Content Manager

Software Version 9.3

Installation and Setup Guide

MICRO FOCUS

Document Release Date: August 2018

Software Release Date: August 2018

Legal notices

Copyright notice

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

Trademark notices

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.

To verify you are using the most recent edition of a document, go to https://softwaresupport.softwaregrp.com/manuals.

You will also receive new or updated editions of documentation if you subscribe to the appropriate product support service. Contact your Micro Focus sales representative for details.

To check for new versions of software, go to https://www.hpe.com/software/entitlements. To check for recent software patches, go to https://softwaresupport.softwaregrp.com/patches.

The sites listed in this section require you to sign in with a Software Passport. You can register for a Passport through a link on the site.

Support

Visit the Micro Focus Software Support Online website at https://softwaresupport.softwaregrp.com.

This website provides contact information and details about the products, services, and support that Micro Focus offers.

Micro Focus online support provides customer self-solve capabilities. It provides 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 support website to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Access the Software Licenses and Downloads portal
- Download software patches
- Access product documentation
- Manage support contracts
- Look up Micro Focus support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require you to register as a Passport user and sign in. Many also require a support contract.

You can register for a Software Passport through a link on the Software Support Online site.

To find more information about access levels, go to https://softwaresupport.softwaregrp.com/web/softwaresupport/access-levels.

Contents

Installation and Setup Guide

Introduction

This Content Manager installation and setup guide describes Content Manager and the process of installing, upgrading, removing, configuring and backing up Content Manager and its core components and data.

Even if you are familiar with Content Manager (TRIM, Records Manager) from earlier versions, it is recommended you read this guide in its entirety before you set out to deploy Content Manager.

Audience

This guide assumes you are qualified IT support personnel with extensive knowledge of Microsoft Windows and the client server architecture, and system administrator with a sound understanding of Windows Services and Group Policy.

Chapters Summary

Chapter 2 describes Content Manager, its architecture and components.

Chapter 3 gives a broad overview of the installation process and its requirements.

Chapter 4 contains step-by-step instructions for the different installation types.

Chapter 5 is about upgrading Content Manager.

Chapter 6 is about removing Content Manager from a computer.

Chapter 7 is about the network users group and the Content Manager Services account.

Chapter 8 is about backing up and restoring your data.

Appendix A lists the steps you need to take to create a working Content Manager system.

Appendix B is about installing and setting up Thin Office integration.

Appendix C contains troubleshooting tips.

Appendix D is about Content Manager Render configuration.

Appendix E is about a database for demonstration purposes.

Appendix F is about the user setup executable.

Appendix G is about Geographical Information System (GIS) Data Integration.

Appendix H is about installing and setting up Media Server.

Appendix I is about upgrading SQL Server connection strings.

Appendix J is about special database configurations.

Related Documents

- **CM9.3_Spec.pdf** for system specifications and requirements
- **TRIMEnterpriseStudio.chm** for post-installation dataset and server configuration and maintenance
- Content Manager Help file **TRIM.chm** for post-installation system setup

About Content Manager

Content Manager architecture

Content Manager is a multi-tiered application with a number of server-side components that are scalable and extensible.

A multi-tier application is an application that uses more than two tiers or layers between user and data.

Advantages of a multi-tier architecture:

- Reduction of network traffic
- Reduction of the effects caused by network latency
- Reduction of the load on the database server
- Spreading of the processing workload (load balancing)

The Content Manager architecture utilizes a server component that runs as a Windows service. Communication between the server and the clients takes place over TCP connections, using Windows Active Directory for authentication and encryption.

An organization with multiple branches can run a wide area network (WAN) to allow functionality for all branches while centralizing management functions such as backup and disaster recovery.

The typical deployment model is to put a Workgroup Server in each branch and the database and store in a central location. The WAN then acts only as the conduit to update the metadata about documents. The Workgroup Server's cache, other defined items and the authoritative document are stored centrally.

Content Manager contains the option to use a Workgroup Server on the database LAN for querying the dataset, whereas updates to the database would still use the Workgroup Server on the WAN. Especially for organizations using Oracle RDBMS, this can lead to significantly better performance for searches.

Workgroup Server

The Workgroup Server is the key component in the Content Manager architecture for:

- Supporting client connectivity
- Providing connections to
- primary database

- content index
- document stores

Workgroup Servers do the bulk of the work in a networked installation of Content Manager and should be positioned in your network to provide distribution of load.

The main tool to administer your Content Manager Workgroup Server and the other Content Manager server and dataset components is Content Manager Enterprise Studio, which installs with the Workgroup Server installation.

Content Manager supports database and object replication and Workgroup Servers enable local users to connect with locally replicated databases and document stores to reduce the impact of the system on network bandwidth.

Clients connect to a named primary Workgroup Server; you can also configure a secondary Workgroup Server for the event that the connection to the primary server fails.

There is no limit to the number of Workgroup Servers within the system; you can use additional Workgroup Servers for load balancing and performance tuning to improve the speed of access to the database for remote users.

The Workgroup Server performs the following functions:

- Managing connections to the database
- Local caching of some of the control tables
- Local caching of documents, email and other objects from the electronic document stores
- Event processing

  Events are actions that can be processed in bulk at specific times or continuously.

Content Manager events include:

- Document content indexing
- Word indexing
- Schedule event triggers
- Mail notification
- Audit log
- Billing log
- User defined events

Web Client

Content Manager Web Client is a zero footprint, platform independent Web application.

Client

The Content Manager client contains all the functionality to manage the Content Manager application including the client interfaces for end users, records managers and system administrators.

The client installation includes the features:

- Standard Content Manager sample data – standard report layouts, noise words, postcodes and web publisher layouts in **C:\Micro Focus Content Manager\Standard Data**.
- Content Manager Image Scanner – a scanning application which enables you to scan documents, images etc. and check them directly in to Content Manager.

  Not available for 64-bit installation.

  > **IMPORTANT:** Before running Content Manager Image Scanner on client machines, you will need to register TRIMSDK.dll, which can be found in the CM installation path.
  > To register the COM SDK, you need to run a Windows Command Prompt with elevated rights, set your directory to where Content Manager is installed and run the COM registration program as follows:
  > **regsvr32 trimsdk.dll**

- Content Manager Lotus Notes integration - to integrate Content Manager with Lotus Notes mail clients.

  The Lotus Notes add-in integration file **TSJLNInst.nsf** installs to **C:\Micro Focus Content Manager**.

  Not available for 64-bit installation.

  > **IMPORTANT:** Before running and configuring the Lotus Notes integration on client machines, you will need to register TRIMSDK.dll, which can be found in the CM installation path.
  > To register the COM SDK, you need to run a Windows Command Prompt with elevated rights, set your directory to where Content Manager is installed and run the COM registration program as follows:
  > **regsvr32 trimsdk.dll**

- Content Manager DataPort - Content Manager's data import/export utility for administrators.

Content Manager Desktop

- Content Manager Desktop enables users below administrator level to access the Content Manager search and edit functions without having to use the full Content Manager client.

Dataset

A Content Manager dataset represents a full document and records management system with all the data elements, record objects and repositories.

The dataset consists of a database component on a Relational Database Management System (RDBMS) and a storage component on any storage device on the network.

Each dataset exists independently of others. There is no communication or connection between datasets. You can use the client software to switch between different datasets while server components manage multiple datasets simultaneously.

The dataset contains record metadata and pointers to the electronic documents in the electronic document stores.

Content Manager datasets are stored in a back-end database. This database contains all the information that is unique to the dataset.

Content Manager works with SQL Server, PostgreSQL and Oracle. In order to demonstrate Content Manager, using the supplied Demonstration dataset (DemoDB), you will require SQL Server or SQL Server Express. See **CM9.3_Spec.pdf** for supported RDBMS versions.

Electronic document stores

The electronic document stores are where the electronic files are stored.

The document stores can be in any location to which you can map a UNC path.

You can also use a pool of document stores to enable handling of large amounts of data, run the store unattended for long periods of time and improve store and storage efficiency.

You can also use external stores and use Manage in Place to manage retention in external stores using the IDOL CFS connector framework.

Documents that cannot be added to a store because of a hardware or network failure are stored in a folder to process them later using the Content Manager client.

Document content index

Document content indexing in Content Manager is powered by Micro Focus Intelligent Data Operating Layer (IDOL). See **CM9.3_IDOL_DCI_Install_Config.pdf** for information about installation and configuration of the Content Manager CFS connector for IDOL, and configuring document content indexing.

Service API

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

For more information, see **CM9.3_ServiceAPI.pdf** on your installation media.

Relational Database Management System (RDBMS) requirements

See the Content Manager Specifications and Limitations document **CM9.3_Spec.pdf** on the installation CD or in your installation folder's **Documentation** folder for detailed RDBMS requirements.

RDBMS resource allocation and management

Ongoing dataset storage

As a rule of thumb, the space necessary to store the Content Manager metadata should be equal to the number of records times 5000, expressed in bytes.

For example, if your site anticipates storing 100,000 items, then you will need to allocate 500MB.

However, you should allow room for growth.

Additionally, you need to allocate space to store electronic documents - for example, word processing files, email messages, spreadsheets, etc. - in your document stores and for the document content index.

The space required to store electronic documents in your document stores depends on the amount of electronic document data in the dataset.

For sizing requirements for your document content index, see Document Content Index in Content Manager Enterprise Studio Help.

Storage Files for database objects

Each type of database we support has a default storage file for all its database objects. Content Manager allows users to allocate the database tables and indexes into separate storage files. Although it's not mandatory to separate out these database objects, it can helpful in the situations of where space is limited or for redundancy.

To utilize, use the database-specific administration tool to create these separate storage files. Then you will be able to select them when creating the dataset in Content Manager Enterprise Studio.

For Oracle:

These storage files are defined and identified by tablespaces. The default tablespace is called USERS. The login specified for Oracle will require permissions on the tablespaces to be used by Content Manager.

For Microsoft SQL Server:

These storage files are defined and identified by filegroups. The default filegroup is called PRIMARY.

For PostgreSQL:

These storage files are defined and identified by tablespaces. The default tablespace is called PG_DEFAULT.

About Content Manager Installation

Installation media

You will find the installation files on the installation media.

Media file structure:

- Content Manager - root folder with:
  - **EULA**, **Version**, **ReadMe** and **Contents** files
  - **32BitInstalls** – folder with 32-bit installation files, includes **Setup_CM_x86.exe** file, .msi files and required prerequisite files.
  - **64BitInstalls** – folder with 64-bit installation files, includes **Setup_CM_x64.exe** files, .msi files and required prerequisite files.
  - **Additional Installations** – folder with additional .msi files, e.g. CM_Kofax_x86.msi
  - **Demonstration Database** – folder with demonstration database
  - **Documentation** – folder with documentation
  - **Sup_CD** – folder with CD icon files

> **NOTE:**
> All applications should be closed on the computer before installing Content Manager software
>
> - When an application is running that conflicts with the installation - for example, Microsoft Word - the installation process either attempts to close it or displays a warning message advising you to close the application
> - If you are using the silent installation method, the application cannot be closed and the message to close this program will not appear. This should not be a problem, as silent installations generally run on startup and no programs will be running.
> - Content Manager installations using **Setup_CM_xNN.exe** or **.msi files** do not create a system restore point. If you require a system restore point, create one manually before installation.

Content Manager environment

- Content Manager is a key desktop application. By design, Content Manager should be installed on each computer on a per-machine basis.
- Content Manager's functionality can only be fully realized when it is integrated with other key desktop applications such as word processors, mail systems, spreadsheet applications etc.
- All Content Manager documentation assumes that you followed the recommended method of deployment.

> **NOTE:** Contact software support group or your national distributor if you have difficulty installing Content Manager or for further explanation of any features or functions that may not be fully detailed in either the Content Manager Installation and Setup Guide **CM9.3_Install.pdf**, Content Manager Enterprise Studio Help or Content Manager Help.

Prerequisites

For full specifications and requirements, see **CM9.3_Spec.pdf**.

You must have elevated user rights for any Content Manager installation.

Installation overview

1. Content Manager Workgroup Servers
    a. Determine the layout of your network architecture including the computers that will host the server components of Content Manager.

    > **NOTE:** All required components of Content Manager are installed on each computer for component recognition.
    > During installation, the administrator determines the components to install on each target computer - for example, the Workgroup Server component only on the Workgroup Servers and the client components only on client computers.
    >
    > It depends on the network environment which components to install on each computer.

    b. Ensure that Content Manager supports the server operating system and that it has all the necessary components installed.

    See **CM9.3_Spec.pdf**.

    c. Ensure you have the correct RDBMS client software.

See *RDBMS requirements*.

d. Determine the kind of electronic stores to set up:

- Windows File System
- CFS Connector
- EMC Centera
- Also decide whether to use document store pooling or nominated stores.

  In the Content Manager Help file, see **Creating Document Stores**.

2. Network settings

a. Create the new domain user account that Content Manager will use to create the database and run the Workgroup Servers.

For example, you could call it **CMServices**. See *Network user group and the CM Services account*.

b. Add the user account to the Workgroup Servers.

> **NOTE:** This account must be a member of the local administrators group and should also have the **Log on as a Service** policy assigned.

c. Create and add a user with full access permissions to the administration group for your RDBMS.

d. Create a domain group - the Content Manager user group - and add all the network users that require access to Content Manager, e.g. **CMUsers**.

e. Install the Content Manager components on the appropriate servers.

Find instructions for installing and enabling the components of Content Manager in Network installation.

f. Using Content Manager Enterprise Studio, create the Content Manager dataset.

See Content Manager Enterprise Studio Help – **Creating datasets**.

If you wish to add a dataset for newly supported products such as:

• SQL Server Always On Availability groups

• Azure SQL Server

See Special Database Configurations for details.

g. Add the account to your Content Manager dataset as Location.

User type **Administrator** with **Top security** and **All Caveats** profile is recommended.

In Content Manager Help, see **Creating Locations**.

h. Register the Content Manager Server components as Windows Services.

See Network Users Group and the CM Services Account.

> **NOTE:** For ease of administration, maintenance and secure access, it is recommended you install the Content Manager components as Windows Services.

3. Content Manager client

a. Ensure the client computer has a supported operating system and all the necessary components installed.

See **CM9.3_Spec.pdf**.

b. Install Content Manager on the client computer.

c. Create the user as a Content Manager Location in the dataset.

In Content Manager Help, see **Creating Locations**.

64-bit installation

Install Content Manager in 64-bit environments using the same instructions as for 32-bit environments.

On a 64-bit operating system, 64-bit Content Manager installs to **C:\Program Files**.

On a 64-bit operating system, 64 bit Content Manager uses the same part of the registry as an installation in a 32-bit environment, e.g. **HKEY_LOCAL_MACHINE\Software\Micro Focus**

Installing Content Manager

For Content Manager installation, you have the choice between three methods:

- Network installation for installing or upgrading Content Manager over the network
- *Local installation using Setup_CM_xNN.exe* – for installing or upgrading Content Manager locally on one computer at a time
- *Installation using scripts*, for installation over the network or locally

For maintenance installations, use the same method you used to install Content Manager on the computer originally.

> **NOTE:** When installing Content Manager using **Setup_CM_xNN.exe** all of the required MSIs, that is, the MSIs for the Features being installed, must be copied to the same location that **Setup_CM_xNN.exe** is being run from, or it can be run directly from the **Content Manager_ CDImage ISO**, which has the MSIs in the same location by default.

> **NOTE: Setup_CM_xNN.exe** can be run with command line switches. To display a help dialog showing the available switches, run Setup_CM_xNN.exe -h

When installing Content Manager, the Service account configuration username must follow the Rules for Logon Names as per Microsoft's specifications *https://msdn.microsoft.com/en-us/library/bb726984.aspx* which includes a list of invalid characters for Logon names, " / \ [ ] : ; | = , + * ? < >

> **IMPORTANT:** After installing Content Manager, the **Content Manager Workgroup Service** must be started manually.

Network installation

This is the most common installation for most organizations.

Content Manager is an essential desktop application and therefore, you should install it on a per-machine basis using Group Policy.

Network installation prerequisites

- A system administrator with a sound understanding of Windows Services
- You must have administrator or elevated access rights for the target computers

> **NOTE:** The domain account running the Content Manager services must have the Log on as a service policy assigned.

Network installation steps

1. Follow the steps in *Administrative installation*
2. Follow the steps in *Group Policy installation*

   -- or –

   Follow the steps in *Installation using scripts*
3. After completing the installation, continue setup by working through Appendix A *Steps to Setting up a Working System*

Administrative installation

Overview

1. Perform an administrative installation and set the desired properties using the command line
2. Using Group Policy, use the **.msi** file that was saved to the administrative install point to install Content Manager on the target computers.

   If you are not using Group Policy, use a script file to run the **.msi** file which was copied to the administrative installation point.
3. This file will use the properties you selected during the administrative installation.

Administrative installation steps

1. Open a command prompt as administrator, for example, by right-clicking it in the **Start** menu, and then clicking **Run as administrator**
2. Enter one of the example command lines, and edit it to suit your needs in the next step, before pressing **ENTER** for either:
   - x86 installation, for which only the client feature is supported:

     msiexec /a "C:\Users\username\Desktop\CM_x86.msi" /q /l*vx "C:\Users\username\Desktop\Install_Log86.txt" TARGETDIR="C:\CMEnterpriseInstall\" ADMININSTALLDIR="C:\Program Files\Micro Focus\Content Manager" ADDLOCAL=HPTRIM,Client HPTRIMDIR_ADMIN="C:\Micro Focus Content Manager" PRIMARYURL="PrimaryWorkgroupURL:PortNo" SECONDARYURL="SecondaryWorkgroupURL:PortNo" DEFAULTDBNAME="DemoDB"

DEFAULTDB="45" TRIM_DSK="1" TRIMREF="DSK" STARTMENU_FOLDER_ ADMIN="Content Manager" AUTOGG="1" WORD_ON="1" EXCEL_ON="1" POWERPOINT_ON="1" PROJECT_ON="1" OUTLOOK_ON="1" AUTHMECH="0"

- x64 installation, for which all features are supported and included in this example:

  msiexec /a "C:\Users\username\Desktop\CM_x64.msi" /q /l*vx "C:\Users\username\Desktop\Install_Log.txt" TARGETDIR="C:\CMEnterpriseInstall\" ADMININSTALLDIR="C:\Program Files\Micro Focus\Content Manager" ADDLOCAL=HPTRIM,Client,Server,TRIMWORKGROUP,IDOLALL,EMAILMANAGER HPTRIMDIR_ADMIN="C:\Micro Focus Content Manager" PRIMARYURL="PrimaryWorkgroupURL:PortNo" SECONDARYURL="SecondaryWorkgroupURL:PortNo" DOMAINNAME="domain" SERVICEUSER="serviceusername" SERVICEPASS="serviceuserpassword" DEFAULTDBNAME="DemoDB" DEFAULTDB="45" TRIM_DSK="1" TRIMREF="DSK" STARTMENU_FOLDER_ADMIN="Content Manager" AUTOGG="1" WORD_ON="1" EXCEL_ON="1" POWERPOINT_ON="1" PROJECT_ON="1" OUTLOOK_ON="1" AUTHMECH="0"

3. Edit the command to suit your needs, for example the properties:
   - **C:\Users\username\Desktop\CM_x64.msi** - .msi file location
   - **C:\Users\username\Desktop\Install_Log.txt** – installation log file location and name
   - **TARGETDIR** – location of unpacked .msi file, and where the Group Policy Object (GPO) will need to be pointed for a subsequent Group Policy installation
   - **ADMININSTALLDIR** – final installation directory to which Content Manager will be installed during Group Policy installation
   - **ADDLOCAL** – installs the features listed, which must be separated by commas:
     - **HPTRIM** – core libraries. Required.
     - **Client** - client features, which include Image Scanner, Lotus Notes integration add-in, standard sample data, and DataPort import and export tool
     - **Server** – server features – only available for x64 installations
     - **TRIMWORKGROUP** – Content Manager Workgroup Server.
     - Only available for x64 installations.
     - **IDOLALL** – include this property if IDOL components are already installed and you want to reinstall them. If you chose not to continue to use IDOL, this property can be left out and the IDOL components will not be installed.

