

# Content Manager

Software Version 23.4

SAP Integration

**opentext™**

Document Release Date: September 2025  
Software Release Date: September 2025

## Legal notices

Copyright 2008-2025 Open Text

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

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

## 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

- Content Manager SAP Integration ..... 4
  - Introduction ..... 4
- Content Manager SAP ArchiveLink Server ..... 4
- Installing the Content Manager SAP ArchiveLink Server ..... 5
  - Prerequisites ..... 5
  - Installation steps ..... 5
  - Sending SAP certificates ..... 9
  - Viewing SAP repos in Content Manager ..... 9
- Configurations for OpenID connect confidential client ..... 11
  - Content Manager Enterprise Studio ..... 11
  - Content Manager client application ..... 12
  - Update the appsettings.json file ..... 13

## Content Manager SAP Integration

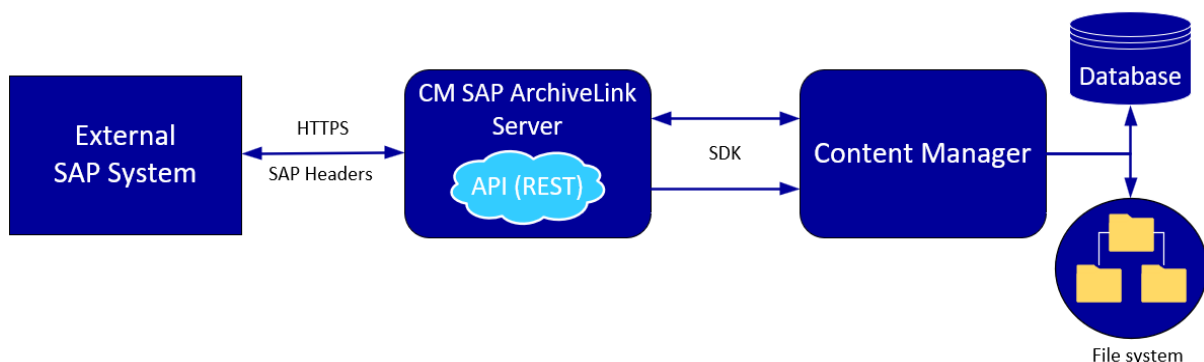
### Introduction

OpenText Content Manager integrates with SAP which allows the SAP system to be configured to use the Content Manager records and document management capabilities to manage the electronic documents. This document describes how to install and configure the software components required for this integration, and also outlines the options available for managing the Content Manager records associated with SAP documents.

### Content Manager SAP ArchiveLink Server

The Content Manager SAP integration module includes CM SAP ArchiveLink Server that provides connectivity between SAP system and Content Manager.

The following image provides a general outline of how the components are combined together to provide the software solution.



The CM SAP ArchiveLink Server, which is hosted on IIS, is a connector between the SAP system and the Content Manager application.

The SAP system shares the certificate and registers the content repository with the Content Manager through the CM SAP ArchiveLink Server. When the SAP system raises a request (for example, view, bulk update, or get) to the CM SAP ArchiveLink Server, it validates the request via the certificate. If the certificate matches with the one registered with Content Manager, then Content Manager executes the requests.

**NOTE:** If the SAP system does not provide the format (MIME type) of the document being recorded into Content Manager, then the document will be stored with a .bin extension.

The communication between the SAP system and CM SAP ArchiveLink Server is through HTTPS with a valid certificate and the communication between the CM SAP ArchiveLink Server and Content Manager is through SDK.

The CM SAP ArchiveLink Server supports integrated and confidential client authentication methods. The trusted user is mandatory for both integrated and confidential client authentication methods.

## Installing the Content Manager SAP ArchiveLink Server

This section describes the prerequisites and the installation steps required to install the CM SAP ArchiveLink Server.

