Content Manager

Software Version 25.1

OpenID Connect authentication

opentext™

Document Release Date: October 2024
Software Release Date: January 2025

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.

Support

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

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

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

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

Contents

Introduction 4

ADFS for Native client 5
- Configure ADFS 5
- Configure OpenID settings in Content Manager 12

ADFS for Web Client and Service API 14
- Create the ADFS application 14
- Add the settings to the Web Client 16
- Configure ADFS for the Office integration access 16
- Add Office integration to the settings of the Web Client 18

Azure AD for WebClient, Mobile App and Service API 19
- Create the Azure AD application 19
- Configure for mobile 21
  - Add the mobile redirect URI 21
  - Add the mobile redirect URI to the Service API 21
- Configure authentication in hptrim.config 21
- Enable redirect 22
- Allow users (Web Client only) 22
- Logout 23
- Allow anonymous access in IIS 23

Azure AD for Content Manager desktop 24
- Create the Azure AD application 24
- Configure authentication in Content Manager Enterprise Studio 25
- Configure Azure AD for Office integration access 26

Google authentication 28
- Create the Google credentials 28
- Configure authentication in hptrim.config 28
- Enable redirect 29
- Logout 29
- Allow anonymous access in the IIS 29

Introduction

This document provides high level information for you to configure OpenID Connect authentication with Content Manager.

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 Service API, and in Content Manager Enterprise Studio for the desktop client.

ADFS for Native client

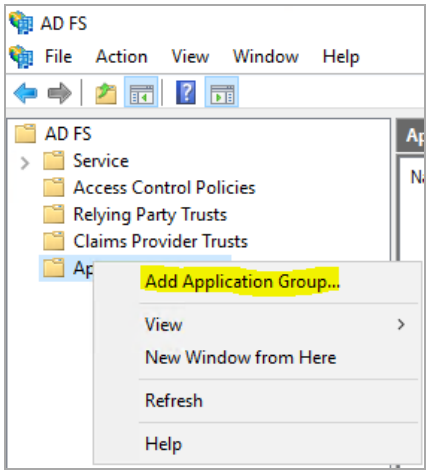
As of Content Manager 10 the Content Manager web applications (Service API, WebDrawer and Web Client) have an OpenID Connect authentication provider built in.

This section describes creating an ADFS application and configuring the Windows native Content Manager client.

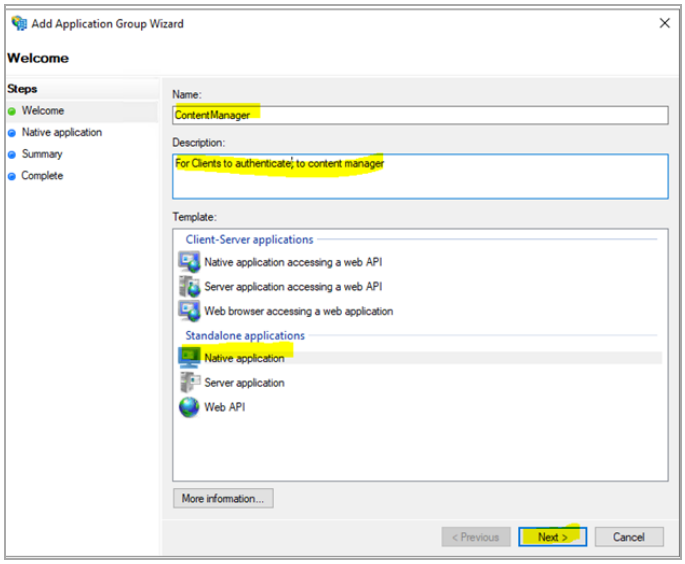
Configure ADFS

To setup ADFS to support OpenID for Content Manager native, perform the following steps:

1. Log on to your ADFS Server and create an application group.

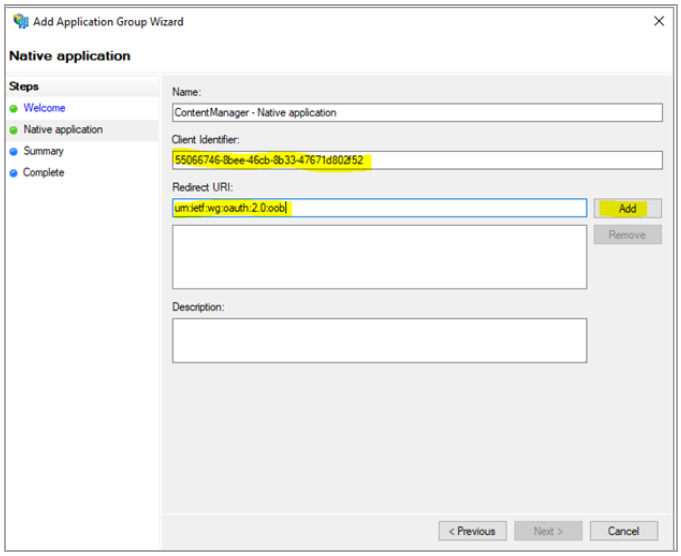


2. Enter the name and the description for the group, then select **Native application**. Click **Next**.

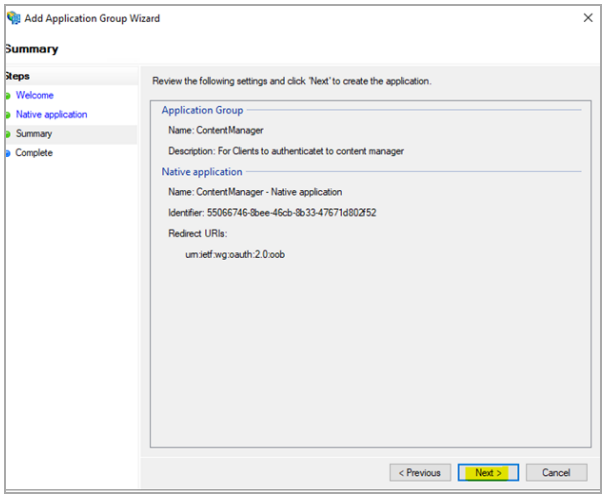


3. Configure the group.

   Note the client identifier for later use and enter the value ‘https://127.0.0.1’ in Redirect URI, click **Add** and then click **Next**.