    - **EMAILMANAGER** - installs the Automated Email Management service, a utility to import emails into Content Manager that have been journaled and deposited into a nominated folder

- **HPTRIMDIR_ADMIN** – data folder for server data. See also *Data Folder*. The MSI Property, HPTRIMDIR_ADMIN, sets the folder which is used to store server logs and configuration data, as well as client side features, such as Report Templates and Directory Synch staging folders. If this property is not set, the installer will choose a default location and this will be on the disk volume that has the largest amount of free space. If an installation is carried out using a command line or a batch file script, this property must be set explicitly if the default behavior is undesired.
- **PRIMARYURL** – type a URL, hostname or IP address of the Workgroup Server. Optionally, type in the Port Number the client should use to connect to the Workgroup Server. This should be separated from the Workgroup Server URL by a colon (:). If this is left blank, it will default to 1137.
- **SECONDARYURL** – type a URL, hostname or IP address of the Secondary Workgroup Server. Optionally, type in the Port Number the client should use to connect to the Workgroup Server. This should be separated from the Workgroup Server URL by a colon (:). If this is left blank, it will default to 1137.
- **DOMAINNAME** – network domain name
- **SERVICEUSER** – the user account that you created to run the Content Manager services, which must have the Log on as a service policy assigned, for example, **RMServices**
- **SERVICEPASS** – the services account password
- **DEFAULTDBNAME** – your default Content Manager dataset name
- **DEFAULTDB** – your default Content Manager dataset ID
- **TRIM_DSK** – desktop shortcuts
    - **1** to install

      Leave out the property to not install desktop shortcuts
- **TRIMREF** – application to use for Content Manager reference files (***.tr5**)
    - **TRIM** – Content Manager
    - **DSK** – Content Manager Desktop
- **STARTMENU_FOLDER_ADMIN** – Windows **Start** menu folder under which Content Manager programs appear

- **AUTOGG** – global settings
  - **1** – to use global settings for users
  - Leave this property out of the command line to not use global settings for users
- **WORD_ON** – Microsoft Office Word integration
  - 1 – enables Word integration
  - **0** - for no integration
- **EXCEL_ON** – Microsoft Office Excel integration
  - **1** – enables Excel integration
  - **0** - for no integration
- **POWERPOINT_ON** – Microsoft Office PowerPoint integration
  - **1** – enables PowerPoint integration
  - **0** - for no integration
- **PROJECT_ON** – Microsoft Office Project integration
  - **1** – enables Project integration
  - **0** - for no integration
- **OUTLOOK_ON** – email integration
  - **1** – Content Manager in Outlook
  - **0** - for no integration
- **AUTHMECH** – authentication mechanism
  - **0** – Integrated Windows Authentication
  - **1** – Explicit Windows Authentication
  - **2** – ADFS Authentication
  - **3** – Google Apps Authentication

> **CAUTION:**
> You can also use the following properties in the command lines, which enables you to set specific locations for the corresponding Content Manager data folders, for example, if you needed them to be in users' H:\ drives for some reason.
>
> However, changing these data folder locations is not recommended.

> By not including those properties in the command line, the installer uses user-specific paths on each computer.

USER_LEX_FOLDER_ADMIN – installation location of the Content Manager user dictionary

CLIENT_APPDATA_FOLDER_ADMIN – the location of Content Manager data files

CLIENT_LOCAL_APPDATA_FOLDER_ADMIN – the location of Content Manager data files.

OFFLINE_DATA_FOLDER_ADMIN – the location of Content Manager offline data files

4. Press **ENTER**.

   The **.msi** file for installation using Group Policy has been created in the target directory as **CM_x86.msi** or **CM_x64.msi**.

5. To continue with installing the generated .msi file using Group Policy, see *Group Policy installation*

Group Policy installation

1. You must have carried out the steps described in *Administrative installation* before installing Content Manager through Group Policy.
2. Use Group Policy to install the configured .msi package on the target computers:
   a. Content Manager Workgroup Servers
   b. Content Manager clients

> **NOTE:** One advantage of a Group Policy rollout is that the installation runs with elevated access rights on the target computer and all repairs or modifications to the installation on the target computer run with elevated access rights.

Installing Web applications by using MSI files

Content Manager Web applications and services cannot be installed as features of the main Content Manager .msi files. They have their own .msi files that you need to use to install them. These are:

- Web Client – **CM_WebClient_x64.msi**
  For an example script, see *Installing Web Client using a script*.
- Service API – **CM_Service_API_x64.msi**.
  For an example script, see *Installing Service API using a script*.
- WebDrawer – **CM_WebDrawer_x64.msi**.
  For an example script, see *Installing WebDrawer using a script*.

Alternatively, use **Setup_CM_x64.exe**, in which all the above are available as features.
See *Local installation using Setup_CM_xNN.exe*.

Installing Content Manager without using Group Policy

To install Content Manager without using Group Policy, for example, on a local single computer, you need to either:

- Use **Setup_CM_xNN.exe** for your computer's architecture – see *Local installation using Setup_CM_xNN.exe*
- Create a script to use an .msi file to install Content Manager silently in the background, without dialog boxes or other user interaction – see *Installation using scripts*

Local installation using Setup_CM_xNN.exe

Installation Notes

- When installing Content Manager using **Setup_CM_xNN.exe** all of the required MSIs, that is, the MSIs for the Features being installed, must be copied to the same location that **Setup_CM_xNN.exe** is being run from, or it can be run directly from the **Content Manager_CDImage ISO**, which has the MSIs in the same location by default.
- When installing Content Manager using **Setup_CM_xNN.exe** there will always be more than one entry in the Windows **Control Panel → Programs and Features** panel. To ensure all entries are properly removed when uninstalling, **Setup_CM_xNN.exe** should be used to uninstall Content Manager, if it was used for the installation. Similarly, if an MSI was used to install the product, it should be used to uninstall it.
- The size displayed in the Windows **Control Panel → Programs and Features** panel for the Content Manager xNN entry is the estimated size of a full installation, comprising of all Content Manager components, regardless of if they were installed or not.
- **Setup_CM_xNN.exe** will attempt to download missing prerequisites, for example, .NET Framework, as a result, customers should ensure internet access is available during the installation otherwise errors will be encountered. If access to the internet cannot be established, ensure all documented prerequisites are installed prior to installing Content Manager.
- When installing using **Setup_CM_x86.exe** the installation will install the Data Folder to the drive that has the largest capacity available. If there is a requirement to install this directory to a specific drive, then use the command line installation option.If the installation has been done using **Setup_CM_x86.exe** the Data Folder can be manually moved and then change the registry entries under **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Micro Focus\Content Manager** to reflect the new path.

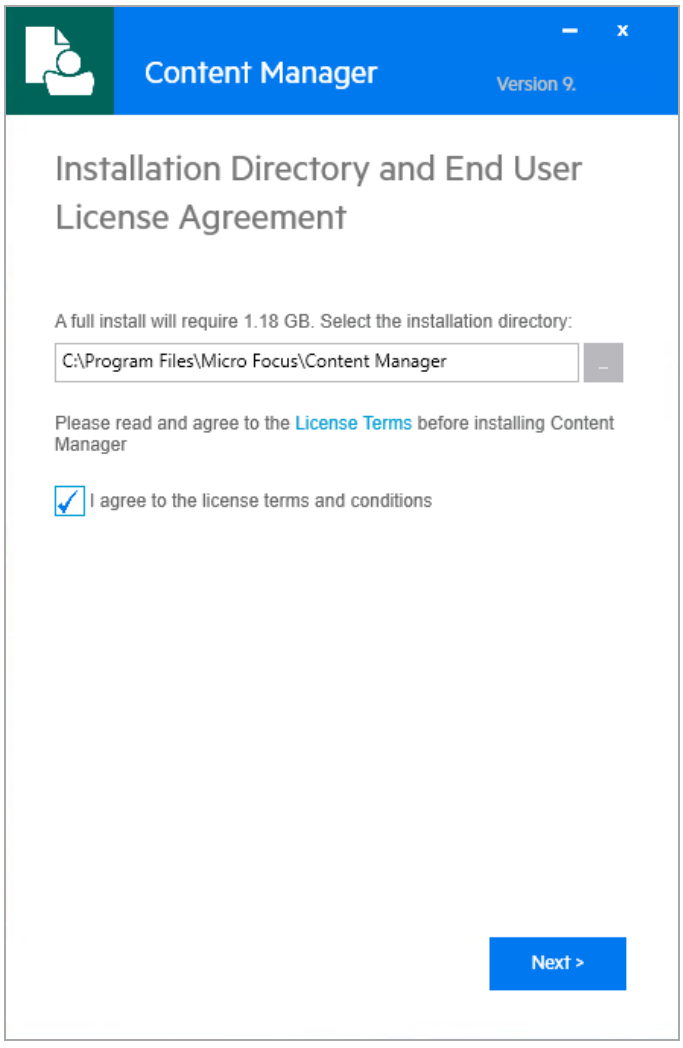
Installation Steps

1. Run the relevant installation file **Setup_CM_xNN.exe** using **Run as administrator.**
   It depends on your selections which dialogs and options appear.

   If the installation is run without Administrator privileges an error will be displayed, prompting you to run the installation using **Run as administrator**.

   > **NOTE:** Server features are not supported on 32-bit computers.

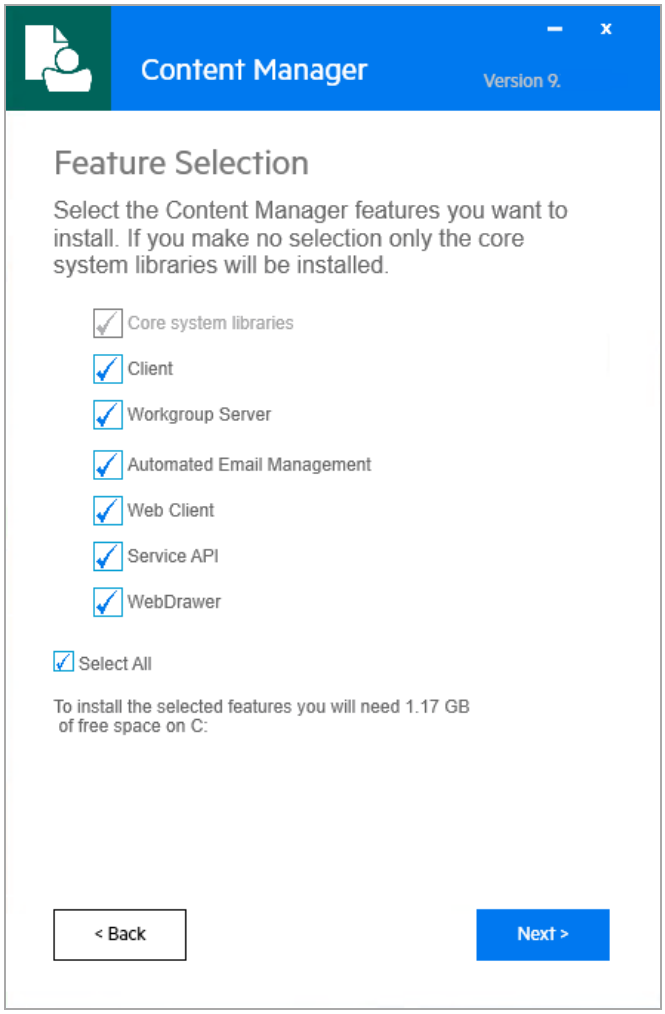
   The **Installation Directory and End User License Agreement** dialog appears:



2. Select the installation folder.
   The default is **C:\Program Files\Micro Focus\Content Manager**, and it is recommended to use the default folder.

3. Select **I agree** to the license terms and conditions, and then click **Next**.

   The **Feature Selection** dialog appears:



4. Select the features and click **Next**. Content Manager installs all necessary prerequisites.

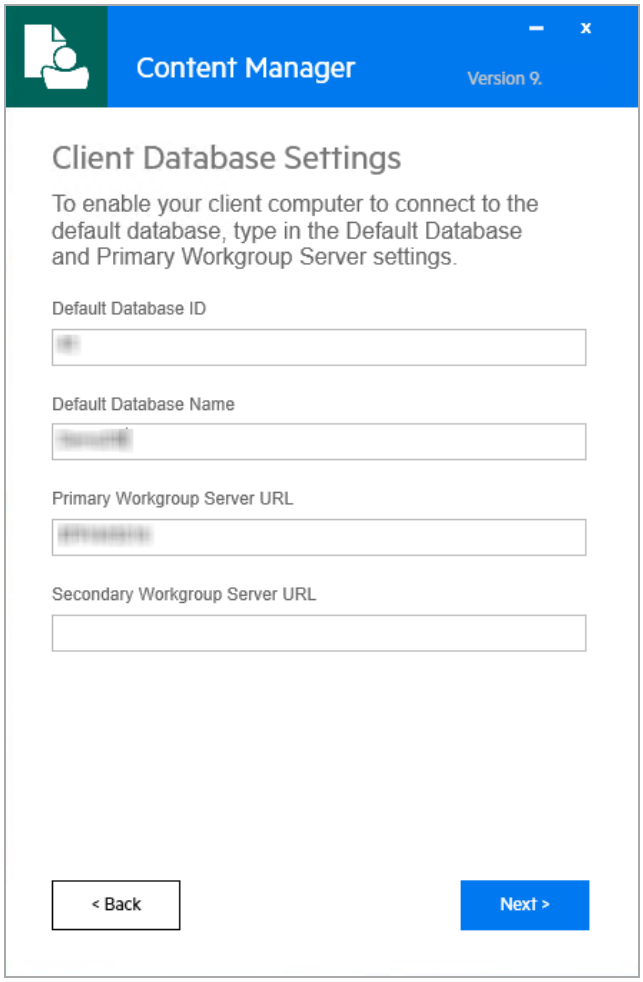
   - **Core system libraries** – required for all new installations
   - **Client** – installs the client features. See *Client*.
   - **Workgroup Server** – installs and registers an Content Manager Workgroup Server and Content Manager Enterprise Studio on this computer. See *Workgroup Server*.
   - **Automated Email Management** – installs the Automated Email Management service, a utility to import emails into Content Manager that have been journaled and deposited into a nominated folder.

- **Web Client** – installs a zero footprint, platform independent Content Manager web application. See *Web Client*. Also see **CM9.3_Web-Client-Install.pdf** for post installation configuration steps.
- **Service API** – to install the Content Manager Service API. See *Service API*. For additional information see **CM9.3_ServiceAPI.pdf** for details, as well as the installed ServiceAPI help files.
- **WebDrawer** – to install the web application WebDrawer, which provides read-only access to Content Manager records. See also **CM9.3_WebDrawer.pdf**.

> **IMPORTANT:** If you're *upgrading* Content Manager using **Setup_CM_xNN.exe** on an environment that has the IDOL Services installed, the **Feature Selection** dialog will include a **IDOL Main Service (OEM)** option. If you wish to continue to use IDOL after upgrading, select this option.

5. Click **Next**.

   The **Client Database Settings** dialog appears:



6. Use this dialog to set up your Content Manager client to Workgroup Server default connection settings.

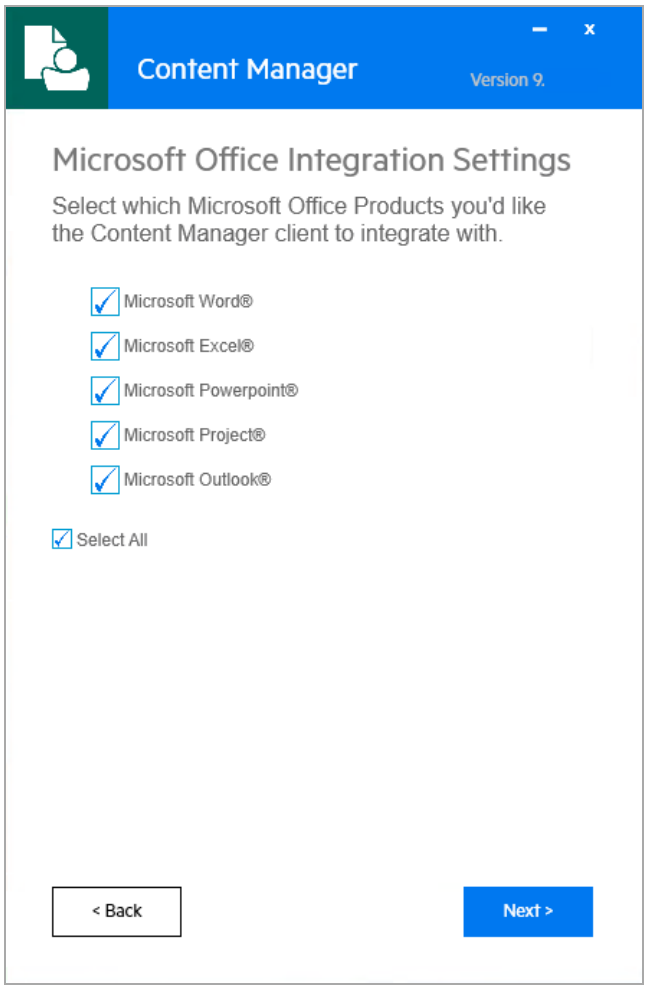
   You can change these settings after installation using the Content Manager client.

   - **Default Database ID** - the unique identifier for the dataset to which the client should connect. Use Content Manager Enterprise Studio to create the dataset and its ID.
   - **Default Database Name** – name of database, for example, **companyDB**
   - **Primary Workgroup Server URL** – type a URL, hostname or IP address of the Workgroup Server. Optionally, type in the Port Number the client should use to connect to the Workgroup Server. This should be separated from the Workgroup Server URL by a colon (:). If this is left blank, it will default to 1137.
   - **Secondary Workgroup Server URL** – type a URL, hostname or IP address of the Secondary Workgroup Server. Optionally, type in the Port Number the client should use to

connect to the Workgroup Server. This should be separated from the Workgroup Server URL by a colon (:). If this is left blank, it will default to 1137.

