Content Manager

Software Version 24.2

Web Client Installation and Configuration

opentext™

Document Release Date: April 2024
Software Release Date: April 2024

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

Content Manager Web Client

Introduction

The purpose of the Content Manager Web client is to provide zero-footprint browser-based access to a Content Manager database.

Content Manager Web Client uses the responsive design paradigm. The responsive design feature allows Content Manager Web Client to automatically adjust and layout the content of the application to suite the specific device.

Audience

This document is for administrators who need to install and configure the Content Manager Web client.

> **IMPORTANT:** For installation and upgrade information, please see **CM24.2_Install.pdf**.

System requirements

For operating system and browser requirements for Content Manager Web client, see **CM24.2_Spec.pdf**.

Pre-requisites

Web Servers

The requirements for the Content Manager Web Client Server are the same as for a Content Manager Workgroup Server plus the additional requirements below.

See **CM24.2_Spec.pdf** for Content Manager specifications and limitations.

Additional requirements:

- Microsoft Internet Information Server (IIS) 7.5, 8.0 or 8.5 with Microsoft .Net Framework 4.5.
- The correct Roles Services for the respective Web Server under Windows Server 2012 need to be configured and installed.

Configuration

Setting up Single Sign On (SSO) authentication for the Web Client

The Content Manager Web Client can be setup to use Single Sign On (SSO) for authentication.

In this instance, SSO is used to refer to the task of identity federation, which is authenticating with a web application located outside your organisation boundary using your organisation credentials. This might be achieved in a variety of ways, such as, a WS-Fed solution like ADFS (or Azure AD) or one of the many public SAML providers (OneLogin, Ping Identity and Okta).

Once the Content Manager Service API has been installed, navigate to http://localhost/CMServiceAPI/help/authentication for an in-depth overview of how to integrate the Web Client with ADFS.

After integrating the Web Client with ADFS, the key **useADFS** needs to be changed to **true** in the file hprmServiceAPI.config.

<!-- Web Client configuration -->

```
<setup databaseId="45" searchAhead="true" workpath="C:\Micro Focus Content
Manager\ServiceAPIWorkpath\Uploads" useADFS="true" />
```

Configuring Document Viewer

The Content Manager Web Client provides generic document viewer to view different types of documents. If you want to view your document in the native application, you can bypass Content Manager document viewer for those file types. Depending on the browser you are using, the document will be opened in another tab or you will be prompted to save and download the file to your local system.

To bypass document viewer, navigate to **Settings > Document Viewer** tab and select the file type or extension from the drop-down for the **Bypass Content Manager Viewer for these File Types** option.

If the file type or extension you are looking for is not available in the drop-down, you need to add the required file type to the list of files in the **bypassViewerFileTypes** attribute in the **hprmServiceAPI.config** file located in Content Manager Web Client install folder (e.g, C:\Program Files\Micro Focus\Content Manager\Web Client).

For example,

```
<setup databaseId="45" searchAhead="false" workpath="C:\Micro Focus Content
Manager\ServiceAPIWorkpath\Uploads"
bypassViewerFileTypes
="*.JPEG;*.JPG;*.PNG;*.TXT;*.GIF;*.BMP;*.MPG;*.MPEG;*.XML;*.TIFF;*.TIF;*.PDF;*.CSV"
disableDownloadDocument="true"/>
```

Managing Content Manager Web Client Security

This section assumes you are familiar with the following technologies:

- Microsoft Internet Information Server (7+ and 8+)
- Content Manager Enterprise Studio

Background

For the Content Manager Web Client to work, it needs to be able to connect to the Content Manager Workgroup Server. The Content Manager Web Client can connect to the local Content Manager Workgroup Server or a remote Content Manager Workgroup Server. To connect, the Content Manager Web Client IIS account must be the same as the Content Manager Workgroup Server service account. Additional configuration will be required if the Content Manager Web Client IIS account is different to the Content Manager Workgroup Server service account.

Why impersonation delegation?

In Windows, the Content Manager desktop client logs onto a Content Manager Workgroup Server using the user’s Windows credentials. The Content Manager Web Client is essentially a Content Manager client that connects the Web Client user to the Content Manager Workgroup Server. The Web Client service account needs to log onto the Content Manager Workgroup, not as itself, but as the Web Client user account. This process is called impersonation.

Security would be compromised if any account were to be allowed to impersonate any other account. In Content Manager Enterprise Studio, configure a list of trusted server accounts. These trusted server accounts are allowed to impersonate other accounts. It is important that you keep this list of accounts as short as possible, and that the accounts listed in it are not compromised. When the Content Manager Web Client attempts to log onto the Content Manager Workgroup Server, the Content Manager Workgroup Server checks that the Web Client is running under a trusted server account.

The authentication settings allow the Web Client user to connect to a Content Manager Workgroup Server in a double hop environment, where the user logs on to the Content Manager Web Client using NTLM. The Windows NT Challenge/Response authentication does not support double-hop impersonations (in that once passed to the IIS server, the same credentials cannot be passed to a back-end server for authentication.

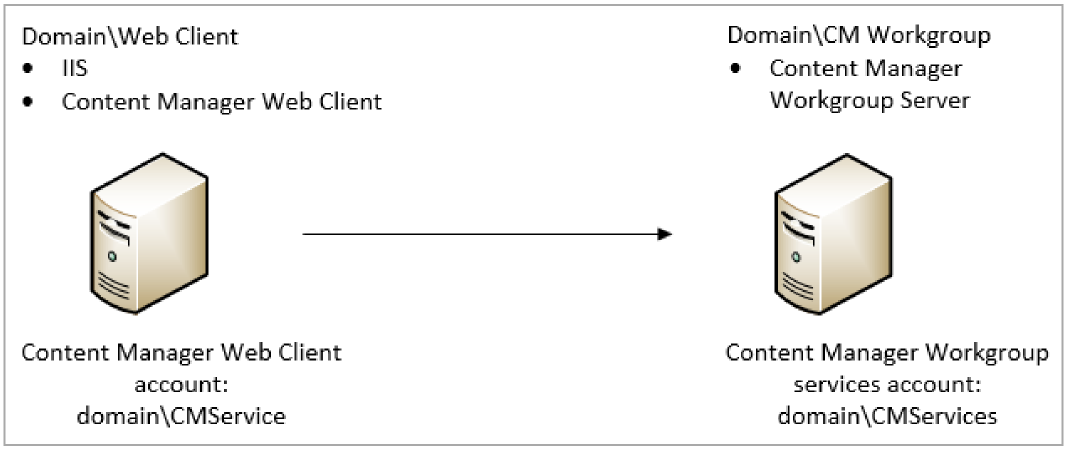
See also http://support.microsoft.com/kb/264921, section Windows NT Challenge / Response.

> **NOTE:** The Content Manager Workgroup Server service account is automatically trusted. If the Web Client runs under the same account as the Content Manager Workgroup Server, it is not be necessary to configure it in Content Manager Enterprise Studio as a trusted server account.

Content Manager Web Client account is the same as Content Manager Workgroup Server account

In this instance, no additional configuration is needed. If your Content Manager Workgroup Server account is **domain\trimservices**, where **domain** is your organization’s domain name and **trimservices** is the domain user name, the account that runs your Content Manager Web Client must also be **domain\trimservices**.

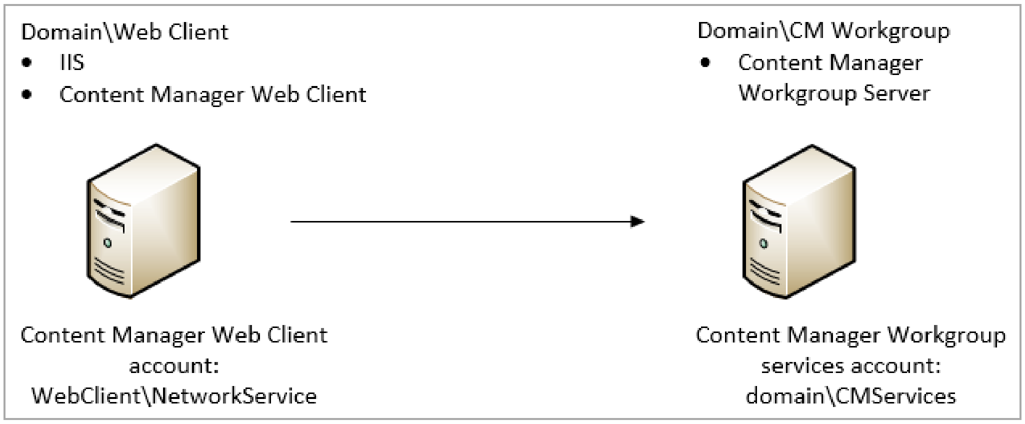
For example, in the deployment scenario below, you will not need to do any additional configuration because the Content Manager Web Client and the Content Manager Workgroup Server are both running as **TRIM\trimservices** account.


Domain\Web Client
• IIS
• Content Manager Web Client
Domain\CM Workgroup
• Content Manager Workgroup Server
Content Manager Web Client account: domain\CMService
Content Manager Workgroup services account: domain\CMServices

Content Manager Web Client account is different to Content Manager Workgroup Server account

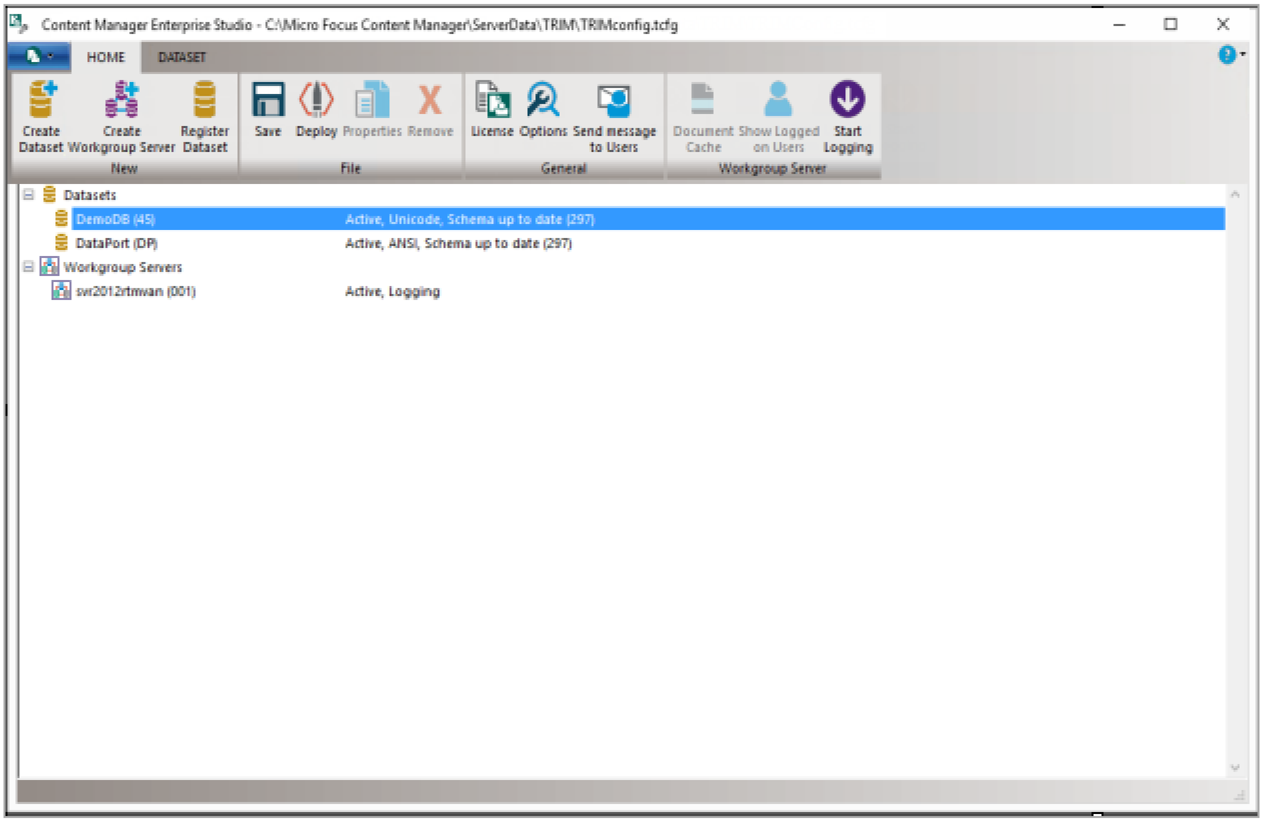
If the Content Manager Web Client IIS account is different to the Content Manager Workgroup Server service account, the Content Manager Web Client IIS account must be added to the list of authorized user accounts that the Content Manager Workgroup Server will trust with supplying valid user credentials.

For example, if the Content Manager Web Client instance runs as Network Services (**Web Client\Network Services**) and the Content Manager Workgroup Server runs as **TRIM\trimservices**, you will need to add **TRIM\Web Client$** in the trusted user list in Content Manager Enterprise Studio. This is because Network Services will try to log on to Content Manager Workgroup Server as **TRIM\Web Client$ (domainName\computerName$)**.


Domain\Web Client
• IIS
• Content Manager Web Client
Domain\CM Workgroup
• Content Manager Workgroup Server
Content Manager Web Client account: WebClient\NetworkService
Content Manager Workgroup services account: domain\CMServices

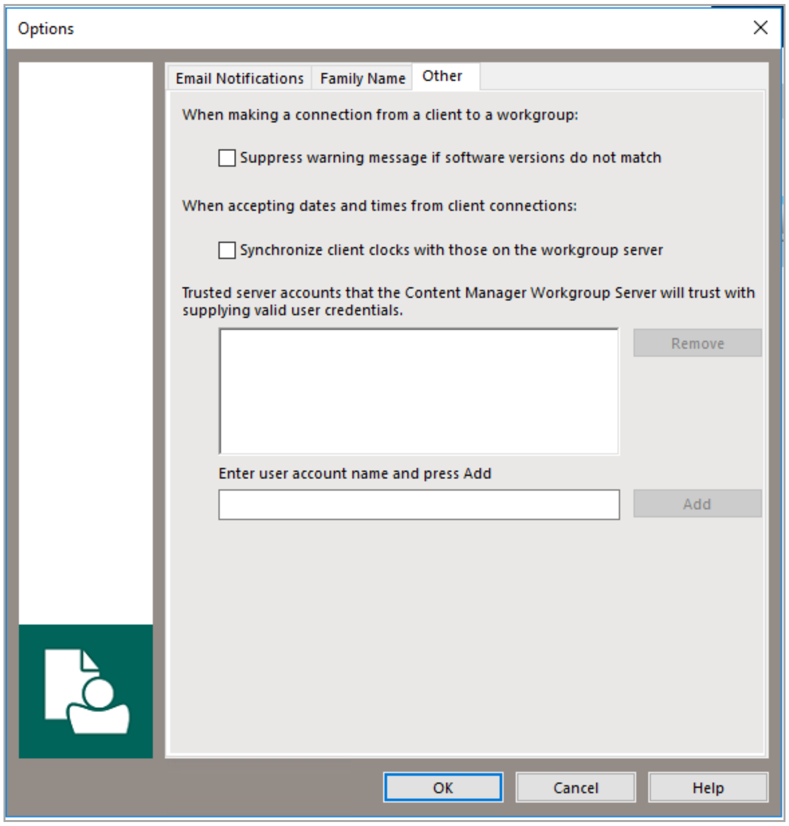
Adding the authorized account that the Content Manager Workgroup Server will trust with supplying valid user credentials:

1. As an Administrator, open **Content Manager Enterprise Studio**, select the dataset name that is the authorized account is to be added to, from the **Home** tab, on **General** group, click **Options**.



```
Datasets
    DemoDB (45)            Active, Unicode, Schema up to date (297)
    DataPort (DP)          Active, ANSI, Schema up to date (297)
Workgroup Servers
    svr2012rtmwan (001)    Active, Logging
```

2. On the displayed **Options** dialog, click **Other**.



Options

When making a connection from a client to a workgroup:

□ Suppress warning message if software versions do not match

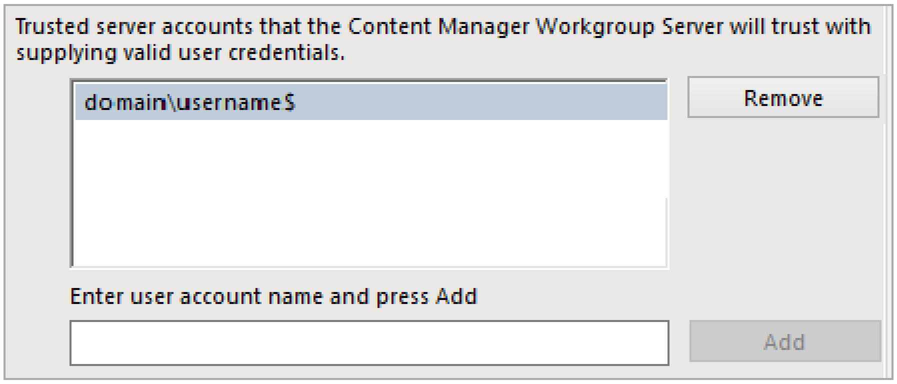
When accepting dates and times from client connections:

□ Synchronize client clocks with those on the workgroup server

Trusted server accounts that the Content Manager Workgroup Server will trust with supplying valid user credentials.

Enter user account name and press Add

3. In the field **Enter user account name type** the full account name (domain\user) for the Content Manager Web Client and then click **Add**.



Trusted server accounts that the Content Manager Workgroup Server will trust with supplying valid user credentials.

domain\username$

Enter user account name and press Add

4. Click **OK**.
5. On the **Content Manager Enterprise Studio** dialog, from the **Home** tab, on the **File** group, click **Save** and then click **Deploy**.

By default, the Content Manager Web Client runs under the IIS application pool's identity which is Network Services. When the Content Manager Web Client runs as Network Services, IIS will try to log onto the Content Manager Workgroup Server as **domainName\computerName$**, where domain name is your organization domain and **computerName$** is your computer account. This domain account is created automatically when the computer is joined to the domain.

For the Network Services account to be able to log on to the Content Manager Workgroup Server, change the Content Manager Web Client identity from the Network Services account to the account that runs the Content Manager Workgroup Server . Otherwise, add the computer account of the computer that the Content Manager Web Client is running on (**domainName\computerName$**) to the trusted account list in Content Manager Enterprise Studio.

By default, the Content Manager Web Client runs as Network Services and will try to connect to the Content Manager Workgroup Server as TRIM\WEB$. You can change the Content Manager Web Client application identity by creating a new IIS application pool and set the new application pool identity to a domain service account. If this account is the same as the Content Manager Workgroup Server account, you will not have to add this account to the trusted list in Content Manager Enterprise Studio.

Example: running Content Manager Web Client as a domain account

For the Content Manager Web Client to connect to the Content Manager Workgroup Server as domain account, the following conditions must be met:

- Content Manager Web Client identity must be set by changing the application pool identity to the domain account that you want
- The domain account must be in the trusted account list in Content Manager Enterprise Studio You will need to change the application pool identity that the Content Manager Web Client is using. It is recommended to create a new application pool and set this pool identity to the domain user account. For information on how to do this, please consult Microsoft’s guides on how to create an IIS application pool.
- IIS 7+ http://technet.microsoft.com/en-us/library/cc731784(WS.10).aspx

Prevent Download

If your organization has a requirement to disable the Download functionality of the Web Client so users cannot create local copies of the documents, this can be done by adding a new attribute to Web Client **hprmServiceAPI.config**.

When this attribute is set to true:

- The **Download** option will not be available on the Preview panel
- The **Generate URL Link** option will not be available on the Preview panel, and
- Users will not be able to use the Check Out option from the record details component.

> **NOTE:** The **Check Out and Edit** functionality is not affected by this attribute.

To disable the Download functionality:

1. On the machine where the Web Client is installed and configured, navigate to the installation directory, by default, this is C:\Program Files\Micro Focus\Content Manager\Web Client.
2. As an administrator, open **hprmServiceAPI.config** in a text editing application, e.g. Notepad ++
3. To the **<setup>** section, add **disableDownloadDocument="true"**, e.g.

```
<setup databaseId="45" searchAhead="false" workpath="C:\Micro Focus Content
Manager\ServiceAPIWorkpath\Uploads"
bypassViewerFileTypes="*.JPEG;*.JPG;*.PNG;*.TXT;*.GIF;*.BMP;*.MPG;*.MPEG;*.XML;*.TIF
F;*.TIF;*.PDF;*.CSV" disableDownloadDocument="true"/>
```

4. Save the updated hprmServiceAPI.config

Allowing specific File Types to be uploaded

To allow the uploading of specific File Types to the Web Client, a white list can be added to the **hprmserviceapi.config** file. This list defines what file types can be uploaded to the Web Client, any file types not listed will fail if uploaded.

To create a white list for the Web Client, add the **fileUploadWhiteList** attribute with the accepted file extensions, separate each allowed extension with a comma, to the setup tag in the **hprmServiceAPI.config** file.

For example:

```
<!-- phoenix configuration -->
```

```
<setup databaseId="45" searchAhead="false" advancedSearch="false" workpath="C:\Micro
Focus Content Manager\ServiceAPIWorkpath\Uploads"
fileUploadWhiteList="xlsx,docx,pdf"/>
```

If the **fileUploadWhiteList** attribute is not defined, all file types will be accepted.

Allow file scanning before uploading

To allow file scanning before uploading to the Workgroup server or Document Store, you need to add a configuration attribute. By setting the value of this attribute, you can delay the WebClient record creation process. When you upload the file to the server or document store, a progress message is displayed that the file is being scanned.

To allow file scanning, add the **delayUploadedFileTransferTime** attribute to the setup tag in the **hprmServiceAPI.config** file.

For example,

```
<!--phoenix configuration-->
```

```
<setup databaseId="45" searchAhead="false" workpath="C:\Micro Focus Content
Manager\ServiceAPIWorkpath\Uploads"
bypassViewerFileTypes="*.JPEG;*.JPG;*.PNG;*.TXT;*.GIF;*.BMP;*.MPG;*.MPEG;*.XML;*.TIF
F;*.TIF;*.PDF;*.CSV" delayUploadedFileTransferTime="5000" />
```

If the **delayUploadedFileTransferTime** attribute is set to 0 or not added in the <setup> tag means the feature is disabled. To enable this feature, set the value to any integer greater than or equal to 2 seconds.

Blocked Search Methods

If a Content Manager Administrator blocks a search method, it will not be visible in the Web Client advanced search editor. However, user can still perform a string search which sends the query to the

Content Manager Web Service. By default, these blocked searches will not be blocked by the Content Manager Web Service and will still be executed from the Web Client string search.

In order to force the Web Service to block the blocked search methods from the string search, **preventBlockedSearchMethod** needs to be set to **true** in the Searching config element in **hprmServiceApi.config** under the Web Client install directory.

For example:

```
<hptrim>

...

<searching pageSize="30" searchRecursiveOption="_$_"
preventBlockedSearchMethod="true" />

....

</hptrim>
```

If the **preventBlockedSearchMethod** attribute is not present, the default value is false which means blocked search method will still be executed from the string search field from the Web Client.

Prevent Link Injection

To prevent users from inserting malicious link in to the application, a new attribute can be added to the **hprmServiceAPI.config** file. Enabling this attribute prevents user from modifying the links when viewing the documents.

Add the attribute **disableKeyViewURL** and set the value to **true** in the **setup** tag of **hprmServiceAPI.config** file.

For example:

```
<setup databaseId="45" disableKeyViewURL="true" searchAhead="false"
advancedSearch="false" workpath="C:\Micro Focus Content
Manager\ServiceAPIWorkpath\Uploads"
fileUploadWhiteList="xlsx,docx,pdf"/>
```

When you view the document, the link is now not clickable.

Allow CheckOut to OneDrive

To allow CheckOut to OneDrive, you need to add a configuration attribute. By setting this attribute to **true**, users will be able to CheckOut to OneDrive. The ☁ icon will be available in the **Actions and Properties** panel of the Content Manager Web Client.