### Prerequisites

Before you begin, make sure the following prerequisites are met on the system where you will host the CM SAP ArchiveLink Server:

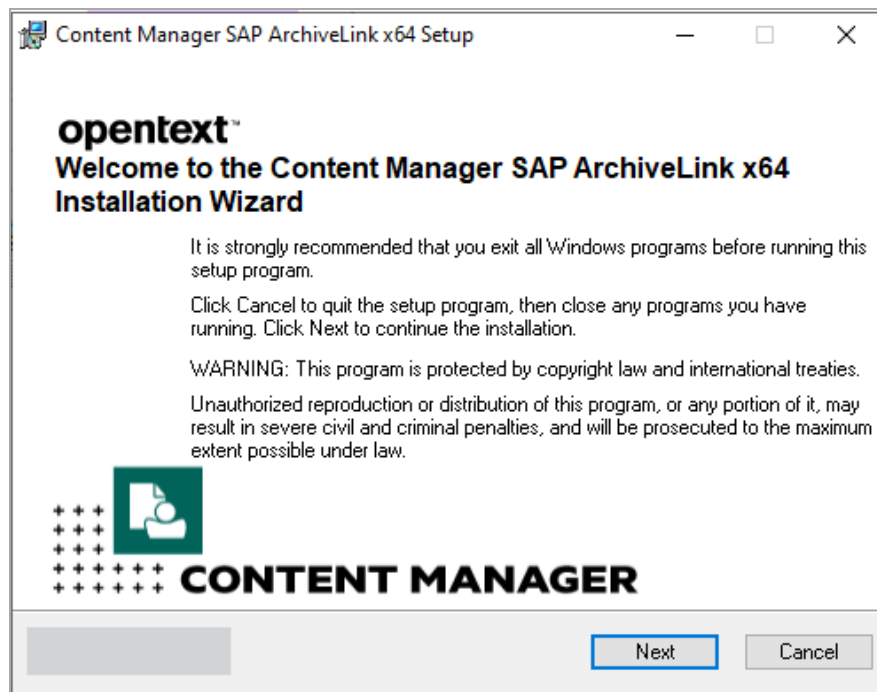
1. .Net 8 host bundle is installed.
2. The Workgroup Server or the Content Manager 64-bit client is installed on the same system where you will install the CM SAP ArchiveLink Server.

### Installation steps

1. On your installation medium, locate the installation file and run it as administrator:

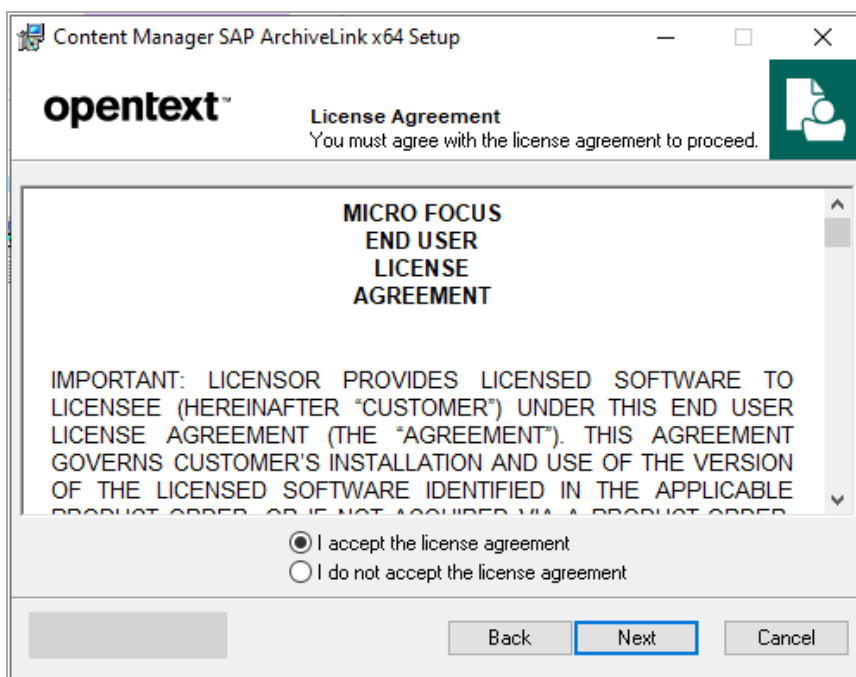
**CM\_SAPArchiveLink\_x64.msi**

The Welcome screen appears.