7. Click **Next**.

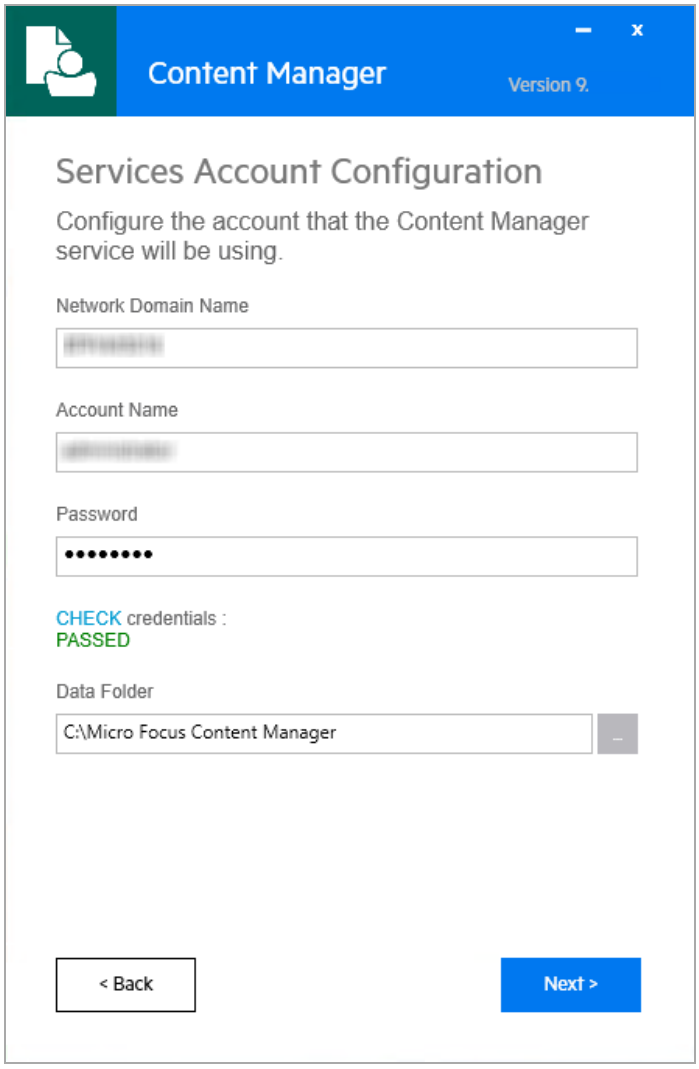
   The **Microsoft Office Integration Settings** dialog appears:



8. Select the MS Office products to integrate with Content Manager client.
   This enables you to open and save documents in these applications directly from and to Content Manager.

9. Click **Next**.

   The **Services Account Configuration** dialog appears:



10. Type the domain name and the user details for the Content Manager services user account. Content Manager uses the information from this dialog to configure the access permissions set up in your Content Manager environment and provide the necessary access to users.
The Content Manager Servers are installed and registered as Windows Services.
The account to run the services, for example, **CMServices**, must have the policy Log on as a service assigned.

- **Network Domain Name** - type the domain name on which the Content Manager services will be running

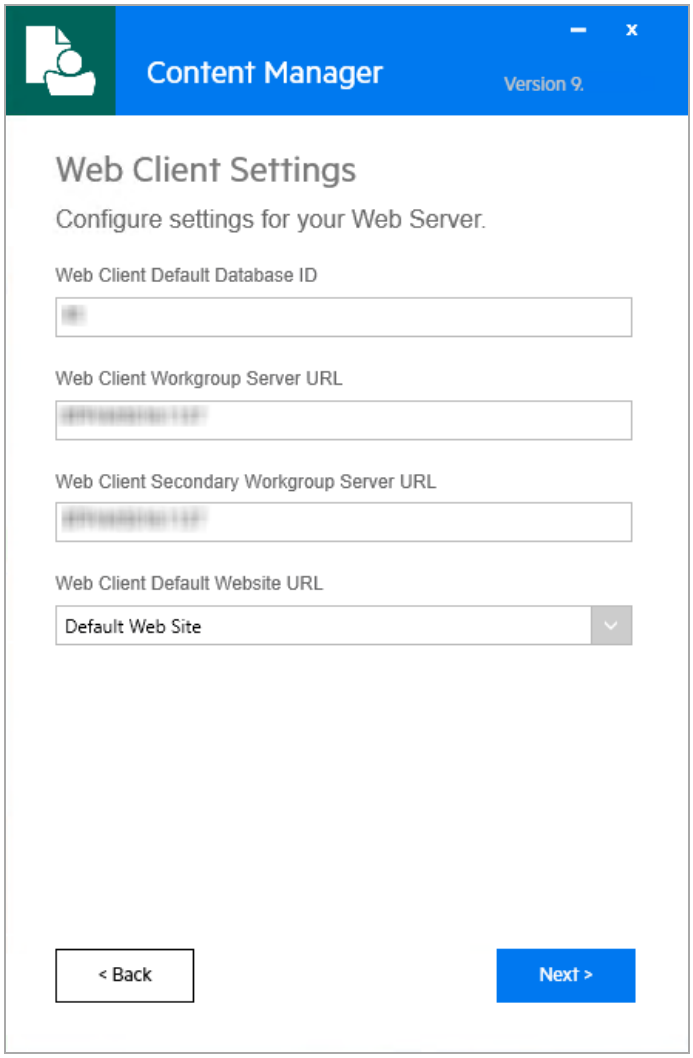
> **NOTE:** If you intend to use a local user to run your services:
>
> a. Type the name of your computer in the **Domain Name field**

b. Specify a local user in the **User Name** field to run your Content Manager services.

- **Account Name** - type the name of the account that you created to run the Content Manager services, for example, **CMServices**.
  The Content Manager Workgroup Service and WebDrawer Service log on with this account. This account also has access permissions to the Content Manager Workgroup Server.
- **Password** - type the password for the services account
- **Check credentials** – click to check that you entered an account with correct user name, password and credentials. A notice appears: **Passed or Failed**.
- **Data Folder** – it is recommended to keep the default, **C:\Micro Focus Content Manager**. Installation folder for the folders:
  - **ServerData** – Workgroup Server data folder
  - **ServerLocalData** – Workgroup Server log files folder
  - **ServiceAPIWorkPath** – Content Manager Service API folder
  - **Standard Data** – the standard data required by Content Manager, e.g. default Report templates etc.
  - **WebClientWorkpath** – Content Manager Web Client folder
  - **WebDrawerWorkPath** – Content Manager WebDrawer folder
  - **WebServerWorkPath** – Content Manager Web Server folder

11. Click **Next**.

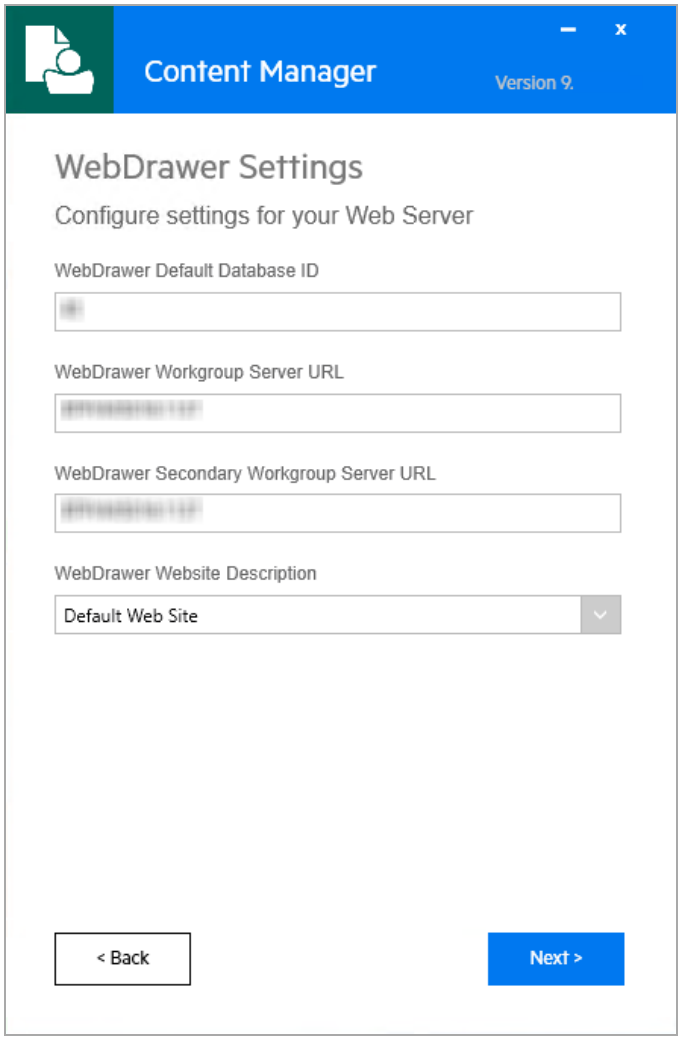
    The **Web Client Settings** dialog appears:



12. Enter the Web client settings:
    - **Web Client Default Database ID**
    - **Web Client Workgroup Server URL**
    - **Web Client Secondary Workgroup Server URL**
    - **Web Client Default Website URL**

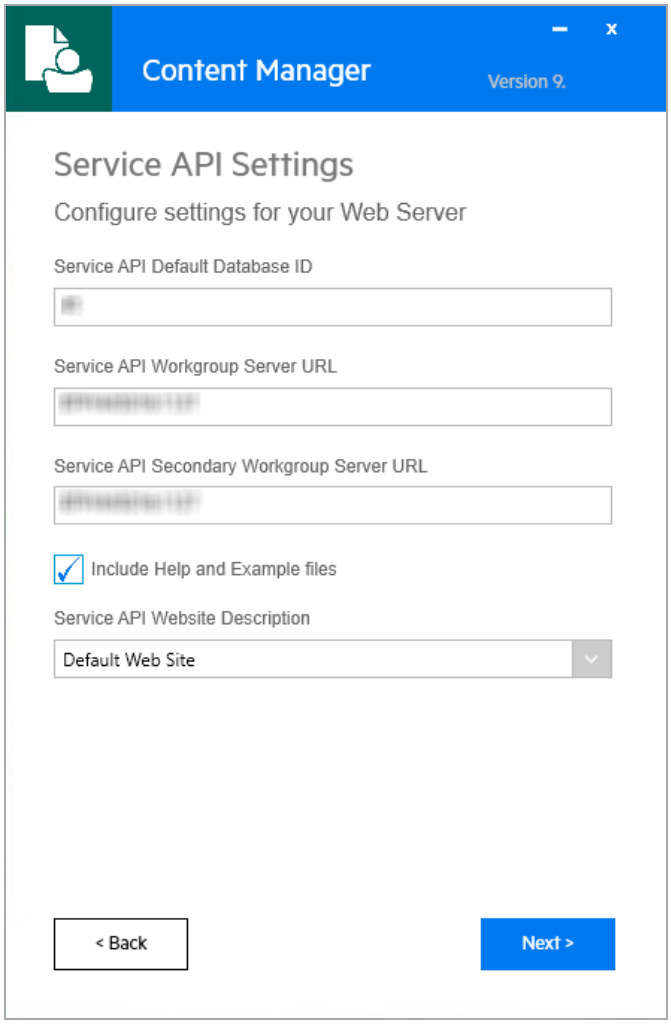
    Also see **CM9.3_Web-Client-Install.pdf** for post installation configuration steps.
13. Click **Next**.

    The **WebDrawer Settings** dialog box appears:



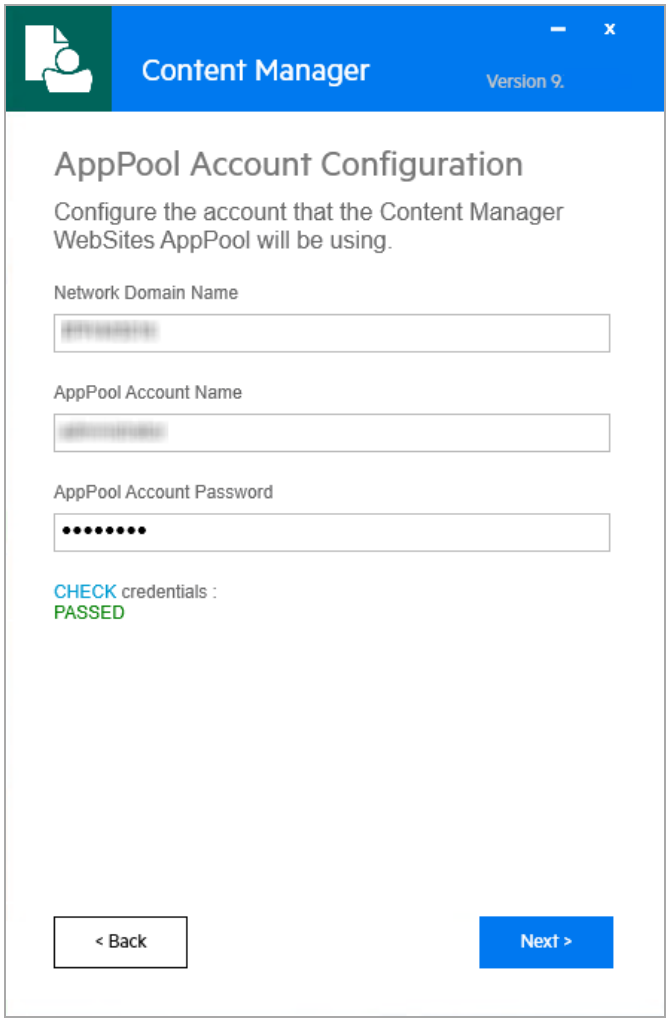
14. Enter the WebDrawer settings:
    - **WebDrawer Default Database ID**
    - **WebDrawer Workgroup Server URL**
    - **WebDrawer Secondary Workgroup Server URL**
    - **WebDrawer Website Description**
15. Click **Next**.

    The **Service API Settings** dialog appears:



16. Enter the Service API settings:
    - **Service API Default Database ID**
    - **Service API Workgroup Server URL**
    - **Service API Secondary Workgroup Server URL**
    - **Include Help and Example files** – clear this option to exclude the ServiceAPI Help and Example files from the installation. It is recommended that these are not installed on a production server. See **CM9.3_ServiceAPI.pdf** for details.
    - **Service API Website Description**
17. Click **Next**.

    The **AppPool Account Configuration** dialog appears:



18. Enter the AppPool account details:
    - **Network Domain Name**
    - **AppPool Account Name**
    - **AppPool Account Password**
    - **Check credentials** – click to check that the account has the required permissions

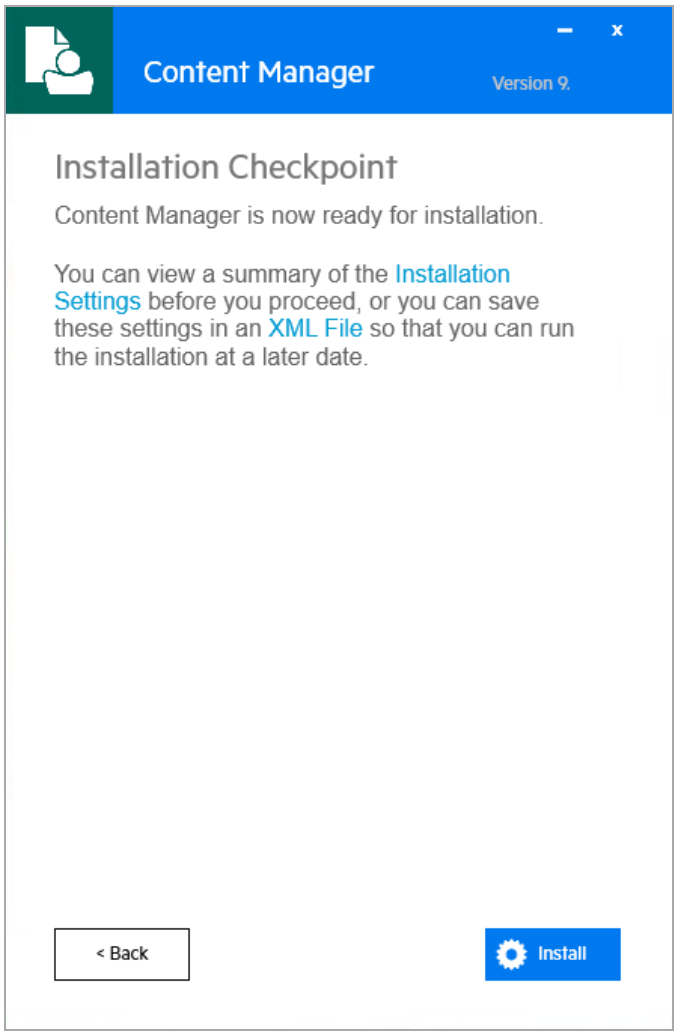
> **CAUTION:**
> If any of the Web applications such as Web Client, ServiceAPI or WebDrawer are being installed, the AppPool account details are mandatory. You will not be able to install the applications if you leave these fields blank.

> **CAUTION:**
> The user account that is used as the identity for the AppPool Accounts requires full

> access rights to the associated Websites workpath folders, for example, C:\Micro Focus Content Manager\ServiceAPIWorkpath; C:\Micro Focus Content Manager\WebClientWorkpath, etc. Insufficient permissions to this folder results in an **Access Violation** error when trying to upload an electronic document to Content Manager.

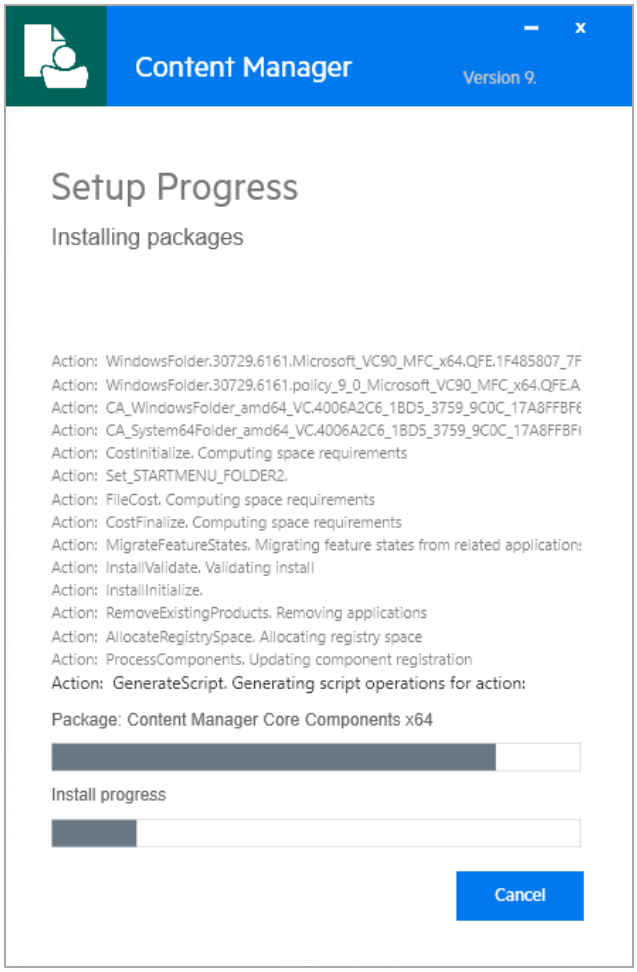
19. Click **Next**.