To allow CheckOut to OneDrive, add the **enabledCheckOutToOneDrive** attribute to the **setup** tag in the **hprmServiceAPI.config** file.

For example,

```
<!--phoenix configuration-->

<setup databaseId="45" searchAhead="false" enabledCheckOutToOneDrive="true"
workpath="C:\Micro Focus Content Manager\ServiceAPIWorkpath\Uploads"
```

```
bypassViewerFileTypes="*.JPEG;*.JPG;*.PNG;*.TXT;*.GIF;*.BMP;*.MPG;*.MPEG;*.XML;*.TIF
F;*.TIF;*.PDF;*.CSV"  />
```

Prevent checking out to OneDrive

You can prevent users from checking out document(s) to OneDrive by adding **preventOneDriveCheckoutExtensions** attribute to the **hprmServiceAPI.config** file. With this attribute, provide a list of file extension(s) for which you want to prevent checking out to OneDrive.

With this option set in the **hprmServiceAPI.config** file, the OneDrive or Cloud icon is disabled in the Web Client for the file extension(s) specified in the list.

Add the attribute **preventOneDriveCheckoutExtensions** and provide a list of file extension(s) in the **hptrim** tag of **hprmServiceAPI.config** file.

For example:

```
<hptrim xmlns="http://HP.HPTRIM.CMIS/hptrimConfig.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" poolSize="1000" trace="true"
indexPagePath="/Home" notFoundErrorHandler="/APIErrorPages/NotFound"
globalErrorHandler="/APIErrorPages/GlobalErrors" uploadBasePath="C:\Micro Focus
Content Manager\ServiceAPIWorkpath\Uploads" autoPoolClean="true"
serviceFeatures="Html,Json,Razor,Xml,PredefinedRoutes"
preventOneDriveCheckoutExtensions="doc,xls,txt"
xsi:noNamespaceSchemaLocation="hptrimConfig.xsd">
```

Setting a custom logo

You can now customise the logo in Web Client by changing the image file. To set the custom logo in Web Client, follow these steps:

1. Launch the Web Client. The OpenText Content Manager logo is displayed on the top left corner of the Web Client.
2. Navigate to the following location: **C:\Program Files\Micro Focus\Content Manager\Web Client\Content\img\**.
3. Replace the **cm_68_68.png** image file with the desired logo.

   > **NOTE:** Make sure that the file name of the new image is same as the old one, i.e., **cm_68_68.png**.

4. Refresh the Web Client system.

   The new logo is displayed on the top left corner of the Web Client.

Enable System Monitor event processor for view counter

The view counter depends on the System Monitor event processor and hence this needs to be enabled in the Content Manager Enterprise Studio for the dataset.

To enable the System Monitor event processor, perform the following steps:

1. Right-click on the dataset for which you want to enable System Monitor event processor.
2. Navigate to **Event Processor > Configure**.

   The Configure Event Processing for Dataset dialog is displayed.
3. In the Configure Processes tab, select **Enabled** from the drop down of **Configuration status** for **System Monitor**.
4. Select the workgroup server on which the System Monitor should be enabled and click **OK**.
5. In the Content Manager Enterprise Studio, **Save** and **Deploy** the dataset to the workgroup server.

Troubleshooting

Authentication Prompts

Issue

Content Manager Web Client prompts users for authentication although their credentials are valid.

Solution

In **Web.config**, **set clientCredentialType** to **Windows** if it is set to **NTLM**:

```
<transport clientCredentialType="Windows" />
```

A Note to Administrators Regarding Systems Options

When the system options are changed using the Content Manager client, the IIS application pool associated with the Content Manager Web Client virtual directory or the Web site needs to be recycled.

This will not affect other Web sites or virtual directories on the IIS server. The assumption is that the implementation of the Content Manager Web Client needs to have its own application pool.

1. Open **Internet Information Services (IIS) Manager**.
2. Expand the Server Name, click on **Application Pools**.
3. Right-click on **ContentManagerAppPool**, click **Recycle** from the **Application Pool Tasks**.

Installer Behavior When Installing to Invalid Web Site

When installing Content Manager Web Client to an invalid Web site, e.g. one that uses port 80 and no host name, the installer installs Content Manager Web Client to the default Web site instead.

If the Web site that the installer used is incorrect, you can use IIS to move the installation. See Moving the installation to another Web site below

Moving the installation to another Web site

1. In IIS, right-click the Web site you want the Web Client to work under and using **Add Application**, point it to the **Web Client directory**.
2. Complete the required details on the **Add Application** dialog and then click **OK**.
3. Change the port or add the host name under **Bindings**.
4. To avoid confusion, under **Default Web Site**, remove **Content Manager Web Client** by right-clicking it and clicking **Remove**.

Editing hprmServiceAPI.config

The file **hprmServiceAPI.config** in the installation folder has the following section, which the installation sets automatically:

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

<hptrim>

<setup databaseId="45"  useBrowserPDFViewer="false"

searchAhead="true" workpath="C:\Micro Focus Content
Manager\ServiceAPIWorkpath\Uploads" useADFS="false" />

</hptrim>
```

When the settings are not correct, you should correct them manually.

The parameters refer to:

- **DatabaseId** - database id
- **useBrowserPDFViewer** - the value indicates whether the PDF document is viewed in its native format using a PDF Viewer or HTML
- **SearchAhead** – the value indicates whether the automatic type ahead when searching is turned on or off
- **Workpath** - the path where the Content Manager Web Client stores temporary user uploaded files before the database stores these temporary files
- **useADFS** - the value indicates whether Single Sign On authentication for the Content Manager Web Client is on or off

Cross-site Request Forgery

Background

"A common type of attack on websites is referred to as cross-site request forgery (often abbreviated as CSFR or XSFR). When users visit a malicious website or open a malicious email message or instant message, code can attach to their browser and can secretly submit harmful requests on a site where the users are authenticated. In effect, the malicious site forges ("spoofs") requests so that they appear to come from a legitimate user."

From https://msdn.microsoft.com/en-us/library/system.web.helpers.antiforgery(v=vs.111).aspx

In 9.0, the Content Manager Web Client introduced an Anti-forgery mechanism to protect users from such attack. This Anti-forgery mechanism is turned off by default. This can be turned on by adding the **requireAntiForgeryToken="true"** within the <hptrim> element in **hprmServiceAPI.config** in Web Client installation directory, by default, this is C:\Program Files\Micro Focus\Content Manager\Web Client

For example:

```
<hptrim requireAntiForgeryToken="true" poolSize="1000" indexPagePath="/Home"
notFoundErrorHandler="/APIErrorPages/NotFound"
```

```
globalErrorHandler="/APIErrorPages/GlobalErrors" uploadBasePath="C:\Micro Focus
Content Manager\ServiceAPIWorkpath\Uploads" autoPoolClean="true"
serviceFeatures="Html,Json,Razor,Xml" xmlns="http://HP.HPTRIM.CMIS/hptrimConfig.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="hptrimConfig.xsd">
```

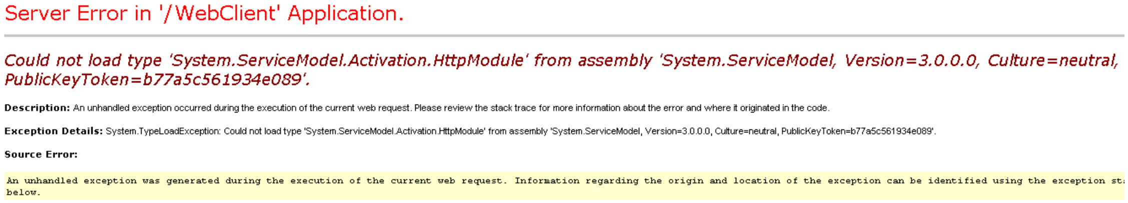
The effect of this is, when user logs in, the Content Manager Web Client will generate an anti-forgery token to be included for all HTTP POST to the server for the current user. POST request will be rejected if it does not include the anti-forgery token.

This applies to all POST request such as : create, update record, file upload.

Error navigating to the Content Manager Web Client

Issue

Error received when attempting to navigate to the Content Manager Web Client after installation:



Server Error in '/WebClient' Application.

Could not load type 'System.ServiceModel.Activation.HttpModule' from assembly 'System.ServiceModel, Version=3.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089'.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.TypeLoadException: Could not load type 'System.ServiceModel.Activation.HttpModule' from assembly 'System.ServiceModel, Version=3.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089'.

Source Error:

```
An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can be identified using the exception st
below.
```

Summary

The error message may appear when trying to navigate to the Content Manager for the first time.

You may encounter this error message when either an earlier version of the .NET Framework has been installed or .NET 3.0 WCF HTTP Activation is enabled after .NET Framework 4.0/4.5 has been installed.

Solution

Run the following command line:

Aspnet_regiis.exe. /iru

The Aspnet_regiis.exe file can be found in one of the following locations:

- %windir%\Microsoft.NET\Framework\v4.0.30319
- %windir%\Microsoft.NET\Framework64\v4.0.30319 (on a 64-bit computer)

Source: See http://support.microsoft.com/kb/2015129

Getting 401 unauthorized when using FQDN or custom host header

Issue

When navigating to the Content Manager Web Client using either the fully qualified domain name (FQDN) or a custom host header, *HTTP 401.1 – Unauthorized: Login Failed* message is displayed.

Summary

The error message is displayed even when the user enters correct credentials when prompted. This occurs when the CM Web Client uses Integrated Windows Authentication and has a name that is mapped to the local loopback address.

Changing the Date Format when using the (.) separator

Issue

If a user changes the Date Separator from either a forward slash (/) or a dash (-) to a period, and then changes the Date Format setting to either dd/mm/yyyy or mm/dd/yyyy, date searches might not return correct results.

Solution

Wait for the application pool to recycle automatically in due time or manually recycle the application pool.

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 **hprmServiceAPI.config** file located in install folder (example, **C:\Program Files\Micro Focus\Content Manager\Web Client**) 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="XXXXXXXXX"
clientSecret="XXXXXXXXXXXXXX"
issuerURI="https://vlab025580.dom025500.lab:8443/nidp/oauth/nam/.well-known/openid-
configuration"
appIdURI="XXXXXXXXXXXXXX" />
</openIdConnect>
</authentication>
```

Appendix A
Configuring WebDav

In Content Manager 9.0, a new **Check Out and Edit** option was introduced as an addition to the existing Check Out and Check In options that check the document out to a local directory and requires the user to browse to that location to check the document in after it has been modified. This new option allows users, accessing the Content Manager Web Client via a supported version of Chrome, Microsoft Edge, and Firefox, to check out an electronic document and edit it directly in its authoring application.

This new option utilizes a workpath directory on the Web Client Web Server. When a user checks out a document using this new option, the document is saved as a working copy in a sub-directory on the Web Client Web Server. The user can make edits and save the document, and at their convenience, using the Content Manager Web Client, they can check the document back into the Content Manager database.

This appendix covers the configuration of the Server, Internet Information Services Manager (IIS) and Web Server directory to enable the new WebDAV **Check Out and Edit** option for both Office and non Office documents.

- Configuring WebDav for Office documents, on the next page
- Configuring WebDav for non Office documents, on page 34 (From 23.3 onwards)

> **NOTE:** This feature does not work with non-Windows authentication in the WebClient. If you are using non Windows Authentication (eg ADFS, OpenID) **do not** complete the following WebDAV configuration steps in your environment.

Configuring WebDav for Office documents

This section includes information about installing WebDav publishing, enabling and configuring WebDav for IIS, enabling and configuring Directory Browsing, adding authoring rule, configuring the workpath folder, and editing hprmServiceAPI.config.

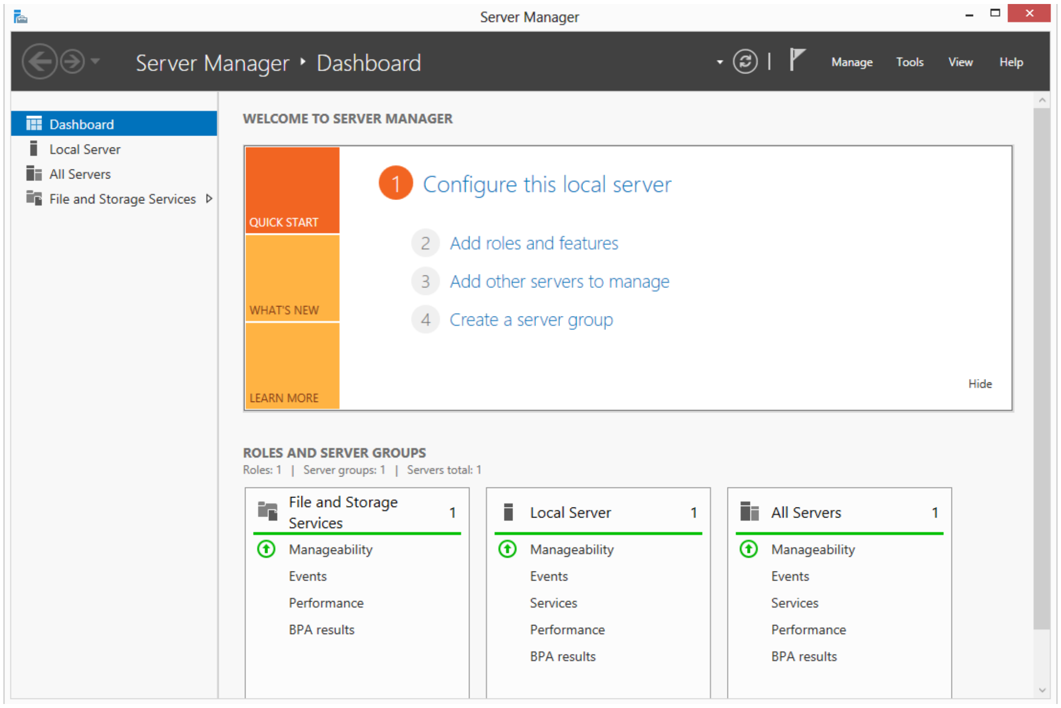
> **NOTE:** The .mdb (Microsoft Access) format is not supported as part of the new WebDav implementation because its not available as part of Microsoft Office URI schemes.

Configuring and Installing WebDav Publishing

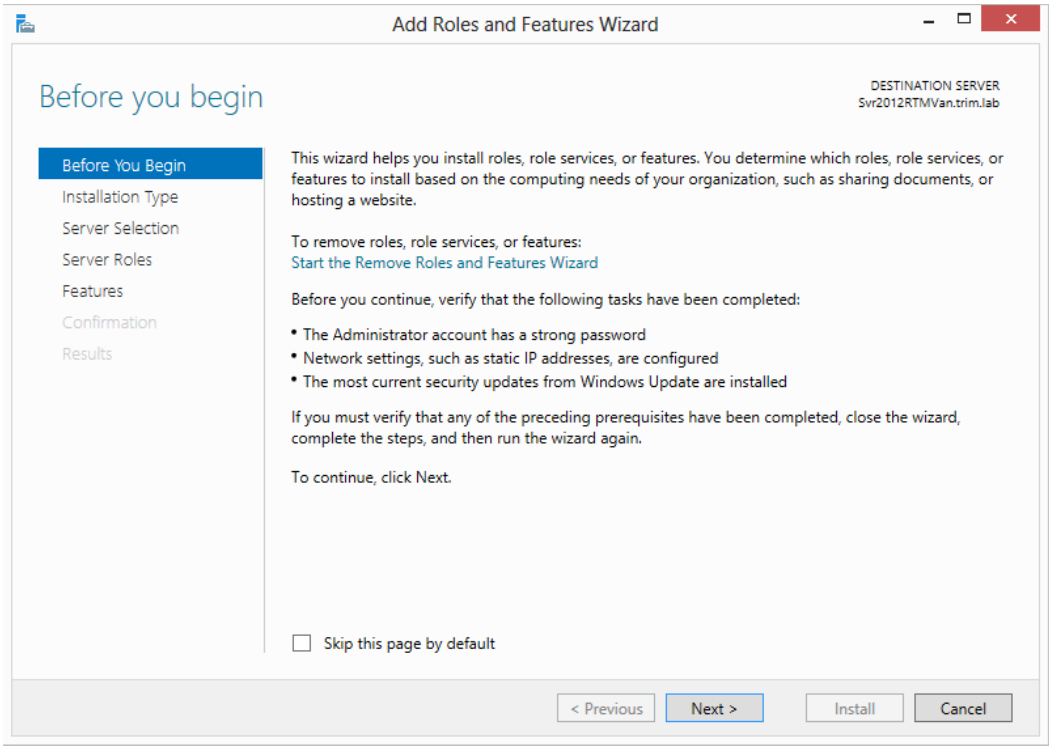
> **NOTE:** These instructions are for a Web Server that is already configured for the Content Manager Web Client. If you are a new site, please following the installation and configuration instructions found in Installation and Configuration

To enable the new Check Out and Edit option, the Web Server needs to have the WebDav Publishing role installed.

1. Open the Server Manager.
2. On the Server Manager Dashboard, click **Add roles and features**.



3. Click **Next** on the **Add Roles and Features Wizard**.



Add Roles and Features Wizard

Before you begin

DESTINATION SERVER
Svr2012RTMVan.trim.lab

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

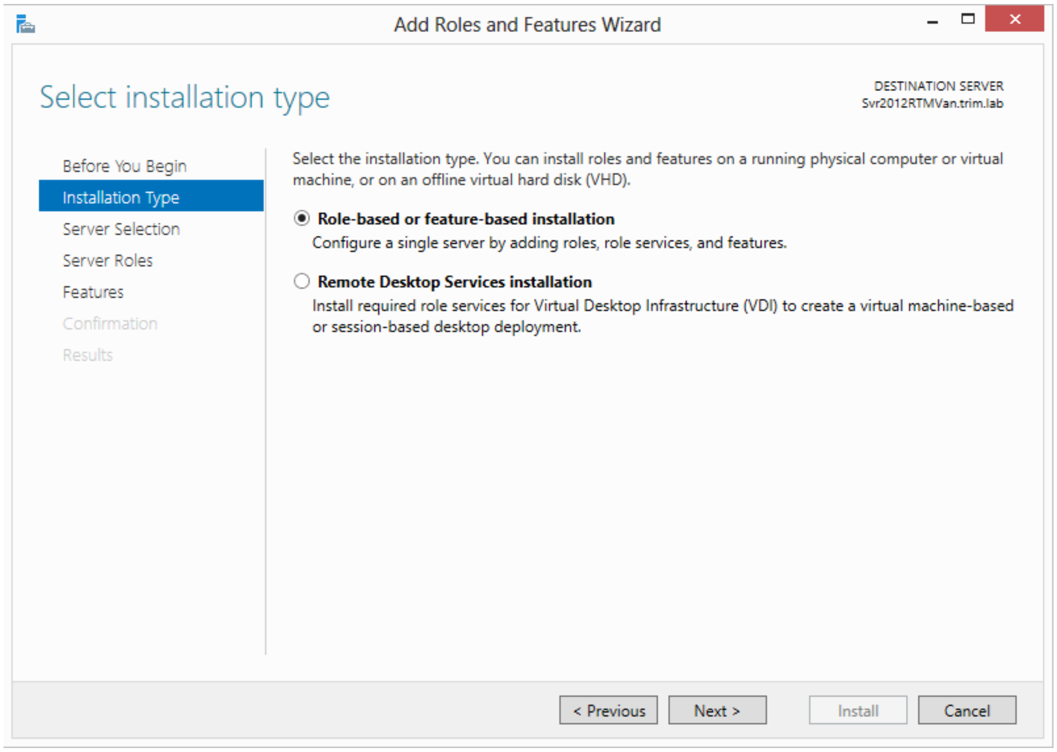
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

4. Select Role-based or feature-based installation and then click **Next**.



Add Roles and Features Wizard

Select installation type

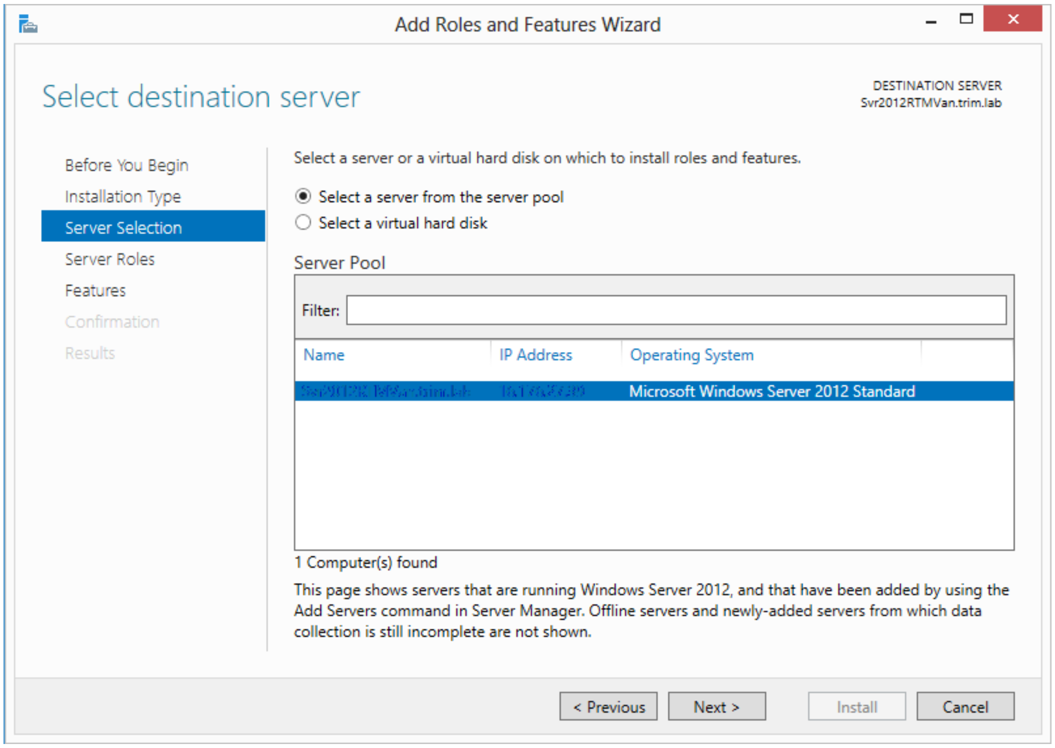
DESTINATION SERVER
Svr2012RTMVan.trim.lab

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

5. Select the Server that the Roles and Features are to be installed on, and then click **Next**.



Select destination server

DESTINATION SERVER
Svr2012RTMVan.trim.lab

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

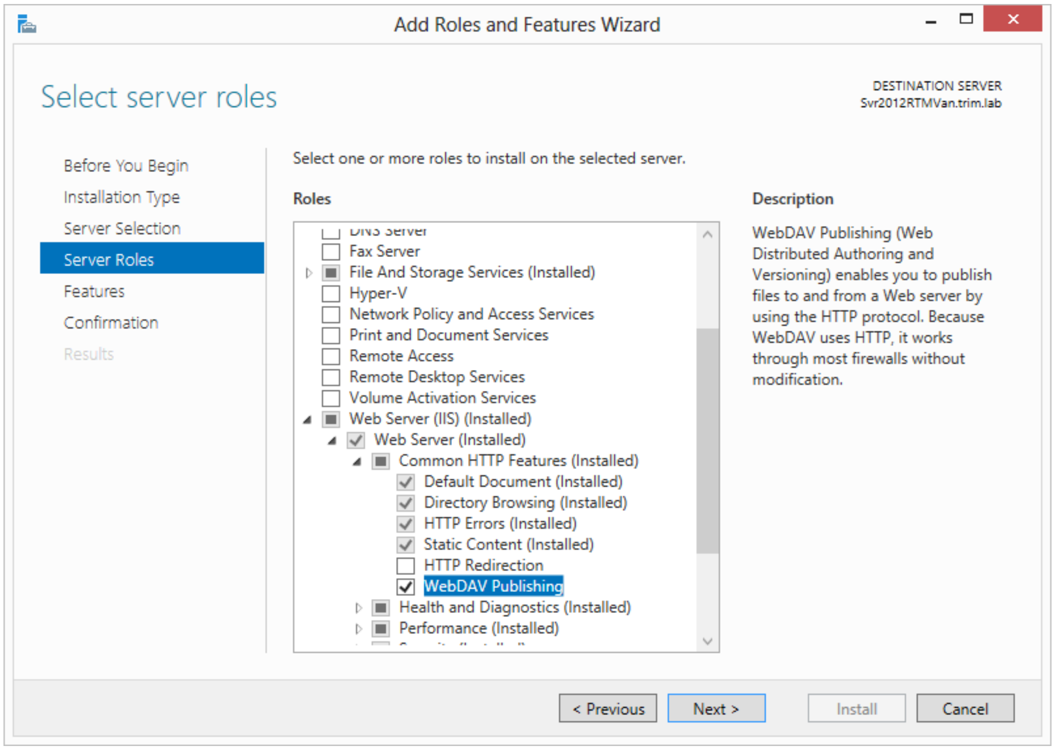
Filter:

Name	IP Address	Operating System
[redacted]	[redacted]	Microsoft Windows Server 2012 Standard

1 Computer(s) found

This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

6. From the displayed Roles list, expand **Web Server (IIS)**, navigate to **Web Server** > **Common HTTP Features** and select **WebDav Publishing**, and then click **Next**.