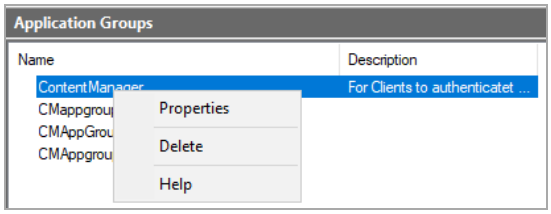


4. Review the settings and click **Next**.

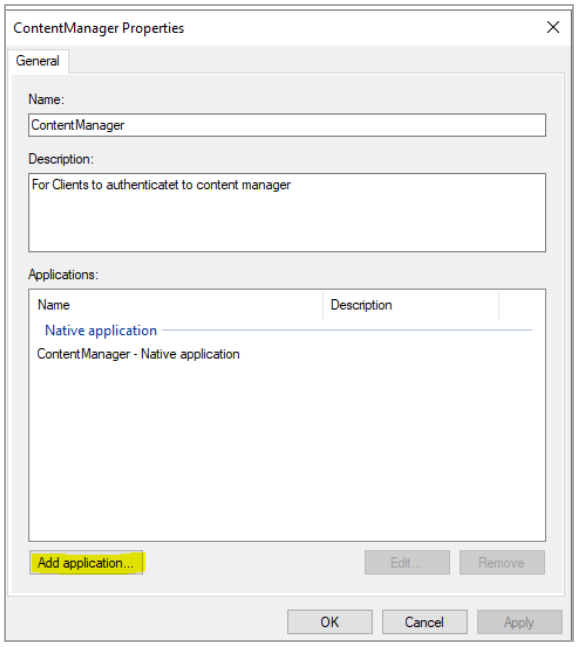


5. Modify application group properties.

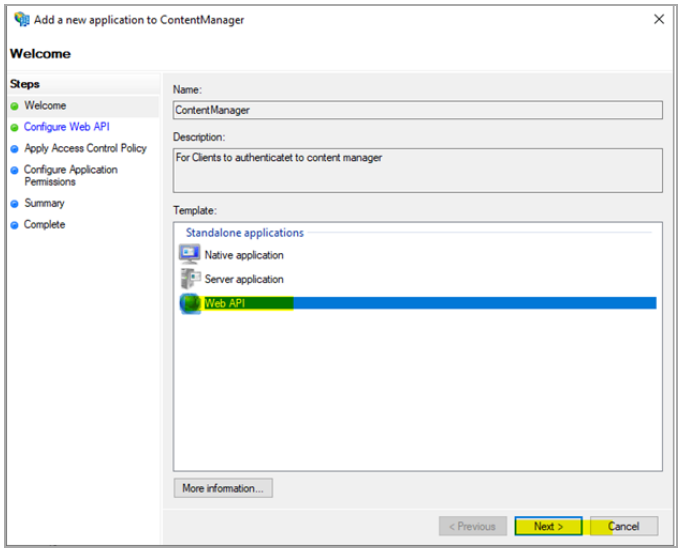
   Once this has been completed, right-click the application group and select **Properties**.



6. Click **Add application**.

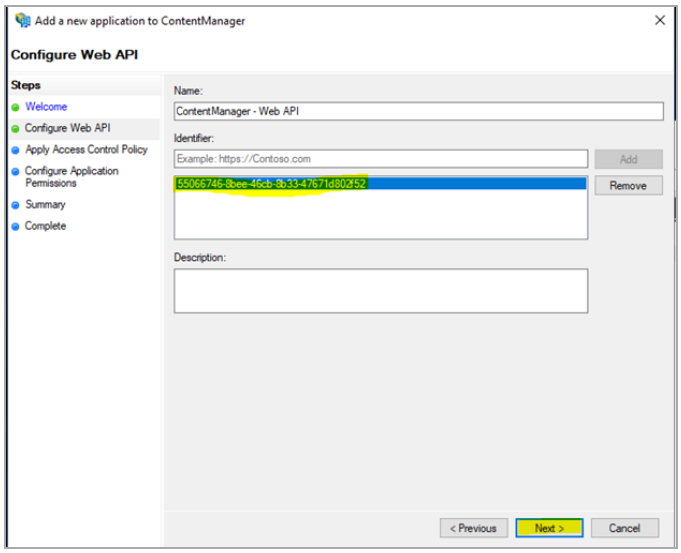


7. Select **Web API** as the **Template**.

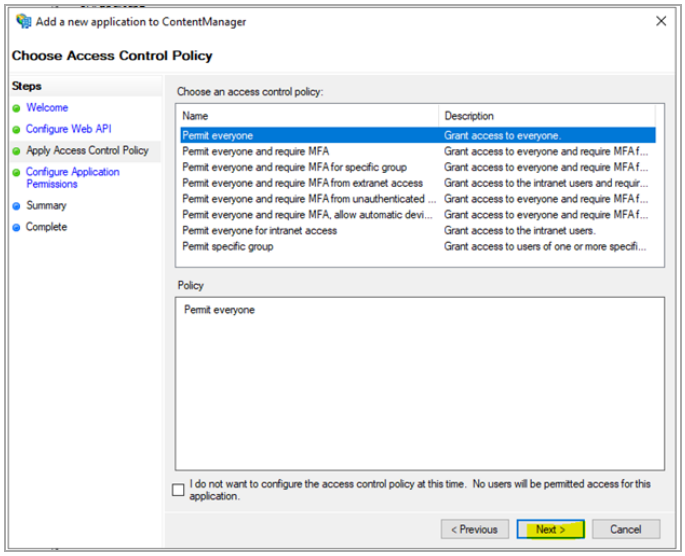


8. Configure the Web API.

   Add the Redirect to be the same as the client ID of the Native application that you previously copied. Click **Next**.