    The **Installation Checkpoint** dialog appears:

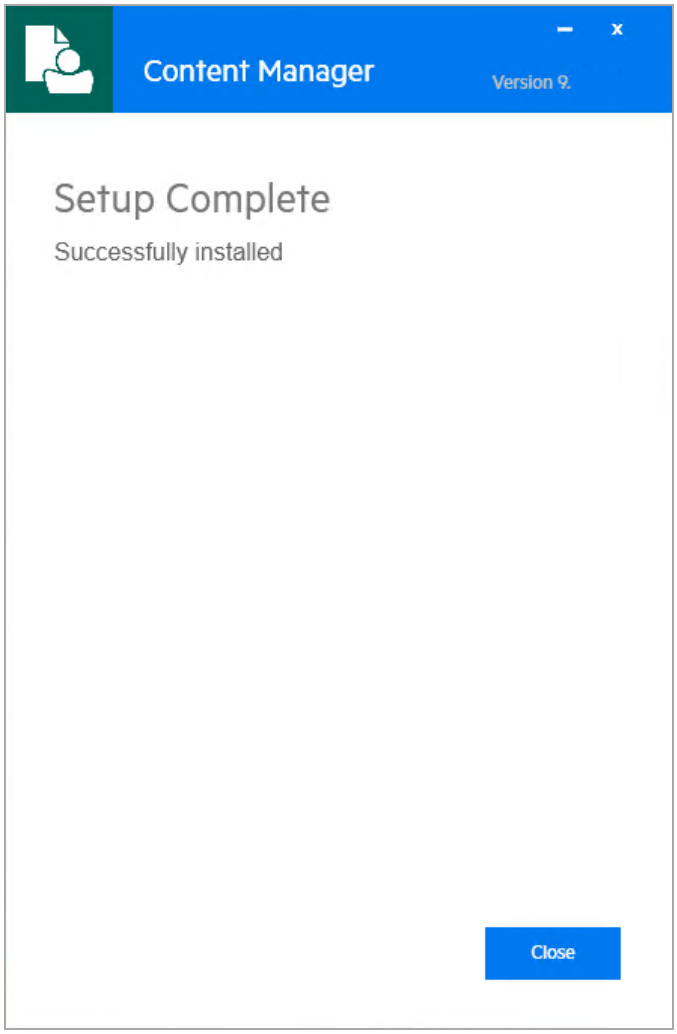


20. Follow the instructions for an installation summary or **.xml** file, and then click **Install** to install the selected features.

    The **Setup Progress** dialog appears:



When the installation is finished, the **Setup Complete** dialog appears:



Your Content Manager installation is complete.

21. Click **Close** to close Content Manager setup.

Setup_CM_xNN.exe log files

The log files created when installing Content Manager using Setup_CM_xNN.exe are written to the user's Temp folder, e.g.C:\Users\<username>\AppData\Local\Temp

The files created depends on the options selected on the Feature Selection dialog when **Setup_CM_xNN.exe** is run. Each file will have a date/time stamp appended to it, as well as the MSI/feature name.

Log files that may be created are:

- Content_Manager_x64_20160526092026_002_hprm64.log – created when the Content Manager Client, WorkGroup Server, IDOL Main Service, IDOL Content Service and/or Render features are selected and installed.

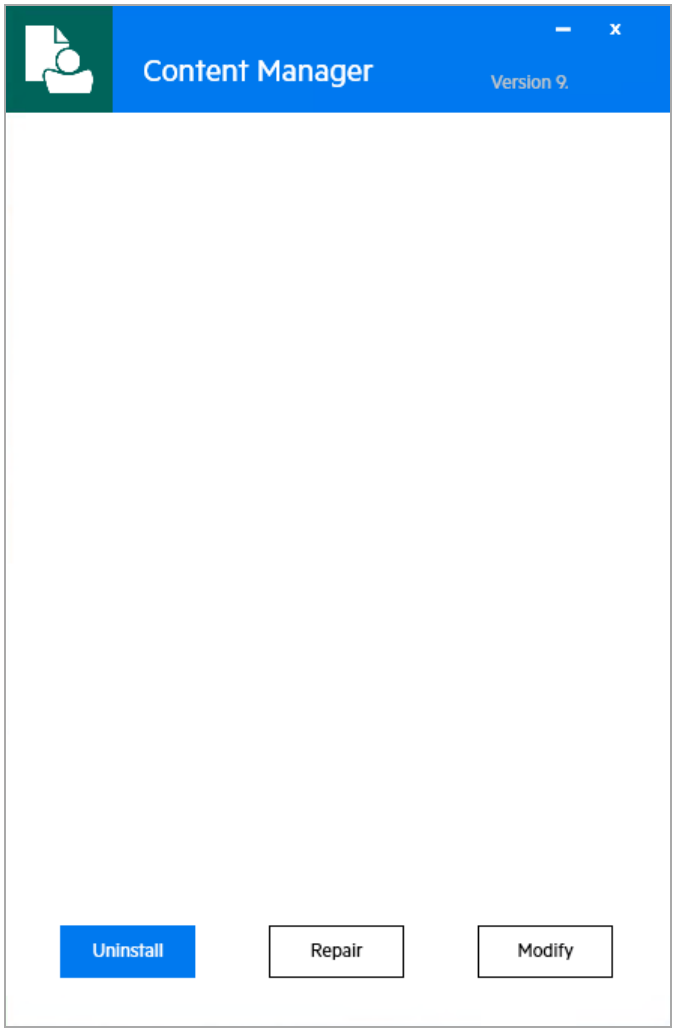
- Content_Manager_x64_20160526092026_004_webclient64.log – created when the Web Client feature is selected and installed.
- Content_Manager_x64_20160526092026_005_serviceapi64.log – created when the ServiceAPI feature is selected and installed.
- Content_Manager_x64_20160526092026_006_webdrawer64.log – created when the WebDrawer feature is selected and installed.
- Content_Manager_x64_20160526092026.log – created when Setup_CM_xNN.exe is run.

Maintenance installation using Setup_CM_xNN.exe

Use a maintenance installation to change the installed features, repair or remove the installation.

1. Using your Windows installation function, select **Content Manager xNN** and click the appropriate **Uninstall** or **Change** button.

   The maintenance dialog box appears:



2. Click one of the options:
   - **Uninstall** - see *Uninstall*
   - **Repair** - see *Repair*
   - **Modify** - see *Modify*

Repair

Repair re-installs only the features which were selected during the installation or the latest modification to the installation.

If you have Content Manager Servers running as services, then you will need to re-type the user password for the services to be re-installed correctly.

Repairing an installation

1. In the maintenance dialog box, click **Repair**.

   The *Setup Progress* dialog appears.

   When finished, the *Setup Complete* dialog appears.

2. Click **Close**.

   The Content Manager installation has been repaired.

Uninstall

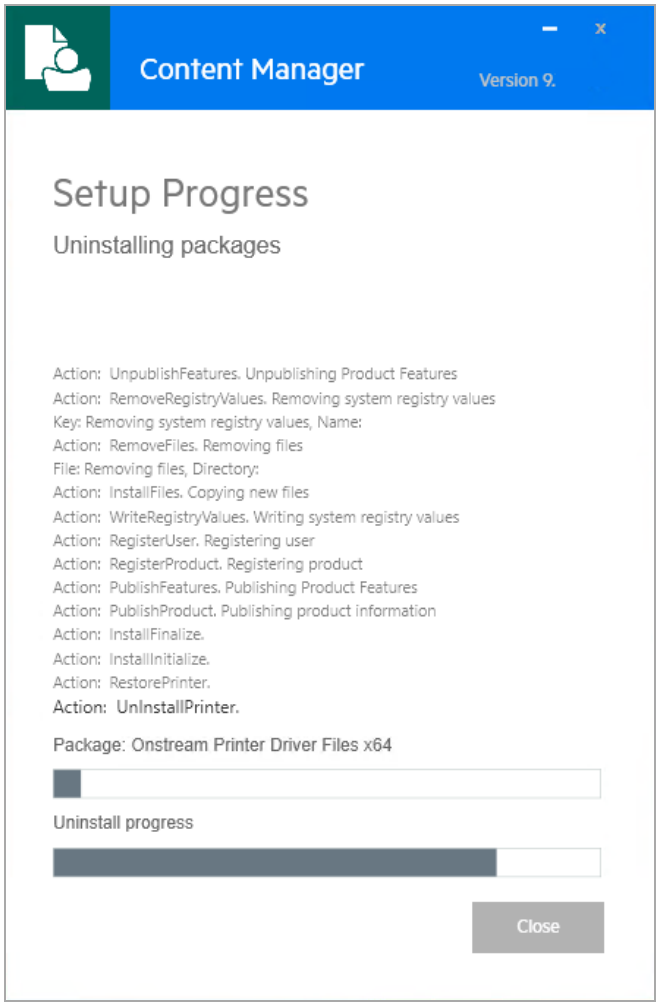
Uninstall removes Content Manager from your computer.

Before removing Content Manager, see *Removing Content Manager*.

Removing an installation

1. In the *maintenance* dialog box, click **Uninstall**.

   The **Setup Progress – Uninstalling packages** dialog appears:



The **Setup Complete – Successfully uninstalled** dialog appears.

2. Click **Close**.

   The Content Manager installation has been removed from the computer.

Modify

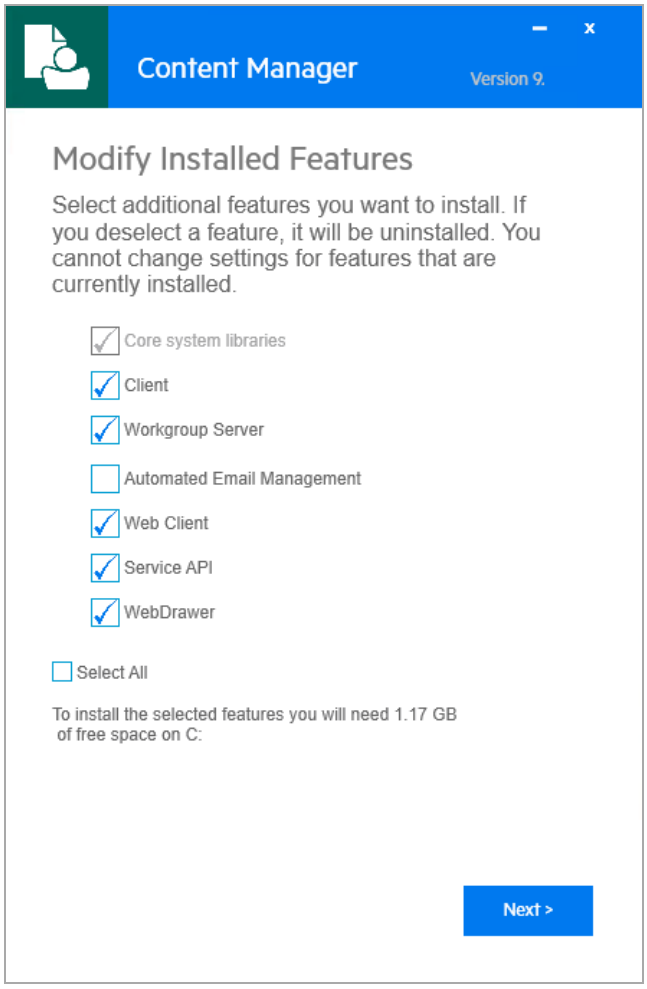
Modify enables you to add or remove Content Manager features.

It will only add or remove the features you choose. It will not perform a full reinstallation.

Modifying an installation

1. In the *maintenance* dialog box, click **Modify**.

   The **Modify Installed Features** dialog box appears:



2. Update the selection of features and click **Next**.

   The **Installation Checkpoint** dialog appears.

3. Follow the instructions for an installation summary or **.xml** file, and then click **Install** to update the feature selection.

   The **Setup Progress** dialog appears, and once the installation is complete, the **Setup Complete** dialog appears.

4. Click **Close**.

   The Content Manager installation has been modified.

Installation using scripts

Installation using scripts is an option to install Content Manager components locally or over the network.

While installation of the main Content Manager components using scripts is very common, there are also a number of **.msi** files for peripheral Content Manager applications on the Content Manager installation media that you need to install using scripts. You will find example scripts and explanations of the script properties for those installations in this section.

> **NOTE:**
> Installations of Content Manager using scripts cannot ensure that the target computer has Group Policy set so that installations run using elevated access rights.
>
> If the installation does not use elevated access rights at all, or only for the installation and not for any post-installation tasks, then these tasks may not complete correctly, for example, self-repair.
>
> If elevated access rights are not available for the target computer, it is recommended that either:
>
> - All users logging on to that computer have sufficient access permissions to perform installation tasks, including writing and deleting files to the Program Files and System32 folders and writing to the registry
>
> or --
>
> - You make the installation functions in the Windows Control Panel ✹ Programs and Features function unavailable.
>
> This will prevent users from performing repairs or modifications to the installation.

When you are using a script to install Content Manager components, all installation properties must be in a single line.

The sample scripts install all the features available with the main installation program by using a script file.

Please note that installation on x86 architecture computers does not support server features.

There are additional properties which are not included in the example scripts, which you will find under *Script properties*.

You can copy the scripts, but to make them work, you will have to change certain values like file locations, or user and computer names.

Example scripts

Installing main Content Manager components using a script

You do not need to use this installation method if you are using Group Policy installation as described in *Group Policy installation*.

1. You must have carried out the steps described in *Administrative installation* before installing Content Manager using a script over a network
2. Create a script according to the installation requirements for the client computers.

The Content Manager **.msi** installation does not support a parameter file; therefore, you must set each property that you want to install on the command line.

3. Run the script on the target computer.

Content Manager installs with the features you selected.

x86 (client only) installation script example

"C:\Users\username\Desktop\CM_x86.msi" /q /l*vx "C:\Users\username\Desktop\InstallBatch.txt" INSTALLDIR="C:\Program Files\Micro Focus\Content Manager\" ADDLOCAL=HPTRIM,Client HPTRIMDIR="C:\Micro Focus Content Manager" DEFAULTDBNAME="DBName" DEFAULTDB="DBID" STARTMENU_NAME="Content Manager" TRIM_DSK="1" TRIMREF="DSK" PRIMARYURL="PrimaryWorkgroupURL:PortNo" SECONDARYURL="SecondaryWorkgroupURL:PortNo" AUTOGG="1" WORD_ON="1" EXCEL_ ON="1" POWERPOINT_ON="1" PROJECT_ON="1" OUTLOOK_ON="1" AUTHMECH="0"

x64 installation script example

"C:\Users\username\Desktop\CM_x64.msi" /q /l*vx "C:\Users\username\Desktop\Installlog.txt" INSTALLDIR="C:\Program Files\Micro Focus\Content Manager\" ADDLOCAL=HPTRIM,Client,Server,TRIMWORKGROUP,IDOLALL,EMAILMANAGER HPTRIMDIR="C:\Micro Focus Content Manager" DOMAINNAME="domainname" SERVICEUSER="username" SERVICEPASS="userpassword" DEFAULTDBNAME="DBName" DEFAULTDB="DBID" STARTMENU_NAME="Content Manager" TRIM_DSK="1" TRIMREF="DSK" PRIMARYURL="PrimaryWorkgroupURL:PortNo" SECONDARYURL="SecondaryWorkgroupURL:PortNo" AUTOGG="1" WORD_ON="1" EXCEL_ ON="1" POWERPOINT_ON="1" PROJECT_ON="1" OUTLOOK_ON="1" AUTHMECH="0"

Script properties

The script properties listed below are for standard scripted installations. For properties for administrative installations, see the section *Administrative installation steps*.

- **C:\Users\username\Desktop\CM_xNN.msi** - .msi file location
- **C:\Users\username\Desktop\Install_Log.txt** – installation log file location and name
- **ADDLOCAL** – installs the features listed, which must be separated by commas:
  - **HPTRIM** – core libraries. Required.
  - **Client** - client features, which include Image Scanner, Lotus Notes integration add-in, standard sample data, and the DataPort import and export tool

    - **Server** – server features – only available for x64 installations
    - **TRIMWORKGROUP** – Content Manager Workgroup Server. Only available for x64 installations.
    - **IDOLALL** – include this property if IDOL components are already installed and you want to reinstall them. If you chose not to continue to use IDOL, this property can be left out and the IDOL components will not be installed.
    - **EMAILMANAGER** - installs the Automated Email Management service, a utility to import emails into Content Manager that have been journaled and deposited into a nominated folder
- **HPTRIMDIR** – data folder for server data. See also *Data Folder*. The MSI Property, HPTRIMDIR, sets the folder which is used to store server logs and configuration data, as well as client side features, such as Report Templates and Directory Synch staging folders. If this property is not set, the installer will choose a default location and this will be on the disk volume that has the largest amount of free space. If an installation is carried out using a command line or a batch file script, this property must be set explicitly if the default behavior is undesired.
- **DOMAINNAME** – network domain name
- **SERVICEUSER** – the user to run the Content Manager services, who must have the Log on as a service policy assigned, e.g. CMServices
- **SERVICEPASS** – the services account password
- **DEFAULTDBNAME** – your Content Manager dataset name
- **DEFAULTDB** – your Content Manager dataset ID
- **STARTMENU_NAME** –Windows Start menu folder under which Content Manager programs appear
- **TRIM_DSK** – desktop shortcuts. 1 to install, leave out entire property to not install desktop shortcuts.
- **TRIMREF** – application to use for Content Manager reference files (*.tr5)
    - **TRIM** – Content Manager
    - **DSK** – Content Manager Desktop
- **PRIMARYURL** – primary Workgroup Server URL, hostname or IP Address. Optionally, type in the Port Number the client should use to connect to the Workgroup Server. This should be separated from the Workgroup Server URL by a colon (:). If this is left blank, it will default to 1137.

- **SECONDARYURL**– optional – secondary Workgroup Server URL, hostname or IP Address. Optionally, type in the Port Number the client should use to connect to the Workgroup Server. This should be separated from the Workgroup Server URL by a colon (:). If this is left blank, it will default to 1137.
- **AUTOGG** – global settings
  - **1** – to use global settings for users
  - Leave this property out of the command line to not use global settings for users
- **WORD_ON** – Microsoft Office Word integration
  - **1** – enables Word integration.
  - **0** - for no integration.
- **EXCEL_ON** – Microsoft Office Excel integration
  - **1** – enables Excel integration.
  - **0** - for no integration.
- **POWERPOINT_ON** – Microsoft Office PowerPoint integration
  - **1** – enables PowerPoint integration.
  - **0** - for no integration.
- **PROJECT_ON** – Microsoft Office Project integration
  - **1** – enables Project integration.
  - **0** - for no integration
- **OUTLOOK_ON** – email integration
  - **1** – integration through Content Manager in Outlook add-in
  - **0** - for no integration
- **AUTHMECH** – authentication mechanism
  - **0** – Integrated Windows Authentication
  - **1** – Explicit Windows Authentication
  - **2** – ADFS Authentication
  - **3** – Google Apps Authentication

CAUTION:
You can also use the following properties in the command lines, which enables you to set specific locations for the corresponding Content Manager data folders, for example, if you needed them to be in users' H:\ drives for some reason.

However, changing these data folder locations is not recommended.

By not including those properties in the command line, the installer uses user-specific paths on each computer.

USER_LEX_FOLDER – installation location of the Content Manager user dictionary

CLIENT_APPDATA_FOLDER – the location of Content Manager data files

CLIENT_LOCAL_APPDATA_FOLDER – the location of Content Manager data files

OFFLINE_DATA_FOLDER – the location of Content Manager offline data files

Installing Service API using a script

You can also use **Setup_CM_x64.exe** to install this Content Manager component.