2. Click **Next**.

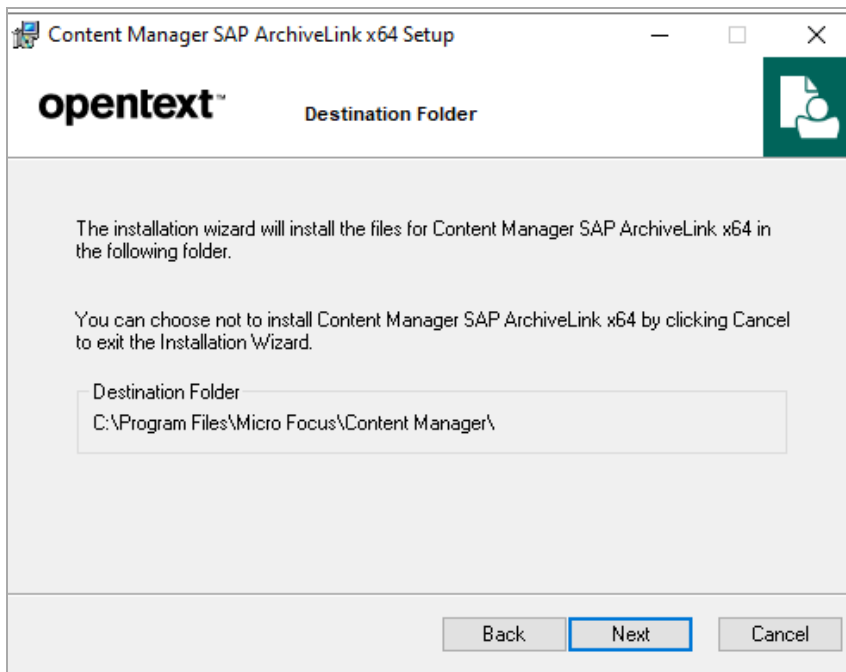
The License Agreement dialog appears.



3. Select **I accept the license agreement** and click **Next**.

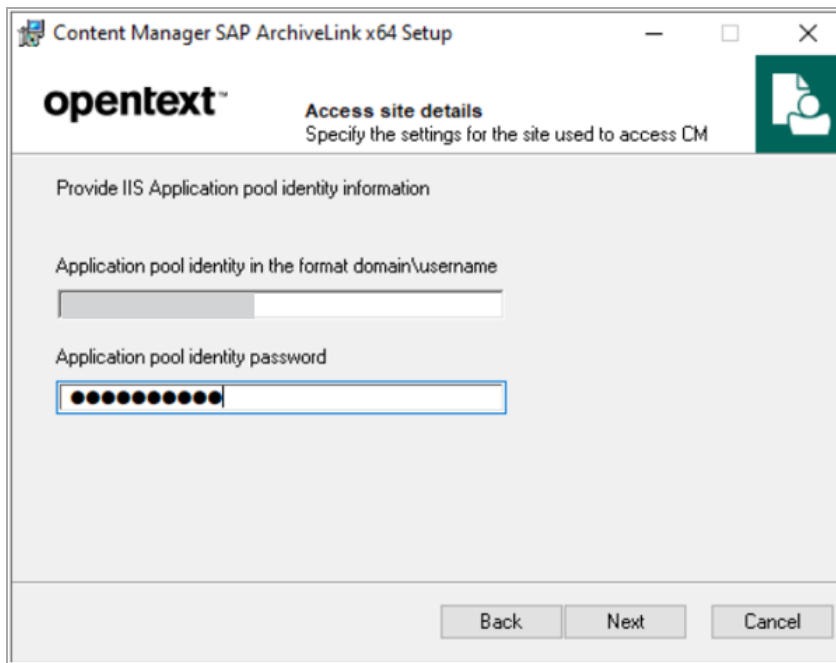
The Destination Folder dialog appears.

Review the installation destination folder information.