Select server roles

DESTINATION SERVER
Svr2012RTMVan.trim.lab

Select one or more roles to install on the selected server.

Roles

- □ DNS Server
- □ Fax Server
- ■ File And Storage Services (Installed)
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- ■ Web Server (IIS) (Installed)
  - ☑ Web Server (Installed)
    - ■ Common HTTP Features (Installed)
      - ☑ Default Document (Installed)
      - ☑ Directory Browsing (Installed)
      - ☑ HTTP Errors (Installed)
      - ☑ Static Content (Installed)
      - □ HTTP Redirection
      - ☑ WebDAV Publishing
    - ■ Health and Diagnostics (Installed)
    - ■ Performance (Installed)

Description

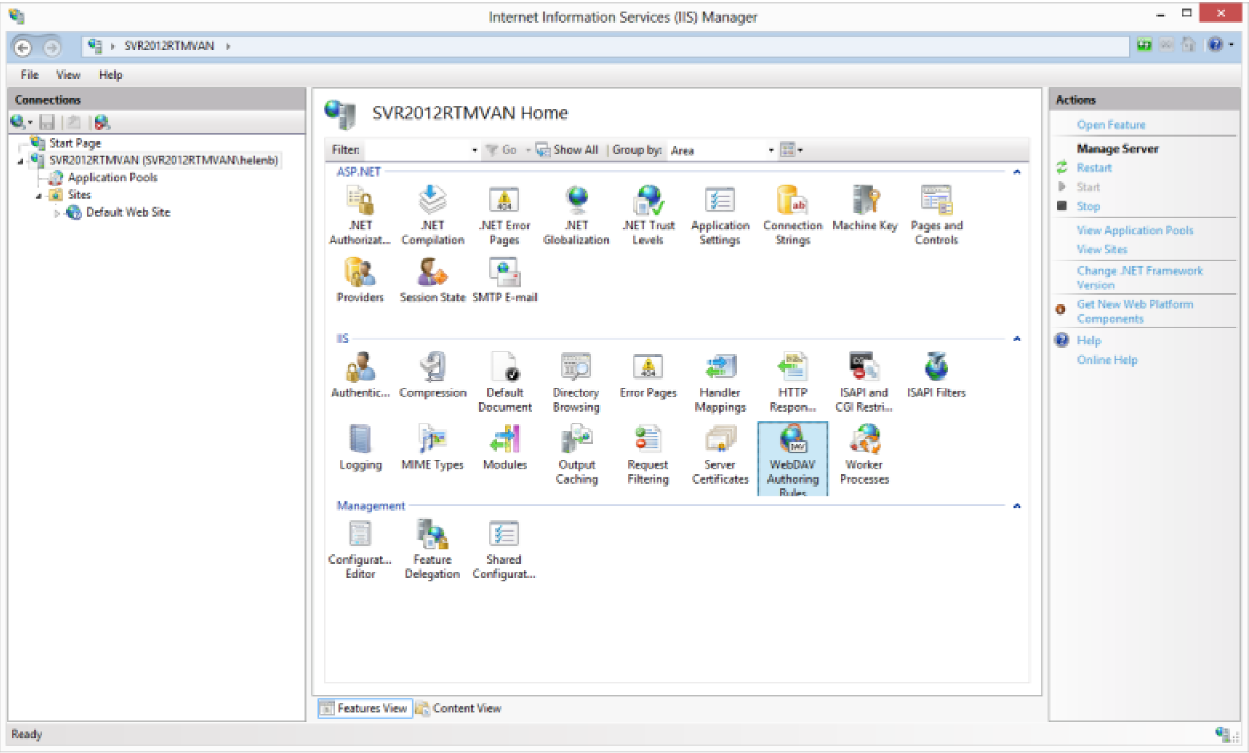
WebDAV Publishing (Web Distributed Authoring and Versioning) enables you to publish files to and from a Web server by using the HTTP protocol. Because WebDAV uses HTTP, it works through most firewalls without modification.

7. Click **Next** on the **Select features** dialog. The **Confirmation installation selections** dialog will be displayed.
8. Click **Install**. Once the installation is complete, click **Close**.

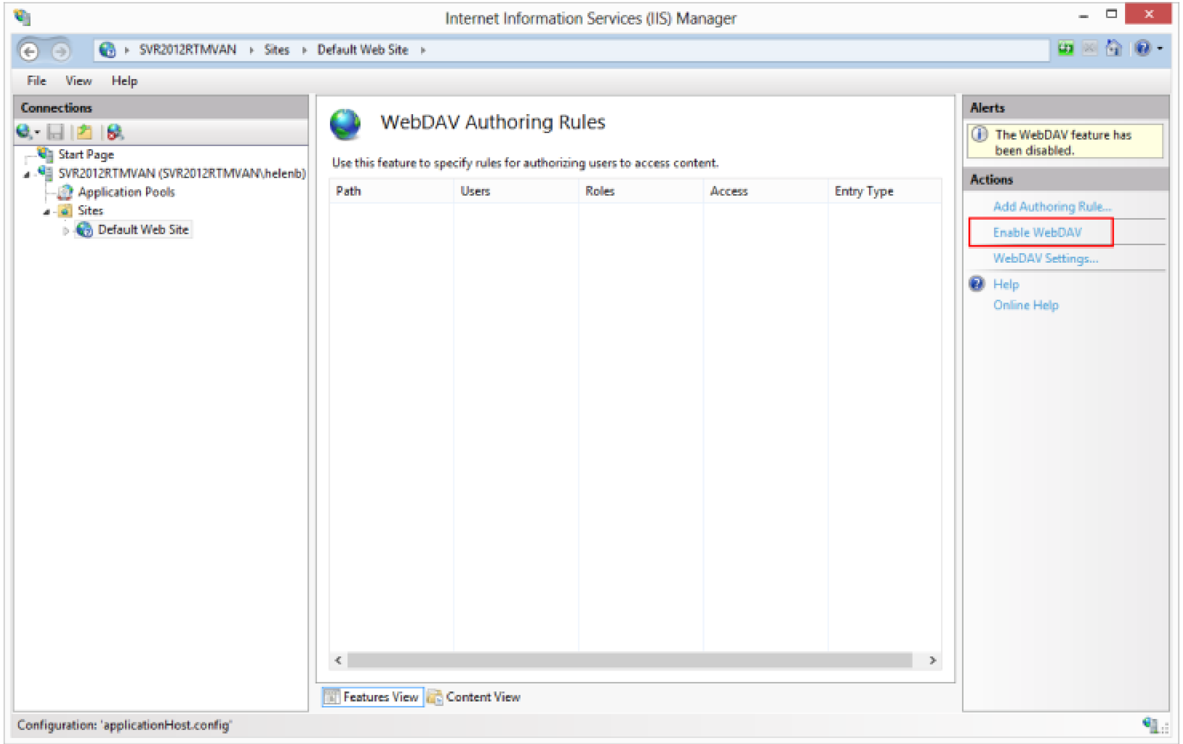
Enabling and Configuring WebDAV in Internet Information Services (IIS)

To enable and configure the WebDAV Settings for IIS

1. Open Internet Information Services (IIS) Manager.
2. Under the defined Web Server name, expand the **Site** node and select the site where the Web Client is installed, e.g. **Default Web Site**.
3. From the **IIS** group, select and open **WebDAV Authoring Rules**.



4. On the **WebDAV Authoring Rules** dialog, click **Enable WebDAV**.



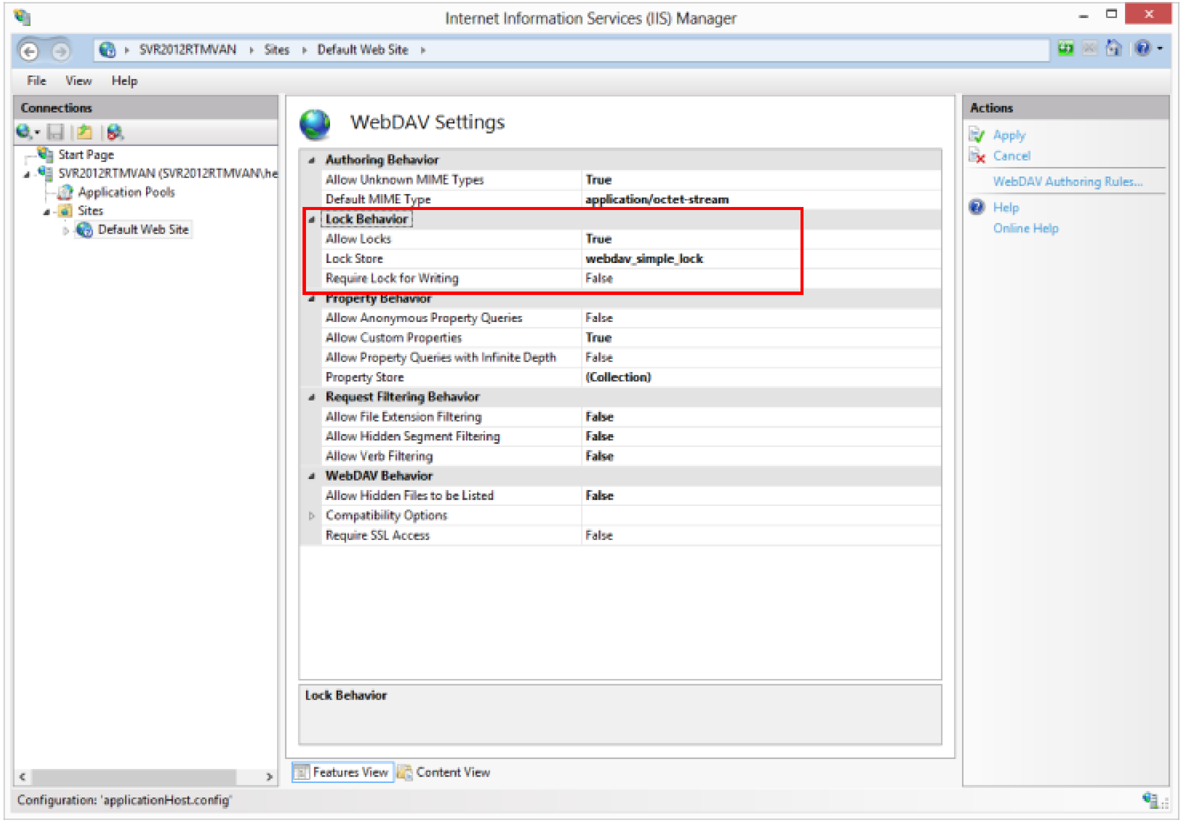
Use this feature to specify rules for authorizing users to access content.

The WebDAV feature has been disabled.

5. On the **WebDAV Authoring Rules** dialog, click **WebDav Settings**.

6. On the **WebDAV Settings** dialog, set the **Lock Behavior** options as follows, and the click **Apply**:
   - **Allow Locks** - True
   - **Lock Store** - webdav_simple_lock

- **Require Lock for Writing** - False

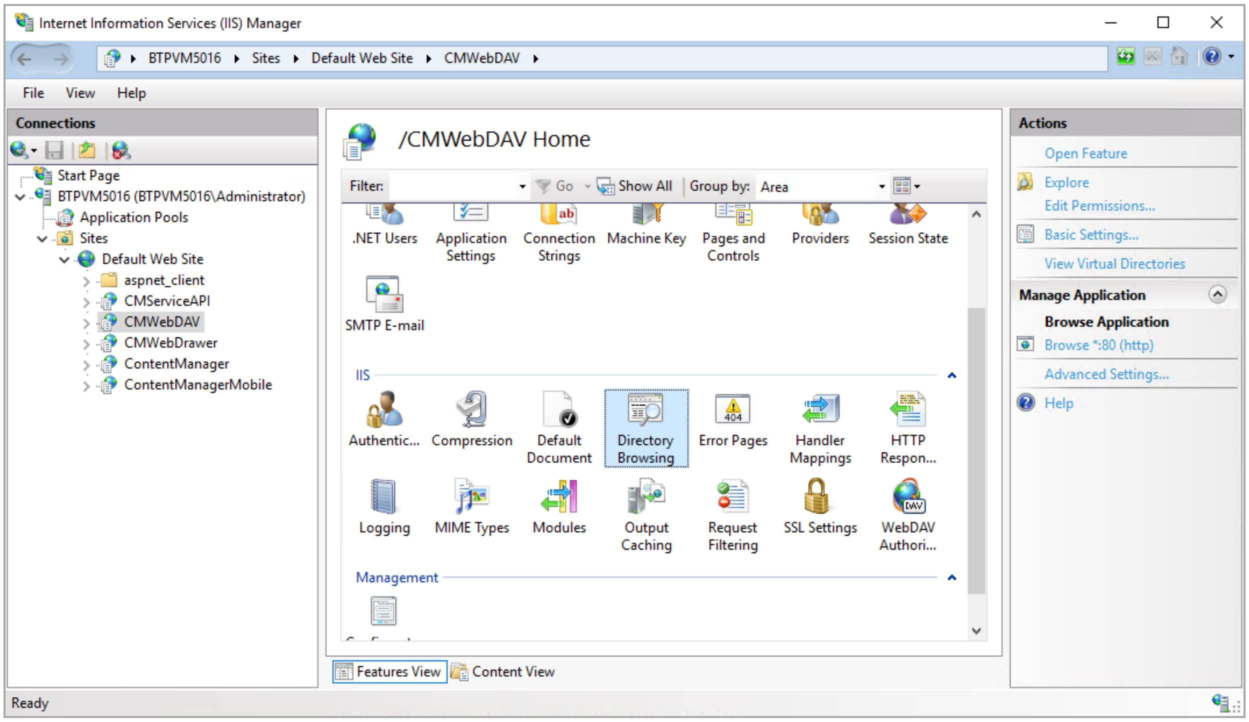


Authoring Behavior	
Allow Unknown MIME Types	True
Default MIME Type	application/octet-stream
Lock Behavior	
Allow Locks	True
Lock Store	webdav_simple_lock
Require Lock for Writing	False
Property Behavior	
Allow Anonymous Property Queries	False
Allow Custom Properties	True
Allow Property Queries with Infinite Depth	False
Property Store	(Collection)
Request Filtering Behavior	
Allow File Extension Filtering	False
Allow Hidden Segment Filtering	False
Allow Verb Filtering	False
WebDAV Behavior	
Allow Hidden Files to be Listed	False
Compatibility Options	
Require SSL Access	False

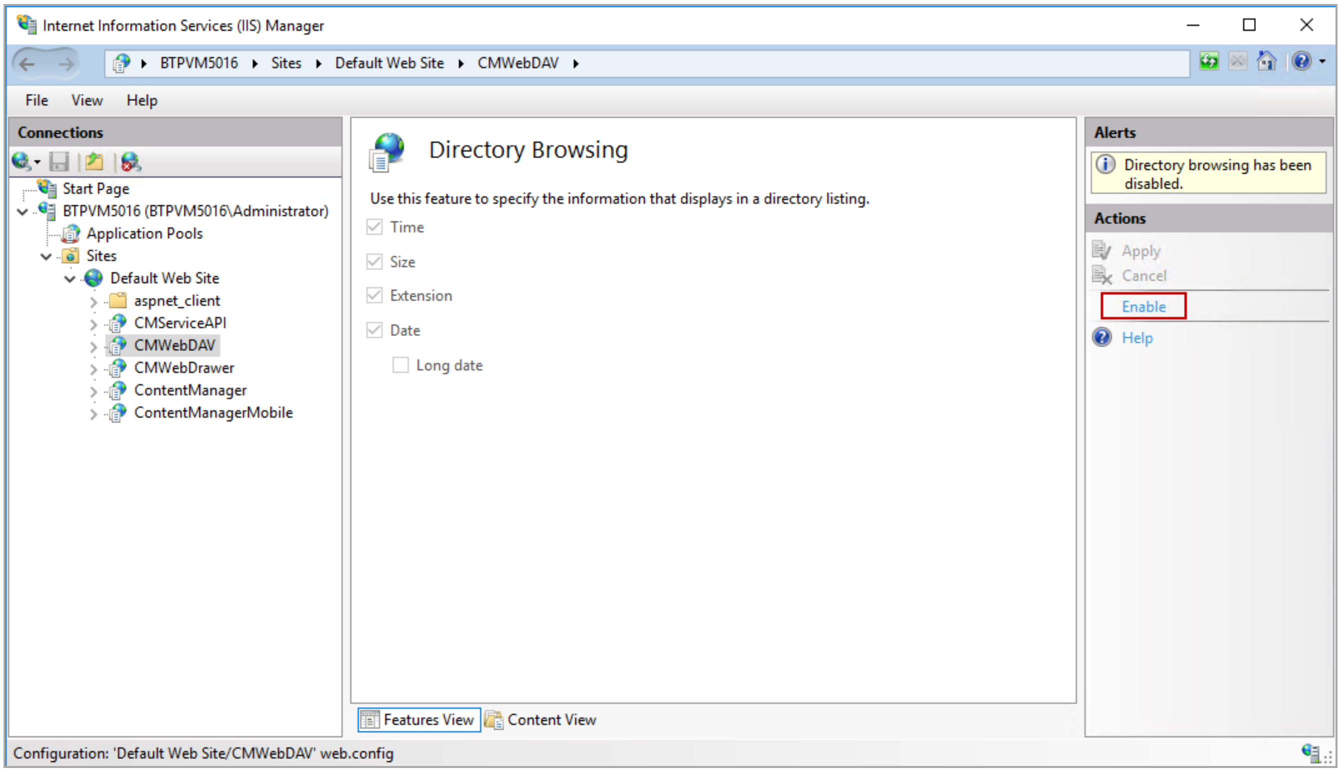
Enabling and Configuring Directory Browsing for CMWebDav

To enable and configure Directory Browsing

1. Once the WebDAV settings have been applied, on the **Connections** panel, expand the **Sites** node, then expand the site node where the Web Client is installed, e.g. **Default Web Site** and select the **CMWebDAV** site.
2. From the **IIS** group, select and open **Directory Browsing**.



3. On the **Directory Browsing** dialog, click **Enable**.



Use this feature to specify the information that displays in a directory listing.

☑ Time

☑ Size

☑ Extension

☑ Date

□ Long date

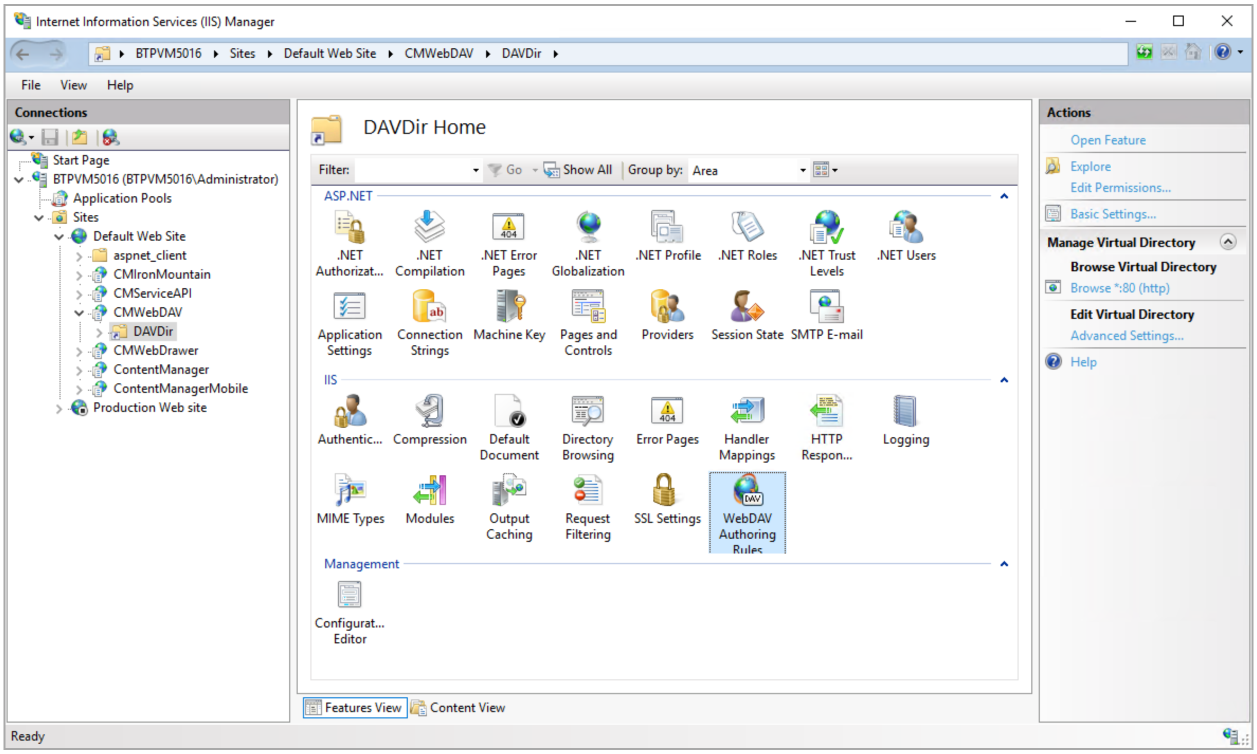
Directory browsing has been disabled.

Configuration: 'Default Web Site/CMWebDAV' web.config

Adding WebDAV Authoring Rules for CMWebDAV

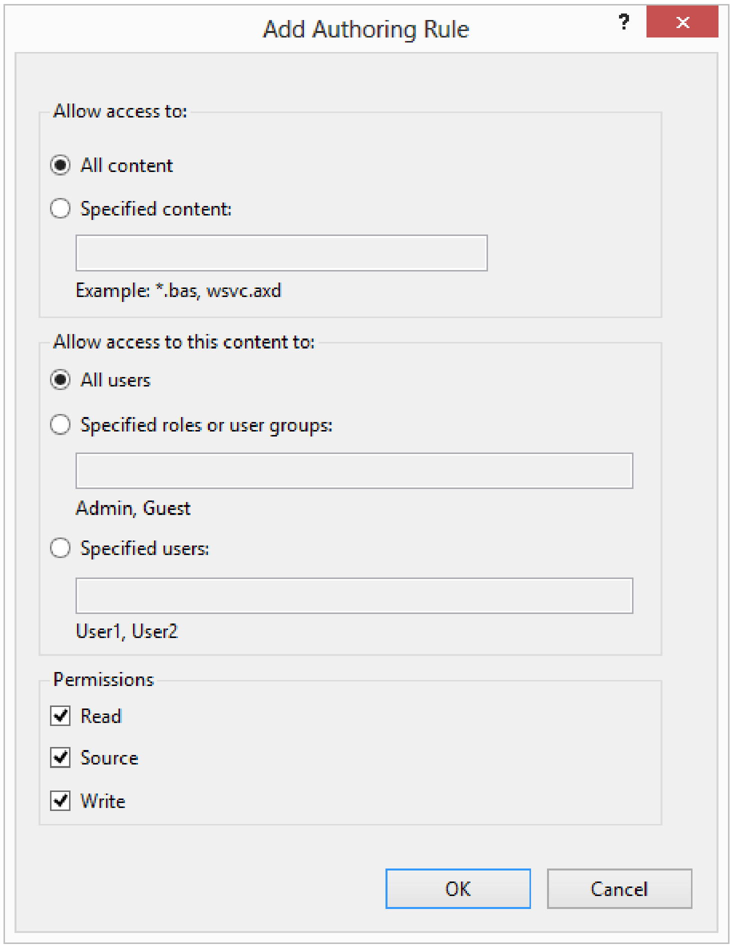
To add Authoring rules

1. Once **Directory Browsing** has been enabled, on the **Connections** panel, expand the **Sites** node, then expand the site where the Web Client is installed, e.g. **Default Web Site** > **CMWebDAV** nodes and select **DAVDir**.
2. From the **IIS** group, select and open **WebDAV Authoring Rules**.