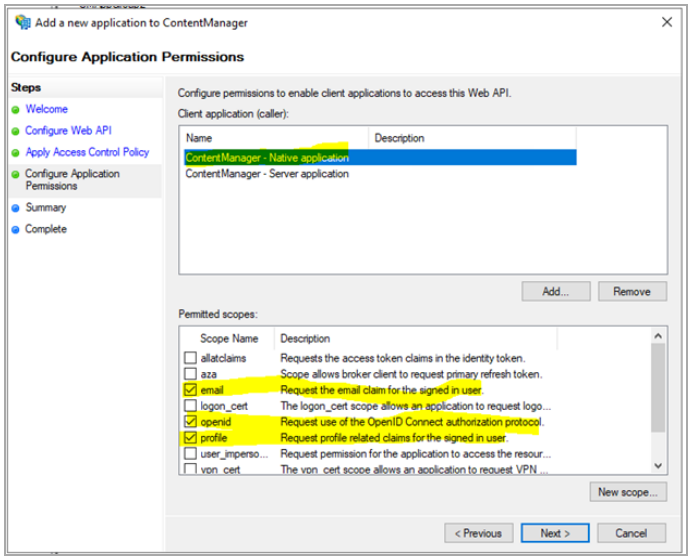


9. Select an appropriate Access Control Policy.

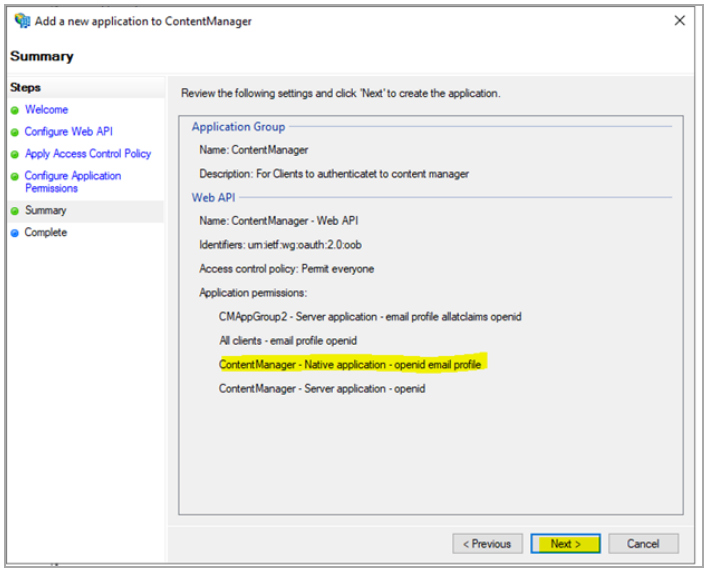


10. Set the scopes.

    Select the Native Application and ensure **email**, **openid**, and **profile** are checked.

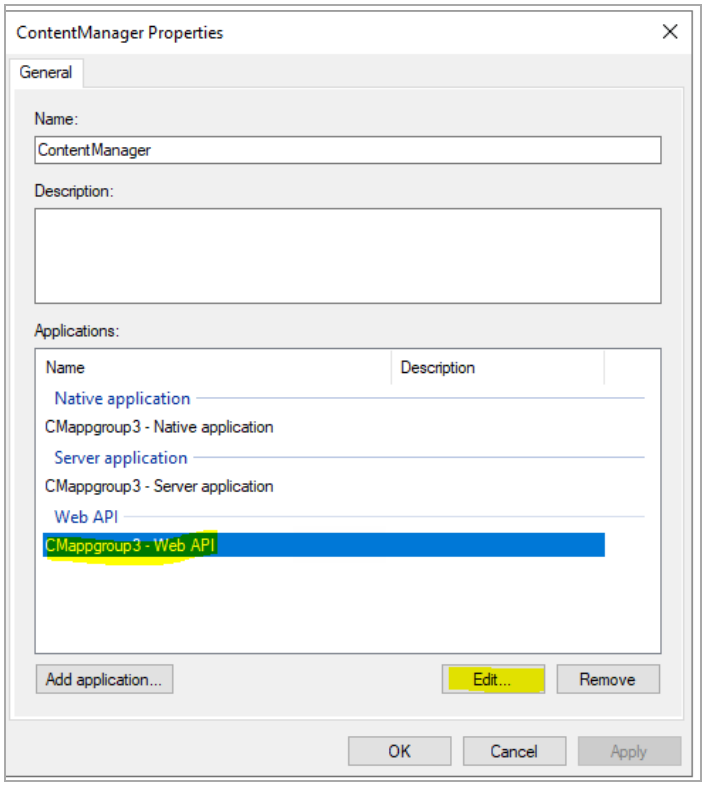


11. Review the configuration, click **Next** and then **Close**.



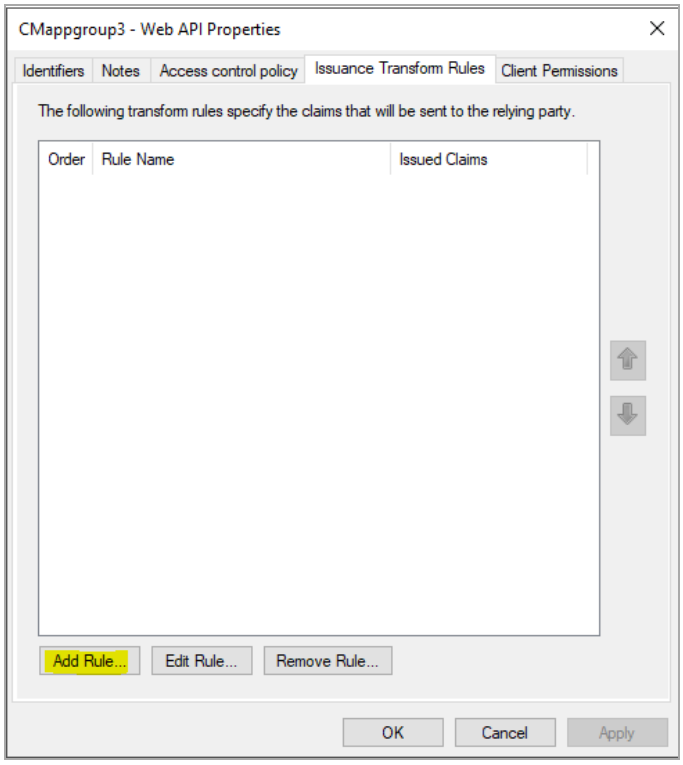
12. Set issuance rules.

    Right-click the app group and select **Properties**, highlight the WEB API application and select **Edit**.



13. Add a rule.

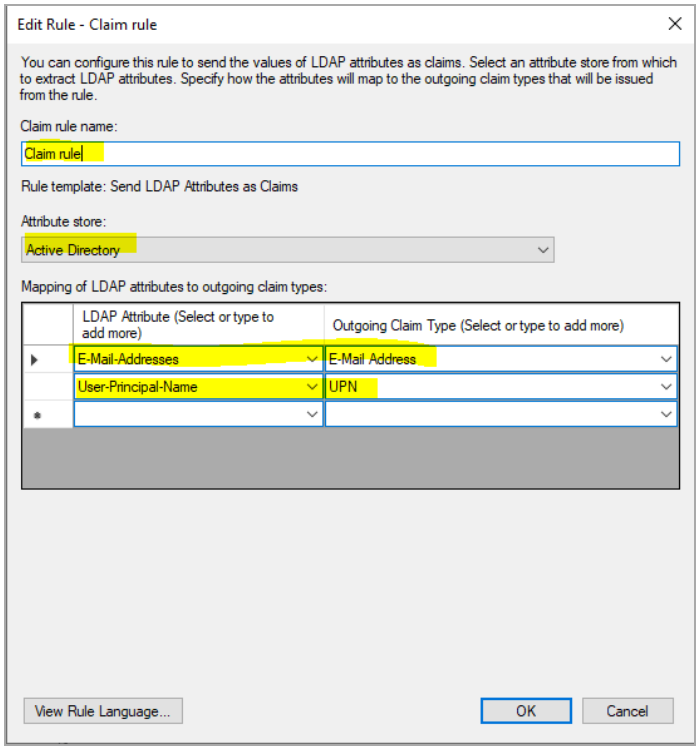
    Navigate to the **Issuance Transform Rules** Tab and click **Add Rule**.