4. Click **Next**.

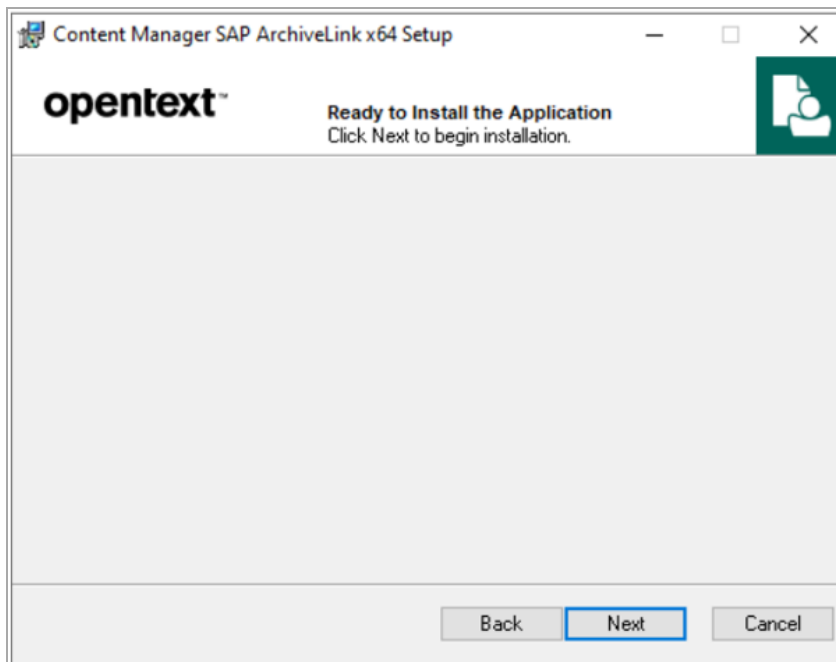
The Access site details dialog appears.



The dialog box is titled "Content Manager SAP ArchiveLink x64 Setup". It features the OpenText logo and a sub-header "Access site details" with the instruction "Specify the settings for the site used to access CM". The main area is titled "Provide IIS Application pool identity information". It contains two input fields: "Application pool identity in the format domain\username" and "Application pool identity password". The password field is currently filled with ten dots. At the bottom, there are three buttons: "Back", "Next", and "Cancel".

5. Enter the Application pool user ID and the password. Click **Next**.

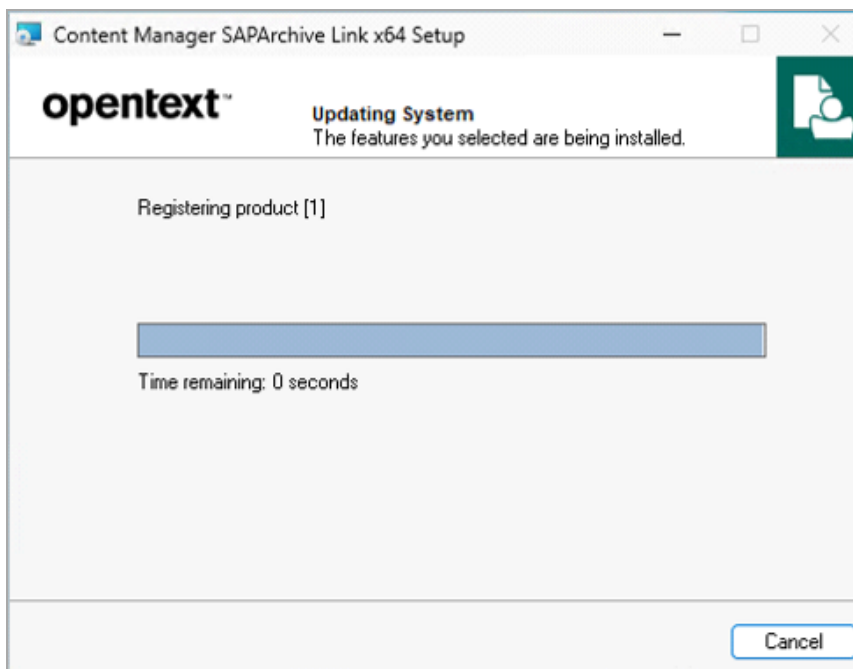
The Ready to install the application dialog appears.