1. Install the Service API prerequisites listed in **CM9.3_Spec.pdf**.
2. Using the Windows **Command Prompt** function as administrator, edit the script to meet your requirements, and run it, for example:
   "C:\Users\username\Desktop\CM_Service_API_x64.msi" /q /l*vx "C:\Users\username\Desktop\ServiceAPIInstall.txt" SERV_API_WEBSITE_DESCRIPTION="Default Web Site" SERV_API_DBID="45" SERV_API_PORT="1137" SERV_API_WG="WorkGroupServer" SERV_API_WG_ALT="AlternativeWorkGroupSrv" SERV_API_PORT_ALT="1138" SERV_API_WEBSITE_IDENTITY_DOMAIN="domainname" SERV_API_WEBSITE_IDENTITY_NAME="username" SERV_API_WEBSITE_IDENTITY_PASSWORD="userpassword" SERV_API_INCLUDE_FILES="1"

Content Manager Service API installs with default values stored in the registry.

ServiceAPI installation script properties

The user needs to be defined before installation and will be used to run the AppPool for Service API.

Service API-specific installation properties:

- **SERV_API_WEBSITE_DESCRIPTION** – Service API default web site address
- **SERV_API_DBID** – default dataset ID for Service API
- **SERV_API_PORT** – default Service API port
- **SERV_API_WG** – default Service API Workgroup Server

- **SERV_API_PORT_ALT** – secondary Service API port for failover
- **SERV_API_WG_ALT** – secondary Service API Workgroup Server for failover
- **SERV_API_WEBSITE_IDENTITY_DOMAIN** – domain name
- **SERV_API_WEBSITE_IDENTITY_NAME** – Service API app pool user name
- **SERV_API_WEBSITE_IDENTITY_PASSWORD** – Service API app pool user password
- **SERV_API_INCLUDE_FILES** – ServiceAPI help and example files
  - 0 – files not installed
  - 1 – files installed

> **NOTE:**
> By default, the ServiceAPI help and examples are not installed.
>
> It is recommended that the help and example files are not installed on a production server for security reasons, see **CM9.3_ServiceAPI.pdf** for details. As a result, if you navigate to the ServiceAPI website and these files are not installed, you will get a HTTP 404 Not Found message.

Installing WebDrawer using a script

You can also use **Setup_CM_x64.exe** to install this Content Manager component.

1. Install the WebDrawer prerequisites listed in **CM9.3_Spec.pdf**.
2. Using the Windows Command Prompt function as administrator, edit the script to meet your requirements, and run it, for example:

"C:\Users\username\Desktop\CM_WebDrawer_x64.msi" /q /l*vx "C:\Users\username\Desktop\WebdrawerInstall.txt" WD_WEBSITE_DESCRIPTION="Default Web Site" WD_DBID="45" WD_PORT="1137" WD_WG="WorkGroupServer" WD_WEBSITE_IDENTITY_DOMAIN="domainname" WD_WEBSITE_IDENTITY_NAME="username" WD_WEBSITE_IDENTITY_PASSWORD="userpassword"

WebDrawer installation script properties

The user needs to be defined before installation and will be used to run the AppPool for WebDrawer.

WebDrawer-specific installation properties:

- **WD_WEBSITE_DESCRIPTION** – WebDrawer default web site address
- **WD_DBID** – default dataset ID for WebDrawer

- **WD_PORT** – default WebDrawer port
- **WD_WG** – default WebDrawer Workgroup Server
- **WD_WEBSITE_IDENTITY_DOMAIN** – domain name
- **WD_WEBSITE_IDENTITY_NAME** – WebDrawer app pool user name
- **WD_WEBSITE_IDENTITY_PASSWORD** – WebDrawer app pool user password

Installing Web Client using a script

You can also use **Setup_CM_x64.exe** to install this Content Manager component.

1. Install the Web Client prerequisites listed in **CM9.3_Spec.pdf**.
2. Using the Windows **Command Prompt** function as administrator, edit the script to meet your requirements, and run it, for example:
   "C:\Users\username\Desktop\CM_WebClient_x64.msi" /q /l*vx "C:\Users\username\Desktop\WebClientInstall.txt" WC_WEBSITE_DESCRIPTION="Default Web Site" WC_DBID="45" WC_PORT="1137" WC_WG="WorkGroupServer" WC_WEBSITE_IDENTITY_DOMAIN="domainname" WC_WEBSITE_IDENTITY_NAME="username" WC_WEBSITE_IDENTITY_PASSWORD="userpassword"

Content Manager Web Client installs with default values stored in the registry.

Web Client installation script properties

The user needs to be defined before installation and will be used to run the AppPool for Web Client.

Web Client-specific installation properties:

- **WC_WEBSITE_DESCRIPTION** – Web Client default web site address
- **WC_DBID** – default dataset ID for Web Client
- **WC_PORT** – default Web Client port
- **WC_WG** – default Web Client Workgroup Server
- **WC_WEBSITE_IDENTITY_DOMAIN** – domain name
- **WC_WEBSITE_IDENTITY_NAME** – Web Client app pool user name
- **WC_WEBSITE_IDENTITY_PASSWORD** – Web Client app pool user password

Installation rules and behavior

- The Content Manager installation is managed. This means that the installation program keeps a record of the Content Manager components that are installed on the computer.

- You need to run any installation with elevated access rights.
  If you are not running the installation using Group Policy, you can set these on a computer using Group Policy set by the domain-wide Group Policy, or on a local computer.
- If the administrator performs the installation through Group Policy, elevated access rights apply to the installation for its life.
  If the system administrator does not perform the installation through Group Policy, the installation does repair, modify etc. as long as the user carrying out the task has elevated access rights - for example, is a local administrator.
  If this is not the case, some installation tasks such as repair or modify will fail because they need elevated access rights to write to the registry and to delete or write files on the computer.
- Content Manager Servers are set to start automatically. Therefore, when a server shuts down or needs to be rebooted, its services start automatically after the reboot.

Upgrading Content Manager

> **NOTE:** The information in this chapter is only relevant if you're upgrading to a major (e.g. 9.0) or minor (e.g. 9.1) version of Content Manager.
> From the Content Manager 9.0 release, we introduced Patch updates. If you're updating to a Patch, for example 9.1 Patch 2, please refer to **Updating_Using_MSPs.pdf** in the Content Manager_CDImage.ISO for details on how to update your software.

Before upgrading any computers in your environment please read these upgrade instructions to the end for an indication and overview of the tasks you need to perform for the upgrade.

Upgrading Content Manager means not only upgrading the software, but in most cases also your dataset. Therefore, it is essential that you have performed database and dataset maintenance, as the upgrade instructions assume that your database is clean and your dataset up-to-date.

Also, before upgrading your Content Manager environment, it is strongly recommended you perform a trial upgrade on a copy of your dataset in a test environment.

This test environment should be isolated from your live environment with no chance of confusing any live and test data.

> **CAUTION:**
> When upgrading Content Manager, if there a reboot flag from Windows updates present, the Content Manager installation dialog will appear telling you that you cannot proceed with the upgrade until you reboot the machine. After rebooting, you need to ensure there are no outstanding Windows updates (all updates must be completed) and you should suspend Windows updates for the duration of the Content Manager upgrade process. If you don't, if Windows updates complete while upgrading this may result in two entries of Content Manager being listed in the Program and Features table.

> **NOTE:** Before any upgrade, backing up your data is essential.

Use the main Content Manager installation file **Setup_CM_xNN.msi** and any other relevant **.msi** or **Setup_CM_xNN.exe** installation files from the Content Manager installation media.

An upgrade installation file searches for an installed instance of the software, installs the new version and removes the previous version, if there is one.

If there is no previous installation, the installer performs a standard installation.

> **NOTE:** When upgrading from a previous version of Records/Content Manager the previously used install paths for both binaries and the WorkingFolders will be used by default if using **Setup_CM_xNN.exe** or if those properties are not included in the script if installing using MSIs

directly. This is because those values are kept in registry and read on upgrade.
These can be modified, however, during the UI phase of the upgrade process if using **Setup_CM_xNN.exe** or if installing using a script then the properties concerned can be set to the new default paths.

If a fresh installation is being done then the new default paths for Content Manager will be used unless the user modifies them via UI or script.

IMPORTANT: When upgrading from 9.2 or 9.2 Patch 1 and you are using Elasticsearch for your content index, the Elasticsearch index for the dataset must be deleted and re-created.

See the Content Manager Enterprise Studio help file and the **CM9.3_ElasticSearchInstall_Config.pdf** for details on how to remove and create an Elasticsearch Index.

If your organization uses the Auto-Classification feature, you will also need to re-run the Classification/Category training.

Version support

You can upgrade to this version of Content Manager only from TRIM 7.2x or Records Manager 8.x.

If you are using older versions of Records Manager or TRIM, you will need to upgrade your existing environment using a staged approach. You will need to upgrade to an earlier version of TRIM/Records Manager first before proceeding to the upgrade to Content Manager.

Depending on your current version you may need to take a number of steps to get to the correct version that supports upgrading to Content Manager. For example, on your TRIM 6.2 installation media, see **TRIMCap2Con.pdf** for upgrades from TRIM Captura to TRIM Context and **TRIMCon2Con.pdf** for upgrades from TRIM Context to TRIM 6.2.

Then refer to upgrade instructions in TRIM 7.2 to complete the steps necessary to get to a suitable version for upgrade.

NOTE: Please contact Software Support if you are looking for assistance in the upgrade from an unsupported version of the product. They can advise a contact in the Micro Focus Software Professional Services team that can provide consulting services for the upgrade.

Mixed environments

To help with the transition to later versions of Content Manager you can, for a short time, run an older version of a Workgroup Server with a newer version of the desktop client. The intent behind this behavior is to allow customers who cannot upgrade both their clients and servers at the same time to deploy the new version in stages.

will support the following type of mixed environment:

The version you're upgrading from	The version you're upgrading to	Examples of supported mixed environments	Examples of unsupported mixed environments
The proceeding minor	The following major or minor	8.1x Workgroup Servers and 8.2x Clients	8.0x Workgroup Servers and 8.2x clients 7.3x Workgroup Servers and 8.2x clients 7.2x Workgroup Servers and 8.2x clients

NOTE: Definitions of the different version types released by Micro Focus can be found at https://softwaresupport.softwaregrp.com/document/-/facetsearch/document/KM02966156

Whilst you can take advantage of this backwards compatibility it is not recommend you allow your environment to operate in a mixed mode for an extended period. Technology differences between versions can mean full product functionality is not always achievable in a mixed environment. This reduced functionality may become difficult for businesses to accommodate over an extended upgrade period. Moving quickly to upgrade both your clients and servers to the same version will allow you to take advantage of all the new and improved functionality in the latest version.

If the gap between the version you're currently on and the version you're upgrading to does not match the supported scenario described above you will have to upgrade your clients and servers at the same time.

Upgrade steps for mixed environments

Upgrade in the following order:

1. Client computers.

   See *Upgrading from TRIM 7.2 to Content Manager , on page 63*

2. All Workgroup Servers.
3. Dataset schema, if necessary

NOTE: All Workgroup Servers must be at the same revision level.

Customized client toolbars and menus

During the upgrade process, Content Manager resets all toolbars and menus to the defaults. In Record Manager 8.2 ribbons have been introduced to replace the toolbars and menus of the previous versions. This will assist in future upgrades as the new ribbon technology will allow users to preserve their customizations.

New user types

The upgrade from Records Manager 8.0x or an earlier version to this version of Content Manager will result in a new structure of user types. The upgrade process converts the legacy user types with a dataset schema change as follows:

- The user type **Administrator** does not change
- **Information Manager** becomes **Records Manager**
- **Information Worker** becomes **Records Co-ordinator**
- **End User** becomes **Knowledge Worker**
- **Contributor** is a new user type – this user type was implemented to cater for specific use cases where users need only very basic Content Manager permissions, such as creating (but not modifying) new records and searching. This typically would be a user who accesses Content Manager via an integrated application, such as Microsoft SharePoint, rather than the Content Manager client or web client.
- **Inquiry User** does not change
- **Custom User** is removed – if required, individual users can be customized from the Location Profile tab. To create a standard set of user permissions, for example for different roles, a user with customized permissions can be created and the **Use Profile of** option can be used.

For specific information about default permissions for each user type, please refer to the Content Manager Help topic **Content Manager Help > Locations and users > Location and user administration > User permissions**.

Before upgrading, make a note of all the existing user types and their permissions in your datasets, as you will have to manually re-create your changes to the default permissions.

To review the user type permissions, on the **Administration** menu, click **System Options**, select the **Permissions** tab, and select the user type to review.

During the upgrade process, Content Manager dynamically assigns users with the legacy user type **Custom** the appropriate new user type that includes all the permissions the user did have previously, and then removes the permissions from the set that the user did not have previously.

After the upgrade, if your database schema has not been upgraded accordingly (using Content Manager Enterprise Studio), then the **Permissions** tab will not be available for users, and users can only create new users with an empty permission set.

After all upgrade steps including the schema upgrade have been completed, use the Permissions tab to apply the customized settings to the new user types in your dataset, if required.

New Retention Schedule triggers and dispositions

The upgrade from Records Manager 8.0x or an earlier version to this version of Content Manager will upgrade the archiving features around Retention Schedules and disposition. The upgrade process removes the legacy Retention Schedule triggers:

- Local Archive
- Interim Archive

The upgrade removes triggers of the above types from your dataset and its Retention Schedules. You should therefore make a note of your Retention Schedule triggers across the dataset and the triggers they use to be able to re-create the triggers you need by using the new trigger types, if necessary:

- Archive (Keep Forever)
- Archive (Transfer Custody)

The upgrade also removes the disposition states:

- Archived (Local)
- Archived (Interim)

The records in your dataset that had a disposition status of **Archived (Local)** or **Archived (Interim)** will have the disposition status **Inactive** after the upgrade.

Given these changes, after completing the upgrade to Content Manager it will be necessary to run the Disposal Calculator from the Content Manager client, from the **Administration** ribbon, click **Other**. This will display the **Record Retention Reindex** dialog. From here you can elect to reindex:

- all records
- records matching a search
- Records with retention Schedules matching a search.
- Additional options are included to exclude records from the reindex.

Conversion of VMBX to EML

A new utility was added to Records Manager 8.2 to allow existing customers to remove email messages stored in VMBX format. This was an old proprietary text format used by early version of TRIM for storage of email messages. The conversion tool will replace the VMBX with a standard EML format. The conversion utility can be run from the Content Manager client, from the **Administration** ribbon, **Conversions** group and click **Mail Message Format**. You can run this utility against:

- all records
- records matching a particular search.

Security Filter Converter

Access control security filtering in Content Manager 9.1 has been optimized to improve performance. As part of this optimization, all discrete groups of users that have been designated in an access control are set up in a special “access control group” object. These access control groups are only ever used “under the hood”, however the process used to convert the Content Manager database to set these groups can take a long time to complete. For this reason, the data conversion was removed from the normal schema upgrade program so that it can be run separately and concurrent with users accessing Content Manager. Only when the conversion is complete and all groups have been verified will Content Manager start using the new security filtering model.

The conversion to the new optimized behavior is undertaken over two stages. The first is run as a part of the normal database upgrade process. The new columns and tables are added into the Schema and initialized as default values. The second stage is implemented as a multi-threaded conversion tool that is accessed from the Content Manager client, from the Administration ribbon, Conversions group. After upgrading to Content Manager 9.1 and upgrading the database Schema, it is mandatory to run this conversion tool. It can be run while users are accessing Content Manager. Only once this second stage of the conversion is complete and all groups have been verified will Content Manager start using the new security filtering model.

The conversion utility can be run against:

• all records

• records matching a particular search,

and is restartable, so if it is interrupted it can be restarted, in which case it will continue from where it left off.

Once the conversion is complete:

(1) Search filtering needed for access control implementation should be much quicker , and

(2) Support for Access Exclusions is available on all types of records, not just Client/Matter records.

Upgrading Content Manager Render

If you're upgrading from Records Manager and you have Render installed, before upgrading to Content Manager, the following steps must be completed.

1. Stop the Records Manager Render Service.
2. Delete TRIMRender_PDF and TRIMRender_TIFF printers.
3. Using **Windows Task Manager**, on the **Details** tab, end the two PrintONstream.exe (PrintOnStream Manager) tasks that will still be running.
4. Uninstall the Onstream Printer files manually.

OnstreamPrinterFiles.msi must be uninstalled from **Control Panel – Programs and Features**.

To uninstall the file:

1. Open the Control Panel and navigate to Programs and Features.
2. From the list of installed programs, find and select the **Onstream Printer Files xnn** and then click **Uninstall**.
3. Click **Yes** to confirm the deletion of the Onstream Printer Driver Files.

   The **Onstream Printer Drivers Files xnn** dialog is displayed.
4. Select **Do not close applications**. (A Reboot may be required), and then click **OK**.

   The Onstream Printer Drivers files will be uninstalled and you can now upgrade to Content Manager following the steps below.

Changes to Content Manager and Outlook after Upgrading

> **NOTE:** Please ensure the following information is communicated to your users as a part of your upgrade communication plan.

After upgrading the client (and/or Web Client software) from Records Manager 8.3 to Content Manager 9.0, when a user logs into the Content Manager client (or Web Client), they will notice that their **Email Links** are now called **Check In Styles**. These are created and accessed in the same ways as they did in the previous version of the software.

After upgrading to Content Manager, there will be no **Styles** listed under the **Check In with Style** option on the **Content Manager** tab in Outlook. To load the upgraded **Check In Styles**, on the **Content Manager** tab, in the **Tools** group, click **Check In Styles**. The **Check In Styles** panel will open and the upgraded C**heck In Styles** will be loaded and users will be able to Check In their emails with a Style.

Upgrading from TRIM 7.2 to Content Manager

Upgrade steps from TRIM 7.2

Upgrade TRIM from version 7 in the following order:

1. Back up all TRIM data.

   See Backing up and Restoring your Data, on page 73.

2. Perform the relevant database and dataset maintenance tasks.

> **NOTE:** If you have existing SQL Server datasets, note down the connection configuration information, this will be needed later.

3. Upgrade TRIM and its peripheral applications on all the TRIM client computers.

   See *Upgrading from TRIM 7.2 to Content Manager , above*

4. Make TRIM unavailable for users.

   In TRIM Enterprise Studio Help, see **Dataset availability and messaging**.

5. If there are TRIM IDOL services running, stop them.

> **IMPORTANT:** See https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result/-/facetsearch/document/KM00209246 for the correct way to shutdown the IDOL services.

> **CAUTION:**
> When upgrading from TRIM 7.2.x or 7.3.x, the root section of Path settings in the IDOL configuration files may revert to the default 'C:\Micro Focus Content Manager\IDOL\'. This will mean that IDOL will not automatically locate any existing index after the upgrade. Note that the current IDOL configuration files are backed up to the IDOL working folder.
>
> Please see **CM9.3_IDOL_DCI_Install_Config.pdf** for more information.
>
> Before starting the IDOL services, please check the IDOL CFG files and ensure the Path settings are pointing to the correct location.

> **NOTE:** In Records Manager 8.2, by default for a new installation, only one Content Service is installed. When upgrading to Content Manager if you previously had two IDOL Content Services these will be preserved and two IDOL Content Services will be installed

> as a part of the upgrade. If you had one or no IDOL Content Services, only one Content Service will be installed.