14. Map attributes.

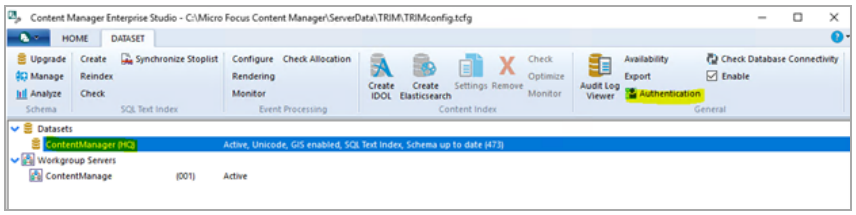
    Give the rule a name, select **Active Directory** as the **Attribute Store**, and add the following mapping of LDAP attributes and click **OK**:

    - **E-Mail-Addresses - E-mail Address**
    - **User-Principal-Name - UPN**

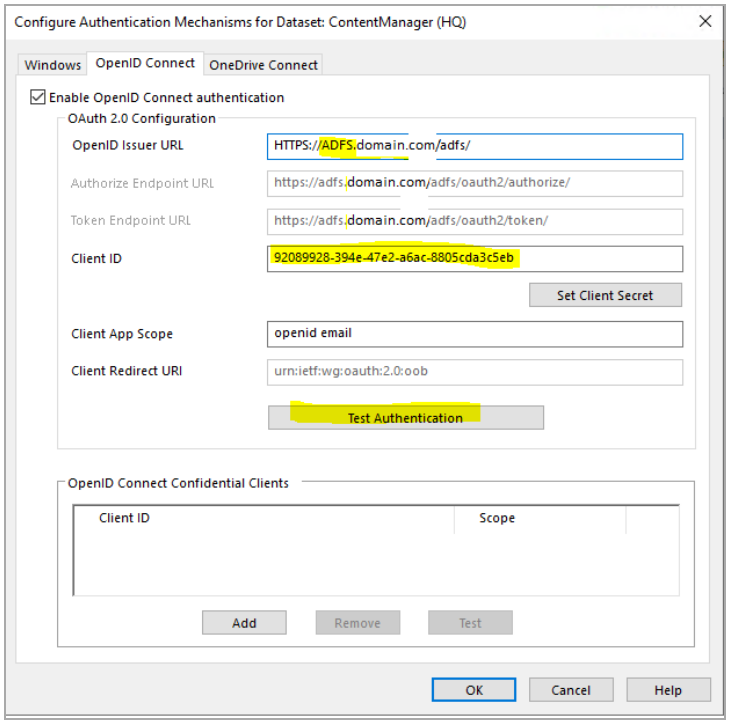


Configure OpenID settings in Content Manager

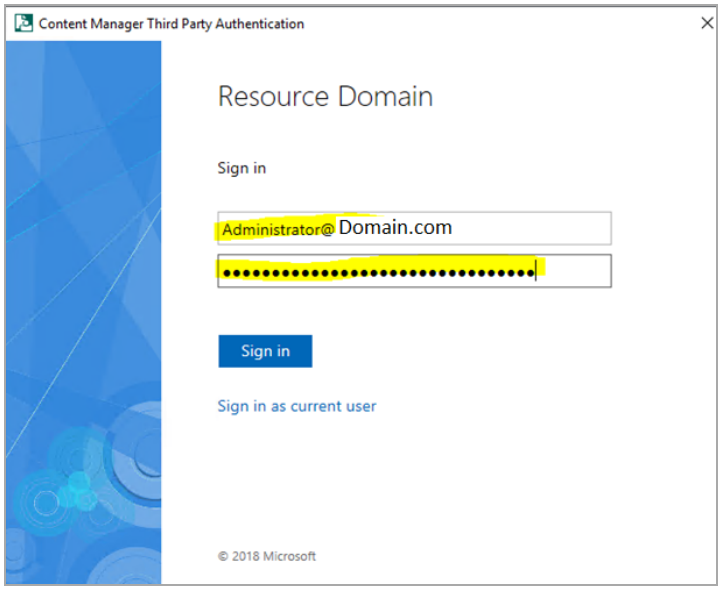
1. Navigate to the Content Manager server and run the Content Manager Enterprise Studio as an Administrator. Right-click the dataset and select **Authentication**.



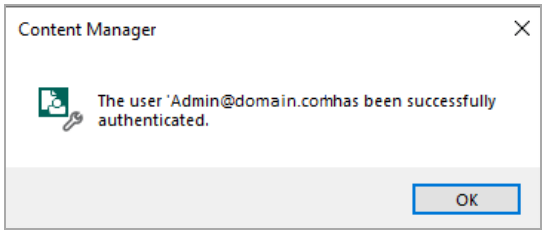
2. Enter the ADFS URL for the ADFS server, the client identifier which was noted earlier (Native Application) and click **Test Authentication**.



3. Enter the user details for a test user and click **Sign in**.



The users email in active directory should appear, if successful.



ADFS for Web Client and Service API

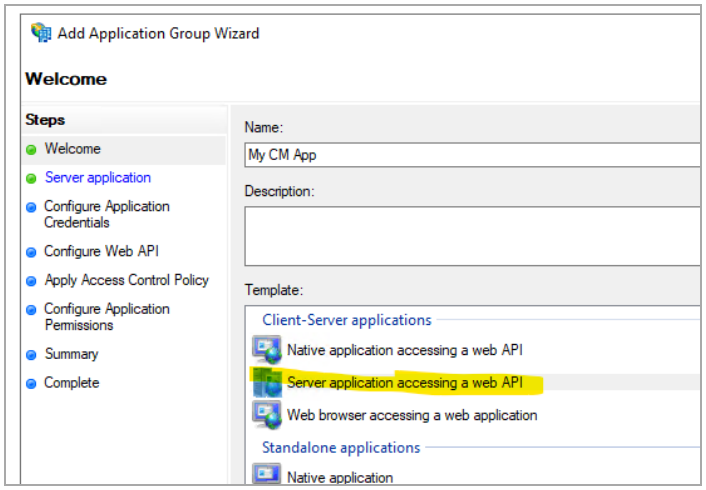
As of Content Manager 10 the web applications (Service API, WebDrawer and Web Client) have a built in OpenID Connect authentication provider.

This section describes creating an ADFS application and configuring the Content Manager web applications.

