

Content Manager

Software Version 25.2

Service API

opentext™

Document Release Date: January 2025
Software Release Date: April 2025

Legal notices

Copyright 2008-2025 Open Text

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.

Microsoft, Office, Windows, Windows Vista, Windows 7, Windows 8 and Windows Server are U.S. registered trademarks of the Microsoft group of companies.

Oracle is a registered trademark of Oracle and/or its affiliates.

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

Content Manager Service API	4
Overview	4
Setup	4
Prerequisites	4
Installation	4
Authentication	5
Upgrading ServiceAPI	5
Getting Started	5
Configuration file	6
Example	6
Multiple configuration files	8
AntiForgeryToken implementation in Service API	8
Setting the scope of the cookies	9
Troubleshooting	10
Uploading files larger than the default size	10
Issue	10
Solution	10
Certificate error	10
Issue	10
Solution	10
Downloading files through Content Manager Service API	11
Issue	11
Solution	11

Content Manager Service API

Overview

The Content Manager Service API is a new Web service designed with a focus on Mobile and Web Consumers.

The bulk of the documentation for the service is hosted within the service itself and can be viewed after installation.

TIP: Additional information on the SDK can be found:

SDK Documents - <https://content-manager-sdk.github.io/Community/>

Samples - <https://github.com/content-manager-sdk/Community/>

Setup

Prerequisites

See **CM25.2_Spec.pdf** for high level prerequisites.

Additionally, the computer which the Content Manager Service API is to be installed on, should have:

- In IIS, **Application Development Features**, the feature **ASP.NET** enabled.
- In IIS, **Security**, either one of the features **Windows Authentication** or **Basic Authentication**, or both enabled.
- .NET registered. If it is not registered, register it by running the command **C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis -e -enable** in a command prompt.

Installation

The Content Manager Service API installs as a feature of the main Content Manager installation. To install it, run **Setup_CM_xNN.exe** from your installation media, and select ServiceAPI in the **Feature Selection** dialog. See **CM25.2_Install.pdf** for details on installing the ServiceAPI. The ServiceAPI can also be installed via script using the **CM_Service_API_x64.msi**, an example script and the script properties can be found in **CM25.2_Install.pdf**.

NOTE: Whenever the ServiceAPI is installed, by default, all help files and examples are not installed. It is recommended that on a production server these are NOT installed as they increase the attack surface for hackers, these files should only be installed in your development environment.

See **CM25.2_Install.pdf** for details for further details on installing the ServiceAPI using **Setup_CM_x64.exe** and **CM_Service_API_x64.msi**.

The service installation does everything that is required for the setup. After completing the installation, you should have the following:

- Folder **C:\Program Files\Micro Focus\Content Manager\Service_API**
- Folder **C:\Program Files\Micro Focus\Content Manager\Service_API\Bin**
- Folder **C:\Micro Focus Content Manager\ServiceAPIWorkpath**

CAUTION: The user account that is used as the identity for the IIS application **CMServiceAPI** requires full access rights to the **C:\Micro Focus Content Manager\ServiceAPIWorkpath** folder. This user is identified during the installation process in the **AppPool Account Configuration** dialog (see **CM25.2_Install.pdf** for further information).

- An IIS application called **CMServiceAPI** which points to the folder **C:\Program Files\Micro Focus\Content Manager\Service_API**

Authentication

By default, the service is set to use Windows authentication. You can change this to basic authentication in IIS, if you wish. If you do so, you will need to configure SSL to protect users' passwords.

Upgrading ServiceAPI

IMPORTANT: When upgrading to Content Manager 23.3, due to the changes in installation paths, the configuration files from the previous version installation paths are not copied into the new C:\Micro Focus Content Manager workpaths. These files will be available in the original installation path and any modifications will need to be copied from these files into the newly installed configuration files installed to, by default, C:\Program Files\Micro Focus\Content Manager.

As a part of the Content Manager upgrade process the ServiceAPI web configuration files, `hptrim.config` and `web.config`, which are installed as a part of the Content Manager installation process are copied to the ServiceAPI work path folder, by default, C:\Micro Focus Content Manager\ServiceAPIWorkpath.

These copied files have the date and time of the upgrade prepended to the file name for easy identification, for example, `04_25_2015_2_23_Service_API_web.config`.

After upgrading any additional configuration fields that were added to the ServiceAPI configuration files can be copied out of these backup files and pasted into the new configuration files installed as a part of the upgrade.