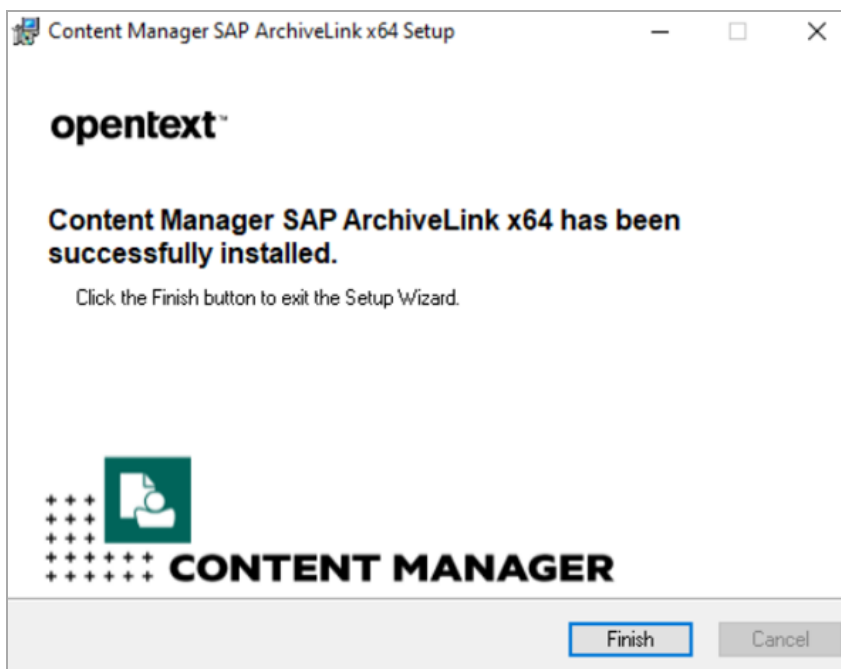
The dialog box is titled "Content Manager SAP ArchiveLink x64 Setup". It features the OpenText logo and a sub-header "Ready to Install the Application" with the instruction "Click Next to begin installation." The main area is empty. At the bottom, there are three buttons: "Back", "Next", and "Cancel". The "Next" button is highlighted with a blue border.

6. Click **Next**.

The Updating system dialog appears.



A message indicating setup status is displayed.



7. Click **Finish** to exit the wizard.

After the successful installation of the CM SAP ArchiveLink Server, a directory (**CMSAPArchiveLink**) and application pool user are created in the IIS. Also a directory (**SAPArchiveLink**) is created in the installation drive which includes the necessary binaries.



## Sending SAP certificates

To send SAP certificates to CM SAP ArchiveLink Server, perform the following:

1. Open the SAP application and navigate to content repository listing.

You can create a new content repository or integrate with an existing one.

2. Navigate to the content repository details page of the content repository you want to connect with CM SAP ArchiveLink Server.

Make sure the following details are filled in appropriately so that Content Manger uses SAP specific record types to archive the data:

- **Document Area:** ArchiveLink
- **Storage type:** HTTP Content Server
- **HTTP server:** CM SAP ArchiveLink Server URL. For example, sapwgs1.testsapad.com.
- **SSL Port number:** 443
- **HTTP Script:** Virtual directory path created by IIS when you install the CM SAP ArchiveLink Server. For example, CMSAPArchiveLink/ContentServer.
- **HTTPS on frontend:** HTTPS required
- **HTTPS on backend:** HTTPS required

3. Click Send Certificate (email icon) to send the certificate to CM SAP ArchiveLink Server. A confirmation message is displayed in the SAP application.