Create the ADFS application

To create the ADFS application,

1. Create a new **Application Group**.
2. Select **Server application accessing a web API** as the template.



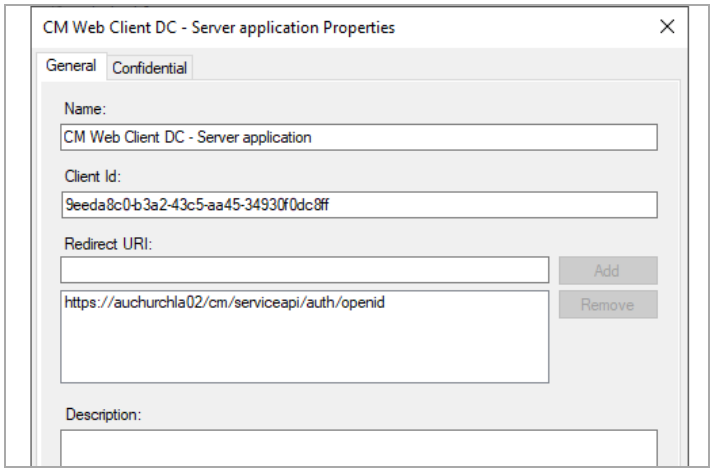
3. Enter a name and click **Next**.

   Note the client identifier.

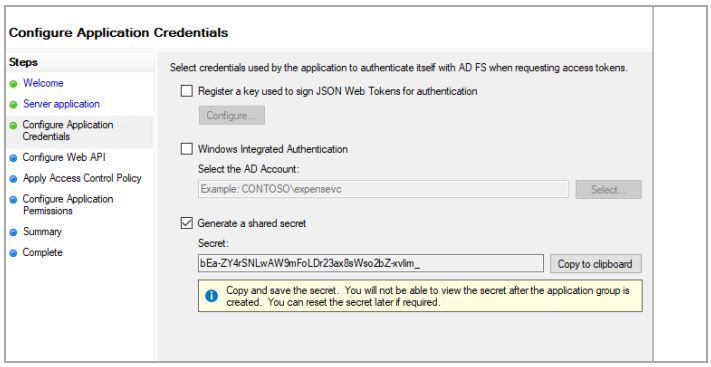
4. Add a Redirect URI.

   The redirect URI must be in lowercase and be the URL of the Content Manager web site with the suffix `/serviceapi/auth/openid`.

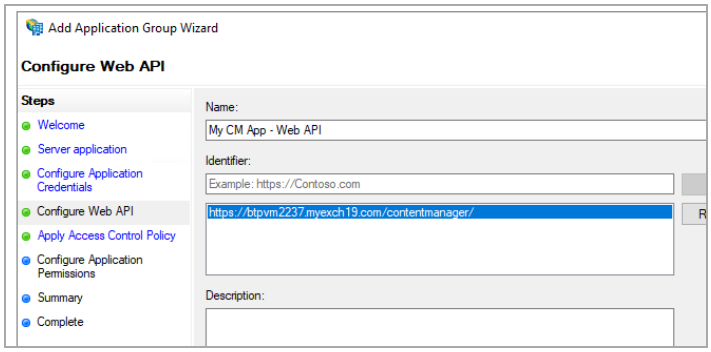
   For example, `https://myserver/contentmanager/serviceapi/auth/openid`.



5. Click **Next**.
6. Generate a shared secret and note the secret.



7. Click **Next**.
8. Add an identifier. For example, `https://MyServer/contentmanager/`.



9. Click **Next**.
10. Choose an access control policy. For example, Give access to everyone.
11. In the **Configure Application permissions**, select **email**, **openid**, and **profile**.
12. Complete rest of the steps in the Application Group.

Add the settings to the Web Client

To configure the Web Client, edit the **hprmServiceApi.config** file and add (or edit) the authentication element to look similar to the example below.

- Client ID and secret (noted in the previous section)
- issuerUri is found in the ADFS console - Endpoints, in the OpenID Connect section.
- Name must be `openid`.

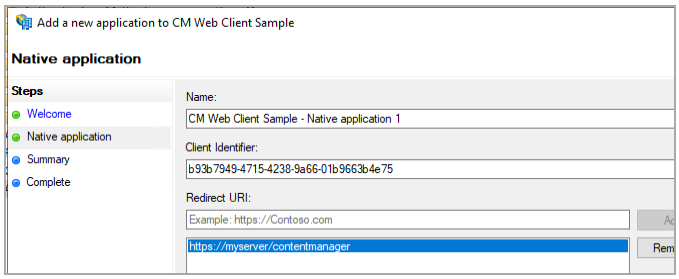
For example,

```
<authentication allowAnonymous="false"slidingSessionMinutes="30">
<openIdConnect>
<add
name="openid"
clientID="CLIENT_ID"
clientSecret="SECRET"
issuerURI="https://MyServer/adfs/.well-known/openid-configuration"/>
</openIdConnect>
</authentication>
```

Configure ADFS for the Office integration access

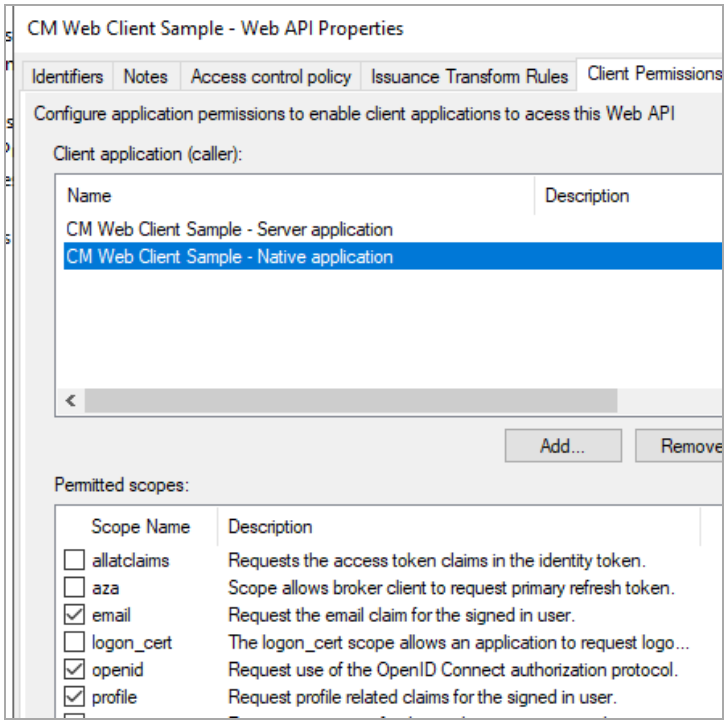
The office integration requires an access token to allow it to authenticate with the Web Client, this can be configured in ADFS.

1. Go to the **Application group** configured in the above section.
2. Click **Add Application** to add a native application.