3. On the **WebDAV Authoring Rules** dialog, click **Add Authoring Rule**. The **Add Authoring Rule** dialog will appear.
4. Create a new rule with the following options selected:
   - **Allow access to** - All content
   - **Allow access to this content to** - All users

- **Permissions** - select Read, Source and Write



Add Authoring Rule

Allow access to:

● All content

○ Specified content:

Example: *.bas, wsvc.axd

Allow access to this content to:

● All users

○ Specified roles or user groups:

Admin, Guest

○ Specified users:

User1, User2

Permissions

☑ Read

☑ Source

☑ Write

5. Click **OK**.

Configuring the CMWebDAV Workpath Folder

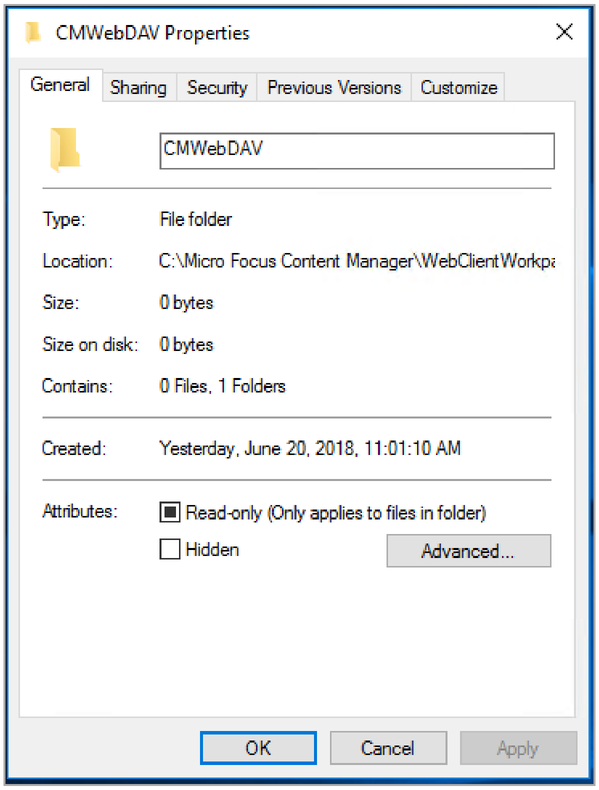
On the Web Server, in the Content Manager Web Client workpath folder, the **CMWebDAV** folder, the Windows File Sharing settings must be updated so all users of the Web Client have Change and Read permissions to this directory. Each document a user checks out and edits using the **Check Out and edit** option in the Web Client, will be saved as a working copy to a sub-directory beneath this directory. Each sub-directory and working copy files are restricted to the Content Manager user who checked them out.

1. On the Content Manager Web Client Web Server, using Windows Explorer, navigate to and open the WebClientWorkPath folder, by default this will be installed to C:\Micro Focus Content Manager\WebClientWorkpath.
2. On **CMWebDAV** folder, right-click and click **Properties**.

Alternatively, in IIS, on the **Connections** panel, expand the **Sites** node, then expand the site node where the Web Client is installed, e.g. **Default Web Site** and select the **CMWebDAV** site, then click **Edit Permissions** from the **Actions** panel.

The **CMWebDAV Properties** dialog will appear.

1. On the **Sharing** tab, click **Advanced Sharing**.



CMWebDAV

Type: File folder

Location: C:\Micro Focus Content Manager\WebClientWorkpa

Size: 0 bytes

Size on disk: 0 bytes

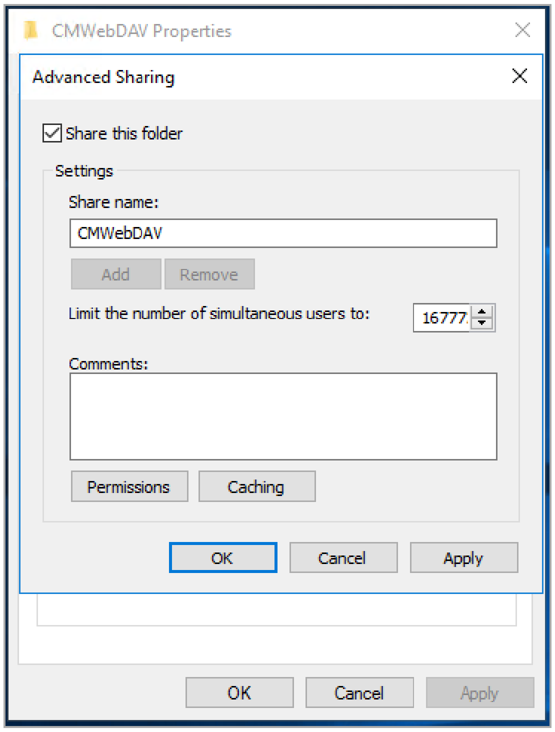
Contains: 0 Files, 1 Folders

Created: Yesterday, June 20, 2018, 11:01:10 AM

Attributes: ■ Read-only (Only applies to files in folder)

□ Hidden

2. On the **Advanced Sharing** dialog, select **Share this folder** and then click **Permissions**.



☑ Share this folder

Settings

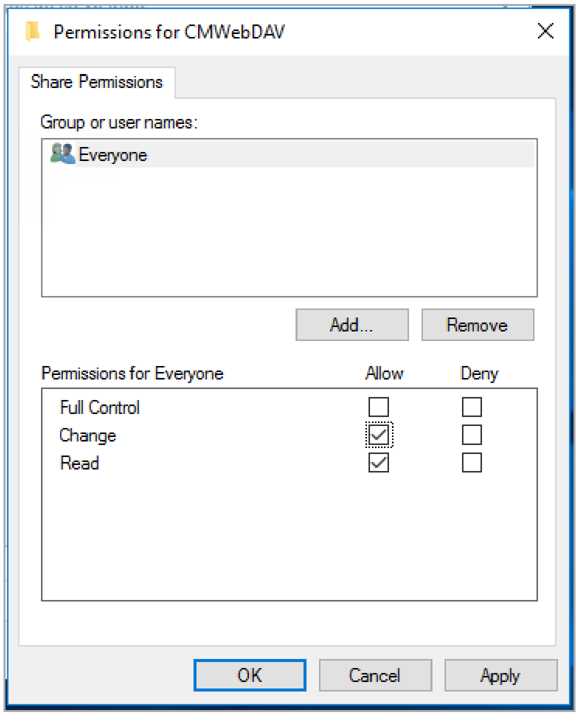
Share name:

CMWebDAV

Limit the number of simultaneous users to: 16777

Comments:

3. On the **Permissions for CMWebDav** dialog, from the list of **Group or user names**, select **Everyone**.
4. From the displayed list of **Permissions for Everyone**, select **Change**, and if not already selected, **Read**.



Permissions for CMWebDAV

Group or user names:

Everyone

Permissions for Everyone	Allow	Deny
Full Control	□	□
Change	☑	□
Read	☑	□

5. Click **Apply** and then click **OK** until you're back to the **CMWebDAV Properties** dialog, then click **Close** to save the new Sharing permissions.

Configuring hprmServiceAPI.config

When installed the **hprmServiceAPI.config** file will contain the relevant section enabling it to load the WebDAV plugin. This section looks like:

```
<pluginAssemblies>

       <add name="TRIMWebClientWebDAV"/>

</pluginAssemblies>
```

> **NOTE:** If you have upgraded from an earlier version of Content Manager, you will need to navigate to the installation directory for the Web Client, for example, C:\Program Files\Micro Focus\Content Manager\Web Client. Open the **hprmServiceAPI.config** file and edit the <add name> property to uncomment and replace <add name="HP.HPTRIM.WebClient.WebDAV"/> property with <add name="TRIMWebClientWebDAV"/>, before saving the changes. If you have made any customizations to the **hprmServiceAPI.config** file you will need to manually copy the customizations from the **hprmServiceAPI.configfile** that is copied to the WebClientWorkpath directory and paste them into the installed **hprmServiceAPI.config**.

Note: If you've enabled the WebDAV module in **hprmServiceAPI.config** and the **Check out and Edit** option is not available in the Web Client, check the logs for errors stating why WebDAV can't be enabled. By default, the error log files are found C:\Micro Focus Content Manager\ServiceAPIWorkpath\logs

Configuring WebDav for non Office documents

From 23.3 onwards, you can configure WebDav to CheckOut and edit non Office documents. To configure WebDav for non Office documents, you need to run **CM_WebClient_WebDAVedit.msi**.

You will be able to run the **CM_WebClient_WebDAVedit.msi** only if **enableWebDAVEdit** attribute is set to **true** in **hprmServiceAPI.config** file. Otherwise, contact your Administrator to either enable the attribute for you or install WebDav for non Office documents on your system.

Example code snippet,

```
<setup databaseId="45" disableKeyViewURL="false" searchAhead="false"
workpath="C:\Micro Focus Content Manager\ServiceAPIWorkpath\Uploads"
bypassViewerFileTypes="*.JPEG;*.JPG;*.PNG;" enableWebDAVEdit="true" />
```

If the **enableWebDAVEdit** attribute is set to **true** in **hprmServiceAPI.config** and you click on WebDav icon for non Office documents, then a message is displayed with a link to download the **CM_WebClient_WebDAVedit.msi**. Run the **CM_WebClient_WebDAVedit.msi** to install WebDav for non Office documents. See, Installing WebDav for non Office documents, below.

The numbering format of **CM_WebClient_WebDAVedit.msi** includes the version number followed by build number with no reference to patch. For example, 23.3.**333**. The numbers 333 is the build number.

> **IMPORTANT:** Before you begin the installation, make sure you have completed all the configuration steps mentioned in Configuring WebDav for Office documents, on page 22.

> **NOTE:** If you have upgraded from previous version of Content Manager and clicking on WebDav icon for non Office document will display a message that new version of the MSI is available and you must install the latest MSI to continue. Click OK to download the latest MSI and run it to install the same.

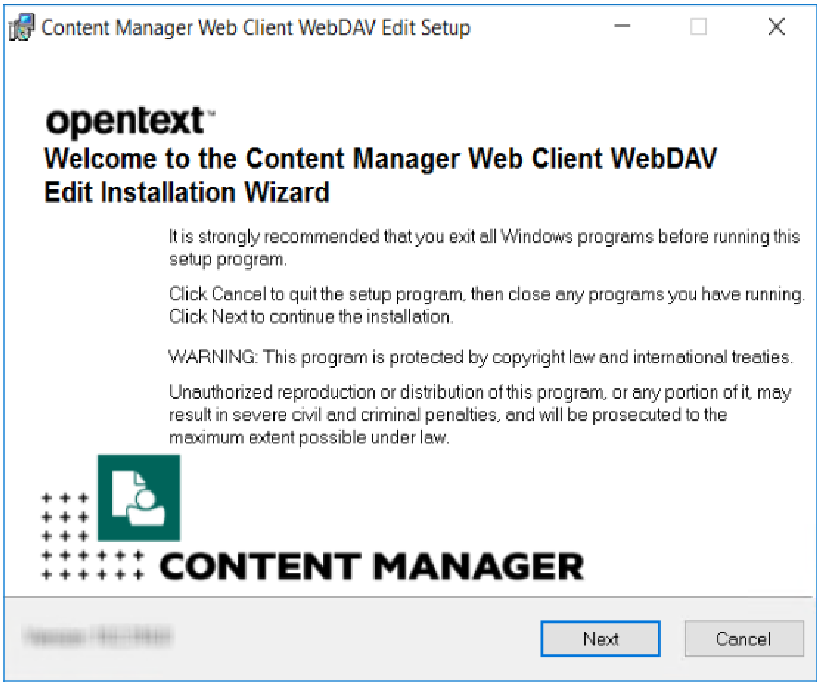
Installing WebDav for non Office documents

> **NOTE:** The WebDav for non Office documents requires .NET Framework 4.7.2 or later.

To install WebDav for non Office documents

1. Navigate to the location where you have saved the **CM_WebClient_WebDAVedit.msi**.
2. Right-click on the **CM_WebClient_WebDAVedit.msi** and select **Run as Administrator** or **Install**.

   The Welcome dialog is displayed.



Welcome to the Content Manager Web Client WebDAV Edit Installation Wizard

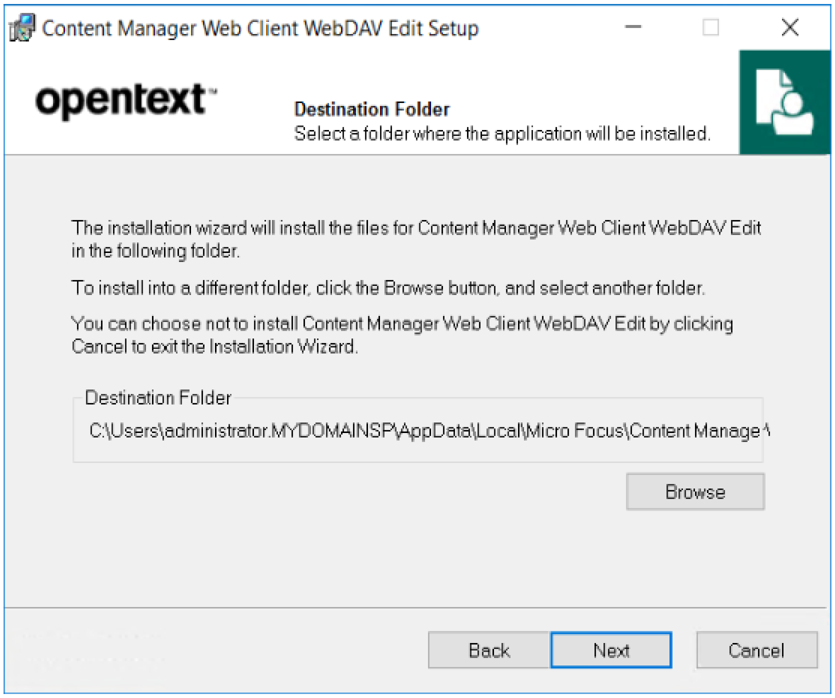
It is strongly recommended that you exit all Windows programs before running this setup program.

Click Cancel to quit the setup program, then close any programs you have running. Click Next to continue the installation.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

3. Click **Next**. The License Agreement dialog is displayed.
4. Select **I accept the license agreement** and click **Next**. The Destination Folder dialog is displayed.



Destination Folder

Select a folder where the application will be installed.

The installation wizard will install the files for Content Manager Web Client WebDAV Edit in the following folder.

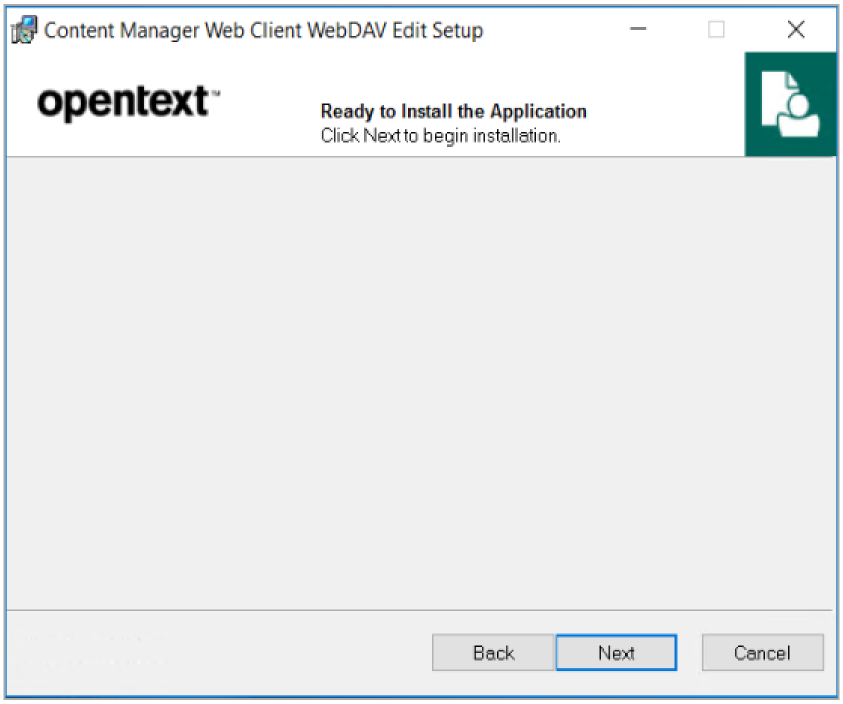
To install into a different folder, click the Browse button, and select another folder.

You can choose not to install Content Manager Web Client WebDAV Edit by clicking Cancel to exit the Installation Wizard.

Destination Folder

C:\Users\administrator.MYDOMAINSP\AppData\Local\Micro Focus\Content Manage\

5. If you want to change the default folder, click **Browse** and change the Destination Folder location. Otherwise, click **Next**. The Ready to Install the Application dialog is displayed.

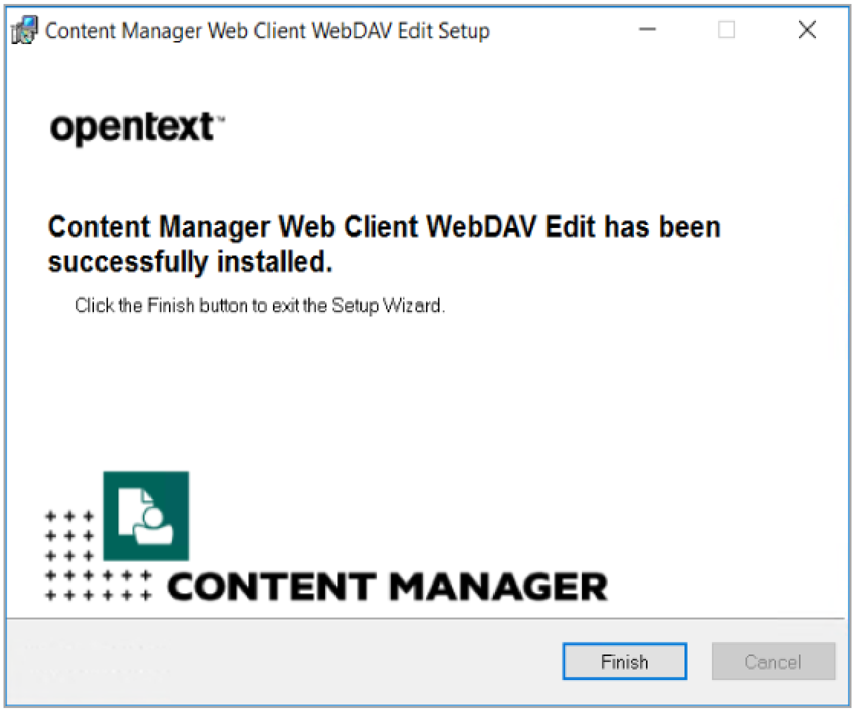


Content Manager Web Client WebDAV Edit Setup

Ready to Install the Application

Click Next to begin installation.

6. Click **Next** to install the application.
7. Once the installation is complete, click **Finish**.



Content Manager Web Client WebDAV Edit Setup

Content Manager Web Client WebDAV Edit has been successfully installed.

Click the Finish button to exit the Setup Wizard.

WebDAV with Load Balancing

Organizations who want to use the WebDAV **Check Out and edit** option in an environment that uses Load Balanced servers will need to modify their WebClient configuration to enable this to work.

If you need multiple server instances, then each instance needs to store and access working copies in the same WebDAV share, and direct the Web browser clients to that share.

The easiest way to do this is to designate one of the instances to store all the working copies. In Content Manager 9.2 or later this can be done by placing the real name of the designated instance into the Application Settings key named 'WebDAVHost'.

You can also use a WebDAV share on an independent host that isn't part of load balancing, but you will need to create the WebDAV share with exactly the same name, path, protocol & port bindings and settings as would be used by the WebDAV share on a stand alone Content Manager Web server setup.

To configure the Content Manager Web Client to use WebDAV with Load Balancing:

1. As an administrator, open the Web Client **web.config** file using a text editor, by default this is installed to C:\Program Files\Micro Focus\Content Manager\Web Client.
2. In the **<appSettings>** section, modify the **<add key="webDAVHost" value=""/>** so the value string contains the name of the server that holds the WebDAV share to be used by all of the Load Balanced Content Manager Web servers, e.g.

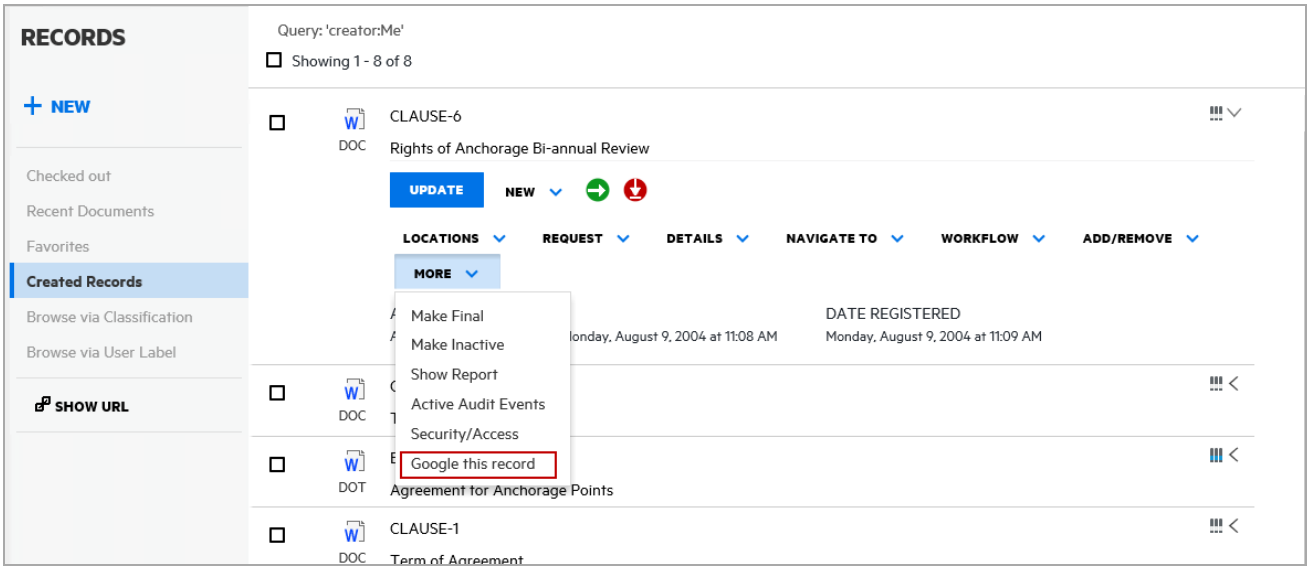
```
<appSettings>

<add key="webpages:Version" value="2.0.0.0"/>

<add key="webpages:Enabled" value="false"/>

<add key="PreserveLoginUrl" value="true"/>

<add key="ClientValidationEnabled" value="true"/>

<add key="UnobtrusiveJavaScriptEnabled" value="true"/>

<add key="webDAVHost" value="CMweb1.loadbalance.com"/>

</appSettings>
```

> **IMPORTANT:** Replace the "webDAVHost" value in the highlighted example with your own value.