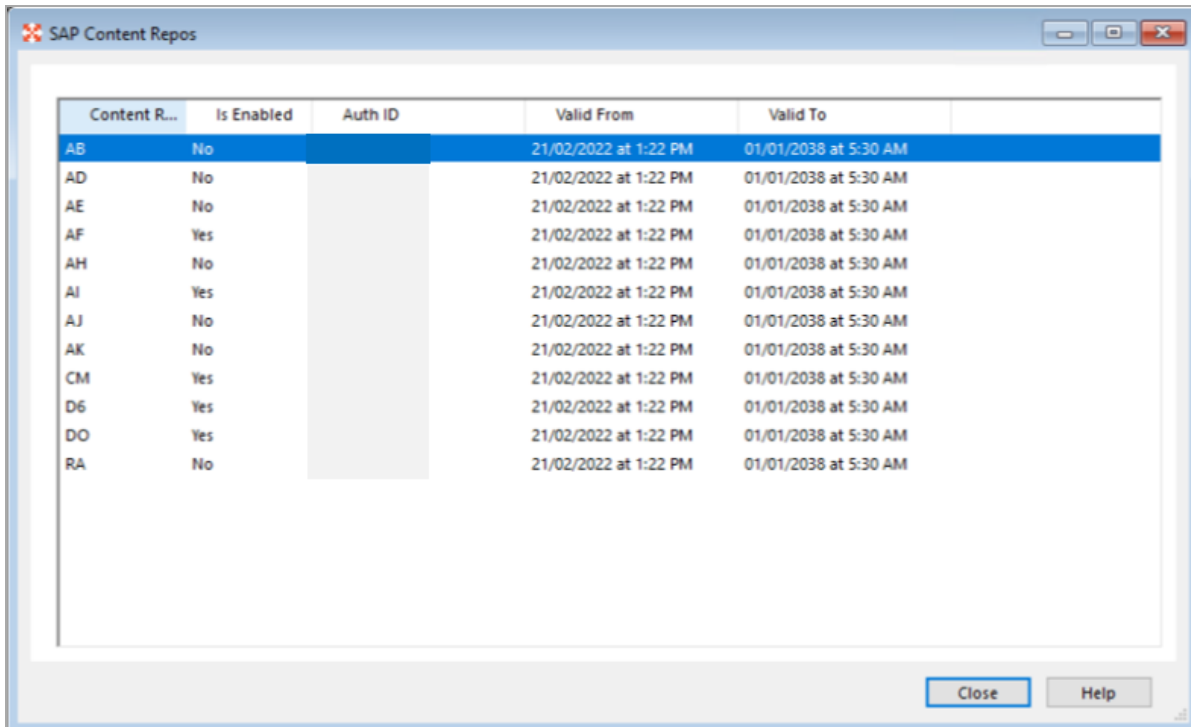
## Viewing SAP repos in Content Manager

**NOTE:** This feature is available in **Administration** tab of Content Manager client for Administrators only. For this feature to be visible in the **Administration** tab, make sure to enable **SAP integration** in the **System Options > Features** tab.

The SAP Content Repos feature lists all the SAP content repositories that are connected to the CM SAP ArchiveLink Server. After you send the certificate from a repository in the SAP application to the CM SAP ArchiveLink Server, you can view the SAP repository in Content Manager SAP Content Repos feature.

You can view **Content Repository ID**, **Auth ID**, **Is Enabled**, **Valid From**, and **Valid To** information.

Right-click on a repository to **Refresh**, **Enable/Disable**, and **Delete** the repository. By default, the newly connected repository is disabled. Right-click and select **Enable** to enable the repository.



The screenshot shows a window titled "SAP Content Repos" with a table listing various content repositories. The table has five columns: "Content R...", "Is Enabled", "Auth ID", "Valid From", and "Valid To". The "Auth ID" column is currently empty for all entries. The "Valid From" column shows a date and time of "21/02/2022 at 1:22 PM" for all entries. The "Valid To" column shows a date and time of "01/01/2038 at 5:30 AM" for all entries. The "Is Enabled" column shows "No" for AB, AD, AE, AH, AJ, AK, and RA, and "Yes" for AF, AI, CM, D6, and DO. The "Content R..." column lists the repository IDs: AB, AD, AE, AF, AH, AI, AJ, AK, CM, D6, DO, and RA.

Content R...	Is Enabled	Auth ID	Valid From	Valid To
AB	No		21/02/2022 at 1:22 PM	01/01/2038 at 5:30 AM
AD	No		21/02/2022 at 1:22 PM	01/01/2038 at 5:30 AM
AE	No		21/02/2022 at 1:22 PM	01/01/2038 at 5:30 AM
AF	Yes		21/02/2022 at 1:22 PM	01/01/2038 at 5:30 AM
AH	No		21/02/2022 at 1:22 PM	01/01/2038 at 5:30 AM
AI	Yes		21/02/2022 at 1:22 PM	01/01/2038 at 5:30 AM
AJ	No		21/02/2022 at 1:22 PM	01/01/2038 at 5:30 AM
AK	No		21/02/2022 at 1:22 PM	01/01/2038 at 5:30 AM
CM	Yes		21/02/2022 at 1:22 PM	01/01/2038 at 5:30 AM
D6	Yes		21/02/2022 at 1:22 PM	01/01/2038 at 5:30 AM
DO	Yes		21/02/2022 at 1:22 PM	01/01/2038 at 5:30 AM
RA	No		21/02/2022 at 1:22 PM	01/01/2038 at 5:30 AM

To view the SAP repos integrated with the Content Manager, perform the following:

1. Open Content Manager client application.
2. Navigate to **Administration > Other > SAP Content Repos**.

A list of SAP content repos are displayed.

## Configurations for OpenID connect confidential client

If you are using OpenID connect confidential client for authentication, make sure that the required information is provided to the Content Manager application for a seamless integration with the SAP system.

### Content Manager Enterprise Studio

In the Authentication dialog box of the dataset, make sure to add the details of the confidential client.