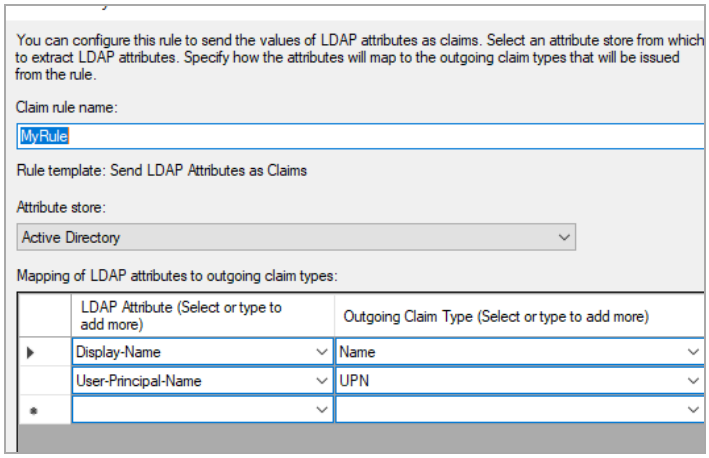


   Preserve the Client ID for later use.

3. Complete rest of the steps for the native application.
4. Edit the Web API application and in the **Client Permissions**, add the new client application selecting the **scopes**, **email**, **openid**, and **profile**.



5. In the **Issuance Transform Rules**, add a new Rule.
6. Select the **Send LDAP Attributes** and click **Next**.
7. Choose the **Active Directory** as the attribute store.
8. Map the following two claims:
   - **Display Name - Name**
   - **User-Principal-Name - UPN**



9. Click **Finish**.

Add Office integration to the settings of the Web Client

In the Content Manager Workgroup Server, navigate to the installation folder, for example **C:\Program Files\Micro Focus\Content Manager\Web Client\ADFS**, and update the **config.xml** as shown below:

- clientAuthority - ADFS authority (https://{adfsdomain}/adfs)
- clientResourceUri - openid (scope of authentication)
- clientID - Native application ClientID
- clientReturnUri – Web Client url

For example,

```
<adfsClient>
<clientAuthority>https://test.com/adfs</clientAuthority>
<clientResourceUri>openid</clientResourceUri>
<clientID>ab999999-999d-9aeb-a999-999b99999a99</clientID>
<clientReturnUri>https://test.com/contentmanager/</clientReturnUri>
</adfsClient>
```

Azure AD for WebClient, Mobile App and Service API

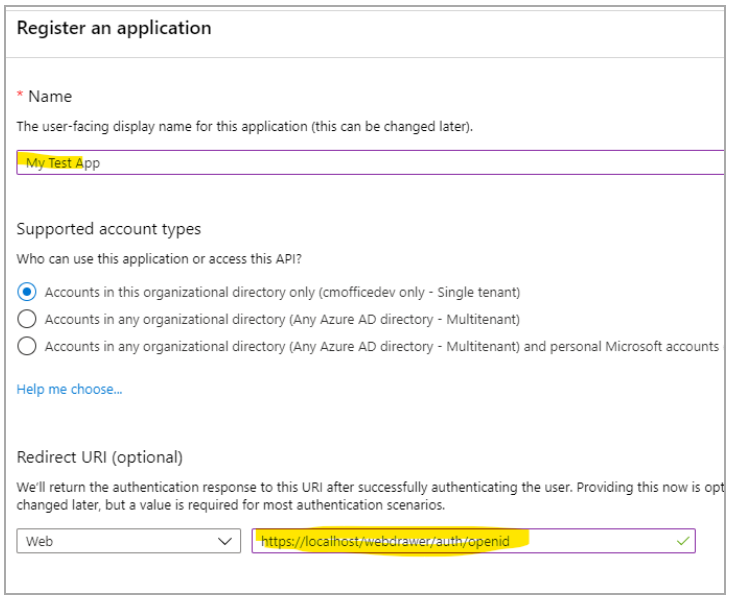
As of Content Manager 10 the web applications (Service API, WebDrawer and Web Client) have a built in OpenID Connect authentication provider.

This section describes creating an Azure AD application and configuring the web application. This document also provides detailed steps required to allow the Content Manager Mobile App to authenticate.

Create the Azure AD application

To create the Azure AD application:

1. From the portal.azure.com, go to Azure AD.
2. Go to **App Registrations** and select **New Registration**.



3. Enter a name.
4. Under Redirect URI leave **Web** selected.

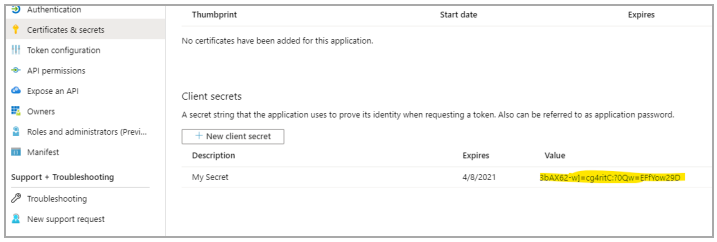
   The value in the Redirect URI is important. It must be lowercase and must be the URL to your application. For example, https://mydomain.com/cmwebdrawer followed by the path to the authentication provider, for example, /auth/openid.

   The /auth/ component is fixed but the 'openid' is the name you will supply in **hptrim.config** later and so can be any string, as long as it matches the value in **hptrim.config**.

For the Web Client the path must include the path to the Service API, for example, https://mydomain.com/contentManager/serviceapi/auth/openid.

5. Add a secret.

   From **Certificates and Secrets**, add a secret and note the secret.



6. Configure Tokens.

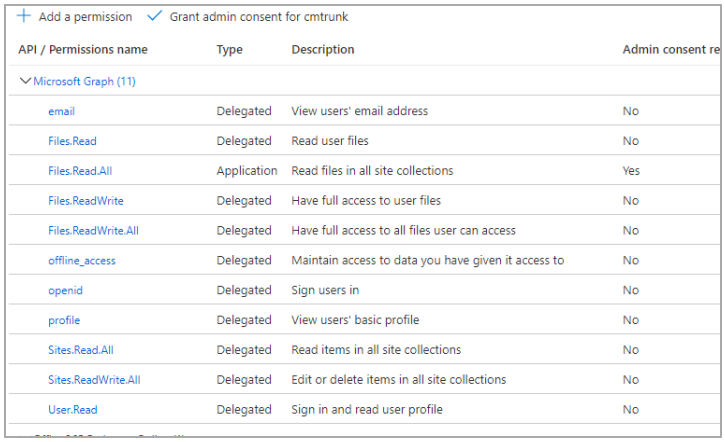
   From the **Authentication** section, select the tokens to be issued and check the option **ID Tokens**.

7. Configure permissions.

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

   - email
   - offline_access
   - openid
   - profile
   - User.Read
   - Files.Read
   - Files.Read.All
   - Files.ReadWrite
   - Sites.Read.All
   - Sites.ReadWrite.All
   - User.Read

   Select **Grant admin consent** to grant access to all permissions.



Configure for mobile

Add the mobile redirect URI

If this Azure app is to be used to connect to the Content Manager Mobile App then,

1. Go to the **Authentication** section and select **Add a platform**.
2. Choose **Mobile and desktop applications** and enter `trimapp://mobile` in the **Custom Redirect URIs** field.