3. Save and close the **web.config** file.

Appendix B
Adding Custom Record Add-ins

Introduced in Records Manager Web Client 8.3, is an option for developers and business partners to add custom code via the record add-in infrastructure. This custom functionality is exposed under the **More** drop-down option on a Record object.



To expose the custom record add-in:

1. In the installation directory for the Web Client, by default this is C:\Program Files\Micro Focus\Content Manager\Web Client, create a folder called **CustomScripts**.
2. Copy the custom code JS file to the **CustomScripts** folder.
3. Open Content Manager Web Client , open a Record and then click **More**. Your new Record Add-in option will be available from the available options.

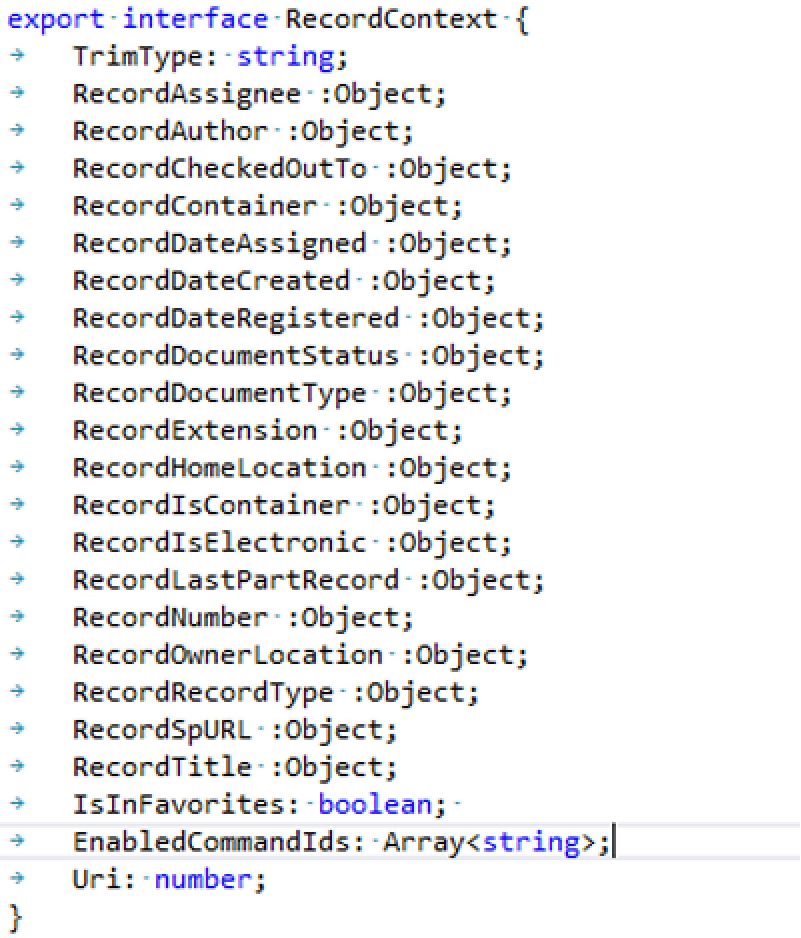
Example Simple Record Add-in

The following example shows how to create a custom record add-in that will, when a user clicks on the option, perform a Google search with the selected record's title.

```
//Wrap your code in a function to avoid conflict

var RMGoogleButtonAddon = function(){

var buttonCaption = "Google this record";

//1 - Create a new instance of a RecordAddonButton

var googleSearchButton  = new HP.HPTRIM.Addon.RecordAddonButton ({

caption : buttonCaption,

clickHandler : function(){

console.log(this.context);

window.open("http://google.com/search?q=" + this.context.RecordTitle.Value)

}

});

//Optional - Perform custom checking before the button is rendered

googleSearchButton.preRender = function(){

var record = this.context;

if(record.RecordTitle.Value == "Microsoft") {

this.setVisible(false);

}

};

//2 - Register the addon button with CustomScriptManager

HP.HPTRIM.Addon.CustomScriptManager.register(googleSearchButton);

}();
```

RecordContext Properties

The clickHandler parameter in the HP.HPTRIM.Addon.RecordAddonButton constructor will be executed when the button is clicked. In this function, you will have access to the current context which is the current record. The properties of the current record object are:



```
export interface RecordContext {
    TrimType: string;
    RecordAssignee :Object;
    RecordAuthor :Object;
    RecordCheckedOutTo :Object;
    RecordContainer :Object;
    RecordDateAssigned :Object;
    RecordDateCreated :Object;
    RecordDateRegistered :Object;
    RecordDocumentStatus :Object;
    RecordDocumentType :Object;
    RecordExtension :Object;
    RecordHomeLocation :Object;
    RecordIsContainer :Object;
    RecordIsElectronic :Object;
    RecordLastPartRecord :Object;
    RecordNumber :Object;
    RecordOwnerLocation :Object;
    RecordRecordType :Object;
    RecordSpURL :Object;
    RecordTitle :Object;
    IsInFavorites: boolean; 
    EnabledCommandIds: Array<string>;
    Uri: number;
}
```

HP.HPTRIM.Addon.RecordAddonButton Methods/Properties

RecordAddonButton supports the following methods and properties:

- **preRender**: this method can be assigned to your custom code when you want to perform any custom logic before the button is rendered
- **setVisible**: this method takes in a Boolean value which will set the visibility of the button.
- **caption**: this property represents the caption of the button.

Deployment

Once the code is written, it will need to be deployed into the{WebClientInstallDir}/CustomScripts folder where WebClientInstallDir is the Content Manager Web Client Installation directory. The CustomScripts folder is not created as a part of the installation process, you will need to manually create the folder before deploying your code.

Record Context Property types

The record context properties are on of a number of different object types, the types of these objects are:

Property	Type
RecordAssignee	Location
RecordAuthor	Location
RecordCheckedOutTo	Location
RecordContainer	Record
RecordDateAssigned	Date
RecordDateCreated	Date
RecordDateRegistered	Date
RecordDocumentStatus	String
RecordDocumentType	String
RecordExtension	String
RecordHomeLocation	Location
RecordIsCheckedOut	Boolean
RecordIsContainer	Boolean
RecordIsElectronic	Boolean
RecordLastPartRecord	Record
RecordNumber	String
RecordOwnerLocation	Location
RecordRecordType	Record Type
RecordRequests	String
RecordSpURL	String
RecordTitle	String
IsInFavorites	Primitive Boolean
EnabledCommandIds	Array of primitive string
Icon	Icon
Uri	Primitive number

Example Object Types

Example object types

The following objects are JSON examples of the types found in the Record context.

Location

```
{

"TrimType": "Location",

"LocationFormattedName": {

"Value": "Full name of Location"

},

"Uri": 9000000000,

"StringValue": "Short name of location"

}
```

Record

```
{
"TrimType": "Record",
"RecordExtension": {
"Value": "PDF"
},
"RecordIsElectronic": {
"Value": true
},
"RecordNumber": {
"Value": "REC_411"
},
"RecordTitle": {
"Value": "My Record Title"
},
"Uri": 9000000378,
"StringValue": "REC_411",
"Icon": {
"IsFileTypeIcon": true,
"IsInternalIcon": false,
"IsValid": true,
"FileType": "PDF",
"Id": "Unknown"
}
}
```

Date

```
{
"IsClear": false,
"IsTimeClear": false,
"DateTime": "2015-11-08T21:48:12.0000000Z",
"StringValue": "9/11/2015 8:48 AM"
}
```

String

```
{
"Value": "A string",
"StringValue": "A string"
}
```

Boolean

```
{
"Value": false,
"StringValue": "Checked In"
}
```

```
},
```

Record Type

```
{
"TrimType": "RecordType",
"RecordTypeAllowParts": {
"Value": true
},
"RecordTypeAllowReplace": {
"Value": true
},
"RecordTypeAllowVersions": {
"Value": true
},
"RecordTypeLevel": {
"Value": 2
},
"RecordTypeMoveWhenReadOnly": {
"Value": false
},
"RecordTypeName": {
"Value": "Document"
},
"RecordTypeStoreType": {
"Value": "UseStore",
"StringValue": "Use A document store"
},
"RecordTypeTitlingMethod": {
"Value": "FreeText",
"StringValue": "Free Text"
},
"RecordTypeUsualBehaviour": {
"Value": "Document",
"StringValue": "Document"
},
"Uri": 2,
"StringValue": "Document",
"Icon": {
"IsFileTypeIcon": false,
"IsInternalIcon": true,
"IsValid": true,
"FileType": "",
"Id": "YellowDoc"
}
}
```

Icon

```
{
"IsFileTypeIcon": true,
"IsInternalIcon": false,
"IsValid": true,
"FileType": "PDF",
"Id": "Unknown"
}
```

Complete Example Record Context

This example shows the properties available on each of the objects in the Record context (summarized earlier in this document). As can be seen most properties are not simple objects but, depending on their type contain a number of properties.

```
{
"TrimType": "Record",
"RecordAssignee": {
"TrimType": "Location",
"LocationFormattedName": {
"Value": "David"
},
"Uri": 1,
"StringValue": "David",
"Icon": {
"IsFileTypeIcon": false,
"IsInternalIcon": true,
"IsValid": true,
"FileType": "",
"Id": "LocPerson"
}
},
"RecordAuthor": {
"TrimType": "Location",
"Uri": 123,
"StringValue": ""
},
"RecordCheckedOutTo": {
"TrimType": "Location",
"Uri": 0,
"StringValue": ""
},
"RecordContainer": {
```

```
"TrimType": "Record",
"Uri": 0,
"StringValue": ""
},
"RecordDateAssigned": {
"IsClear": false,
"IsTimeClear": false,
"DateTime": "2015-11-08T21:48:12.0000000Z",
"StringValue": "9/11/2015 8:48 AM"
},
"RecordDateCreated": {
"IsClear": false,
"IsTimeClear": false,
"DateTime": "2015-08-12T15:22:26.0000000Z",
"StringValue": "13/08/2015 2:22 AM"
},
"RecordDateRegistered": {
"IsClear": false,
"IsTimeClear": false,
"DateTime": "2015-11-08T21:48:12.0000000Z",
"StringValue": "9/11/2015 8:48 AM"
},
"RecordDocumentStatus": {
"Value": "Checked In",
"StringValue": "Checked In"
},
"RecordDocumentType": {
"Value": "Adobe Acrobat Document",
"StringValue": "Adobe Acrobat Document"
},
"RecordExtension": {
"Value": "PDF",
"StringValue": "PDF"
```

```
},
"RecordHomeLocation": {
"TrimType": "Location",
"LocationFormattedName": {
"Value": "Adelaide"
},
"Uri": 9000000000,
"StringValue": "Adelaide",
"Icon": {
"IsFileTypeIcon": false,
"IsInternalIcon": true,
"IsValid": true,
"FileType": "",
"Id": "LocUnit"
}
},
"RecordIsCheckedOut": {
"Value": false,
"StringValue": "Checked In"
},
"RecordIsContainer": {
"Value": false,
"StringValue": "No"
},
"RecordIsElectronic": {
"Value": true,
"StringValue": "Yes"
},
"RecordLastPartRecord": {
"TrimType": "Record",
"RecordExtension": {
"Value": "PDF"
},
"RecordIsElectronic": {
"Value": true
},
"RecordNumber": {
"Value": "REC_411"
},
"RecordTitle": {
"Value": "15-532471"
},
"Uri": 9000000378,
"StringValue": "REC_411",
"Icon": {
"IsFileTypeIcon": true,
"IsInternalIcon": false,
"IsValid": true,
"FileType": "PDF",
"Id": "Unknown"
}
},
"RecordNumber": {
"Value": "REC_411",
"StringValue": "REC_411"
},
"RecordOwnerLocation": {
"TrimType": "Location",
"LocationFormattedName": {
"Value": "Adelaide"
},
"Uri": 9000000000,
"StringValue": "Adelaide",
"Icon": {
"IsFileTypeIcon": false,
"IsInternalIcon": true,
"IsValid": true,
"FileType": "",
"Id": "LocUnit"
}
},
"RecordRecordType": {
"TrimType": "RecordType",
"RecordTypeAllowParts": {
"Value": true
},
"RecordTypeAllowReplace": {
"Value": true
},
"RecordTypeAllowVersions": {
"Value": true
},
"RecordTypeLevel": {
"Value": 2
},
"RecordTypeMoveWhenReadOnly": {
"Value": false
},
"RecordTypeName": {
"Value": "Document"
},
"RecordTypeStoreType": {
"Value": "UseStore",
"StringValue": "Use A document store"
},
"RecordTypeTitlingMethod": {
"Value": "FreeText",
"StringValue": "Free Text"
},
"RecordTypeUsualBehaviour": {
"Value": "Document",
"StringValue": "Document"
},
"Uri": 2,
"StringValue": "Document",
"Icon": {
"IsFileTypeIcon": false,
"IsInternalIcon": true,
"IsValid": true,
"FileType": "",
"Id": "YellowDoc"
}
},
"RecordRequests": {
"Value": "",
"StringValue": ""
},
"RecordSpURL": {
"Value": "",
"StringValue": ""
},
"RecordTitle": {
"Value": "15-532471",
"StringValue": "15-532471"
},
"IsInFavorites": false,
"EnabledCommandIds": [
"Properties",
"RecCheckOut",
"RecCheckIn",
"RecNewPart",
"RecNewVersion",
"RecAddRetrieveTemporaryRequest",
"RecContainer",
"RecOwnerLoc",
"RecAddContact",
"ShowContacts",
"RecCurrentLoc",
"RecHomeLoc",
"RecRemoveContact",
"RecShowRequests",
"RecAddRetrieveTemporaryRequest",
"RecAddRetrieveRecurrentRequest",
"RecAddRetrievePermanentRequest",
"RecAddPickupTemporaryRequest",
"RecAddPickupPermanentRequest"
],
"Icon": {
"IsFileTypeIcon": true,
"IsInternalIcon": false,
"IsValid": true,
"FileType": "PDF",
"Id": "Unknown"
},
"Uri": 9000000378
```

Appendix C Configuring OpenID connect

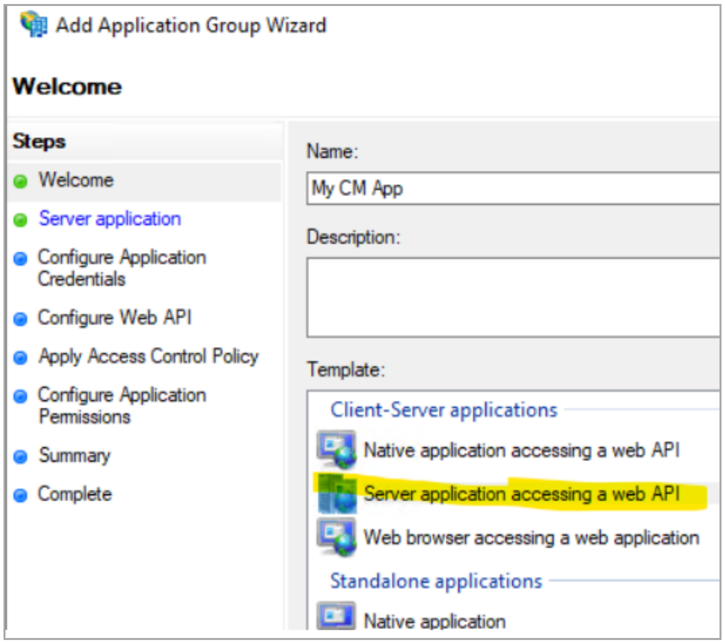
OAuth authentication is managed via OpenID connect authentication. The authentication is configured in your Identity Provider (e.g. Azure AD) and then the appropriate details are stored in Content Manager in the hptrim.config file, for the Web Client and ServiceAPI. The following sections describes creating ADFS applications, Azure AD applications, Google credentials and configuring the Content Manager web application.

Configuring Active Directory Federation Services (ADFS) authentication

Creating an ADFS application

To create an ADFS application, perform the following:

1. Create a new Application Group.
2. In the Add Application Group wizard Welcome page, type the name in the **Name** field and select **Server application accessing a web application** template. Click **Next**.



Add Application Group Wizard

Welcome

Name: My CM App

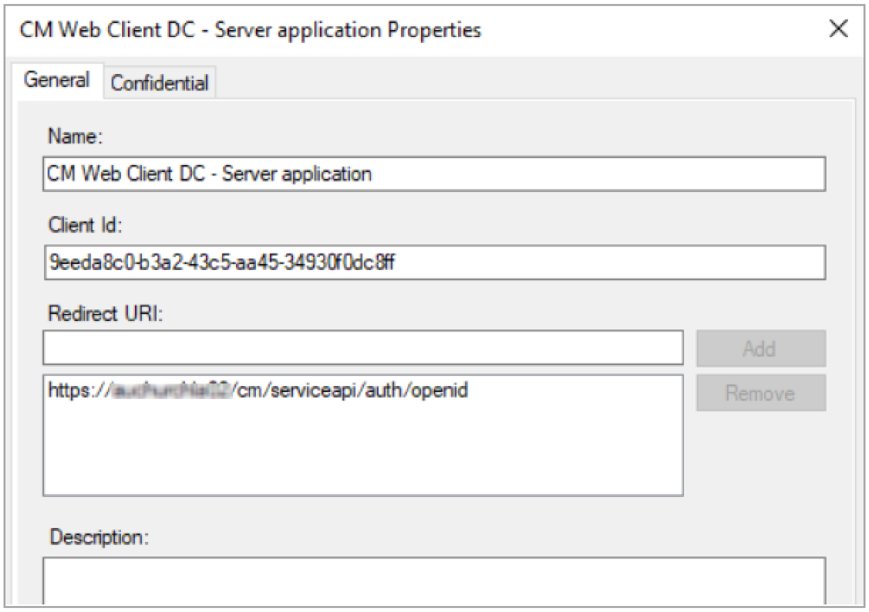
Description:

Template: Server application accessing a web API

Steps
Welcome
Server application
Configure Application Credentials
Configure Web API
Apply Access Control Policy
Configure Application Permissions
Summary
Complete
Client-Server applications
Native application accessing a web API
Server application accessing a web API
Web browser accessing a web application
Standalone applications
Native application

3. In the Server application page General tab, type the name in the **Name** field, note the **Client Id** and add a **Redirect URI**.

> **NOTE:** Make sure that the Redirect URI is in lowercase and is the URL of the Content Manager web site with the suffix **/serviceapi/auth/openid**. For example, https://myserver/contentmanager/serviceapi/auth/openid.



CM Web Client DC - Server application Properties

Name: CM Web Client DC - Server application

Client Id: 9eeda8c0-b3a2-43c5-aa45-34930f0dc8ff

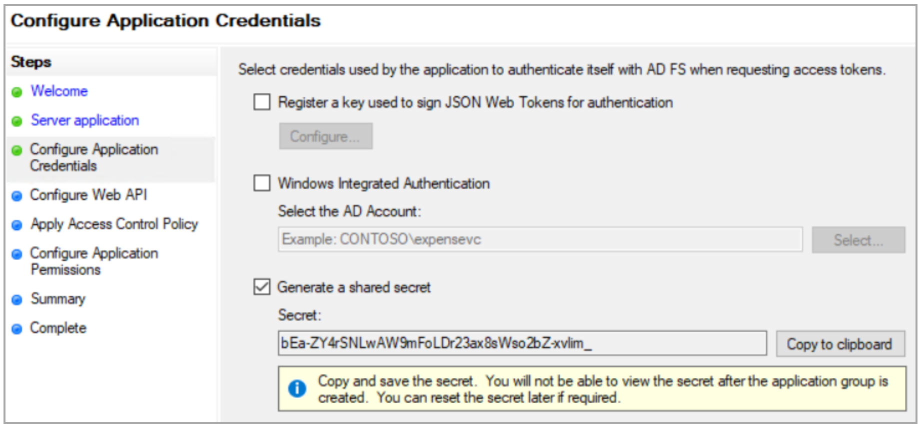
Redirect URI:

https://[redacted]/cm/serviceapi/auth/openid

Description:

4. Click **Next**.

5. In the Configure Application Credentials page, select **Generate a shared secret** checkbox. Make a note of it or copy it to the clipboard.



Configure Application Credentials

Steps
Welcome
Server application
Configure Application Credentials
Configure Web API
Apply Access Control Policy
Configure Application Permissions
Summary
Complete

Select credentials used by the application to authenticate itself with AD FS when requesting access tokens.

□ Register a key used to sign JSON Web Tokens for authentication

□ Windows Integrated Authentication

Select the AD Account: Example: CONTOSO\expensevc

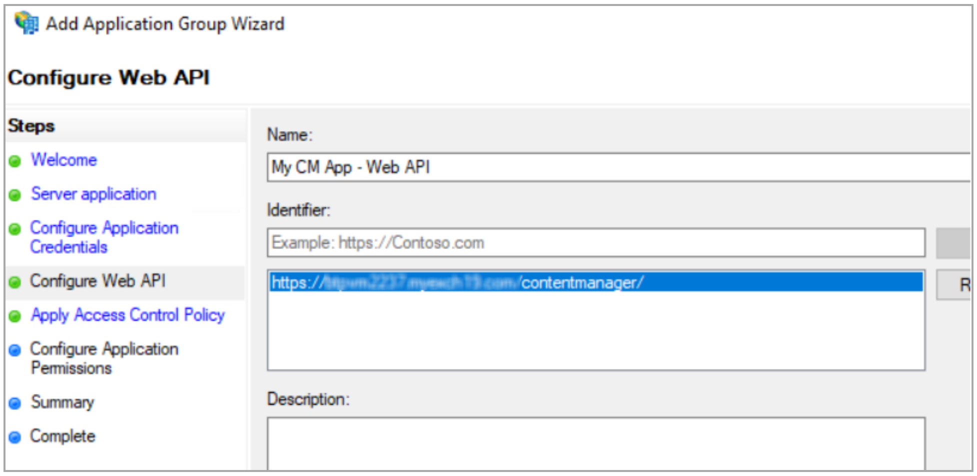
☑ Generate a shared secret

Secret: bEa-ZY4rSNLwAW9mFoLDr23ax8sWso2bZ-xvlim_

Copy and save the secret. You will not be able to view the secret after the application group is created. You can reset the secret later if required.

6. Click **Next**.

7. In the Configure Web API page, add an identifier. For example, https://MyServer/contentmanager/.



Add Application Group Wizard

Configure Web API

Steps

- Welcome
- Server application
- Configure Application Credentials
- Configure Web API
- Apply Access Control Policy
- Configure Application Permissions
- Summary
- Complete

Name:

My CM App - Web API

Identifier:

Example: https://Contoso.com

https://[redacted]/contentmanager/

Description:

8. Click **Next**.
9. In the Apply access control policy page, choose an access control policy. For example, Give access to everyone.
10. Click **Next**.
11. In the Configure application permissions page, select email, openid, and profile checkboxes.
12. Verify the information in the Summary page and complete creating the new application group.

Updating hprmServiceAPI.config

To configure the Content Manager Web Client, edit the hprmServiceAPI.config file and add (or edit) the authentication element.

1. Navigate to the Content Manager Web Client install folder. For example, C:\Program Files\Micro Focus\Content Manager\Web Client.
2. Open the hprmServiceAPI.config file in a text editor.
3. Add the **useADFS** parameter and set it to **true**. For example,

```
<!-- Web Client configuration -->
<setup databaseId="45" searchAhead="true" workpath="C:\Micro Focus Content
Manager\ServiceAPIWorkpath\Uploads" useADFS="true" />
```

4. Add the **<authentication>** element. For example,

```
<authentication allowAnonymous="false" slidingSessionMinutes="30">
  <openIdConnect>
    <add
      name="openid"
      clientID="Client ID noted when creating Application group"
      clientSecret="Client secret noted when creating Application group"
      issuerURI="https://yourvm.myexch19.com/adfs/.well-known/openid-
configuration"
  </openIdConnect>
</authentication>
```

You can find the issuerURI in the AD FS console - Endpoints, in the OpenID Connect section.