See **CM25.2_Install.pdf** for details on upgrading the ServiceAPI.

Getting Started

The first thing to do before beginning development against the Content Manager Service API is to make sure you can access it. This can be done by pointing any Web browser at the following address:

<http://localhost/CMServiceAPI> - where *localhost* can be replaced by the IP address of the host computer.

After supplying authentication details as required, you will be forwarded to this page:

<http://localhost/CMServiceAPI/help/index>

Here you will find more detailed instructions on how to utilize the Content Manager Service API.

NOTE: The above steps are only required when you install the Content Manager ServiceAPI in your development environment. If you navigate to the ServiceAPI website and the help and example files are not installed you will get a HTTP 404 Not Found message.

Configuration file

Although the installation should create a correct configuration file, you may wish to change it later. It is saved in **C:\Program Files\Micro Focus\Content Manager\Service_API\hprim.config**.

Some of the relevant options are:

Option	Description
poolSize	The service pools database connections to improve performance. poolSize is the number of connections pooled before the server attempts to start removing stale connections from the pool.
autoPoolClean	When removing stale database connections from the pool, the service will operate in in one of two ways: <ul style="list-style-type: none"> • Auto - a task will run in the background to remove stale entries • Not auto - as each request comes in, it will attempt to remove stale entries before continuing with the request
databaseId	The service supports one Content Manager database at a time. Set the ID here.
workgroupServer port	The Workgroup Server port as set in Content Manager Enterprise Studio.
workgroupServer name	Use local if the service is on the same computer as the Workgroup Server. Otherwise, use the server name.
workgroupServer workPath	File system location that Content Manager uses to cache documents as users download them.

Example

The following example contains a number of options not described in the preceding table. These are for the purpose of modifying the Service API behavior and are described in more detail in the on-line documentation published within the Service API.

```
<?xml version="1.0" encoding="utf-8" ?>
```

```

<hptrim poolSize="1000"
  autoPoolClean="true"

  xmlns="http://HP.HPTRIM.CMIS/hptrimConfig.xsd"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="hptrimConfig.xsd">

  <setup databaseId="D1" />
  <workgroupServer port="1137"
    workPath="C:\Micro Focus Content Manager\ServiceAPIWorkpath"
    name="local"
  />
  <defaultProperties>
    <clear />
    <add name="Location" properties="FormattedName" />
    <add name="Classification" properties="Title" />
    <add name="Record" properties="Title" />
  </defaultProperties>
  <customPropertySets>
    <clear />
    <add name="RecordMobileList"
      trimType="Record"
      properties="Title,DocumentSize,OwnerLocation,DocumentType,DateModified,DateLastUpdated,Classification,IsElectronic,Extension,Icon,IsContainer,Number,IsFavorite"
    />
    <add name="RecordMobileSync"
      trimType="Record"
      properties="Container"
      propertySets="MobileList"
    />
    <add name="SavedSearchMobileList"
      trimType="SavedSearch"
      properties="Name,Description,Icon,QueryString,FilterString,SortString,IsFavorite"
    />

```

```

<add name="TodoItemMobileList"
      trimType="SavedSearch"
      properties="Todo,Assignee,DateDue" />
<add name="PropertyOrFieldDefMobileDetails"
      trimType="SavedSearch"
      properties="Caption"
    />
<add name="RecordMobileDetails"
      trimType="Record"
      properties="IsFavorite,Extension,DateModified,SuggestedFileName"
      propertySets="DataGridVisible,Detailed"
    />
</customPropertySets>
</hptrim>

```

Multiple configuration files

A single Service API instance may host multiple configuration files (and thus datasets) as long as there are multiple matching IIS applications.

For more details to host a second configuration file, see *Multiple config files* section in Service API help located at <http://localhost/CMServiceAPI/help/configsettings>, where *localhost* is the system where Service API is installed.

AntiForgeryToken implementation in Service API

The Service API is built using ServiceStack libraries which support AntiForgery implementation only using MVC (Model-View-Controller), which are used to protect against cross-site request forgery attacks.

The AntiForgeryToken implementation in Service API is form-based and is only necessary when forms are involved. If you're consuming the Service API through API calls, AntiForgeryToken is not required.

In the Service API `hptrim.config` file, the **requireAntiForgeryToken** attribute should be set to **false** in the **hptrim** tag when there is no form based interaction. Otherwise, a "Could not deserialize request" 403 error will be thrown.