Add the mobile redirect URI to the Service API

The redirect URI set above must be included in the Service API **hptrim.config**. To do this, add the **authentication and openIdConnect** elements.

For example,

```
<authentication allowAnonymous="false"slidingSessionMinutes="60">
<openIdConnect>
<addname="mobile"
clientID="[CLIENT ID from Azure App]"
clientSecret="[SECRET from Azure APP]"
issuerURI="[OpenID Connect metadata document from endpoints in Azure App]"
redirectUri="trimapp://mobile" />
</openIdConnect>
</authentication/>
```

Configure authentication in hptrim.config

To use the Azure AD app created above, edit the **hptrim.config** (or **hprmServiceAPI.config** in the Web Client) so that it has an authentication similar to the one below:

1. The name must match the last segment of the Redirect URI path.
2. Client ID is the application ID from the Azure AD Overview.
3. The secret is the one saved when creating the App. If it was not saved, created a new one in Certificates and Secrets.
4. Get the issuerUri from **Overview > Endpoints > OpenID Connect metadata document**.

For example,

```
<authentication allowAnonymous="false"slidingSessionMinutes="60">
<openIdConnect>
<add
name="openid"
clientID="ae99999d-99e9-9ecc-b9eb-99d9d999dd"
clientSecret="_MqXXXXXXXXXXXXXXG[sp3GrMfD:"
issuerURI="https://login.microsoftonline.com/09999ee9-9999-9999-9d9a-
999999999/v2.0/.well-known/openid-configuration"/>
</openIdConnect>
</authentication>
```

Enable redirect

The Web Client will not re-direct the authentication endpoint unless the Html feature is enabled in **hprmServiceAPI.config**, perform the following steps:

1. Edit the **hprmServiceAPI.config** file.
2. Find the property named **serviceFeatures**.
3. Add the feature **Html**.

Allow users (Web Client only)

For the Web Client, find the **web.config** file and find the **Location** element with the path **serviceapi** in the **web.config** file. It should contain the element `<allow users="*" />` within its authorization element.

For example,

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

```
...
  </location>
```

Logout

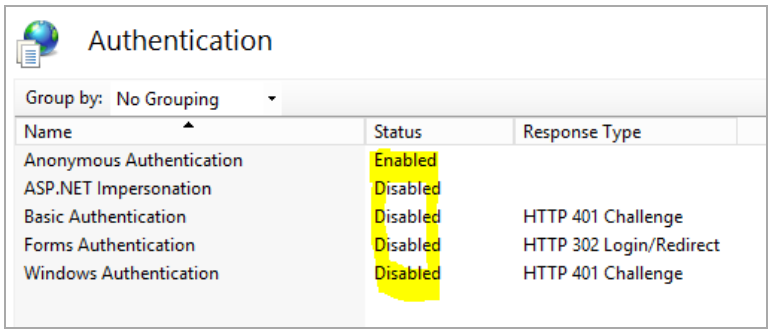
For WebDrawer the logout link is configured in the uiSettings. It should contain `~/auth/logout`. In the Web Client a logout link will be displayed automatically when OpenID Connect authentication is enabled.

For example,

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

Allow anonymous access in IIS

The IIS will not handle authentication, so use IIS Manager to allow anonymous access only.



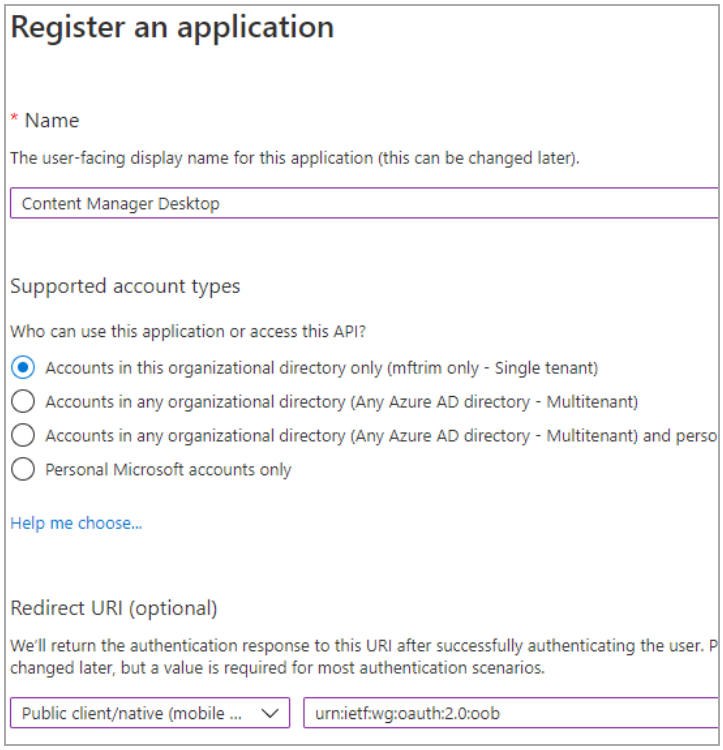
Azure AD for Content Manager desktop

OpenID Connect may be used to authenticate with the Content Manager desktop client, this section describes how to configure this.

Create the Azure AD application

To create the Azure AD application:

1. From the portal.azure.com, go to Azure AD.
2. Go to **App Registrations** and select **New Registration**.



3. Enter a name.
4. Select **Public native client** in the Redirect URI.
5. Enter the redirect Uri as 'urn:ietf:wg:oauth:2.0:oob'.
6. Configure permissions.

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

   - email
   - offline_access

- openid
- profile
- User.Read
- Files.Read
- Files.Read.All
- Files.ReadWrite
- Sites.Read.All
- Sites.ReadWrite.All
- User.Read