As a part of the Content Manager upgrade process the IDOL_TRIM configuration files that are installed as a part of the Content Manager installation process are copied to the IDOL working folder, which by default is C:\Micro Focus Content Manager\IDOL

These copied files have the date and time of the upgrade prepended to the file name for easy identification.

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

6. Stop the TRIM Workgroup service.
7. Shut down all the Workgroup Servers.
8. Using **Setup_CM_64.exe**, upgrade the TRIM Workgroup Server software on all Workgroup Servers.
9. Nominate one computer as designated administrator computer. If the computer has TRIM in a version before 7.2 installed, modify the installation to remove the **Server** feature **Demonstration Database**, if it is installed.
10. On the administrator computer, install or upgrade TRIM Enterprise Studio using **Setup_CM_64.exe**.
11. On the administrator computer, run the new version of Content Manager Enterprise Studio.

    > **IMPORTANT:** If you have existing SQL Server datasets – they will no longer work as previously configured. See Upgrading SQL Server Connection Strings for details on how to correct these.

    Upgrade all registered dataset schemas.

    In Content Manager Enterprise Studio Help, see **Upgrading a dataset schema**.

    If you wish to add a dataset for newly supported products such as:

    - SQL Server Always On Availability groups
    - Azure SQL Server

    See Special Database Configurations for details.
12. In Content Manager Enterprise Studio, review the Workgroup Server configuration, in particular

event processing.

In Content Manager Enterprise Studio Help, see *Configuring event processing*.

13. Make changes as necessary and save the new configuration
14. Start the Content Manager Workgroup Servers
15. In Content Manager Enterprise Studio, deploy the new configuration
16. Bring Content Manager online.

The upgrade is complete.

Upgrading client computers from TRIM 7.2

In addition to the main TRIM client software, client computers may have different TRIM peripheral applications and extensions installed.

These should always be the same version and build number as the TRIM main client software.

Upgrade steps for client computers:

1. If the computer has Microsoft Excel add-ins for earlier versions of Records Manager or TRIM installed, remove them according to the instructions in your Microsoft Excel add-in documentation
2. Using the Windows **Programs** function, check which TRIM peripheral applications and extensions are installed on the computer
3. Remove those peripheral applications which are no longer required on the computer by using the Windows **Programs** function
4. Ensure the client computer has a supported operating system and all the necessary components installed. See **CM9.3_Spec.pdf**.
5. Upgrade the main TRIM client software using **Setup_CM_NN.exe** from the installation media.
6. Restart the computer
7. Upgrade the remaining peripheral TRIM applications using the respective **.msi** files from the installation media. See *Upgrading TRIM peripheral applications from version 7.2* below

Upgrading TRIM peripheral applications from version 7.2

WebDrawer ISAPI and Records Manager 8 WebDrawer

TRIM 7 WebDrawer ISAPI is not supported in Records Manager 8. Records Manager 8 WebDrawer is an entirely new application.

TRIM 7 WebDrawer ISAPI customized templates do not work with Records Manager 8 WebDrawer.

The recommended steps:

1. Take a note of all WebDrawer ISAPI configuration details.
2. In a controlled environment, install and configure Records Manager 8 WebDrawer according to your requirements according to the instructions in **CM9.3_WebDrawer.pdf**
3. Remove WebDrawer ISAPI 7.
4. Install new Records Manager 8 WebDrawer.

Upgrading from earlier versions of Records Manager 8

Upgrade steps from Records Manager 8

Upgrade to Content Manager from version 8 in the following order:

1. Back up all Records Manager data.

See Backing up and Restoring your Data, on page 73.

2. Perform the relevant database and dataset maintenance tasks.

> **NOTE:** If you have existing SQL Server datasets, note down the connection configuration information, this will be needed later.

3. Upgrade Content Manager and its peripheral applications on all the Content Manager client computers.

See *Upgrading client computers from earlier versions of Records Manager 8, on page 68*.

4. Make Content Manager unavailable for users.

In Content Manager Enterprise Studio Help, see **Dataset availability and messaging**.

5. If there are Content Manager IDOL services running, stop them.

> **IMPORTANT:** See https://softwaresupport.softwaregrp.com/group/softwaresupport/search-result/-/facetsearch/document/KM00209246 for details on the correct way to shutdown the IDOL services.

5. Stop the Content Manager Workgroup service.
6. Shut down all the Workgroup Servers.
7. Use Setup_CM_x64.exe to upgrade the Content Manager Workgroup Server software on all Workgroup Servers.
8. Nominate one computer as designated administrator computer.

9. On the administrator computer, install or upgrade Content Manager Enterprise Studio using **Setup_CM_x64.exe**.
10. On the administrator computer, run the new version of Content Manager Enterprise Studio.

    > **IMPORTANT:** If you have existing SQL Server datasets – they will no longer work as previously configured. See Upgrading SQL Server Connection Strings for details on how to correct these.

    Upgrade all registered dataset schemas.

    In Content Manager Enterprise Studio Help, see **Upgrading a dataset schema**.

    If you wish to add a dataset for newly supported products such as:

    - SQL Server Always On Availability groups
    - Azure SQL Server

    See Special Database Configurations for details.
11. In Content Manager Enterprise Studio, review the Workgroup Server configuration, in particular event processing.

In Content Manager Enterprise Studio Help, see **Configuring event processing**.

12. Make changes as necessary and save the new configuration.
13. Start the Content Manager Workgroup Servers.
14. In Content Manager Enterprise Studio, deploy the new configuration.
15. Bring Content Manager online.

The upgrade is complete.

> **NOTE:** From Records Manager 8.2, by default for a new installation, only one Content Service is installed. When upgrading to Content Manager, if you previously had two IDOL Content Services these will be preserved and two IDOL Content Services will be installed as a part of the upgrade. If you had one or no IDOL Content Services, only one Content Service will be installed.
>
> As a part of the Content Manager upgrade process the IDOL_TRIM configuration files that are installed as a part of the Content Manager installation process are copied to the IDOL working folder, which by default is C:\Micro Focus Content Manager\IDOL
>
> These copied files have the date and time of the upgrade prepended to the file name for easy identification.

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

Upgrading client computers from earlier versions of Records Manager 8

In addition to the main Content Manager client software, client computers may have different Content Manager peripheral applications and extensions installed.

These should always be the same version and build number as the Content Manager main client software.

Upgrade steps for client computers:

1. Using the Windows **Programs** function, check which Records Manager peripheral applications and extensions are installed on the computer.
2. Remove those peripheral applications which are no longer required on the computer by using the Windows **Programs** function.
3. Ensure the client computer has a supported operating system and all the necessary components installed.
   See **CM9.3_Spec.pdf**.
4. Upgrade the main Content Manager client software using **Setup_CM_xNN.exe** from the installation media.
5. Restart the computer.
6. Upgrade the remaining peripheral Content Manager applications using the respective **.msi** files from the installation media.

Upgrading and Global Settings

When you upgrade from a pre-8.2 version of Records Manager, the Global Settings are not retained and will need to be reconfigured and deployed after upgrading to Content Manager .

Upgrading Offline Records

It is recommended users check in their Offline Records files and folders before an upgrade to version 9.

Before upgrading to a 64-bit Content Manager client, you must check in all documents from Offline Records to prevent data loss.

Copies of Configuration Files

> **IMPORTANT:** When upgrading to Content Manager 9.3, due to the changes in installation paths, the configuration files from the previous version installation paths are not copied into the new C:\Micro Focus Content Manager workpaths. These files will be available in the original installation path and any modifications will need to be copied from these files into the newly installed configuration files installed to, by default, C:\Program Files\Micro Focus\Content Manager

As a part of the upgrade process, to preserve any additional configuration settings that may have been made, we make copies of various Content Manager configuration files. These files are copied to the relevant working folder for the module/application and are prepended with the date and time the upgrade was done, as well as the name of the module/application, for example the ServiceAPI web.config file is copied and renamed to 05_17_2015_9_58_Service_API_web.config

> **NOTE:** If you have customized any of the properties of the configuration files, after upgrading you will need to manually copy these customized settings into the installed versions of the configuration files .

> **CAUTION:** Do not overwrite the installed version of the configuration files with the copied versions as there may be new configuration properties that will be lost if the file is replaced with the copied version.

Module	Files	Copied from (default)	Copied to
Web Client	hprmServiceAPI.config web.config	C:\Program Files\Micro Focus\Content Manager\Web Client	C:\Micro Focus Content Manager\WebClientWorkpath File name prepended with date and time of the upgrade plus WebClient
WebDrawer	hptrim.config web.config	C:\Program Files\Micro Focus\Content Manager\WebDrawer	C:\Micro Focus Content Manager\WebDrawerWorkpath File name prepended with date and time of the upgrade plus WebDrawer
ServiceAPI (see Note below)	hptrim.config web.config	C:\Program Files\Micro Focus\Content Manager\Service_API	C:\Micro Focus Content Manager\ServiceAPIWorkpath File name prepended with date and time of the upgrade plus Service_API

IDOL Content Indexing	TRIM Content Service 1.cfg TRIM IDOL Service.cfg	C:\Program Files\Micro Focus\Content Manager\IDOL\TRIM Content Service 1 C:\Program Files\Micro Focus\Content Manager\IDOL\TRIM IDOL Service	C:\Micro Focus Content Manager\IDOL File name prepended with date and time of the upgrade plus IDOL
Iron Mountain integration	web.config TRIMIronMountain.xml	C:\Program Files\Micro Focus\Content Manager\IronMtnWarehouseInteg C:\Program Files\Micro Focus\Content Manager\IronMtnWarehouseInteg\bin	C:\Micro Focus Content Manager\IronMtnWarehouseInteg File name prepended with date and time of the upgrade plus IronMountain
oneilbridge integration	ONeilbridge.xml	C:\Program Files\Micro Focus\Content Manager\ONeilWarehouseInteg	C:\Micro Focus Content Manager\ONeil File name prepended with date and time of the upgrade plus ONeil
EmailLink	trimlink.hptrim.config	C:\Program Files\Micro Focus\Content Manager\EmailLink	C:\Micro Focus Content Manager\EmailLink File name prepended with date and time of the upgrade plus EmailLink

IMPORTANT: After upgrading your **ServiceAPI** instance, in the installation directory, rename the **hptrim.config.template** file to **hptrim.config** and replace the existing **hptrim.config** file. Any customizations will have to be manually copied from the original **hptrim.config** and added to the 'new' file.

Removing Content Manager

1. Use the Windows **Control Panel** → **Programs and Features** function to remove all peripheral Content Manager applications, modules and components, for example:
   - Web Client, ServiceAPI, Office Integration, Kofax, etc.
2. Remove Content Manager using the Windows **Control Panel** → **Programs and Features** function.

The installer requires the Microsoft .NET Framework 4.6.2 (the recommended minimum version) to remove Content Manager.

> **NOTE:** You can remove it when all Content Manager components are removed.
> User data folders – the installation program does not remove the user's **AppData** folders when removing Content Manager, as these folders may contain user-created data.
>
> By default, these folders are located in the user's profile area, for example, **C:\Users\<USER>\AppData\Roaming\Micro Focus\Content Manager** and **C:\Users\<USER>\AppData\Local\Micro Focus\Content Manager**

Network user group and the CM Services account

The Content Manager Services account is the proxy that enables communication between the Content Manager Servers. You can choose any name for this account. All Content Manager documentation sometimes uses the example name **CMServices** for this account, but of course the name you chose may be different.

1. In **Computer → Manage → Local Users and Groups**, create the individual network user names that will log on to Content Manager, if they do not exist
2. Add these network login names eventually to the Content Manager database so that the users can log on to Content Manager directly using their network logins
3. Create an Content Manager Services account, for example named **CMServices**, which will be used to run Content Manager Server components

NOTE: Write down the account name and password you have chosen as you will need it later. Ensure you have created the account with the necessary permissions before proceeding. You will need no other accounts for the RDBMS.

CAUTION:
The installation process does not add the services user to the **Log on as a service** policy for any computer running a Content Manager service.

To start any of the Content Manager services, include the services user in the Log on as a service policy on the computer; otherwise the services will fail to start and cause the error message:

Services

Could not start the Content Manager Workgroup Server services on Local Computer. Error 1069: The Services did not start due to a logon failure.

The solution is to re-type the password for the services user in the properties of one of the services, which will add the user to the Log on as a Service policy and return the message:

Services

The account mydomain\CMServices has been granted the Log On As A Service right.

The Log on as a service policy is in Local Security Settings under User Rights Assignments.

Backing up and Restoring your Data

It is important that you back up the contents of your Content Manager dataset including electronic stores regularly, preferably daily.

You will find the recommended backup strategy in the following topics of this document.

Remember that this is your data and it is your responsibility to make adequate backups.

Your business relies on this data to survive; therefore it is very important that you make appropriate backups to protect your data.

We urge you not to be complacent. Loss of data is quite a common occurrence. Some of the reasons for losing data are listed in the following topics.

Reasons for backing up

A number of factors can result in the loss of data:

- Power fluctuation or blackout
- System failure
- Theft
- Operator error
- Communications (network) failure
- Malicious damage

Backup strategy

To ensure optimum performance of your Content Manager dataset, we recommend regular maintenance and to consider the following as part of a comprehensive backup and recovery plan.

This is not an exhaustive list:

- Back up before initial installation and upgrades
- Back up daily - this is the minimum recommended
- Maintain multiple generations of backups to protect against backup corruption, for example, three generations of each backup media before re-use
- Backup media should be verified regularly

- Make sure you know how to restore from your backup, should the need arise, i.e. regular practice of restoration to verify the process and ensure personnel are familiar with the requirements
- Off-site storage of backup media in case of fire, theft, local disaster etc.

Dataset components

The components that should be backed up on a regular basis for your particular environment require thought and planning.

All the components combine to create a matched set of data.

To ensure the integrity of your data, it is recommended you back up the data as one set and if necessary, restore it as a complete set. In most instances, all data as one set would be ideal; but as a minimum, you should back up all primary data.

Splitting the database components into primary and ancillary data results in these lists:

Primary data

- Database tables (relational database metadata)
- Electronic document stores
- Document content search indexes
- Audit logs

Ancillary data

- User Offline Records folders
- User configuration files
- Queue processing folders
- Document content search indexes
- Audit logs

Both document content search indexes and audit logs appear under each of the headings above. Whether either is considered primary or ancillary data is site specific.

You can regenerate the entire structure of document content search indexes from the documents themselves; therefore you may consider these non-core structures. However, it can take so much time to regenerate a full set of content indexes that you should consider them to be primary data.

Audit logs are used to varying degrees depending on the implementation of Content Manager. Whether you consider audit logs primary or ancillary data depends on the use of such logs by your organization - simple reference item, critical security feature or something else?

A backup and recovery plan must decide under which category each falls, and treat them appropriately.

The purpose of backups is to ensure that you can recover your data, should something go wrong. Whatever the reason for the loss of data may have been - if you have adequate backups, you can minimize or even eliminate loss of service and data.

Backups are an integral part of your everyday computer housekeeping and should be regular practice.

You should use incremental backup mechanisms only with extreme care and after due consideration.

Backup techniques

You can perform two types of backups on a database:

- Hot - while the database is online and usable
- Cold – while the database is closed and not available to users

A cold backup for a Content Manager environment is straightforward: All components - relational database, document stores, etc. - are captured in their inactive state.

For a hot backup, you need to be careful and consider how to back up all the primary and optionally ancillary data components of a Content Manager system.

You essentially need to ensure the backup can capture the primary disk structures, like electronic stores, in a stable fashion at the same point in time you are performing a hot backup on the relational database.

Some options to consider:

- Using utility software to take a snapshot of the files and folders
- Using software or hardware replication or mirroring techniques, for example RAID, and associated mirror breaking and recovering features to capture one copy of the files and folders as a point-in-time snapshot
- Using a combination of the above or custom approaches

Always remember, treat your primary and optionally ancillary Content Manager data as one set.

Recovery techniques

Many systems include recovery facilities that enable you to restore to a particular point in time - which may not necessarily be the same point in time of a backup.

Such point-in-time recovery features usually use a database's transaction log to replay activity since a known backup point. This is sometimes referred to as rolling forward.

While you can use such a facility with your Content Manager relational database, remember the collateral impact and therefore steps required on other primary and ancillary data structures. File systems that hold your other Content Manager data structures do not have a transaction log on which

to rely - so rolling forward or rolling back your database requires some effort by you to keep these structures synchronized.

Several options are available if you need a point-in-time recovery:

- Roll forward/back only to a point in time at which a synchronized set of backups is available
- Roll forward/back to a desired point with a plan to accommodate any orphaned or ghost information

Always remember, treat your primary and optionally ancillary Content Manager data as one set.

Appendix A
Steps to Setting up a Working System

This section outlines a sequence of steps you need to go through to set up a working system.

This is often the task of a system administrator. Some of the points below are mandatory for any system to work, whereas some functions are optional. It depends on how you choose to administer your paper and electronic records. Refer to the Content Manager Help file **TRIM.chm** topics specified for a detailed explanation of each function and further guidance on how to complete each step.

Bookmark this section so that you can come back to it while you complete the steps.

The mandatory steps have an asterisk behind them.

1. **Install RDBMS software on the server to host the dataset***
2. **Install Content Manager software on the designated Workgroup Server computers***
3. **Using Content Manager Enterprise Studio, create and register the Content Manager dataset***
4. Using Content Manager:
   a. Set up the security levels and security caveats.*
      See **Security levels administration and Security caveats administration**.
   b. Set up postcodes.
      See **Postal codes**.
   c. Set up the internal and external Locations (Contacts and Organizations)*.
      See **Locations**.
   d. Set up user profiles - login accounts for staff who will use Content Manager*.
      See **Profile tab**.
   e. Set up a Thesaurus.
      See **Thesaurus**.
   f. Set up Classifications.
      See **Classifications**.
   g. Set up Archive Retention Schedules.
      See **Archive Retention Schedules**.
   h. Set up system options.
      See **System Options**.
   i. Set up the Content Manager calendar.
      See **Calendar editor for administrators**.

j. Set up noise words, title words and notes words.
   See **Word indexes**.

k. Recreate word indexes to index the Classifications, Retention Schedules, Thesaurus and other text fields.
   See **Recreate word indexes**.

l. Set up document content indexing and searching.
   In Content Manager Enterprise Studio Help, see **Document content index**.

m. Set up document stores.
   See **Document stores**.

n. Set up Record Types - after you have set up your Record Types, you can begin to create records*.
   See **Record Types**.

o. Set up New Record forms.
   See **Creating New Record forms**.

p. Set up Additional Fields.
   See **Additional Fields**.

q. Set up Lookup Sets.
   See **Creating Lookup Sets**.

r. Set up Actions and Procedures.
   See **Action tracking**.

s. Set up Workflow and Workflow Activities.
   See **Workflow**.

t. Set up record Holds.
   See **Holds**.

u. Set up report layouts.
   See **Report layouts**.

v. Set up Web publisher layouts.
   See **Web Publisher**.

w. Set up barcode scanners.
   See **Barcode scanners**.

x. Set up Space management - the storage space environment that will contain your archived or stored records.
   See **Space management**.

y. Set up electronic document management - desktop integration with other software packages.
   See **Electronic document management**.

z. Set up the user layout options of your Content Manager interface.
   See **Options and Customizing and creating toolbars**.

Content Manager is configured.

You can now start creating records.