> **IMPORTANT:** Replace the clientID, clientSecret, and issuerURI values in the highlighted example with your own value.

Enabling redirect

The Web Client will not redirect the authentication endpoint unless the Html feature is enabled in hprmServiceAPI.config file.

To enable redirect, perform the following:

1. Navigate to the Content Manager Web Client install folder and open the hprmServiceAPI.config in a text editor.
2. Search for the serviceFeatures property.
3. Add the feature Html.

   For example,

   ```
   <hptrim xmlns="http://HP.HPTRIM.CMIS/hptrimConfig.xsd"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" poolSize="1000"
   trace="true" indexPagePath="/Home"
   notFoundErrorHandler="/APIErrorPages/NotFound"
   globalErrorHandler="/APIErrorPages/GlobalErrors" uploadBasePath="C:\Micro Focus
   Content Manager\ServiceAPIWorkpath\Uploads" autoPoolClean="true"
   serviceFeatures="Json,Razor,Xml,Html,PredefinedRoutes"
   xsi:noNamespaceSchemaLocation="hptrimConfig.xsd">
   ```

Updating web.config file

To be able to open and edit the documents using the thin office integration, you need to update the web.config file.

To update the web.config file

1. Open the Web Client web.config file using a text editor, by default this is installed to C:\Program Files\Micro Focus\Content Manager\Web Client.
2. In the **<system.web>**section, locate the **<authorization>** section and replace the **<deny users="?" />** parameter with **<allow users="*" />** parameter.

   For example,

   ```
   <location path="serviceapi">
   <system.web>
   <httpHandlers>
   <add path="*"
   type="ServiceStack.WebHost.Endpoints.ServiceStackHttpHandlerFactory,
   ServiceStack" verb="*" />
   </httpHandlers>
   <authorization>
   <allow users="*" />
   ```

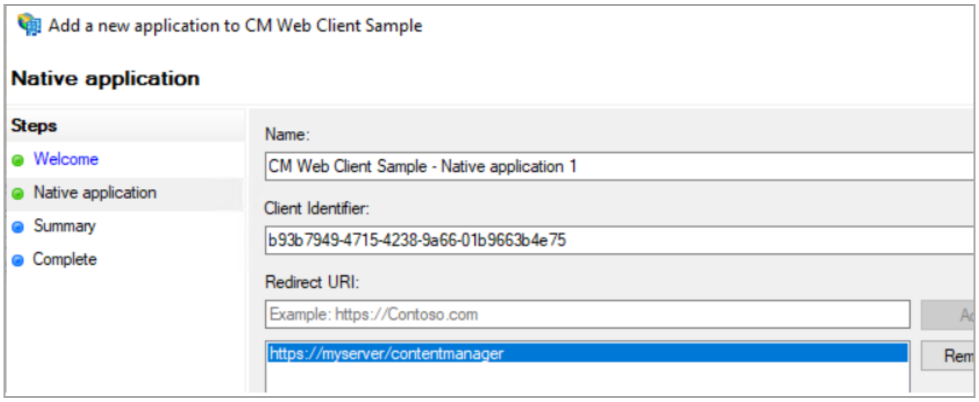
```
</authorization>
</system.web>
```

3. Save and close the web.config file.

Configuring the ADFS for Office/Outlook Addins

The office integration requires an access token to allow it to authenticate with the Web Client, this can be configured in ADFS, perform the following:

1. Go to the Application Group created earlier in Creating an ADFS application, on page 54.
2. Click **Add Application** to add a native application and note the Client ID for later use.



Add a new application to CM Web Client Sample

Native application

Steps
- Welcome
- Native application
- Summary
- Complete

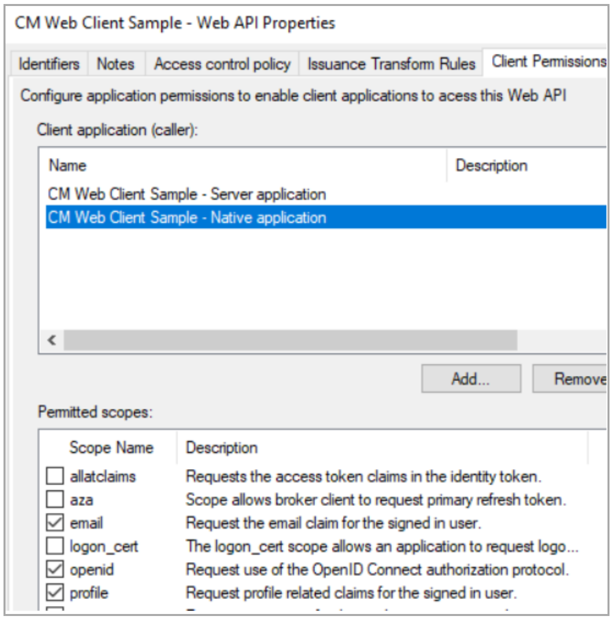
Name: CM Web Client Sample - Native application 1

Client Identifier: b93b7949-4715-4238-9a66-01b9663b4e75

Redirect URI: Example: https://Contoso.com

https://myserver/contentmanager

3. Complete the native application steps.
4. In Configure Web API and configure Application Permission pages, add the new client application and select the scopes email, openid and profile checkboxes.



CM Web Client Sample - Web API Properties

Configure application permissions to enable client applications to acess this Web API

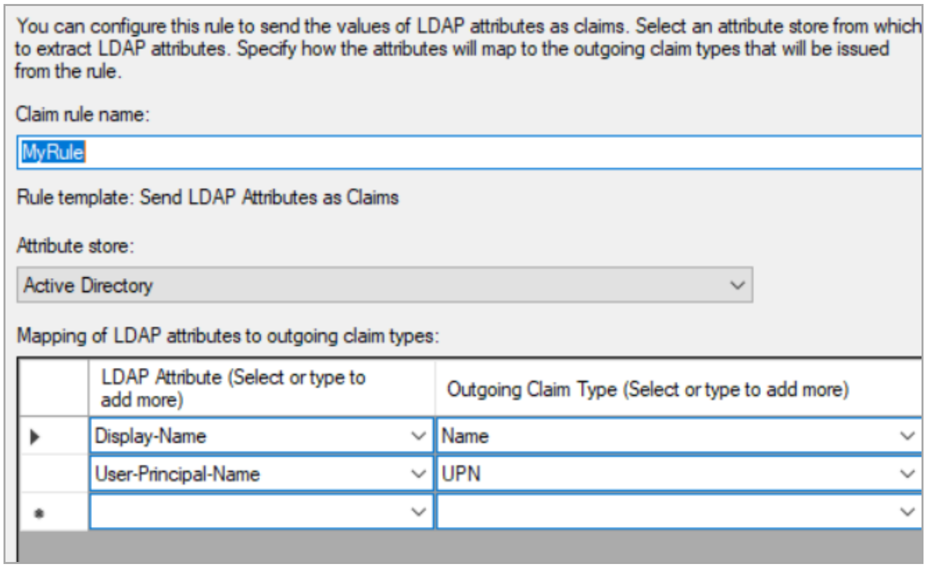
Client application (caller):

Name	Description
CM Web Client Sample - Server application	
CM Web Client Sample - Native application	

Permitted scopes:

Scope Name	Description
□ allatclaims	Requests the access token claims in the identity token.
□ aza	Scope allows broker client to request primary refresh token.
☑ email	Request the email claim for the signed in user.
□ logon_cert	The logon_cert scope allows an application to request logo...
☑ openid	Request use of the OpenID Connect authorization protocol.
☑ profile	Request profile related claims for the signed in user.

5. In Issuance Transform Rules page, add a new Rule.



You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

MyRule

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	Display-Name	Name
	User-Principal-Name	UPN
*		

6. Select **Send LDAP Attributes** and click **Next**.
7. Choose **Active Directory** as the attribute store.
8. Map the following claims:
   - Display Name - Name
   - User-Principal-Name - UPN
9. Complete and **Finish** the steps.

Add the office integration settings to the Web Client

The office integration authentication settings are stored in the file ADFS\config.xml in the web client install directory. To add the settings, perform the following:

1. Navigate to the Content Manager Web Client install folder and find the folder ADFS. For example, C:\Program Files\Micro Focus\Content Manager\Web Client\ADFS.
2. Open the file config.xml file in a text editor.
3. Add the **<adfsClient>** element. For example,

```
<adfsClient>
  <clientAuthority>URL to your AD FS server</clientAuthority>
  <clientResourceUri>relying party identifier from the AD FS Web
API</clientResourceUri>
  <clientID>Client ID from the AD FS native application</clientID>
  <clientReturnUri>Redirect URI from the AD FS native
application</clientReturnUri>
</adfsClient>
```

> **IMPORTANT:** Replace the clientAuthority, clientResourceUri, clientID, and clientReturnUri values in the highlighted example with your own value.

> **NOTE:** Make sure that the clientResourceUri is exactly same as the value used in **ADFS Application Group > Web API > Relying Party** Identifier and the clientReturnUri is exactly same as the value used in **ADFS Application Group > Native Application > Redirect URI**. This is because, the Office integration compares this configuration data with the existing identifier in ADFS, which is case sensitive. Therefore, any difference will result in a failure of the integration.

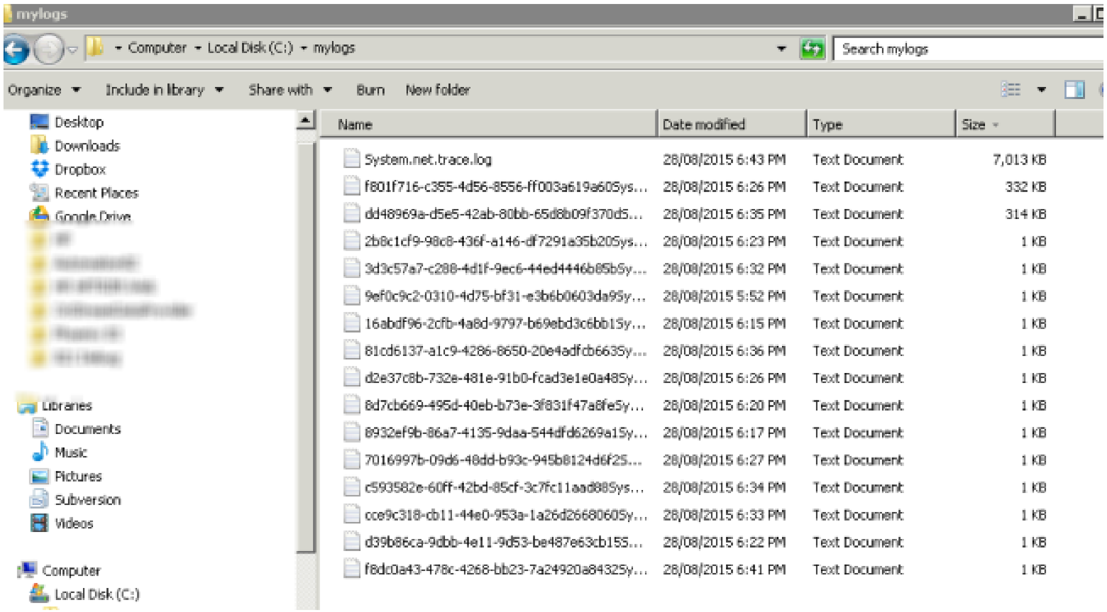
Frequently Asked Questions

How do I enable more logging?

In order to make it easier to troubleshoot problems, it will be useful to enable additional logging. In the Web.config, before the end of Configuration, insert the following config. Change the path in the initializeData attribute under *sharedListeners* to where you want the log to be written to.

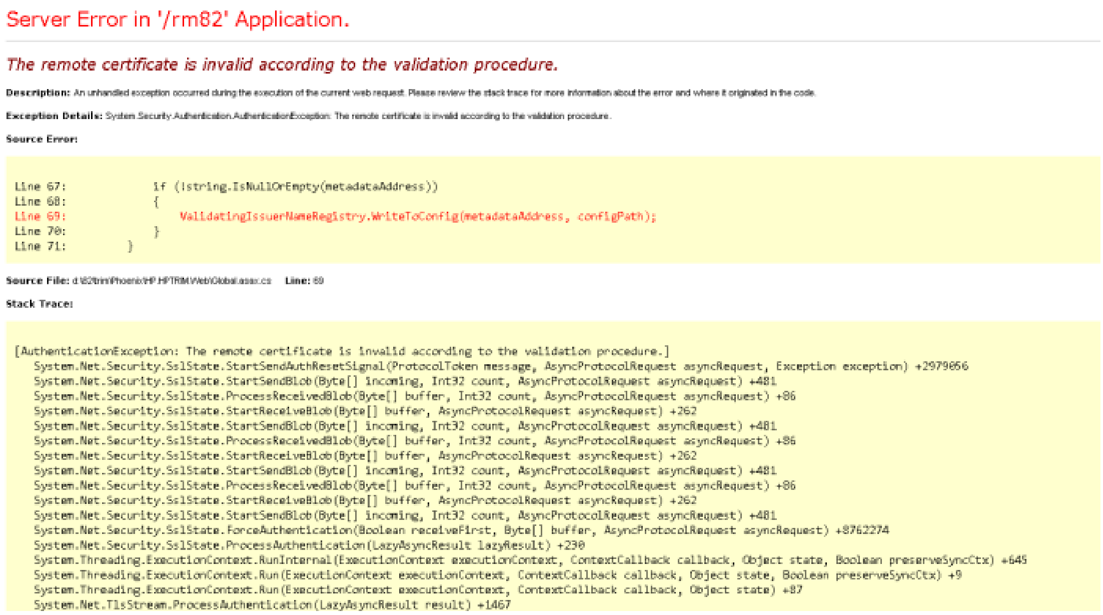
```
<system.diagnostics>
    <trace autoflush="true" />
    <sources>
      <source name="System.Net">
        <listeners>
          <add name="System.Net" />
        </listeners>
      </source>
      <source name="System.Net.HttpListener">
        <listeners>
          <add name="System.Net" />
        </listeners>
      </source>
      <source name="System.Net.Sockets">
        <listeners>
          <add name="System.Net" />
        </listeners>
      </source>
      <source name="System.Net.Cache">
        <listeners>
          <add name="System.Net" />
        </listeners>
      </source>
    </sources>
    <sharedListeners>
      <add name="System.Net" type="System.Diagnostics.TextWriterTraceListener"
initializeData="C:\mylogs\System.net.trace.log" traceOutputOptions="ProcessId,
DateTime" />
    </sharedListeners>
    <switches>
      <add name="System.Net" value="Verbose" />
      <add name="System.Net.Sockets" value="Verbose" />
      <add name="System.Net.Cache" value="Verbose" />
      <add name="System.Net.HttpListener" value="Verbose" />
    </switches>
  </system.diagnostics>
```

You should then see the logs created. If you don’t see the log files generated, manually create the mylogs folder.



Name	Date modified	Type	Size
System.net.trace.log	28/08/2015 6:43 PM	Text Document	7,013 KB
f801f716-c355-4d56-8556-ff003a619a60Sys...	28/08/2015 6:26 PM	Text Document	332 KB
dd48969a-d5e5-42ab-80bb-65d8b09f370d5...	28/08/2015 6:35 PM	Text Document	314 KB
2b8c1cf9-98c8-436f-a146-df7291a35b20Sys...	28/08/2015 6:23 PM	Text Document	1 KB
3d3c57a7-c288-4d1f-9ec6-44ed4446b85bSy...	28/08/2015 6:32 PM	Text Document	1 KB
9ef0c9c2-0310-4d75-bf31-e3b6b0603da95y...	28/08/2015 5:52 PM	Text Document	1 KB
16abdf96-2cfb-4a8d-9797-b69ebd3c6bb15y...	28/08/2015 6:15 PM	Text Document	1 KB
81cd6137-a1c9-4286-8650-20e4adfcb6635y...	28/08/2015 6:36 PM	Text Document	1 KB
d2e37c8b-732e-481e-91b0-fcad3e1e0a485y...	28/08/2015 6:26 PM	Text Document	1 KB
8d7cb669-495d-40eb-b73e-3f831f47a8fe5y...	28/08/2015 6:20 PM	Text Document	1 KB
8932ef9b-86a7-4135-9daa-544dfd6269a15y...	28/08/2015 6:17 PM	Text Document	1 KB
7016997b-09d6-48dd-b93c-945b8124d6f25...	28/08/2015 6:27 PM	Text Document	1 KB
c593582e-60ff-42bd-85cf-3c7fc11aad885ys...	28/08/2015 6:34 PM	Text Document	1 KB
cce9c318-cb11-44e0-953a-1a26d26680605y...	28/08/2015 6:33 PM	Text Document	1 KB
d39b86ca-9dbb-4e11-9d53-be487e63cb155...	28/08/2015 6:22 PM	Text Document	1 KB
f8dc0a43-478c-4268-bb23-7a24920a84325y...	28/08/2015 6:41 PM	Text Document	1 KB

The remote certificate is invalid according to the validation procedure



Server Error in '/rm82' Application.

The remote certificate is invalid according to the validation procedure.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Security.Authentication.AuthenticationException: The remote certificate is invalid according to the validation procedure.

Source Error:

```
Line 67:            if (!string.IsNullOrEmpty(metadataAddress))
Line 68:            {
Line 69:                ValidatingIssuerNameRegistry.WriteToConfig(metadataAddress, configPath);
Line 70:            }
Line 71:        }
```

Source File: d:\82\trim\Phoenix\HP.HPTRIM\Web\Global.asax.cs **Line:** 69

Stack Trace:

```
[AuthenticationException: The remote certificate is invalid according to the validation procedure.]
   System.Net.Security.SslState.StartSendAuthResetSignal(ProtocolToken message, AsyncProtocolRequest asyncRequest, Exception exception) +2979056
   System.Net.Security.SslState.StartSendBlob(Byte[] incoming, Int32 count, AsyncProtocolRequest asyncRequest) +481
   System.Net.Security.SslState.ProcessReceivedBlob(Byte[] buffer, Int32 count, AsyncProtocolRequest asyncRequest) +86
   System.Net.Security.SslState.StartReceiveBlob(Byte[] buffer, AsyncProtocolRequest asyncRequest) +262
   System.Net.Security.SslState.StartSendBlob(Byte[] incoming, Int32 count, AsyncProtocolRequest asyncRequest) +481
   System.Net.Security.SslState.ProcessReceivedBlob(Byte[] buffer, Int32 count, AsyncProtocolRequest asyncRequest) +86
   System.Net.Security.SslState.StartReceiveBlob(Byte[] buffer, AsyncProtocolRequest asyncRequest) +262
   System.Net.Security.SslState.StartSendBlob(Byte[] incoming, Int32 count, AsyncProtocolRequest asyncRequest) +481
   System.Net.Security.SslState.ProcessReceivedBlob(Byte[] buffer, Int32 count, AsyncProtocolRequest asyncRequest) +86
   System.Net.Security.SslState.StartReceiveBlob(Byte[] buffer, AsyncProtocolRequest asyncRequest) +262
   System.Net.Security.SslState.StartSendBlob(Byte[] incoming, Int32 count, AsyncProtocolRequest asyncRequest) +481
   System.Net.Security.SslState.ForceAuthentication(Boolean receiveFirst, Byte[] buffer, AsyncProtocolRequest asyncRequest) +8762274
   System.Net.Security.SslState.ProcessAuthentication(LazyAsyncResult lazyResult) +230
   System.Threading.ExecutionContext.RunInternal(ExecutionContext executionContext, ContextCallback callback, Object state, Boolean preserveSyncCtx) +645
   System.Threading.ExecutionContext.Run(ExecutionContext executionContext, ContextCallback callback, Object state, Boolean preserveSyncCtx) +9
   System.Threading.ExecutionContext.Run(ExecutionContext executionContext, ContextCallback callback, Object state) +87
   System.Net.TlsStream.ProcessAuthentication(LazyAsyncResult result) +1467
```

This is most likely caused by a certificate error. By enabling logging, the error may be something along these lines below.

System.Net Information: 0 : [9504] SecureChannel#3908756 - Remote certificate has errors:

System.Net Information: 0 : [9504] SecureChannel#3908756 - A certificate chain could not be built to a trusted root authority.

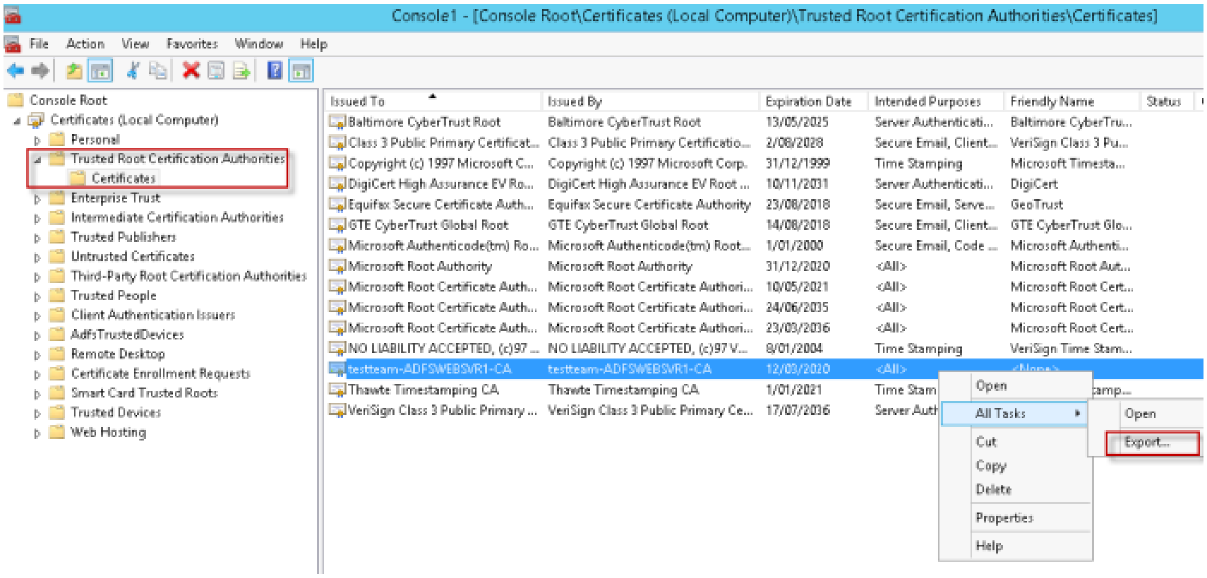
System.Net Information: 0 : [9504] SecureChannel#3908756 - Remote certificate was verified as invalid by the user.

System.Net Error: 0 : [9504] Exception in HttpWebRequest#2237113:: - The underlying connection was closed: Could not establish trust relationship for the SSL/TLS secure channel.

