Content Manager

Software Version 24.4

OpenID Connect authentication

opentext

Document Release Date: October 2024 Software Release Date: October 2024

Legal notices

Copyright 2008-2024 Open Text

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

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

Documentation updates

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

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

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	
Configure ADFS	
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	
Add Office integration to the settings of the Web Client	18
Azure AD for WebClient, Mobile App and Service API	
Create the Azure AD application	
Configure for mobile	21
Add the mobile redirect URI	
Add the mobile redirect URI to the Service API	21
Configure authentication in hptrim.config	21
Enable redirect	
Allow users (Web Client only)	
Logout	
Allow anonymous access in IIS	23
Azure AD for Content Manager desktop	
Create the Azure AD application	24
Configure authentication in Content Manager Enterprise Studio	
Configure Azure AD for Office integration access	
Google authentication	
Create the Google credentials	
Configure authentication in hptrim.config	
Enable redirect	
Logout	
Allow anonymous access in the IIS	

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.

翰 Add Application Gro	up Wizard X
Welcome	
Steps	Name:
Welcome	ContentManager
Native application Summary Complete	Description: For Clients to authenticate, to content manager
	Template: Client-Server applications Server application accessing a web API Server application accessing a web API Web browser accessing a web application Standalone applications Server application Standalone applications Web API Server application Server application Web API
	More information
	< Previous Next > Cancel

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**.

翰 Add Application Group	Wizard	×
Native application		
Steps Welcome Native application Summary Complete	Name: Content Manager - Native application Client Identifier: 65566546-68ee 46cb-8b33-47671d800f52 Redirect URI: um ieff wg cauth-2 0 cobl	Add
	Description:	
	< Previous Next >	Cancel

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

翰 Add Application Grou	ip Wizard	×
Summary		
Reps	Review the following settings and click 'Next' to create the application.	
Welcome Native application Summary Complete	Application Group Name: ContentManager Description: For Clients to authenticatet to content manager	_
	Native application Name: Content Manager - Native application Identifier: 5506574-62 Nate: Abs. 33.47671d02/52 Redirect: UBIs: um3eff.vg.oauth:2.0xxxb	
	< Previous Next > Can	icel

5. Modify application group properties.

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

Application Grou	ps	
Name		Description
ContentManage CMappgrou CMAppGrou CMAppgrou	Properties	For Clients to authenticatet
	Delete	
	Help	

6. Click Add application.

ContentManager Properties		×
General		
Name:		
ContentManager		
Description:		
For Clients to authenticatet to content mana	ger	
Applications:		
Name	Description	
Native application		
ContentManager - Native application		
Add application	Edit	Remove
	OK Cancel	Apply

7. Select Web API as the Template.

🏟 Add a new application to	ContentManager >	<
Welcome		
Steps	Name:	
Welcome	ContentManager	1
Configure Web API	Description:	1
 Apply Access Control Policy 	For Clients to authenticatet to content manager	1
 Configure Application Permissions 		
 Summary 	Template:	ĺ.
Complete	Standalone applications Native application Prever application Velo API More information	
	< Previous Next > Cancel	

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**.

Configure Web API		
Steps	Name:	
Welcome	ContentManager - Web API	
Configure Web API	dentfier.	
 Apply Access Control Policy 	Fyamole: https://Contoso.com	Add
 Configure Application Remissions 	Renorate Rev. to the anti-fation real	700
Summany	9506574956665466056653476718802252	Hemove
Complete		
Complete		
	Description:	

9. Select an appropriate Access Control Policy.

Choose Access Contro	I Policy	
Steps	Choose an access control policy:	
Welcome	Name	Description
Configure Web API	Permit everyone	Grant access to everyone
Apply Access Control Policy	Permit everyone and require MFA	Grant access to everyone and require MFA f
Configure Application Permissions	Permit everyone and require MFA for specific group Permit everyone and require MFA from extranet access	Grant access to everyone and require MFA f Grant access to the intranet users and requir
Summary Complete	Permit everyone and require MFA from unauthenticated Permit everyone and require MFA, allow automatic devi Permit everyone for intranet access Permit specific group	Grant access to everyone and require MFA1 Grant access to everyone and require MFA1 Grant access to the intranet users. Grant access to users of one or more specifi
	Pemit everyone	is time. No users will be permitted access for this