See Content Manager Help topic **Creating records**.

Appendix B
Installing and Upgrading the Thin Office and Outlook Integration

Overview

The Content Manager thin integration with Microsoft Office and Outlook enables users to use a ribbon tab to access Content Manager directly from their Microsoft Office and Outlook applications without the need to have the Content Manager client installed on their computer. Instead, they connect to Content Manager by using the Content Manager Web Client.

While the installation runs for all users of the computer by default, the IT administrator can create a registry key on the computer for specific users that stops the setup of Content Manager Thin Client for these users. It must also have a value of **1**.

To exclude a user from Content Manager Thin Client setup on a computer, under their profile, create the new registry key: **HKEY_CURRENT_USER\SOFTWARE\Micro Focus\Content Manager**.

Then create a string value key in Content Manager with the name **ThinOfficeDisabled** and a value of **1**.

Specifications and requirements

For specifications and requirements, see **CM9.3_Spec.pdf** in your Content Manager **Documentation** folder in the installation folder or the installation media.

Additionally, users of the Content Manager Thin integration with Office and Outlook should set Internet Explorer to check for newer versions of stored pages **Every time I visit the webpage**. This option is in **Tools > Internet options** and under **Browsing history**, **Settings**. This is also a required setting to run Content Manager Web Client.

Installation steps

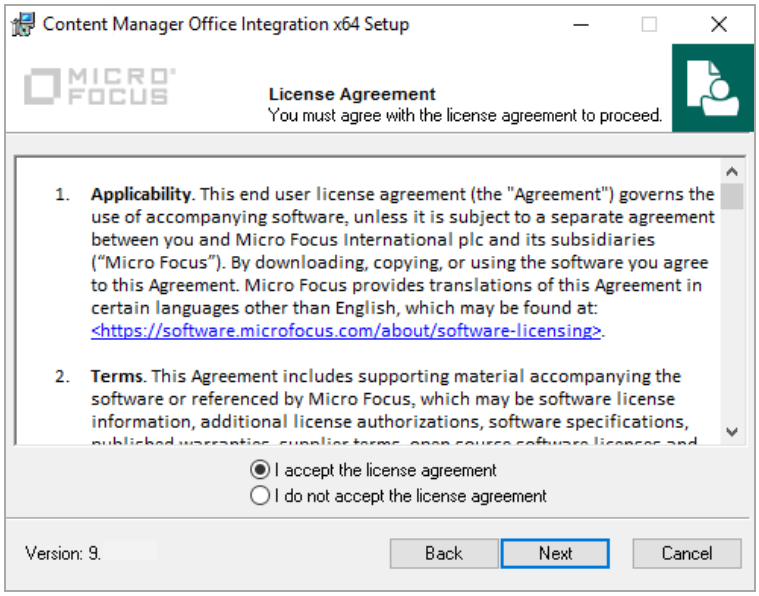
1. On your installation medium, locate the installation file and run it as administrator:

   CM_ThinOfficeIntegration_xNN.msi

   The installation dialog appears:

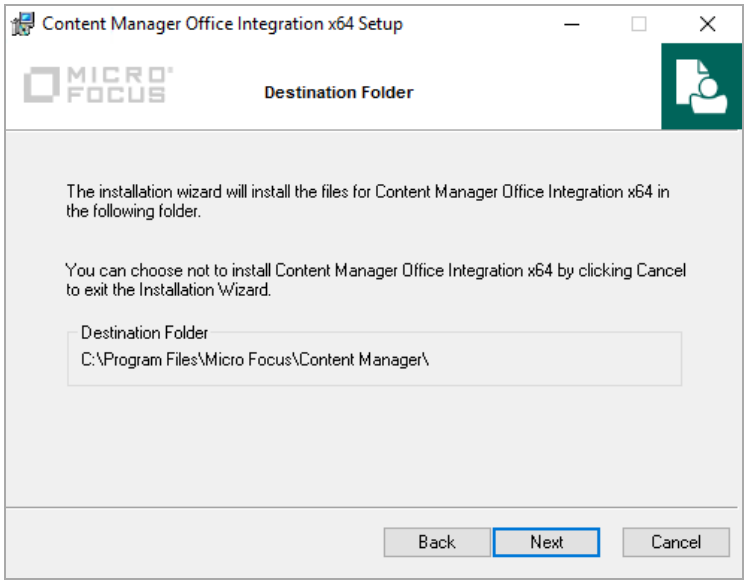
2. Click **Next**.

   The **License Agreement** dialog appears:



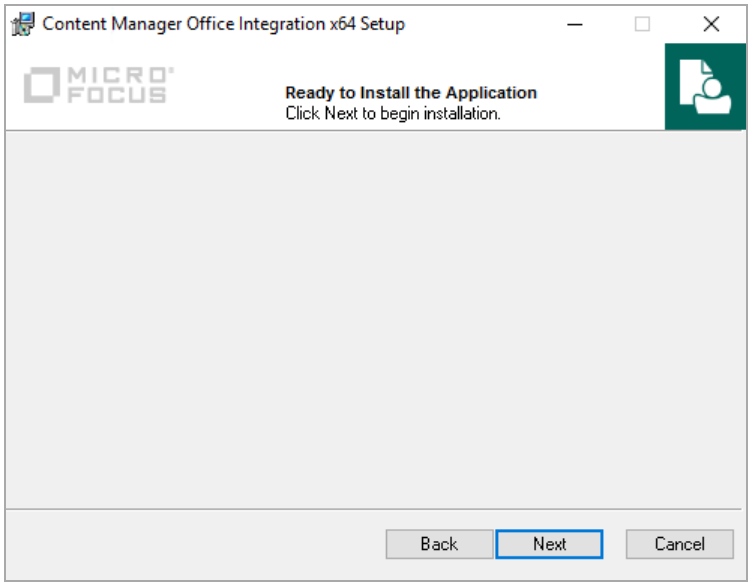
3. Select **I accept the license agreement** and click **Next**.

   The **Destination Folder** dialog appears:



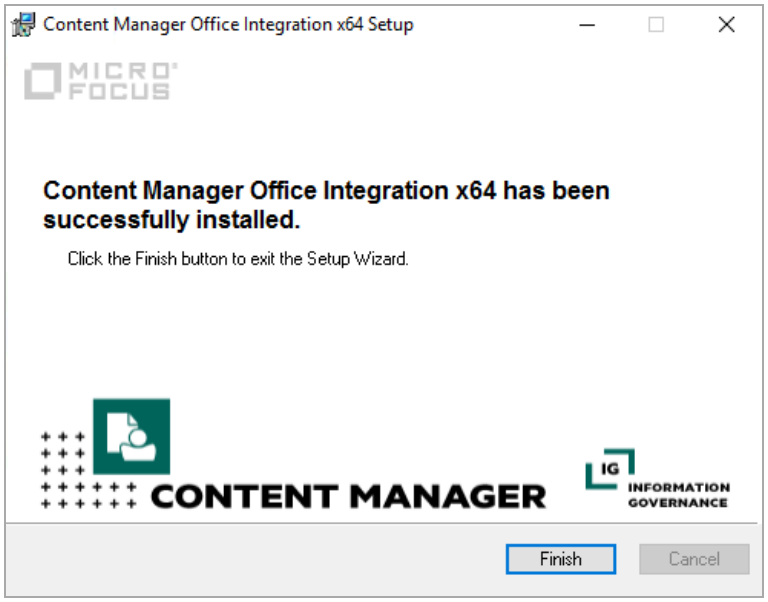
4. Click **Next**.

   The **Ready to Install the Application** dialog appears:



5. Click **Next**.

   Content Manager Thin Office integration is installed.



6. Click **Finish**.

   To uninstall the Content Manager Thin Office integration, use the Windows **Control Panel > Programs > Programs and Features** function and uninstall the Content Manager Office Integration xNN instance.

> **TIP:** The required directory for the **Preferences** file is **C:\Users\<username>\AppData\Roaming\Micro Focus\Content Manager\OfficeIntegration**. This file will be automatically created when a user accesses the Office integration for the first time and they will need to define their settings from the Office, or Outlook, **File** - **Content Manager Options** menu; or it can be pushed out as a part of the installation process, with the required properties pre-defined.

Upgrading the Thin Office and Outlook Integration

To upgrade the Thin Office integration see the installation steps in Installation steps, on page 80.

After upgrading from 8.3 to Content Manager 9.0 there are some configuration steps to undertake and some changes to the application that users need to be aware of.

Configuration Requirements after Upgrade

As a part of the upgrade process from Records Manager 8.3 to Content Manager 9.x, you will need to re-enter the **WebClient URL** that the Thin Office integration connects to. This can be done on a user by user case via the **Options** panel in Outlook, or the System Administrator can roll out a copy of the **Preferences** file with the **<RMClientURL><http://WebClientURL></RMClientURL>** property already defined as a part of a Group Policy, or similar, installation. The required directory for the

Preferences file is **C:\Users\<username>\AppData\Roaming\Micro Focus\Content Manager\OfficeIntegration**.

If users created **Check In Styles** in Records Manager Thin Outlook Integration that had no defined Record Type, after upgrading, these **Check In Styles** will not be available in Content Manager. An error message will be displayed when the user first attempts to open the Outlook integration advising that there was an error when attempting to upgrade and that they should check the **CatalgoueOptions.broken** log file for more information. By default, the **CatalogueOptions.broken** log file is installed to, **C:\Users\<username>\AppData\Roaming\Micro Focus\Content Manager\OfficeIntegration**

The **Check In Styles** that were not upgraded will have to be manually created in Content Manager.

> **NOTE: Check In Styles**, that have an associated Record Type, that were created in Records Manager 8.3 will be upgraded to Content Manager 9.x but only after a valid **Web Client URL** is added to the in the **Options** panel within MS Outlook, or the user's **Preference** file is updated.

Appendix C Troubleshooting

Troubleshooting the Workgroup Server

Workgroup Server does not start

1. Check login parameters
2. Check Windows event viewer
3. Check the Workgroup Server log files

Crashdump files

When the Workgroup Server experiences a general protection fault, by default, it creates:

- one large .dmp file per crash per hour.

You can adjust the frequency by using the registry dword **crashdumpfrequency** and the value means files per day.

- one small .dmp file per crash
- one log file per crash

You can use a registry key to modify the type of data that the large .dmp file includes:

HKEY_LOCAL_MACHINE\SOFTWARE\Micro Focus\Content Manager\WorkgroupServerConnection with the dword **CrashDumpType**.

The value should be one of the ones listed in this site: *http://msdn.microsoft.com/en-us/library/ms680519(VS.85).aspx*, for example 0x1227.

A Workgroup Server saves the diagnostic files to:

C :\Micro Focus Content Manager\ServerLocalData\TRIM\Log\<crash-file¬number>.log

C :\Micro Focus Content Manager\ServerLocalData\TRIM\Log \<crash-file¬number>. dmp

A Content Manager client computer by default, saves crashdump files to:

C:\Users\<user>\AppData\Local\Micro Focus\Content Manager\<dataset ID>\Temp.

Rendering module output does not appear

When the Content Manager rendering module fails to render the long-term storage format of documents, it may record the message in the render log file:

Error: Printer output file did not appear: [7: printer file failed to appear within timeout] [Info: C:\Users\<*username*>\AppData\Local\Micro Focus\Content Manager\out.pdf]

This is usually due to incorrect print processor configuration.

To fix this issue:

1. In the Windows **Printers** dialog box, right-click **TRIMRender_PDF**, click **Properties**.

   The **TRIMRender_PDF Properties** window appears.

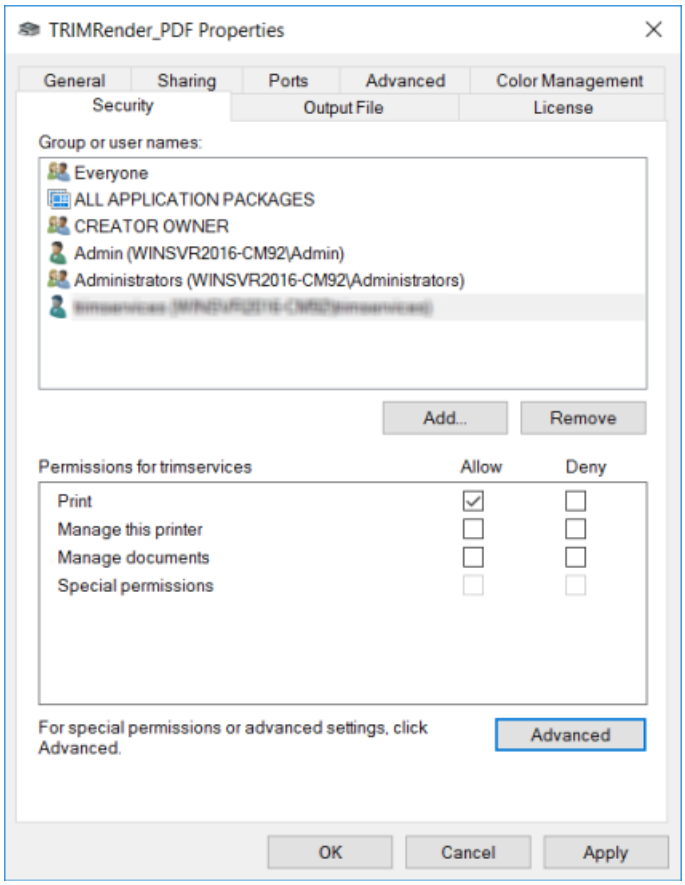
2. On the **Advanced** tab, click **Print Processor**

3. For **Print processor**, select **PrintOnstream Driver** and for **Default data type**, select **NT EMF 1.003**

Appendix D
Document Render

Securing the print drivers

After installation of Content Manager, the print drivers, **TRIMRender_PDF** and **TRIMRender_TIFF**, associated with the Document Rendering process should be updated to ensure the Content Manager Services account, e.g. **CMServices**, has **Print** permissions for the drivers.



Printing preferences

The Document Rendering processor uses the Onstream systems print drivers to render documents into renditions. The drivers come with default settings which may not necessarily suit your needs.

Changing the settings

1. In the Printers and Faxes folder, right-click the **TRIMRender_PDF** driver and select **Printing**.

   The **TRIMRender_PDF Printing Preferences** dialog appears.

3. In the **Output File** tab, change the **Paper Size** settings to suit your needs.
4. Change the **Resolution** settings to suit your needs.
5. Apply other printing preferences as required.

Print Verbs

Overview

In a Windows environment, when you right-click a file in Windows Explorer and click **Print**, the associated application, e.g. XYZ, opens, prints the file and exits, displaying as little as necessary to complete the task.

It does so because it invokes the verb **print**.

The Content Manager Rendering module also invokes the verb print programmatically during the rendering process.

When the installed application is not printing .xyz documents correctly and you want to print them using a command other than the default print verb, it may be necessary to manually edit the print verbs in the registry.

Changing a Print Verb

> **CAUTION:**
> Only qualified administrators should make changes to the registry
>
> Please make a backup of your registry before proceeding
>
> Mistakes changing registry settings can lead to unrecoverable errors and the computer being unusable.

For more information on print verbs and how to print, for example, .xyz files with a different application that has a command line switch for printing, please refer to Microsoft documentation. Depending on your knowledge, this could be a starting point:

http://msdn2.microsoft.com/en-us/library/aa969321.aspx#anyfiletype

See **TRIMEnterpriseStudio.chm** for information about functionality and operation of the Content Manager Rendering module.

Appendix E
Demonstration Database

Installation and Setup

Overview

The Content Manager installation media contains a Content Manager database you can use as a demonstration or test database. It contains sample data including Record Types, a Thesaurus, Classifications, Actions, Procedures, different Location types, records and attached electronic documents. It is designed to be a stand-alone version of an Content Manager database to demonstrate what you can store in Content Manager and how its components work together.

Setting up the demonstration database

Prerequisites

- Content Manager must be installed
- Microsoft SQL Server 2008, 2008 R2 or later or one of their Express editions must be installed
- The user must be a member of the computer group **SQLServerMSSQLUser$<computer name>$SQLEXPRESS** or their equivalents

Extracting the file

The file on the Content Manager installation media is **Demonstration Database\DemoDB.zip**.

1. Unpack the file **DemoDB.zip**.
   It unpacks to the sub-folder **DemoDB** with a directory structure for the document store (**\45\2\00**), which is required for the demonstration database to function correctly.
   You can move the document store structure to any writable location; however, for ease of use, it is recommended that you keep them in the same directory structure as the demonstration database.

Setup

1. In SQL Server, create a new database and name it **DemoDB**
2. Using SQL Server2008, 2008 R2 or later, restore the database backup **DemoDB.bak** from the Content Manager installation media to a new destination folder in **C:\Micro Focus Content Manager\ServerData**, for example, **DemoDB**.

The Content Manager installation creates the folder **ServerData**. However, for the restore, you can use any location outside the folder **Program Files** that you can write to.

The restore creates the files **DemoDB.mdf** and **DemoDB.ldf** in your destination folder.

3. Start Content Manager Enterprise Studio
4. Right-click **Datasets** and click **Register Dataset**.
   The dialog **Register New Dataset– Identification** appears.
5. Fill in the fields:
   - **Dataset Name** – enter **DemoDB**
   - **Dataset Identifier** – enter **45**
6. Select **Microsoft SQL Server** and click **Next**.
   The dialog Register **New Dataset – Connection** appears.
7. In the field **OLE DB Connection String**, click KwikSelect and in the dialog **Data Link Properties**, set up the database connection:
   a. In the field **Select or enter Server name**, enter your computer name followed by **\SQLEXPRESS**, if you are using SQL Server Express
   b. Under **Information to log on to the server**, select **Use Windows NT Integrated security**
   c. Under **Select the database on the server**, select **DemoDB**
   d. Click **Test Connection**. If the connection fails, check you followed the previous steps correctly.
   e. Click **OK**. The dialog **Data Link Properties** closes and you are using the dialog **Register New Dataset – Connection** again.
8. For **Guest Login**, enter **DEMO** in upper case and click **Next**.

   The dialog **Register New Dataset – Options** appears.
9. Click **Next**.

   The dialog **Register New Dataset – Document Store** appears.
10. In the field **Path for Default Document Store**, click KwikSelect to select the folder **DemoDB**
11. Click **Finish**.

    A warning message about UNC paths may appear, which is not relevant for a demonstration setup. You can ignore it and click **OK**.

    The dataset appears in the list of datasets.

12. Configure event processing so that document content processing is enabled
13. Right-click the dataset, point to **Content Index** and click **Create Content Index**.
14. Start Content Manager and click **File – Open**.

    The dialog **Open Content Manager Dataset** appears.
15. Click **Add**.

    The **Add Datasets – Choose Machine** dialog appears.
16. Select **Choose Local Datasets** and click **Next**.

    The dialog **Add Datasets – Available Datasets** appears.
17. Tag the new dataset and click **Finish**.
18. In the dialog **Open Content Manager Dataset**, select the new dataset and click **OK** to open it.

    You are now logged on to the database as Peter Abbott, who is a Content Manager administrator.
19. Create a new administrator login for yourself you can use for future logins.
20. In Content Manager, create the document content index by using the **Reindex** function.

The setup is complete.