Solution

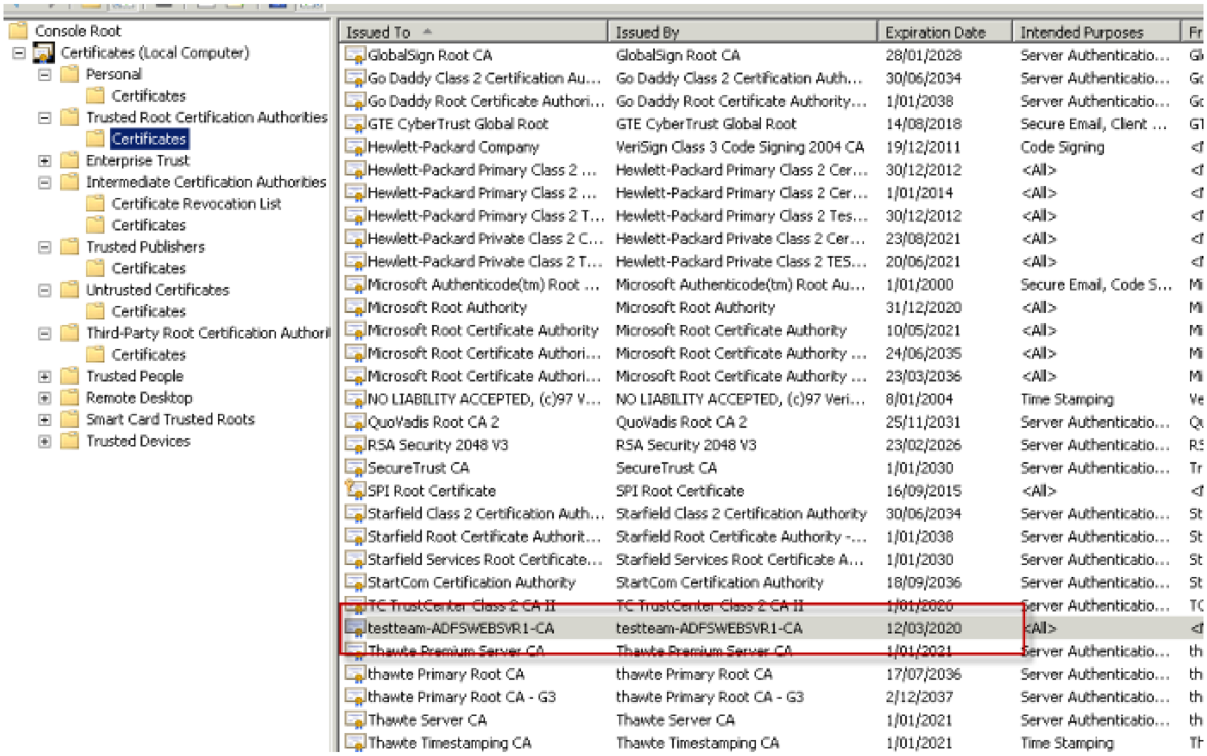
To resolve this problem, the root certificate from the ADFS server must be trusted by the client. Log on to the ADFS Server, export the required certificate from a trusted root authority and import it on the client's machine into the trusted root authority.

To export certificate, on the AD FS Server, please refer to the following screenshot:


Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
AdfsTrustedDevices
Remote Desktop
Certificate Enrollment Requests
Smart Card Trusted Roots
Trusted Devices
Web Hosting
Open
All Tasks
Cut
Copy
Delete
Properties
Help
Open
Export...

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status
Baltimore CyberTrust Root	Baltimore CyberTrust Root	13/05/2025	Server Authenticati...	Baltimore CyberTru...	
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	2/08/2028	Secure Email, Client...	VeriSign Class 3 Pu...	
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	31/12/1999	Time Stamping	Microsoft Timesta...	
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	10/11/2031	Server Authenticati...	DigiCert	
Equifax Secure Certificate Auth...	Equifax Secure Certificate Authority	23/08/2018	Secure Email, Serve...	GeoTrust	
GTE CyberTrust Global Root	GTE CyberTrust Global Root	14/08/2018	Secure Email, Client...	GTE CyberTrust Glo...	
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	1/01/2000	Secure Email, Code ...	Microsoft Authenti...	
Microsoft Root Authority	Microsoft Root Authority	31/12/2020	<All>	Microsoft Root Aut...	
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	10/05/2021	<All>	Microsoft Root Cert...	
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	24/06/2035	<All>	Microsoft Root Cert...	
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	23/03/2036	<All>	Microsoft Root Cert...	
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 V...	8/01/2004	Time Stamping	VeriSign Time Stam...	
testteam-ADFSWEBSVR1-CA	testteam-ADFSWEBSVR1-CA	12/03/2020	<All>	<None>	
Thawte Timestamping CA	Thawte Timestamping CA	1/01/2021	Time Stam	tamp...	
VeriSign Class 3 Public Primary ...	VeriSign Class 3 Public Primary Ce...	17/07/2036	Server Auth		

After the export is successful, you can import this certificate to the client's machine (into the Trusted Root Certificate Authorities).



- Console Root
  - Certificates (Local Computer)
    - Personal
      - Certificates
    - Trusted Root Certification Authorities
      - Certificates
    - Enterprise Trust
    - Intermediate Certification Authorities
      - Certificate Revocation List
      - Certificates
    - Trusted Publishers
      - Certificates
    - Untrusted Certificates
      - Certificates
    - Third-Party Root Certification Authori
      - Certificates
    - Trusted People
    - Remote Desktop
    - Smart Card Trusted Roots
    - Trusted Devices

Issued To	Issued By	Expiration Date	Intended Purposes	Fr
GlobalSign Root CA	GlobalSign Root CA	28/01/2028	Server Authenticatio...	Gl
Go Daddy Class 2 Certification Au...	Go Daddy Class 2 Certification Auth...	30/06/2034	Server Authenticatio...	Gc
Go Daddy Root Certificate Authori...	Go Daddy Root Certificate Authority...	1/01/2038	Server Authenticatio...	Gc
GTE CyberTrust Global Root	GTE CyberTrust Global Root	14/08/2018	Secure Email, Client ...	GT
Hewlett-Packard Company	VeriSign Class 3 Code Signing 2004 CA	19/12/2011	Code Signing	<f
Hewlett-Packard Primary Class 2 ...	Hewlett-Packard Primary Class 2 Cer...	30/12/2012	<All>	<f
Hewlett-Packard Primary Class 2 ...	Hewlett-Packard Primary Class 2 Cer...	1/01/2014	<All>	<f
Hewlett-Packard Primary Class 2 T...	Hewlett-Packard Primary Class 2 Tes...	30/12/2012	<All>	<f
Hewlett-Packard Private Class 2 C...	Hewlett-Packard Private Class 2 Cer...	23/08/2021	<All>	<f
Hewlett-Packard Private Class 2 T...	Hewlett-Packard Private Class 2 TES...	20/06/2021	<All>	<f
Microsoft Authenticode(tm) Root ...	Microsoft Authenticode(tm) Root Au...	1/01/2000	Secure Email, Code S...	Mi
Microsoft Root Authority	Microsoft Root Authority	31/12/2020	<All>	Mi
Microsoft Root Certificate Authority	Microsoft Root Certificate Authority	10/05/2021	<All>	Mi
Microsoft Root Certificate Authori...	Microsoft Root Certificate Authority ...	24/06/2035	<All>	Mi
Microsoft Root Certificate Authori...	Microsoft Root Certificate Authority ...	23/03/2036	<All>	Mi
NO LIABILITY ACCEPTED, (c)97 V...	NO LIABILITY ACCEPTED, (c)97 Veri...	8/01/2004	Time Stamping	Ve
QuoVadis Root CA 2	QuoVadis Root CA 2	25/11/2031	Server Authenticatio...	Qu
RSA Security 2048 V3	RSA Security 2048 V3	23/02/2026	Server Authenticatio...	RS
SecureTrust CA	SecureTrust CA	1/01/2030	Server Authenticatio...	Tr
SPI Root Certificate	SPI Root Certificate	16/09/2015	<All>	<f
Starfield Class 2 Certification Auth...	Starfield Class 2 Certification Authority	30/06/2034	Server Authenticatio...	St
Starfield Root Certificate Authorit...	Starfield Root Certificate Authority -...	1/01/2038	Server Authenticatio...	St
Starfield Services Root Certificate...	Starfield Services Root Certificate A...	1/01/2030	Server Authenticatio...	St
StartCom Certification Authority	StartCom Certification Authority	18/09/2036	Server Authenticatio...	St
TC TrustCenter Class 2 CA II	TC TrustCenter Class 2 CA II	1/01/2026	Server Authenticatio...	TC
testteam-ADFSWEBSVR1-CA	testteam-ADFSWEBSVR1-CA	12/03/2020	<All>	<f
Thawte Premium Server CA	Thawte Premium Server CA	1/01/2021	Server Authenticatio...	th
thawte Primary Root CA	thawte Primary Root CA	17/07/2036	Server Authenticatio...	th
thawte Primary Root CA - G3	thawte Primary Root CA - G3	2/12/2037	Server Authenticatio...	th
Thawte Server CA	Thawte Server CA	1/01/2021	Server Authenticatio...	th
Thawte Timestamping CA	Thawte Timestamping CA	1/01/2021	Time Stamping	Th

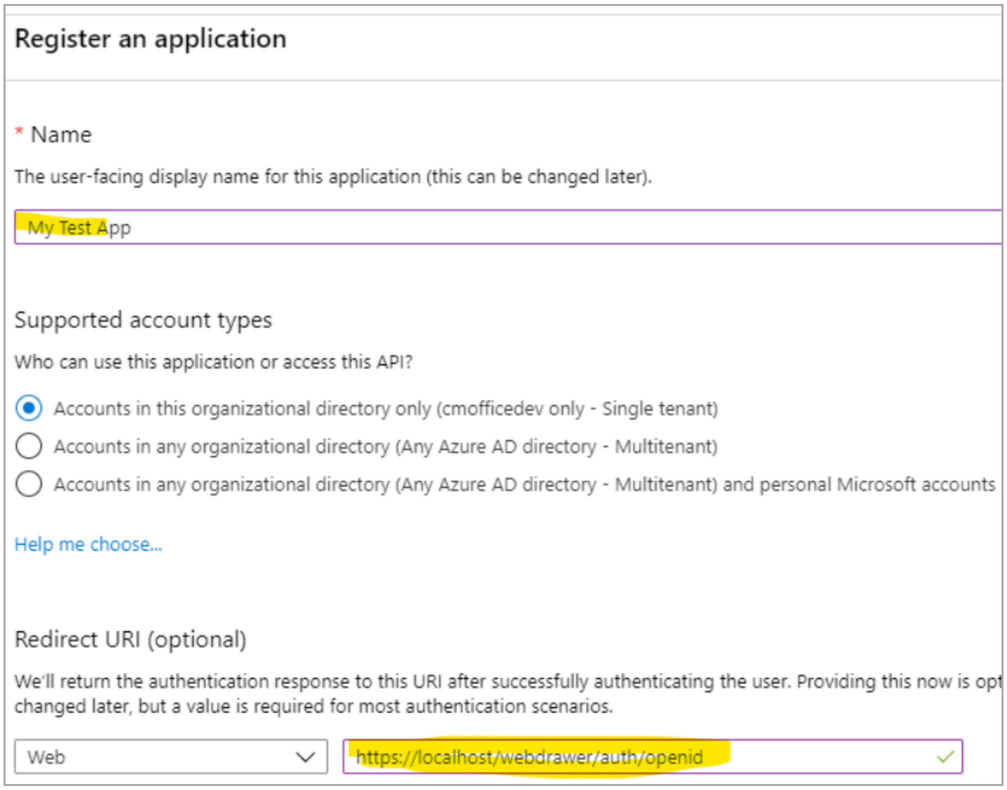
Configuring Azure AD authentication

Creating Azure AD application

To create the Azure AD application, perform the following:

1. Open the following URL portal.azure.com.
2. Click **Azure Active Directory > App registrations > New registration**.

   The **Register an Application** page is displayed.



Register an application

* Name

The user-facing display name for this application (this can be changed later).

My Test App

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (cmofficedev only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts

Help me choose...

Redirect URI (optional)

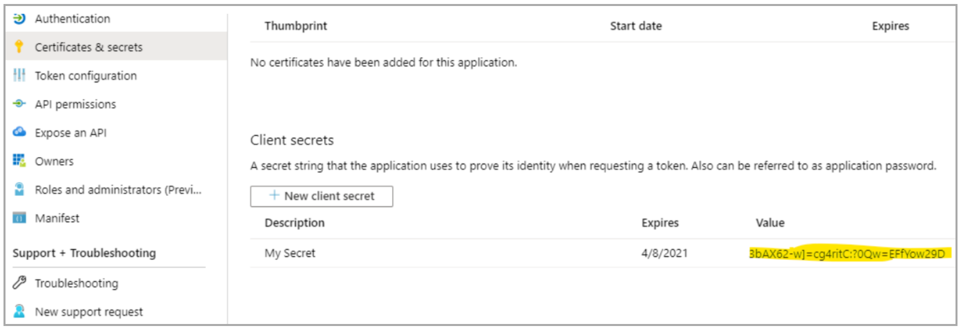
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is opt
changed later, but a value is required for most authentication scenarios.

Web ⌄ https://localhost/webdrawer/auth/openid ✓

3. Type a name for your new application in the **Name** field.
4. Select the **Supported account types**.

   For more information on each option of **Supported account types**, click **Help me choose**.
5. For **Redirect URI**, leave the **Web** selected.

   > **NOTE:** The value in Authorized redirect URIs must be in lowercase and the URL to your application (e.g. https://mydomain.com/cmwebdrawer) followed by the path to the authentication provider (for example /auth/openid). The /auth/ component is fixed but the 'openid' is the name you will supply in hprmServiceAPI.config later and so can be any string, as long as it matches the value in hprmServiceAPI.config.
   > For the Web Client the path must include the path to the ServiceAPI, for example, https://mydomain.com/contentManager/serviceapi/auth/openid.
6. Click **Register**.
7. Add a secret from the **Certificates and Secrets** and note it for later.



Thumbprint	Start date	Expires

No certificates have been added for this application.

Client secrets

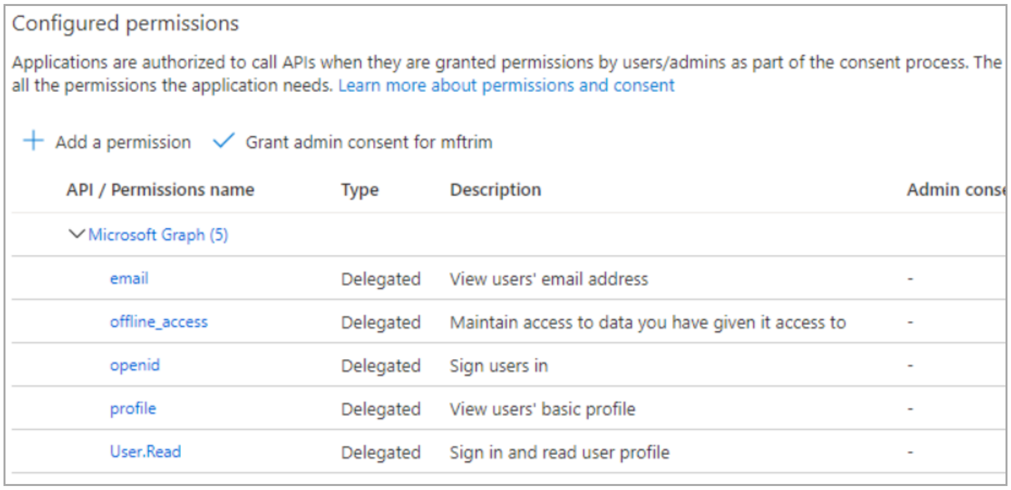
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value
My Secret	4/8/2021	3bAX62-w]=cg4ritC:?0Qw=EFfYow29D

8. From the Authentication section, go to **Select the tokens you would like to be issued** and check the option **ID Tokens**.

9. From API Permissions, add the following delegated Microsoft Graph permissions:

   - email
   - offline_access
   - openid
   - profile
   - User.Read


Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin cons
∨ Microsoft Graph (5)			
email	Delegated	View users' email address	-
offline_access	Delegated	Maintain access to data you have given it access to	-
openid	Delegated	Sign users in	-
profile	Delegated	View users' basic profile	-
User.Read	Delegated	Sign in and read user profile	-

10. Select **Grant Admin Access** permission to grant access to all permissions.

Updating the hprmServiceAPI.config or hptrim.config

To use the Auze AD application, edit the hprmServiceAPI.config in the Web Client or the hptrim.config in Service API and add the **<authentication>** element.

To do this, perform the following:

1. Navigate to the Content Manager Web Client or Service API install folder. For example, C:\Program Files\Micro Focus\Content Manager\Web Client or C:\Program Files\Micro Focus\Content Manager\Service_API.

2. Open the hprmServiceAPI.config pr hptrim.config in a text editor.

3. Add the **<authentication>** element. For example,

```
<authentication allowAnonymous="false" slidingSessionMinutes="60">
  <openIdConnect>
    <add
      name="openid"
      clientID="application ID from the Azure AD application"
      clientSecret="Client secret noted when creating Azure AD application"
      issuerURI="https://login.microsoftonline.com/08363ee4-6592-4325-9d5a-
123456789/v2.0/.well-known/openid-configuration"
    />
  </openIdConnect>
</authentication>
```

   You can get the issuerURI by navigating to **Overview > Endpoints > OpenID Connect metadata** document.

   > **IMPORTANT:** Replace the clientID, clientSecret, and issuerURI values in the highlighted example with your own value.

Enabling redirect

The Web Client will not redirect the authentication endpoint unless the Html feature is enabled in hprmServiceAPI.config file.

To enable redirect, perform the following:

1. Navigate to the Content Manager Web Client install folder and open the hprmServiceAPI.config in a text editor.

2. Search for the serviceFeatures property.

3. Add the feature Html.

   For example,

```
<hptrim xmlns="http://HP.HPTRIM.CMIS/hptrimConfig.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" poolSize="1000"
trace="true" indexPagePath="/Home"
notFoundErrorHandler="/APIErrorPages/NotFound"
globalErrorHandler="/APIErrorPages/GlobalErrors" uploadBasePath="C:\Micro Focus
Content Manager\ServiceAPIWorkpath\Uploads" autoPoolClean="true"
serviceFeatures="Json,Razor,Xml,Html,PredefinedRoutes"
xsi:noNamespaceSchemaLocation="hptrimConfig.xsd">
```

Configuring logout link

For WebDrawer the logout link is configured in the uiSettings element. It should contain '~/auth/logout'.

In the Web Client a logout link will be displayed automatically when OpenID connect authentication is enabled.

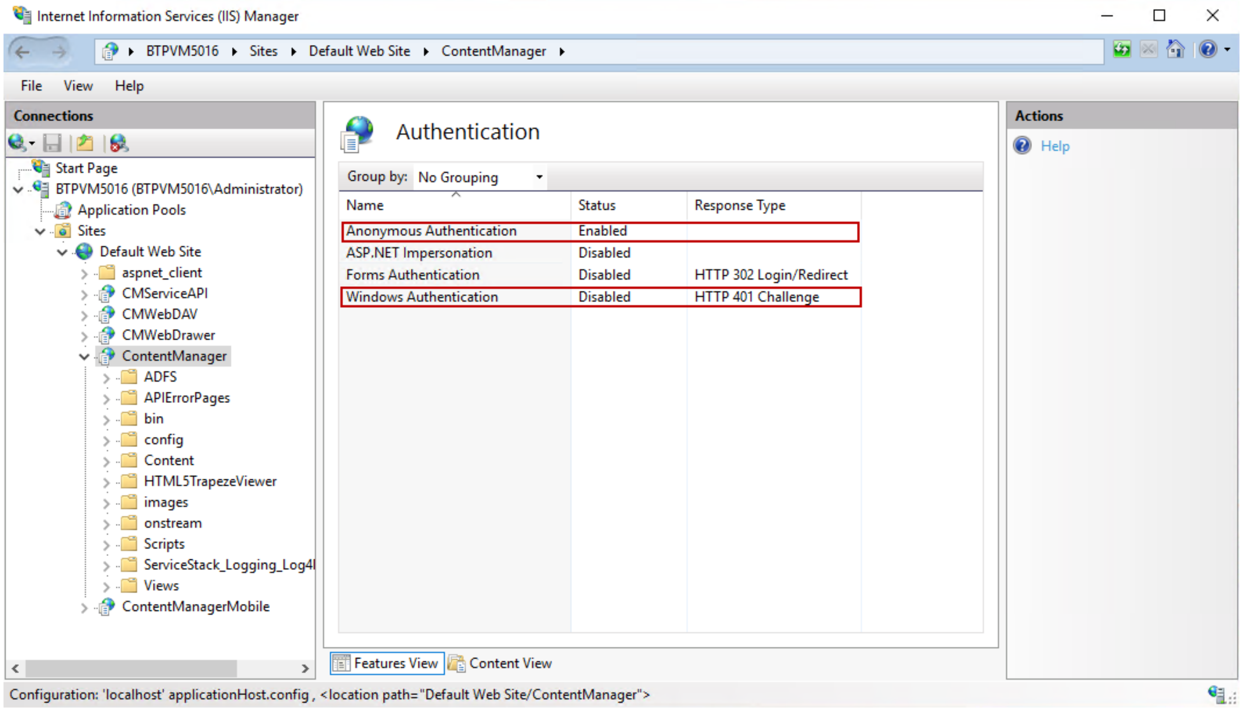
To configure logout link, perform the following:

1. Navigate to the Content Manager Web Drawer install folder. For example, C:\Program Files\Micro Focus\Content Manager\WebDrawer.
2. Open the hptrim.config in a text editor.
3. Add the logoutLink property to the uiSettings element. For example,

```
<uiSettings
  logoutLink="~/auth/logout"
  ...
/>
```

Disabling IIS administration

Given that IIS windows integrated authentication will no longer be used disable it in IIS Manager and enable Anonymous, as seen here:



Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Disabled	HTTP 401 Challenge

Configuration: 'localhost' applicationHost.config , <location path="Default Web Site/ContentManager">

Configuring Web Client Azure OpenID for OneDrive integration

Content Manager Web Client supports checking out and checking in documents from OneDrive if you are logged in via AzureAD.

To configure the Web Client to authenticate via AzureAD, the **clientId**, **clientSecret**, and **issuerURI** parameters are required. These are the parameters noted during Creating an ADFS application, on page 54. The parameters can also be obtained from the Azure App registration portal.

Updating the configuration files

hprmServiceAPI.config

The Content Manager Web Client hprmServiceAPI.config must be updated to link it to Azure AD for authentication; The **clientId**, **clientSecret**, and **issuerURI** parameters along with the Office integration element must be added in the hprmServiceAPI.config file.

Open the hprmServiceAPI.config file in a text editor and add the **<authentication>** element. For example,

```
<authentication  allowAnonymous="false" slidingSessionMinutes="30">
  <openIdConnect>
    <add name="openid"
      clientID="09f0ec5c-87e9-4568-8b60-4eb3e20de75e"
      clientSecret="ejmg+qZ9-Dk_N-uq1NNXFSGzP5fet2m3"
      issuerURI="https://login.microsoftonline.com/08363ee4-6592-4325-9d5a-
5a25e00d482b/v2.0/.well-known/openid-configuration"/>
  </openIdConnect>
</authentication>
<officeIntegration version="1.6.109.0"  guid="5d7bd8ba-11b0-46b1-98ab-95fadd95a97d"/>
```

web.config

If you have proxy settings, you need to bypass the settings in the web.config file.

Add the **</system.webServer>** element. For example,

```
<system.net>
<defaultProxy>
<proxy
usesystemdefault="True"
proxyaddress="http://yourproxy.net:1234"
/>
</defaultProxy>
</system.net>
```

> **IMPORTANT:** Replace the "http://yourproxy.net:1234" value in the highlighted example with your own value.

Once these parameters are configured, you will be redirected to Microsoft login page to login to the Web Client.

Configuring Google authentication

Creating Google credentials

To create Google credentials, perform the following:

1. Open the following URL https://console.developers.google.com/.
2. Click **Credentials** in the left pane and select the **OAuth 2.0 Client IDs**.

3. Set **Web Applications** as Application type.
4. Enter your domain in the **Authorized JavaScript origins**.
5. Enter the redirect URI in the **Authorized redirect URIs**.

   > **NOTE:** The value in Authorized redirect URIs must be in lowercase and the URL to your application (e.g. https://mydomain.com/cmwebdrawer) followed by the path to the authentication provider (for example /auth/openid). The /auth/ component is fixed but the 'openid' is the name you will supply in hprmServiceAPI.config later and so can be any string, as long as it matches the value in hprmServiceAPI.config.
   > For the Web Client the path must include the path to the ServiceAPI, for example, https://mydomain.com/contentManager/serviceapi/auth/openid.