1. Navigate to the Authentication dialog box of the dataset and provide the details for **OpenID Issuer URL**, **Client ID** (The client ID is the ID of the Azure App configured for OpenID), and then click **Add** to add the OpenID Connect Confidential Clients details.

The screenshot shows the 'Register New Dataset - Authentication' dialog box. It contains the following elements:

- Checkboxes:
  - ☒ Enable integrated Windows authentication (Active Directory)
  - ☐ Enable Explicit Windows authentication
  - ☒ Enable OpenID Connect authentication
- Text fields:
  - OpenID Issuer URL
  - Client ID
  - Client Scope (containing 'openid email')
  - Identity Claim (containing 'email')
  - Redirect URL (containing 'https://127.0.0.1')
- Buttons:
  - Set Client Secret
  - Test Authentication
- OpenID Connect Confidential Clients section:
 

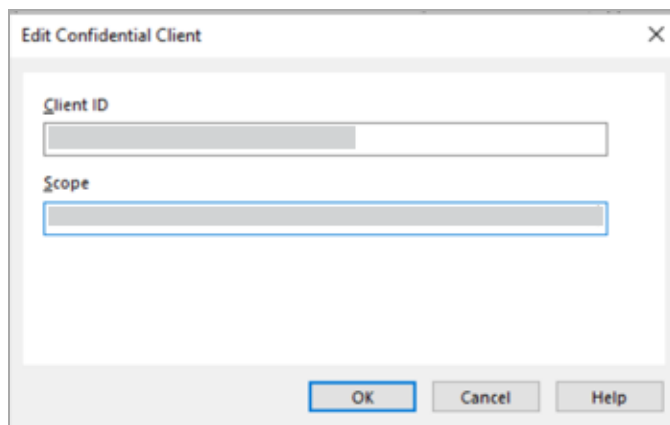
Client ID	Scope
[Empty row with scroll bar]	

 Buttons: Add, Remove, Test.
- Navigation buttons at the bottom: < Back, Next >, Cancel, Help.

The Edit Confidential Client dialog appears.

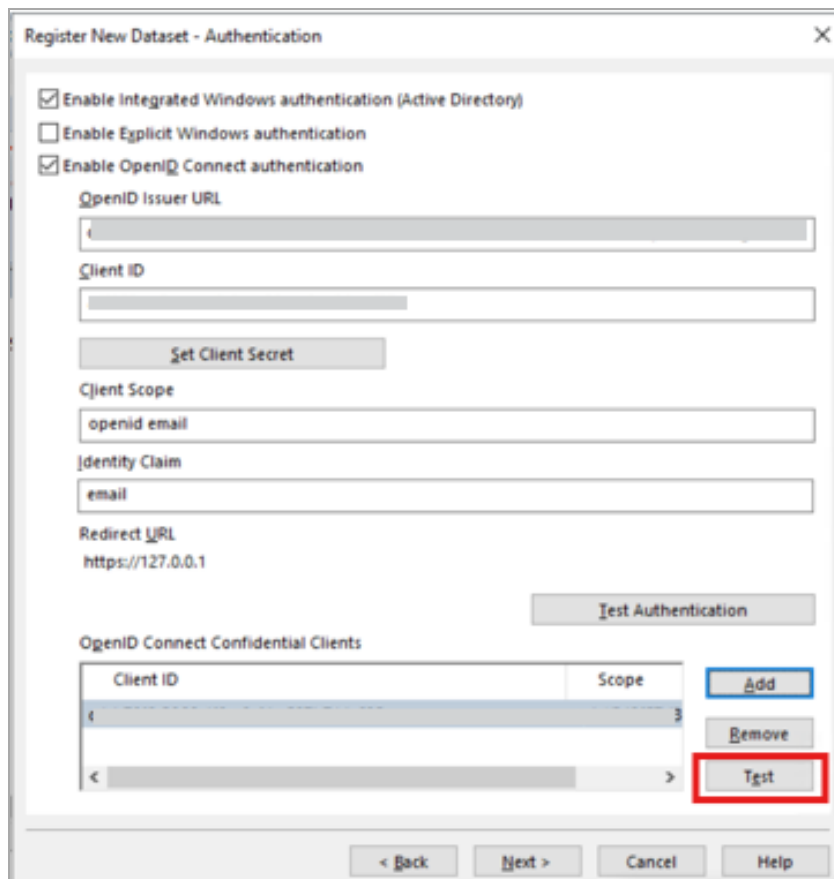
2. Enter the **Client ID** and **Scope** and click **OK**.