10. Set the scopes.

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

Ndd a new application to	ContentManager				>
Configure Application	Permissions				
Steps	Configure permission	is to enable client applications to access thi	s Web API.		
Welcome	Client application (ca	aller):			
Configure Web API	Name	Description			
Apply Access Control Policy	Content Manager	Native application			
Configure Application Permissions	ContentManager -	Server application			
Summary					
Complete					
Complete					
				Add	Remove
	Permitted scopes:				
	Scope Name	Description			^
	allatclaims	Requests the access token claims in the	identity token.		
	aza	Scope allows broker client to request prin	nary refresh toke	en.	
	🗹 email	Request the email claim for the signed in	user.		
	logon_cert	The logon_cert scope allows an applicati	ion to request lo	go	
	🗹 openid	Request use of the OpenID Connect aut	horization protoc	col.	
	profile	Request profile related claims for the sign	ied in user.		
	user_imperso	Request permission for the application to	access the reso	our	
	von cert	The von cert scope allows an application	n to request VPI	N	*
				[New scope

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

Summary		
Summary Steps • Welcome • Configure Web API • Apply Access Control Policy • Configure Application • Permissions • Summary • Complete	Review the following settings and click 'Next' to create the application. Application Group Name: Content Manager Description: For Clients to authenticate to content manager Web API Name: Content Manager - Web API Identifiers: umiseft wg awuth 2.0 coob Access control policy: Pemit everyone Application pemissions: CMAppGroup 2- Server application - email profile allatclaims openid Al clients - email profile openid Content Manager - Native application - openid email profile	
	(Denviour Next) Connel	

12. Set issuance rules.

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

ContentManager Properties	<
General	
Name:	
ContentManager	
Description:	
Applications:	
Name Description	
Native application	
CMappgroup3 - Native application	
Server application	
CMappgroup3 - Server application	
Web API	
CMappgroup3 - Web API	
Add application Remove	
OK Cancel Apply	

13. Add a rule.

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

CMappgroup3 - Web API Properties	×
Identifiers Notes Access control policy Issuance Transform Rules	Client Permissions
The following transform rules specify the claims that will be sent to the	e relying party.
Order Rule Name Issued Claims	3 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
ОК	Cancel Apply

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

dit Ru	ıle - Claim rule					
'ou ca o extra rom the	n configure this rule to send the value: act LDAP attributes. Specify how the al e rule.	s of LE ttribute) AP attributes as o es will map to the o	laims. Select ar outgoing claim ty	n attribute /pes that v	store from whi vill be issued
laim ru	ule name:					
Claim n						
Quia ta	molate: Send I DAP Attributes as Claim					
	inplate. Jenu LDAr Attibutes as Clain	19				
ttribut	e store:					
Active	Directory				\sim	
/lappin	og of LDAP attributes to outgoing claim	types	:			
	LDAP Attribute (Select or type to add more)		Outgoing Claim	Type (Select or t	type to ad	d more)
•	E-Mail-Addresses	~	E-Mail Address			
	User-Principal-Name	~	UPN			`
		~				,
		_				
10						
	Pulo Languago				112	Canaal

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**.

Nindows	OpenID Connect	OneDrive	Conne	đ						
Enable	e OpenID Connect a uth 2.0 Configurati	on	ion							
O	penID Issuer URL		HTTPS:// <mark>ADFS.</mark> domain.com/adfs/							
Au	Authorize Endpoint URL Token Endpoint URL Client ID		https://adfs/domain.com/adfs/oauth2/authorize/							
Tol										
Cli			92089928-394e-47e2-a6ac-8805cda3c5eb							
								Set C	lient Secre	t
Cli	Client App Scope Client Redirect URI		openi	id email						
Cli			urn:ie	tf:wg:oau	th:2.0:oo	b				
				Test	Authen	ticatio	n			
Ор	enID Connect Conf	idential Cli	ents –							
	Client ID						Scope			
		Add		Remo	ve		Test			

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

🔁 Content Manager Third Party	Authentication	×
	Resource Domain	
XX	Sign in	
$\sim N$	Administrator@ Domain.com	
	•••••	
	Sign in	
Tare	Sign in as current user	
08		
	© 2018 Microsoft	

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

Content Manager							
Þ.	The user 'Admin@domain.comhas been successfully authenticated.						
	ОК						

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.

翰 Add Application Group Wizard					
Welcome					
Steps	Name:				
Welcome	My CM App				
Server application	Desertation				
 Configure Application Credentials 					
Configure Web API					
Apply Access Control Policy	Template:				
 Configure Application Permissions 	Client-Server applications				
Summary	Native application accessing a web API				
Complete	Server application accessing a web API				
	Web browser accessing a web application				
	Standalone applications				
	Native application				

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.

