing documents for editing using a native application, such as Microsoft Word

- Download documents for offline viewing

- Edit and view Office documents in OneDrive

Mobile app setup prerequisites

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

- Service API is configured with HTTPS

- Mobile app 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

Supported software requirements

See *Content Manager Specifications and Limitations*, for the supported software requirements of Content Manager Mobile App.

Setup overview

This section briefly describes the steps you need to perform to setup Content Manager Mobile app on your device.

- **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 Content Manager Mobile app setup requires you to create or register a new app and add API permissions, certificates, secrets, and authentication details.
  - **Edit configuration file** - update the hptrim.config configuration file with details required for the Content Manager Mobile app.
- **Verify access to Service API URL** - after completing the setup, verify if you are able to access the Service API URL.

For enabling OpenID Connect authentication, see *Content Manager OpenID Connect authentication* document and configurations specific to Content Manager Mobile app, see Configurations for Mobile App, below.

Configurations for Mobile App

The Content Manager Mobile App requires an instance of the Service API configured to use OpenID Connect for authentication.

Service API

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

Setup script

The simplest way to setup Azure AD and the Service API is to run the setup script which will create:

- an Azure App, and
- sample authentication settings for the **Service API 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.

Once the script is complete there will be a new Azure AD App in your tenant and some sample configuration to be pasted into your **Service API hptrim.config** file.

Manual setup

Service API configuration

The Service API must be configured to support OpenID Connect authentication. For details, see *Content Manager OpenID Connect authentication* document. In addition, the **hptrim.config** file must contain an **add** element with the name **mobile** and the **redirectUri** set to **trimapp://mobile**.

For example,

```
<authentication corsAllowedOrigins="https://mydev.dev:3000" allowAnonymous=="false"
slidingSessionMinutes="30" redirectURI="">
<openIdConnect>
...
<addname="mobile" clientID="[YOUR CLIENT ID]" clientSecret="[YOUR SECRET]"
issuerURI="[YOUR ISSUER URI]" redirectUri="trimapp://mobile"/>
</openIdConnect>
</authentication>
```

Azure app configuration

Ensure the Azure AD App created in the previous step has the following settings (both all in lower case):

- Authentication > Web > Redirect URIs - [SERVICEAPIURI]/auth/mobile. For example, https://acme.com/cmserviceapi/auth/mobile.

- Authentication > Mobile and desktop applications > Redirect URIs - **trimapp://mobile**.

API permissions

In the **API Permissions**, make sure to add the following Microsoft Graph permissions:

- Delegated
    - email
    - Files.Read
    - Files.Read.All
    - Files.ReadWrite

- Files.ReadWrite.All
- openid
- profile

API / Permissions name	Type	Description	Admin conse
+ Add a permission ✓ Grant admin consent for Microfocus			
∨ Microsoft Graph (7)			
email	Delegated	View users' email address	No
Files.Read	Delegated	Read user files	No
Files.Read.All	Delegated	Read all files that user can access	No
Files.ReadWrite	Delegated	Have full access to user files	No
Files.ReadWrite.All	Delegated	Have full access to all files user can access	No
openid	Delegated	Sign users in	No
profile	Delegated	View users' basic profile	No

IMPORTANT: Check In and Check Out files from OneDrive to Content Manager

Make sure to add the following API permissions (**Delegated**) to Check In and Check Out files from OneDrive to Content Manager using Mobile App:

- Files.Read
- Files.Read.All
- Files.ReadWrite
- Files.ReadWrite.All

Log in to Content Manager Mobile app

To log in to Content Manager Mobile app, perform the following steps:

1. Download and install the Content Manager Mobile app from the Google Play Store or Apple App Store.

2. Open the Mobile app. The Connection URL screen is displayed.

3. Enter the Service API URL and click **Connect**. The Microsoft online log in page is displayed.

4. Enter the user credentials and sign in. The Content Manager Mobile app About page is displayed.