6. Click **Create**.

   The Client ID and Client Secret will be displayed. Make a note of the Client ID and Client Secret to be used later.

Updating hprmServiceAPI.config

To use Google credentials, edit the hprmServiceAPI.config and add the **<authentication>** element.

To do this, perform the following:

1. Navigate to the Content Manager Web Client install folder. For example, C:\Program Files\Micro Focus\Content Manager\Web Client.
2. Open the hprmServiceAPI.config file in a text editor.
3. Add the **<authentication>** element. For example,

```
<authentication allowAnonymous="false" slidingSessionMinutes="2">
  <openIdConnect>
    <add
      name="openid"
      clientID="Client ID noted when creating Google credentials"
      clientSecret="Client secret noted when creating Google credentials"
      issuerURI="https://accounts.google.com"
    />
  </openIdConnect>
</authentication>
```

> **IMPORTANT:** Replace the clientID and clientSecret values in the highlighted example with your own value.

Enabling redirect

The Web Client will not redirect the authentication endpoint unless the Html feature is enabled in hprmServiceAPI.config file.

To enable redirect, perform the following:

1. Navigate to the Content Manager Web Client install folder and open the hprmServiceAPI.config in a text editor.
2. Search for the serviceFeatures property.
3. Add the feature Html.

   For example,

   ```
   <hptrim xmlns="http://HP.HPTRIM.CMIS/hptrimConfig.xsd"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" poolSize="1000"
   trace="true" indexPagePath="/Home"
   notFoundErrorHandler="/APIErrorPages/NotFound"
   globalErrorHandler="/APIErrorPages/GlobalErrors" uploadBasePath="C:\Micro Focus
   Content Manager\ServiceAPIWorkpath\Uploads" autoPoolClean="true"
   serviceFeatures="Json,Razor,Xml,Html,PredefinedRoutes"
   xsi:noNamespaceSchemaLocation="hptrimConfig.xsd">
   ```

Configuring logout link

For WebDrawer the logout link is configured in the uiSettings element. It should contain '~/auth/logout'.

In the Web Client a logout link will be displayed automatically when OpenID connect authentication is enabled.

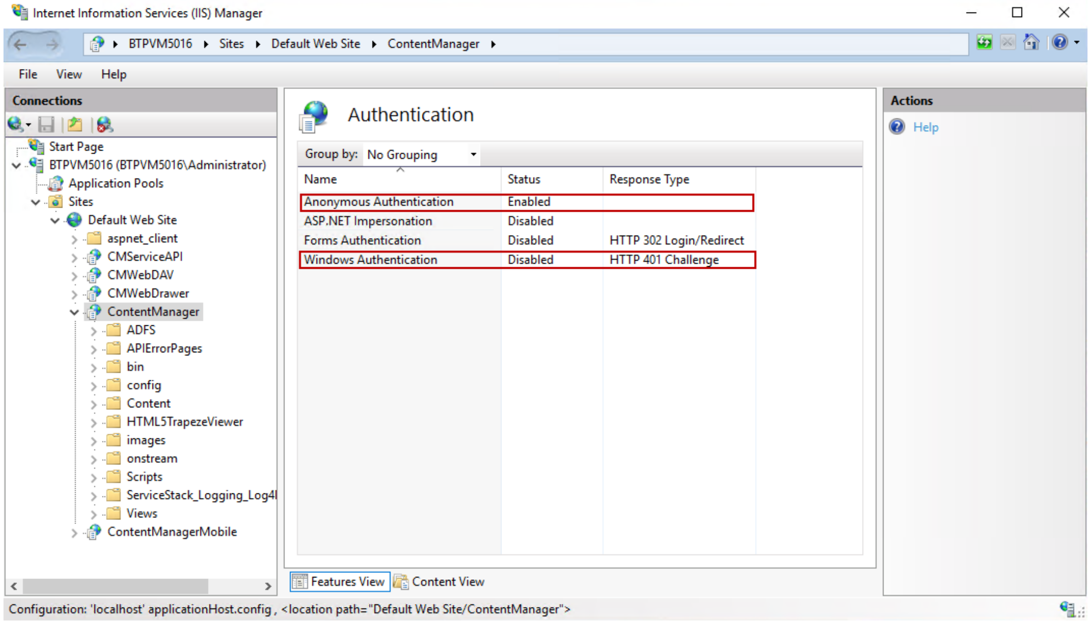
To configure logout link, perform the following:

1. Navigate to the Content Manager Web Drawer install folder. For example, C:\Program Files\Micro Focus\Content Manager\WebDrawer.
2. Open the hptrim.config in a text editor.
3. Add the logoutLink property to the uiSettings element. For example,

   ```
   <uiSettings
     logoutLink="~/auth/logout"
     ...
   />
   ```

Disabling IIS administration

Given that IIS windows integrated authentication will no longer be used disable it in IIS Manager and enable Anonymous, as seen here:



Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Disabled	HTTP 401 Challenge

Configuration: 'localhost' applicationHost.config , <location path="Default Web Site/ContentManager">

Key Protector Tool

The Content Manager Key Protector Tool allows you to encrypt the Client ID and Client Secret for OpenID connect authentication. The tool takes the Client ID or Client Secret as input (`Key`) and provides the encrypted version of the `Key` which can then be used in the place of Client ID or Client Secret in the configuration file (**hprmServiceAPI.config** or **hptrim.config**).

The **TRIMKPTool.exe** tool is available in the **bin**/**Bin** folder of **Web Client**, **WebDrawer**, or **Service_API** in your installation folder. For example, **C:\Program Files\Micro Focus\Content Manager\Service_API\Bin**.

You can run the tool either as a `currentuser`, where the user running the tool must be same as the user running the Web Server (Content Manager Administrator) or as a `localmachine`, where the tool is invoked on the same machine as that of the Web Server.

To encrypt the Client ID or Client Secret, perform the following steps:

1. Navigate to the location where the **TRIMKPTool.exe** tool is available and open the command prompt.

2. Enter **TRIMKPTool.exe** in the prompt and press **Enter**. The tool displays the command line options.

   The following are the available options:

   - `--scope` or `-s`: Scope of the data protection to be applied - `currentuser` or `localmachine`.
   - `--key` or `-k`: Key to encrypt.
   - `--help` or `-h`: Help on Key Protector Tool.

3. Enter the following command in the command prompt:

   ```
   TRIMKPTool.exe -s <currentuser or localmachine> -k <Client ID or Client Secret>
   ```

For example,

```
TRIMKPTool.exe -s currentuser -k L8_-JuMKjsueCCb47ILl09oK23nsHA
```

The encrypted Client ID or Client Secret is displayed.

To get more details on the available options of the tool, enter `TRIMKPTool.exe --help or -h` in the command prompt.

4. Copy and paste the encrypted key in the configuration file.

> **TIP:** For the smooth access and authentication of the Content Manager Web services, make sure to copy and paste the encrypted key properly in the configuration file.

Appendix D
Office Online Integration

Introduction

The Office Online integration is built into the Content Manager Web Client using Web Application Open Platform Interface (WOPI).

From the Web Client interface, it allows online editing of supported Microsoft Office documents to users with an Office Online subscription that includes editing ability.

Overview

Supported Versions of Office Online

The supported version of Office Online Server is 16.0.7766.8550 and later.

If you are installing your own Office Online instance on a local network, then configure to it use either HTTP or HTTPS, but not both.

Supported File Types

Office Online Server delivers browser-based versions of Word, PowerPoint, Excel, and OneNote. Editing is supported for the newer XML style documents (i.e. .docx, .pptx, .xlsx). Older formats such as .doc can be converted to the newer native formats so that they may be edited. This conversion process is usually lossless, but is not guaranteed to be so, and may produce a newer version that is missing certain content or formatting.

The Office Online server broadcasts its capabilities about which actions may be performed on which formats as an XML feed via a HTTP request. The process of determining a server's capabilities via the XML feed is known as 'Discovery'. These capabilities are subject to change - and are highly likely to change - with successive revisions. The Content Manager integration will regularly try to rediscover the capabilities of the Office Online instance, determine which can be used and make them available to Content Manager users when the Office Online instance is upgraded.

Users will not be able to edit the older file types using the zero-footprint integration because Office Online requires the older file type documents to be converted to the newer file format, and hence Content Manager will treat the newly-created newer-format file as a new record when attempting to return it to Content Manager.

Security

Users are issued tokens by the integration that grant them access to view/edit a document from Content Manager. When the Office server communicates with Content Manager on behalf of the user, it presents this token which is decrypted and verified. This token provides all the information we need to manipulate records in Content Manager. The encryption key is configured in one of the web server’s configuration files. It is recommended that this is changed frequently to minimize the chance of security being compromised.

Configuring Office Online integration

Content Manager Web Server Configuration

> **NOTE:** If configuring multiple instances of the Content Manager Web Server in order to use with a load balancer, then each instance within the load balanced cluster must be configured with the same values following the steps below.

- Once you have installed the Content Manager Web Client, from the Web Client installation directory, open the **HPRMServiceAPI.config** file using a text editor and find the section that includes:

  ```
  <pluginAssemblies>

  <!-- <add name="HP.HPTRIM.WebClient.WOPI"/> -->

  <!-- <add name="HP.HPTRIM.WebClient.WebDAV"/> -->

  </pluginAssemblies>
  ```

To enable the WOPI service handler and required buttons within the Web Client, uncomment the **<add name="HP.HPTRIM.WebClient.WOPI"/>** line in **HPRMServiceAPI.config**, and save the changes.

- In **HPRMServiceAPI.config**, find the section with the below attributes:

```
<officeOnlineServer host="" useSSL="true" allowSelfSignedSSL="false" tokenEncKey=""
tokenEncIV=""/>
```

Change the values of the attributes above to reflect your environment, so that 'host' is the **host name** of the Office Online Server, e.g. "myofficeonline.mynetwork.com".

Change the value of 'useSSL' to "false" if you have configured your Office Online Server instance to Allow HTTP and do not wish to use SSL.

Change the value of 'allowSelfSignedSSL' to "true" if you have configured your Office Online Server to use SSL with a Self Signed Certificate - Self Signed Certificates will otherwise be rejected.

Change the value of 'tokenEncKey' to be a 32 byte/64 character hexadecimal string which will be used as an encryption key to encrypt security tokens. As an example, you could use 'b12df00db12df00db12df00db12df00db12df00db12df00db12df00db12df00d'.

Change the value of 'tokenEncIV' to be a 16 byte/32 character hexadecimal string which will be used as an initialization vector for security token encryption. As an example, you could use 'b12df00db12df00db12df00db12df00d'.

Save the changes.

- Open the **web.config** file in the Content Manager Web Client directory using a text editor and find the below section:

  ```
  <modules runAllManagedModulesForAllRequests="true">

  <!-- <add name="WOPIModule" type="HP.HPTRIM.WebClient.WOPI.WOPIModule" /> -->
  ```

```
    </modules>
```

To authenticate the requests from the Office Online server on behalf of the Content Manager user, uncomment **<add name="WOPIModule" type="HP.HPTRIM.WebClient.WOPI.WOPIModule" />** in **web.config**, and save the changes.

User Client Configuration

- The client PC web browsers must be configured to allow pop up windows from the Content Manager Web Client. If pop up windows are not enabled users will be prompted to allow them each time they edit a document, or depending on the settings, they will not be prompted at all, and will not be able to edit their documents using the Office Online editing functionality.

  Update pop-up blocker settings of Chrome, Firefox, or Edge to allow pop windows from the Content Manager Web Client, add the Content Manager Web Client address to the list of trusted sites in the Pop-up Blocker Settings Exceptions list.
- If the Office Online Server is using SSL, the certificate must be trusted by client PCs.

Appendix E
Multi Tenancy Configuration

Scope

This document outlines the steps required to configure Content Manager (CM) 9.2 or later Web Client to support multiple Content Manager datasets.

This document is aimed at system administrators who wish to allow access to multiple Content Managerdatasets from a single server running the Content Manager Web Client.

For the purpose of this document, a tenant consists of an application running in Internet Information Services (IIS) connecting to an existing Content Manager dataset provided by a Workgroup server. Each Content Manager Web Client application on IIS can access exactly one dataset.

> **NOTE:** A Content Manager dataset may be accessed by multiple IIS applications if required.

This document is presented as a guide showing how to set up and configure a new instance of a Content Manager Web Client IIS application connecting to a specific dataset. This process may be repeated to create any number of applications.

This document assumes that the Content Manager Web Client has been installed successfully and is working.

Advanced configuration of IIS applications is out of the scope of this document; for more information please consult the IIS documentation https://www.iis.net/

Configuration Steps

This section will outline the steps to create a new tenant.

Before beginning, ensure that the following information has been gathered:

- Name for the tenant (tenant name)
- Dataset Id of the CM dataset that the tenant will be accessing
- Connection information for the CM workgroup server that the tenant will be connecting to
- The name of the user account on the server that is trusted to connect to the selected CM workgroup server and dataset
- The IIS web site which will host the tenant
- The folder on the web server that will be used as the ‘upload path’ for the tenant. The upload path is the folder used to store files that are being uploaded to the server to be checked into CM.

Create Tenants folder

Underneath the installation folder of the CM web client, which is installed to by default,

C:\Program Files\Micro Focus\Content Manager\Web Client

Create a folder named **Tenants**:

C:\Program Files\Micro Focus\Content Manager\Web Client\Tenants

Create configuration file using sample

Copy the sample configuration file, **Tenant-sample.config** from the Web Client installation directory and paste it into the newly created **Tenants** folder.

Located in the installation folder into the tenants folder underneath the installation folder.

Rename the **Tenant-sample.config** file in the **Tenants** folder to be the name of the Tenant, e.g. ABCorp.config

Update the configuration file

The following sections **must** be updated as per installation of a standard CM Web Client:

- hptrim
- Setup
- Workgroupserver

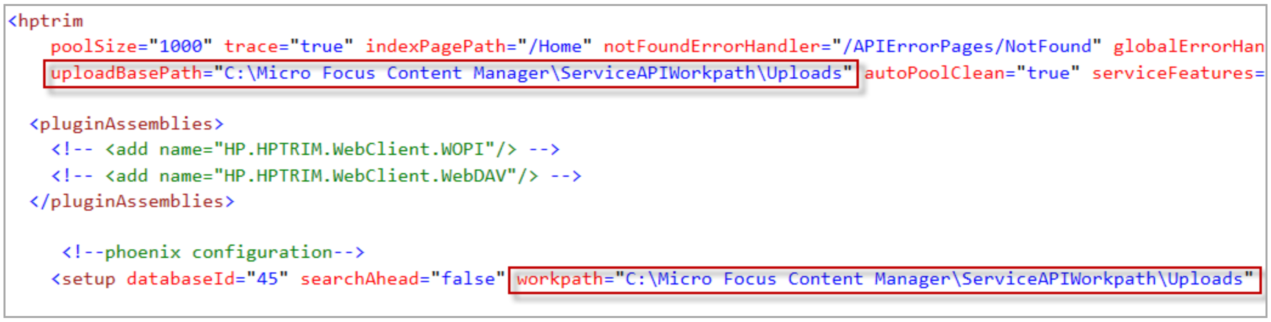
In the **hptrim** section of the config file, example **ABCorp.config**, the upload base path must be set to the folder that will be used as the upload path for the tenant.

In the **setup** section of the config file, example **ABCorp.config**, ensure that the databaseId is set correctly, and the workpath has been set to a unique folder for this tenant.

In the **workgroupserver** section of the config file, example **ABCorp.config**, ensure that the connection details, including port, workpath and name have all been set correctly.

For the above mentioned sections, you can refer **hprmServiceAPI.config** file, as an example.

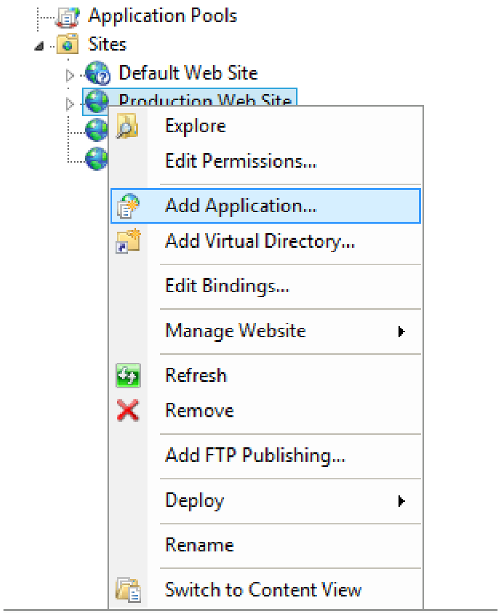
> **NOTE:** The workpath attribute in the WorkgroupServer section and the uploadBasePath in the hptrim section must be the same.



```
<hptrim
    poolSize="1000" trace="true" indexPagePath="/Home" notFoundErrorHandler="/APIErrorPages/NotFound" globalErrorHan
    uploadBasePath="C:\Micro Focus Content Manager\ServiceAPIWorkpath\Uploads" autoPoolClean="true" serviceFeatures=

  <pluginAssemblies>
    <!-- <add name="HP.HPTRIM.WebClient.WOPI"/> -->
    <!-- <add name="HP.HPTRIM.WebClient.WebDAV"/> -->
  </pluginAssemblies>

     <!--phoenix configuration-->
    <setup databaseId="45" searchAhead="false" workpath="C:\Micro Focus Content Manager\ServiceAPIWorkpath\Uploads"
```

Create a web application

Using IIS Manager, under the selected web site for this **tenant**, add an application. The default web site is acceptable to use. Consult the IIS documentation for more information about creating and managing multiple web sites within IIS.

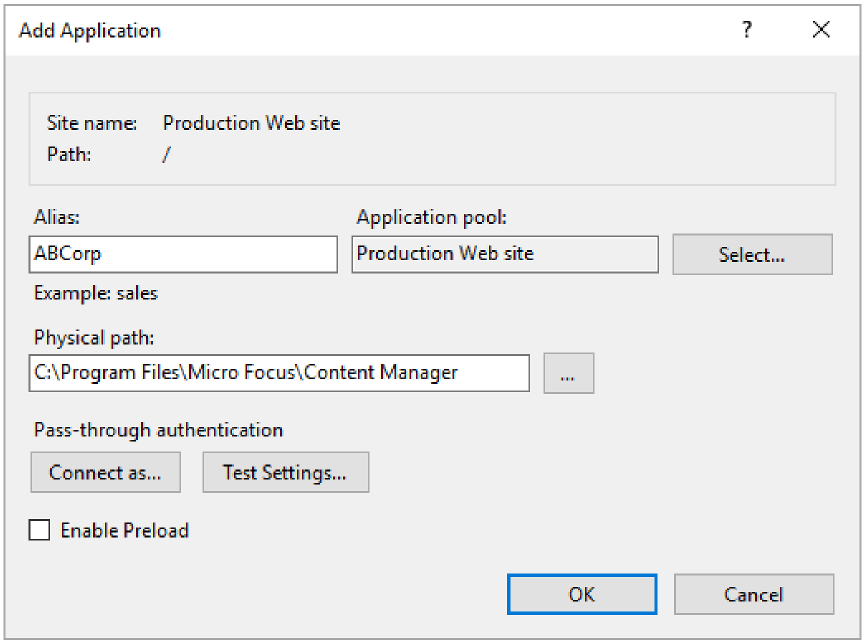


In the Add application dialog, set the alias, physical path and application pool for the tenant.

- Set the Alias of the application to be the Tenant name.
- The physical path of the application should be set to the location that binaries of the CM Web Client were installed, by default:

  C:\Program Files\Micro Focus\Content Manager\Web Client

- Select an Application pool that has an identity that is trusted to connect to the dataset that this instance will be accessing. For information on setting up Application pools in IIS please consult the IIS documentation.


Add Application

Site name: Production Web site
Path: /

Alias: ABCorp

Application pool: Production Web site

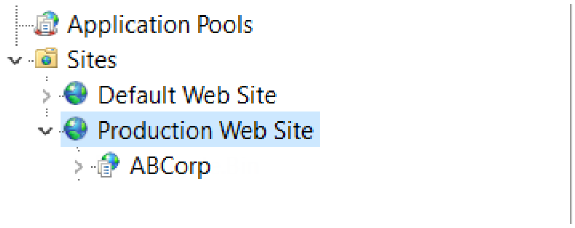
Example: sales

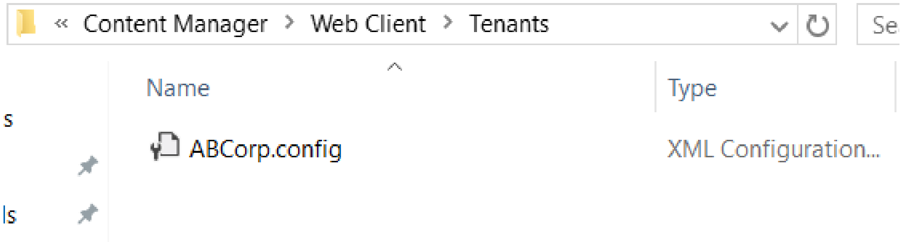
Physical path: C:\Program Files\Micro Focus\Content Manager

Pass-through authentication

□ Enable Preload

> **NOTE:** The application name **must be the same** as the configuration file name in the Tenants folder (excluding the .config) Example – tenant named ‘ABCorp’:





Name	Type
ABCorp.config	XML Configuration...

Update logging

By default only one process can write to the log file. When setting up multiple tenants it is recommended that this is changed by changing the ‘LockinModel’ on Log4Net (minimalLock). Add the highlighted line to the **web.config** file in the directory containing the CM Web Client binaries.

```
<log4net>
    <appender name="RollingFileAppender"
type="log4net.Appender.RollingFileAppender">
      <lockingModel type="log4net.Appender.FileAppender+MinimalLock "/>
      <file value="C:\HPTRIM\ServiceAPIWorkpath\logs\log-file.txt" />
      <appendToFile value="true" />
      <rollingStyle value="Date" />
      <maximumFileSize value="1MB" />
      <staticLogFileName value="true" />
      <maxSizeRollBackups value="10" />
      <layout type="log4net.Layout.PatternLayout,log4net">
        <param name="ConversionPattern" value="%date [%thread] %-5level %logger -
%message%newline" />
      </layout>
    </appender>
    <root>
      <level value="ERROR" />
      <appender-ref ref="RollingFileAppender" />
    </root>
  </log4net>
```

Azure authentication settings

> **NOTE:** This section is applicable only if the Web Client is enabled for Azure authentication in multi tenancy mode.

To access multiple Web Client tenants at the same time using AzureAD authentication, perform the following steps:

1. Open **IIS Manager** and navigate to **Default Web Site**.
2. In the **Actions** panel **> Edit Site**, click **Bindings**.
3. Click **Add**. The **Add Site Binding** window is displayed.
4. Select **Type** as **http**, **IP Address** as **All Unassigned**, and **Port** as **80**.
5. Enter **Host name**, for example, **Bestone.com**.
6. Click **OK**.
7. Repeat steps 3 to 5 and this time, enter **Host name** as, say, **Besttwo.com**.

   Now you can access the first Web Client as **http://Bestone.com/ContentManager** and the Tenant Web Client, as **http://Besttwo.com/CMTenant**.

Appendix F
Configuring Thin Office Integration

Updating web.config file

To be able to open and edit the documents using the thin office integration, you need to update the web.config file.

To update the web.config file

1. Open the Web Client web.config file using a text editor, by default this is installed to C:\Program Files\Micro Focus\Content Manager\Web Client.
2. In the **<system.web>**section, locate the **<authorization>** section and replace the **<deny users="?" />** parameter with **<allow users="*" />** parameter.

   For example,

   ```
   <location path="serviceapi">
   <system.web>
   <httpHandlers>
   <add path="*"
   type="ServiceStack.WebHost.Endpoints.ServiceStackHttpHandlerFactory,
   ServiceStack" verb="*" />
   </httpHandlers>
   <authorization>
   <allow users="*" />
   ```

```
</authorization>
</system.web>
```

3. Save and close the web.config file.