Conindential	
Name:	
CM Web Client DC - Server application	
Client Id:	
9eeda8c0-b3a2-43c5-aa45-34930f0dc8ff	
Redirect URI:	
	Add
https://auchurchla02/cm/serviceapi/auth/openid	Remove

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

Welcome Server application Configure Application
Contingence / opproductor /
Configure Web API Apply Access Control Policy Orfigure Application Permissions Summary Complete

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

Configure Web API						
Steps	Name:					
Welcome	My CM App - Web API					
Server application	lde-t#					
 Configure Application Credentials 	Example: https://Contoso.com					
Configure Web API	https://btpvm2237.myexch19.com/contentmanager/					
Apply Access Control Policy						
 Configure Application Permissions 						
Summary	Description:					
Complete						

- 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.

输 Add a new application to CM Web Client Sample							
Native application							
Steps	Name:						
Welcome	CM Web Client Sample - Native application 1						
Native application	Client Identifier:						
Summary Summary Summary							
Complete							
	Redirect URI:						
	Example: https://Contoso.com Ac						
	https://myserver/contentmanager Rem						

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**.

CM Web C	lient Sa	mple - Web	API Prop	erties			
Identifiers	dentifiers Notes Access control policy Issuance Transform Rules Client Permissio						emissions
Configure application permissions to enable client applications to acess this Web API							
Client ap	plication	(caller):					
Name	Name Description						
CM We	eb Client	Sample - Ser	ver applica	ation			
CM We	eb Client	Sample - Nat	ive applica	ation			
						_	
<							
					Add.		Remove
Permittee	d scopes						
Sco	pe Nam	e Descrip	tion				
🗌 alla	tclaims	Reques	sts the acc	ess token claim	s in the ident	ity token	
aza	l	Scope	allows bro	ker client to requ	iest primary r	efresh tol	ken.
ema ema	ail	Reques	t the emai	il claim for the sig	gned in user.		
	on_cert	The log	on_cert so	cope allows an a	application to	request	logo
ope ope	enid	Reques	t use of th	e OpenID Conn	ect authoriza	ation prote	ocol.
prot	hile	Reques	t profile re	lated claims for t	the signed in	user.	

- 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

	-						
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	Active Directory \checkmark						
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 ~					
	~	~					

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.

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

- 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.

Authentication	Thumbprint	Start date	Expires
📍 Certificates & secrets			
11 Token configuration	No certificates have been added for th	is application.	
 API permissions 			
🔷 Expose an API	Client secrets		
🛤 Owners	A secret string that the application use	is to prove its identity when requesting a token. Also can be	e referred to as application password.
Roles and administrators (Previ	+ New client secret		
Manifest	Description	Expires	Value
Support + Troubleshooting	My Secret	4/8/2021	3bAX62-w]=cg4ritC:?0Qw=EFfYow29D
Troubleshooting			
New support request			

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.

PI / Permissions name	Туре	Description	Admin consent r
Microsoft Graph (11)			
email	Delegated	View users' email address	No
Files.Read	Delegated	Read user files	No
Files.Read.All	Application	Read files in all site collections	Yes
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 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="_MqXXXXXXXXXG[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,

```
<lection 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.

Register an application
* Name
The user-facing display name for this application (this can be changed later).
Content Manager Desktop
Supported account types
Who can use this application or access this API?
Accounts in this organizational directory only (mftrim only - Single tenant)
O Accounts in any organizational directory (Any Azure AD directory - Multitenant)
O Accounts in any organizational directory (Any Azure AD directory - Multitenant) and perso
Personal Microsoft accounts only
Help me choose
Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. P changed later, but a value is required for most authentication scenarios.
Public client/native (mobile) urn:ietf:wg:oauth:2.0:oob

- 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 Connect authentication Azure AD for Content Manager desktop

- 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	Туре	Description	Adm	
✓ 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**.

perties - DB244_14				
Identification	Connection	Documer	nt Storage	Options
Authentication	Microsoft 365	Google Drive	Bulk Load	Storage
Enable Integrated V Enable Explicit Wind Enable OpenID Cor OpenID Issuer UF	Vindows authentication lows authentication Inect authentication	n (Active Directory)		
	-			
Client ID				
Set Cli	ent Secret			
Client Scope				
openid email offi	ce_access			
Identity Claim	-			
email				
Redirect URI				
https://127.0.0.1				
			Tost Authon	tication
OpenID Connect	Confidential Clients		rest Autren	ucation
Client ID	connuential Clients		Ser	
Clencio			34	Add
				Remove
<			>	Test
		ОК	Cancel	Help

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-
ladd8eexxxxb</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.