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

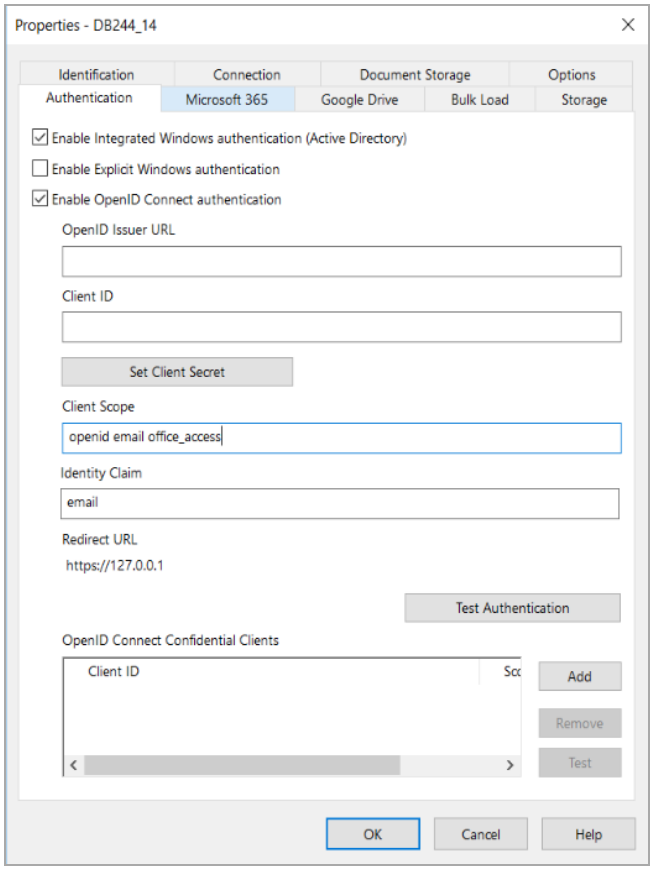
API / Permissions name	Type	Description	Admi
Microsoft Graph (11)			
email	Delegated	View users' email address	No
Files.Read	Delegated	Read user files	No
Files.Read.All	Delegated	Read all files that user can access	No
Files.ReadWrite	Delegated	Have full access to user files	No
Files.ReadWrite.All	Delegated	Have full access to all files user can access	No
offline_access	Delegated	Maintain access to data you have given it access to	No
openid	Delegated	Sign users in	No
profile	Delegated	View users' basic profile	No
Sites.Read.All	Delegated	Read items in all site collections	No
Sites.ReadWrite.All	Delegated	Edit or delete items in all site collections	No
User.Read	Delegated	Sign in and read user profile	No

Configure authentication in Content Manager Enterprise Studio

To use the Azure AD app created above, open the Content Manager Enterprise Studio and perform the following:

1. From the database, select **Authentication > OpenID**.
2. The OpenID Issuer URL is taken from the **Azure App - Overview > Endpoints > OpenID Connect metadata document**.
3. The Client ID is taken from the **Azure App - Overview > Application ID**.
4. Client secret should be empty.

5. Client app scope should contain **openid email offline_access**.



Configure Azure AD for Office integration access

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

1. Create an Azure App for Web Authentication, you may use the one you created to authenticate with the Content Manager Web Client.
2. Create (or edit) the file ADFS\config.xml in your Content Manager Web Client installation folder and set it as follows:
   - **clientAuthority** - for single tenant application, use https://login.microsoftonline.com/{TENANTID}. For multiple tenant application, use https://login.microsoftonline.com/common.
   - **clientResourceUri** - use the scope (**access_as_user**) uri as resource uri. For example, api://test.domain.com/5a93xxx8-07d5-43x9-82e0-d90025ee6xx3/access_as_user.
   - **clientID** - the Application ID from your Content Manager Desktop Azure App.
   - **clientReturnUri** - urn:ietf:wg:oauth:2.0:oob
3. From the Azure App for Web Authentication,

a. Go to **Expose an API** and select **Add a Scope.**

b. Enter the following values:

- **Scope name**: access_as_user
- **Who can consent**: Admins and Users
- **Admin consent display name**: Office can act as the user
- **Admin consent description**: Enable Office to call the add-in's web APIs with the same rights as the current user
- **User consent display name**: Office can act as you
- **User consent description**: Enable Office to call the add-in's web APIs with the same rights that you have

c. Click **Add scope**.

4. From the Content Manager Desktop Azure App, go to **API Permissions** and perform the following:

   a. Select **Add a Permission** and choose **My APIs**.

   b. Select the Web Client Application.

   c. Select the **access_as_user permissions**.

   d. Select **Add permission**.

5. The Web Client authentication information needs to updated to be made aware of the new client, perform the following steps:

   a. From the Content Manager Desktop Azure App, copy the **Application ID URI**. For example, api://cf2501bd-19f9-4ad6-96dc-f5cf7b2b3bf9.

   b. Edit the Web Client **hprmServiceAPI.config** file.

   c. In the **add** element of the openIDConnect element, add a new attribute called **appIdURI**. This is a case sensitive name.

   d. The value of **appIdURI** should be the **Application ID URI** from the Content Manager Desktop Azure App.

For example,

```
<adfsClient>
<clientAuthority>https://login.microsoftonline.com/09a67e4a-46xx-485d-929a-
1add8eexxxxb</clientAuthority>
<clientResourceUri>api://test.domain.com/5a93xxx8-07d5-43x9-82e0-
d90025ee6xx3/access_as_user</clientResourceUri>
<clientID>5a93xxx8-07d5-43x9-82e0-d90025ee6xx3</clientID>
<clientReturnUri>urn:ietf:wg:oauth:2.0:oob</clientReturnUri>
</adfsClient>
```

Google authentication

As of Content Manager 10 the web applications (Service API, WebDrawer and Web Client) have a built in OpenID Connect authentication provider.

This section describes creating Google credentials and configuring the web application.

Create the Google credentials

To create the Google credentials:

1. Go to https://console.developers.google.com/.
2. Select **Credentials > OAuth Client ID**.
3. Set Application type as **Web Application**.
4. Add your domain in the **Authorized JavaScript origins.**

   The value in the Redirect URI is important. It must be lowercase and must be the URL to your application. For example, 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 **hptrim.config** later and so can be any string, as long as it matches the value in **hptrim.config**.

   For the Web Client the path must include the path to the Service API, for example, https://mydomain.com/contentManager/serviceapi/auth/openid.
5. On saving, the Client ID and Client Secret will be displayed, note them for later use.

Configure authentication in hptrim.config

To use the Google credentials created above, edit the **hptrim.config** (or **hprmServiceAPI.config** in the Web Client) so that it has an authentication as follows:

1. The name must match the last segment of the Redirect URI path.
2. Client ID and secret as noted in above section.
3. The issuerURI is: https://accounts.google.com

For example,

```
<authentication allowAnonymous="false" slidingSessionMinutes="2">
<openIdConnect>
<addname="openid"
clientID="999999999999-abcdefghijklmemopqrs.apps.googleusercontent.com"
clientSecret="jl-BiX7685hjgf99999y"
issuerURI="https://accounts.google.com"
/>
```

```
</openIdConnect>
</authentication>
```

Enable redirect

The Web Client will not re-direct the authentication endpoint unless the **Html** feature is enabled in **hprmServiceAPI.config**. To do this:

1. Edit **hprmServiceAPI.config**
2. Find the property named **serviceFeatures**.
3. Add the feature **Html**.

Logout

For WebDrawer the logout link is configured in the uiSettings. It should contain `~/auth/logout`. In the Web Client a logout link will be displayed automatically when OpenID Connect authentication is enabled.

For example,

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

Allow anonymous access in the IIS

The IIS will not handle authentication, so use IIS Manager to allow anonymous access only.