For example,

```

<hptrim serviceFeatures="Razor,Html,Json,Xml,PredefinedRoutes"
...
uploadBasePath="C:\Micro Focus Content Manager\ServiceAPIWorkpath\Uploads"
autoPoolClean="true" debugMode="false"
requireAntiForgeryToken="false">

```


Setting the scope of the cookies

Adding the `<httpCookies requireSSL="true" httpOnlyCookies="true" sameSite="Lax" />` in the **web.config** ensures that all the cookies in your application will be **HttpOnly** and will be sent over secure HTTPS connections by default. This enhances the overall security of your web application.

Add `<httpCookies requireSSL="true" httpOnlyCookies="true" sameSite="Lax" />` parameter in **web.config** under `<system.web>` tag.

For example,

```
<configuration>
<system.web>
<httpCookies requireSSL="true" httpOnlyCookies="true" sameSite="Lax" />
</system.web>
</configuration>
```

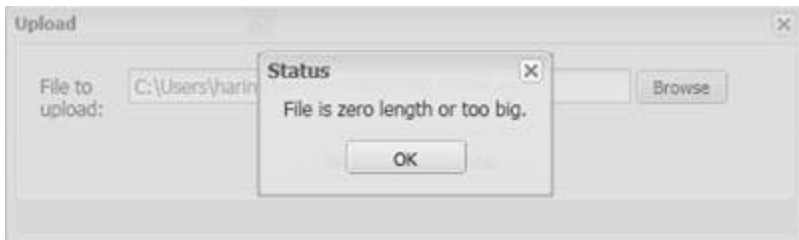
NOTE: Make sure that HTTPS is enabled for your site before setting the `requireSSL="true"`. If this is enabled on an HTTP site, cookies may not work as expected.

Troubleshooting

Uploading files larger than the default size

Issue

When creating new records and uploading files of more than 4096 KB, which is the default size in ASP.NET, the status warning **File is zero length or too big** may appear:



Solution

Change the default request size in the file **web.config**.

In the example below, the parameter **maxRequestLength** in the file has been changed to **51200**, which is the number of KB and equals 50 MB.

```
<configuration>
  <system.web>
    <httpRuntime maxRequestLength="51200"/>
  </system.web>
</configuration>
```

Certificate error

Issue

Re-directing user to sign on page fails due to server certificate issue or error.

Solution

Add the property **bypassConfigCertificateValidation** and set its value to **true** for the **authentication** attribute in the **hptrim.config** file located in install folder (example, **C:\Program Files\Micro Focus\Content Manager\Service_API**) to allow ServiceAPI to bypass certificate error.

For example,

```
<authentication corsAllowedOrigins="https://mydev.dev:3000" allowAnonymous="false"
slidingSessionMinutes="30" redirectURI="" bypassConfigCertificateValidation="true">
```

```

<openIdConnect>
<add
name="openid"
clientID="XXXXXXXXXX"
clientSecret="XXXXXXXXXXXXXXXXXX"
issuerURI="https://vlab025580.dom025500.lab:8443/nidp/oauth/nam/.well-known/openid-configuration"
appIdURI="XXXXXXXXXXXXXXXXXX" />
</openIdConnect>
</authentication>

```

Downloading files through Content Manager Service API

Issue

Issues when downloading files through the Content Manager Service API, where downloading files takes a very long time.

Solution

As part of this, a new parameter, **allowPartialDownload**, is introduced. By default, the value is set to **true** where the files are downloaded chunk by chunk. If the value is set to **false**, the files are downloaded directly.

To download the files directly, open the **hptrim.config** configuration file in a text editor, located in the installation folder (for example, **C:\Program Files\Micro Focus\Content Manager\Service_API\hptrim.config**). Add the parameter, **allowPartialDownload**, and set its value to **false**.

For example,

```

<xs:schema id="cmisConfigSchema"
targetNamespace="http://HP.HPTRIM.CMIS/hptrimConfig.xsd"
elementFormDefault="qualified"
attributeFormDefault="unqualified"
xmlns="http://HP.HPTRIM.CMIS/hptrimConfig.xsd"
xmlns:mstns="http://HP.HPTRIM.CMIS/hptrimConfig.xsd"
xmlns:xs="http://www.w3.org/2001/XMLSchema" allowPartialDownload="false">

```