Here, the Client ID is the ID of the Demon app or Confidential Client App and the scope parameter is build / constructed by concatenating '/.default' to the Application ID URI of the Azure App created for OpenID connect.



The 'Edit Confidential Client' dialog box contains two text input fields: 'Client ID' and 'Scope'. Below these fields are three buttons: 'OK', 'Cancel', and 'Help'.

3. Click **Test** to test the connection. A Client Secret value must be entered, and authentication of the confidential client is then attempted.



The 'Register New Dataset - Authentication' dialog box includes several sections:

- Authentication Options:**
  - ☒ Enable Integrated Windows authentication (Active Directory)
  - ☐ Enable Explicit Windows authentication
  - ☒ Enable OpenID Connect authentication
- OpenID Issuer URL:** A text input field.
- Client ID:** A text input field.
- Set Client Secret:** A button.
- Client Scope:** A text input field containing 'openid email'.
- Identity Claim:** A text input field containing 'email'.
- Redirect URL:** A text input field containing 'https://127.0.0.1'.
- Test Authentication:** A button.
- OpenID Connect Confidential Clients:** A table with columns 'Client ID' and 'Scope'.
 

Client ID	Scope
<	>

 To the right of the table are three buttons: 'Add', 'Remove', and 'Test' (highlighted with a red rectangle).

At the bottom of the dialog are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

## Content Manager client application

In the Network Login page, make sure to add the Object ID of the application.

1. Navigate to the Network Login page of the admin location responsible for the Content Manager and SAP system integration, enable **Accept logins for this user using credentials** option.

2. Enter the **User name** of the admin location.
3. Enter the Object ID of the application in the **Alternative Logins** field.

The screenshot shows a dialog box titled "Position - DhanuDemon" with a sidebar on the left containing the following menu items: General, Address, Electronic Addresses, Associations, Network Login (highlighted), Profile, Access Controls, Active, Notes, and Governance. The main area of the dialog is titled "Accept logins for this user using credentials:" and contains the following fields and options:

- ☒ Accept logins for this user using credentials:
- User name:
- Domain name:
- Alternative logins:
- ☐ Until expiry date:
- ☐ User is a visitor account
- Visitor is registered in home dataset:

At the bottom of the dialog are three buttons: OK, Cancel, and Help.

For example, if you have created an app in MS Azure, navigate to **Enterprise applications > Your application** and copy the Object ID from the Properties of the application.

The screenshot shows a "Properties" dialog box for an application. It has a blue header bar with a white "S" icon. The fields are:

- Name:
- Application ID:
- Object ID:

A "Copied" tooltip is visible over the Object ID field, indicating that the value has been copied to the clipboard.

## Update the appsettings.json file

In the **appsettings.json** file, make sure to add the trusted user as the User name configured in the Network Login of the Content Manager client application.

1. Navigate to the installation folder of the CM SAP ArchiveLink Server. For example, C:\Program Files\Micro Focus\Content Manager\SAPArchiveLink.
2. Open the **appsettings.json** in a text editor.

3. For **TRIMConfig** parameter, enter the details for DatabaseId, WGSName, WGSPort, WorkPath, TrustedUser, ClientId, and ClientSecret attributes.

**NOTE:** Make sure that the value for **WGSName** attribute is always **local** and provide the User name configured in Content Manager client application as the value for the **TrustedUser** attribute.

Sample code snippet of **appsettings.json** file:

```
{
  "Logging": {
    "LogLevel": {
      "Default": "Information",
      "Microsoft.AspNetCore": "Warning"
    }
  },
  "TRIMConfig": {
    "DatabaseId": "PG",
    "WGSName": "local",
    "WGSPort": 1137,
    "WorkPath": "C:\\Micro Focus Content Manager\\ContentServerWorkPath",
    "TrustedUser": "DhanuDemon",
    "WGSAlternateName": "",
    "WGSAlternatePort": 0,
    "ClientId": "cdcbxxxx-3966-4f9a-xxxx-c587b714xxxx",
    "ClientSecret": "ZXxxx@@@YfUyuKIhUWGtcSxxxxxD3c48swD1njxxxh"
  },
  "AllowedHosts": "*"
}
```