Appendix F
User Setup Executable

Overview

The executable **TRIMUserSetup.exe** performs the function of setting up a new user's HKCU registry hive to enable them to run Content Manager using the information provided during setup and recorded in **HKEY_LOCAL_MACHINE\SOFTWARE\Micro Focus\Content Manager\MSI Setup**.

The executable has replaced the executable **TRIMAutoDeploy.exe**.

TRIMUserSetup.exe runs the first time a user logs on and then not again unless an update of Content Manager has been performed.

Deactivating the Content Manager user setup executable

Overview

You should only deactivate the user setup executable if instructed to do so by Content Manager Support.

You can use the following script and Group Policy object to deactivate the Content Manager user setup executable through the registry.

The registry key **TRIMUserSetup_On** is in **HKEY_LOCAL_MACHINE\Software\Micro Focus\Content Manager\MSISettings** and has a default value of **1**. **TRIMUserSetup.exe** checks this value and will only run if it is set to 1. You can change this through Group Policy to be 0.

Deactivation works through a combination of a script and a Group Policy object.

Creating the script

The following script will prevent the user setup executable from creating HKCU registry keys. It should be saved in the folder **%windir%\system32 \GroupPolicy\Machine\Scripts\Logon**.

```
Set Sh = CreateObject("WScript.Shell")

Key = "HKEY_LOCAL_MACHINE\"

SH.RegWrite Key & "Software\Micro Focus\

Content Manager\MSISettings\TRIMUserSetup_On", 0, "REG_SZ"
```

Applying the script to Group Policy

1. From the **Start** menu, type **Run** and press **Enter**

   Type **GPedit.msc** and press **Enter**

   Navigate to **User Configuration - Windows Settings - Scripts (Logon/Logoff)**

   Right-click **Logon** and select **Properties**

   Click **Add**.
   The logon script you saved earlier should appear in the default scripts folder.

   Select the logon script and click **OK** twice

Appendix G
Geographical Information System (GIS) Data Integration

The following information provides additional configuration information for the GIS Integration:

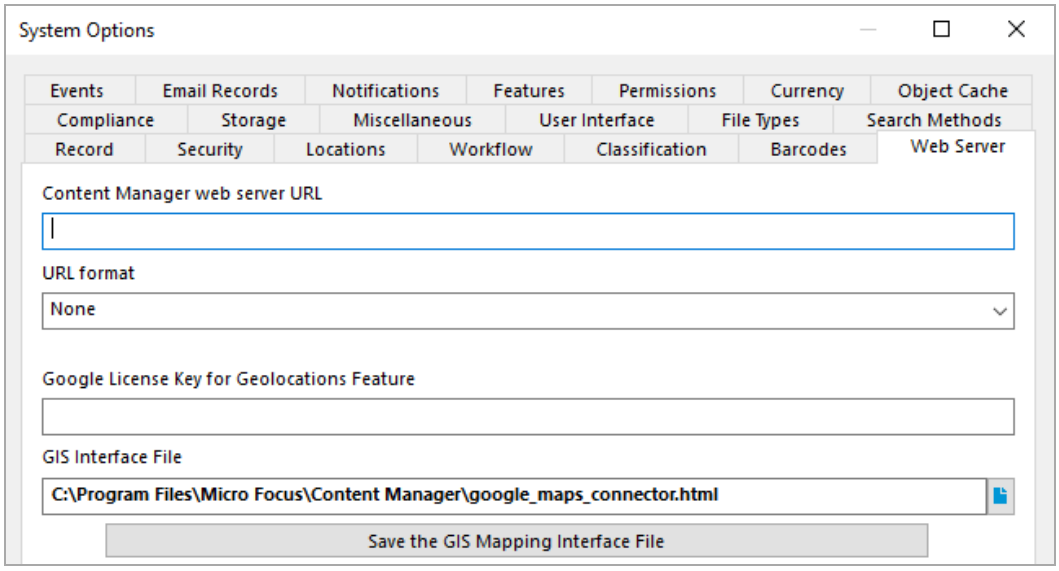
Google License Key

By default Content Manager client ships with the free version of the Google Maps API, however this has some limitations. For unrestricted use you may need to buy a license from Google. The key can be added to the Content Manager System Option – Web Server – Google License Key for Geolocation Feature.

> **NOTE:** If your organization is using the GPS feature in the Content Manager Web Client, you will require a Google License Key for this feature to work.

Default Mapping Provider

The main API used is the google_maps_connector.html file, located in the Content Manager binaries path which is set by default in Content Manager System Options – Web Server – GIS Interface File.



Using a different mapping provider

Any mapping provider that has a java script API can be used instead of the Google mapping option. This will require code to be written in the either the google_maps_connector.html file or saved as an

html file into the Content Manager System Options – Web Server – GIS Interface File.

Supported WKT Formats

Content Manager only supports the following Well-Known Text (WKT) formats, a text markup language for representing vector geometry objects:

l POINT (lng lat) lng and lat are decimal numbers such as 145.533829.

l LINESTRING (lng lat, lng lat) a 2 point line or

l LINESTRING (lng lat, lng lat, lng lat) a 3 point line.

l POLYGON ((lng lat, lng lat, lng lat, …)) for any number of points >= 3

HTML functions

The important functions within google_maps_connector.html file.

HPRM_Mapping_resetGPSData()

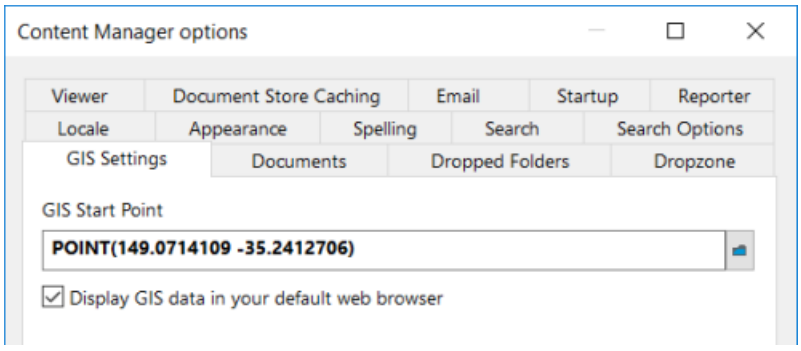
HPRM_Mapping_getGPSData()

HPRM_Mapping_setGPSData()

These javascript functions are called from the main Content Manager client and must be present in the html file, otherwise Content Manager will report an error.

HPRM_Mapping_setGPSData()

This function is called to set the map to the initial location. Users can set a location meaningful to them on the GIS Settings tab in Content Manager. This user option is access from the File menu and click Options. Once a Location or record has been created, the initial state of the map will be the geolocation of the Location or record.



The arguments to this function are pairs of numbers. The 1st pair is

l X, 0 where X is 0 for a POINT, 1 for a LINESTRING or 2 for a POLYGON

l The remaining pairs are each point latitude then longitude – expressed as decimal format

HPRM_Mapping_getGPSData()

This function is called to get the point or points from the map. The function must return the GPS data in WKT format as described above.

HPRM_Mapping_resetGPSData()

This function is called when the user presses the Reset button on the Content Manager GPS Browser Dialog. It resets the map to the location or record's original GPS data. For information about using the Geographical Information System Data Integration, refer to the user help:

Content Manager Help > Locations and users > Location and user administration > Geo Locations

Appendix H
Content Manager Media Server

Content Manager uses Media Server to perform optical character recognition (OCR) on images. This enables users to search the content of image files like any other document.

Prerequisites and Requirements

These instructions assume you have already successfully installed and configured:

- Content Manager Workgroup Server (64-bit) 9.x

To use the Media Server with Content Manager for OCR, your system must meet the following requirements:

- Content Manager Media Server must be installed on a computer on your network. You can install it by using **CM_MediaServer_x64.msi** from your Content Manager installation media, which is described below. It installs as the service **Content Manager Media Server**. For OEM IDOL environments, you can install it by using **CM_IDOLComponents_x64.msi** from your Content Manager installation media, see **CM9.3_IDOL_DCI_Install_Config.pdf** for details.
- You must have a license for the **OCR Image Processing** module and the **Document Rendering** Feature must be enabled in the Content Manager client.
- The **OCR Server Name** and **OCR Server Port** must be specified in the **Configuring Rendering** - **OCR** tab in Content Manager Enterprise Studio.

Installation steps

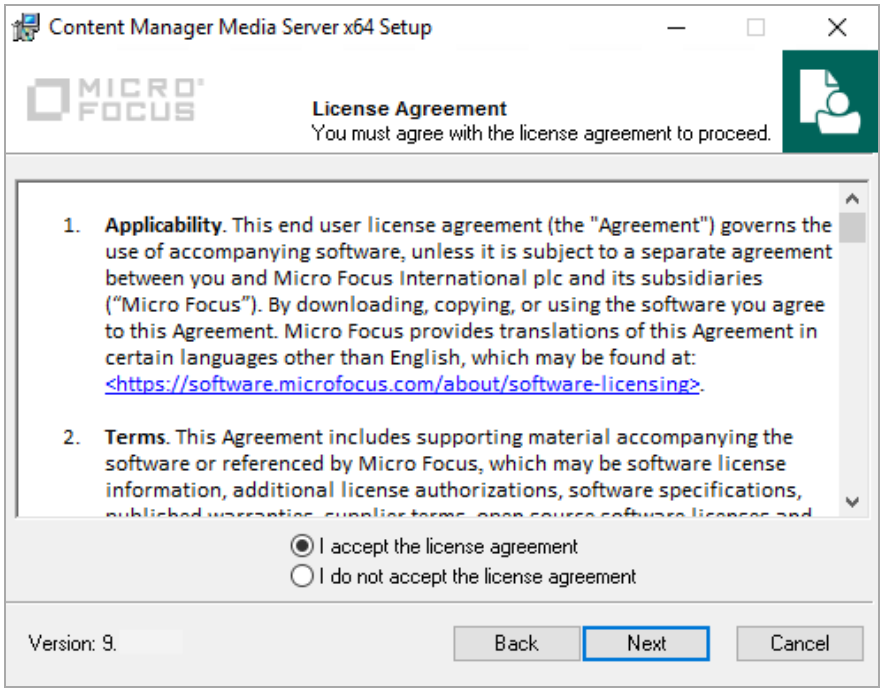
1. On your installation medium, locate the installation file and run it as administrator

   CM_MediaServer_x64.msi

   The **Welcome to the Content Manager IDOL Media Server x64 Installation Wizard** dialog appears:

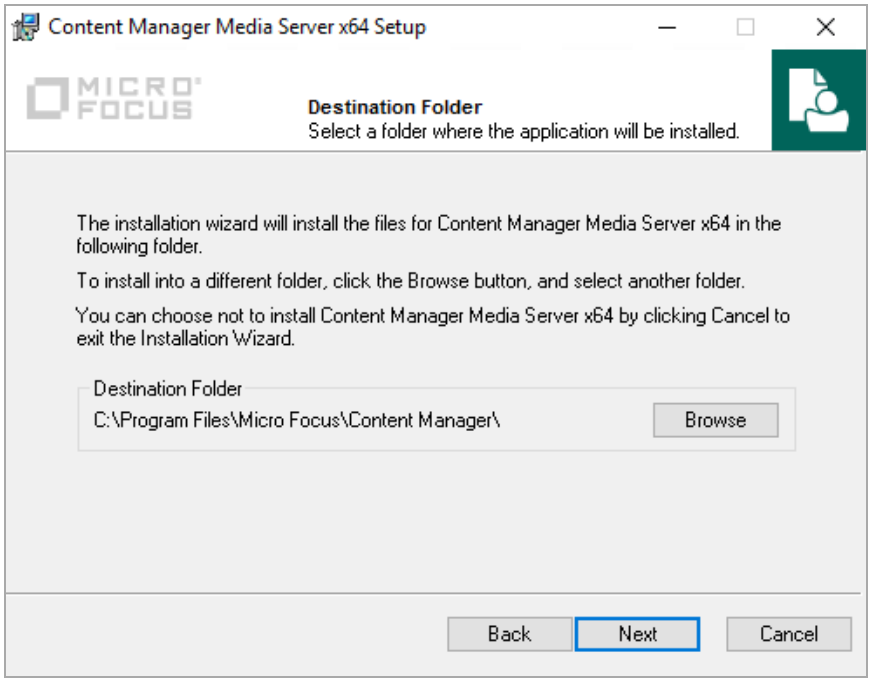
2. Click **Next**.

   The **License Agreement** dialog appears:



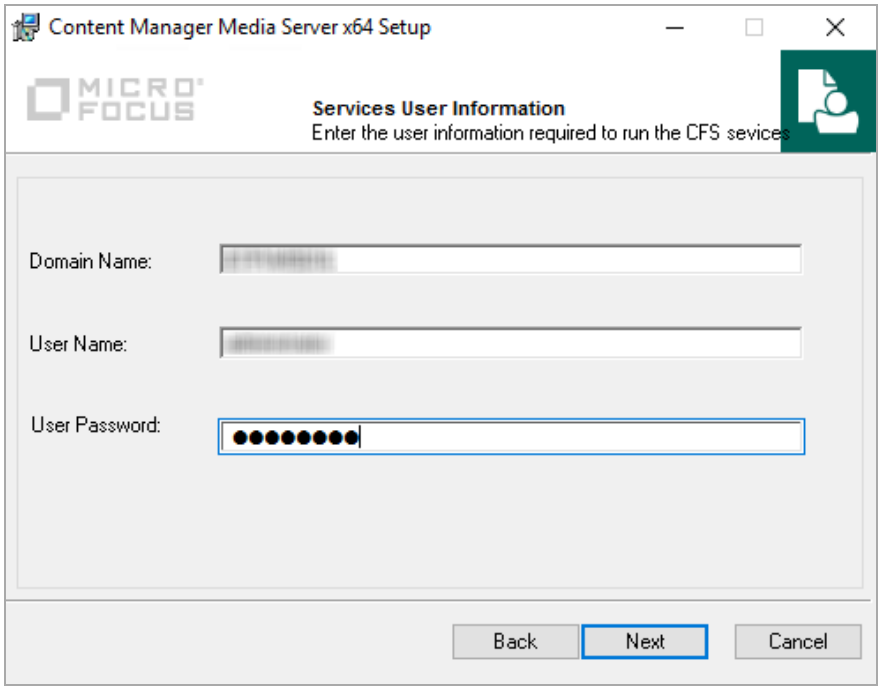
3. Select **I accept the license agreement** and click **Next**.

   The **Destination Folder** dialog appears:



4. Change the installation folder if the default is not suitable (this is not recommended) and click **Next**.

   The **Services User Information** dialog appears:

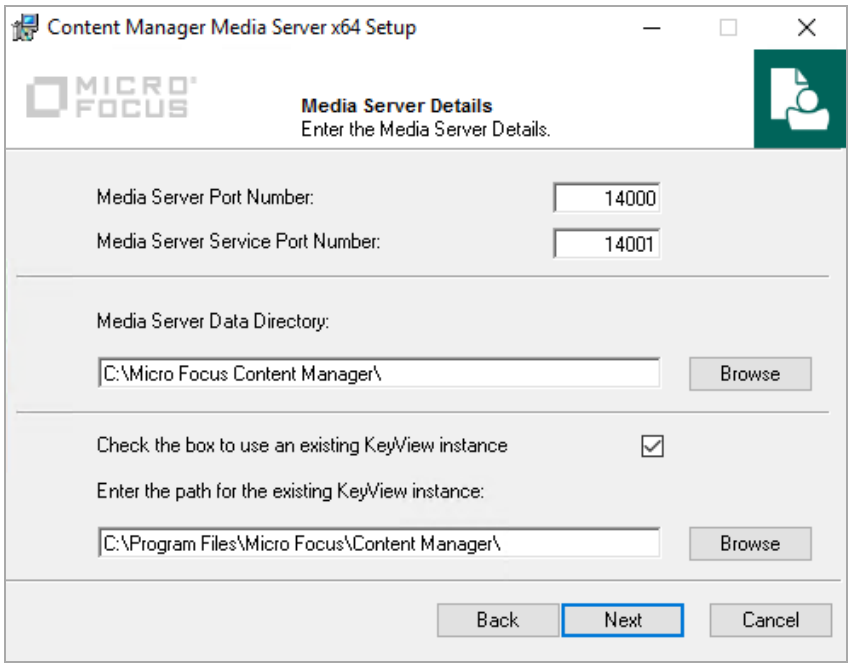


5. Enter the details of the user account to run the Services in the fields:

- **Domain Name** – type in the Domain Name.
- **User Name** – type in the User Name of the account to run the Image services e.g. **CMServices**
- **User Password** – type in the user's password.

6. Click **Next**.

   The **Media Server Details** dialog appears:



7. Enter the details for the Media Server in the fields:

   - **Media Server Port Number** – type in the Media Server port number. By default it is 14000.
   - **Media Server Service Port Number** – type in the Media Server port number. By default it is 14001.
   - **Media Server Data Directory** – displays the default path for the Media Server Data Directory. If required, type in a new path.
   - **Check the box to use an existing KeyView instance** – select this option if you already have an instance of KeyView installed, for example, the KeyView instance installed with Content Manager. Media Server needs KeyView to operate correctly.

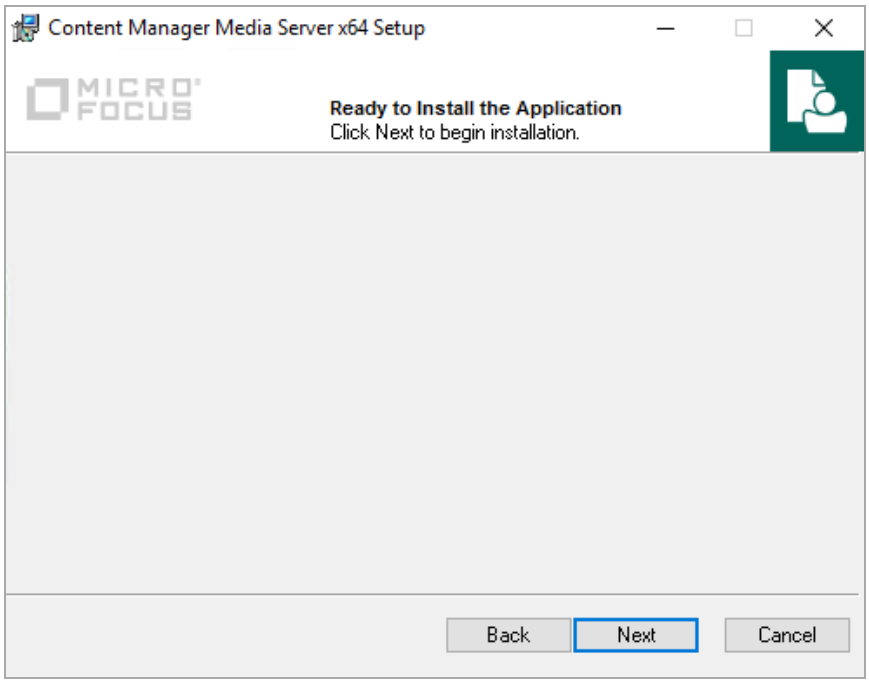
     When selected, the field to specify the location of the KeyView instance becomes available for you to use.

Leave the selection box clear if you do not have an instance of KeyView on the computer, for example, because you are installing Media Server on its own computer. In that case, the installation will also install KeyView.

- **Enter the path for the existing KeyView instance** – displays the default path for the KeyView instance. If required, browse to and select a new path.

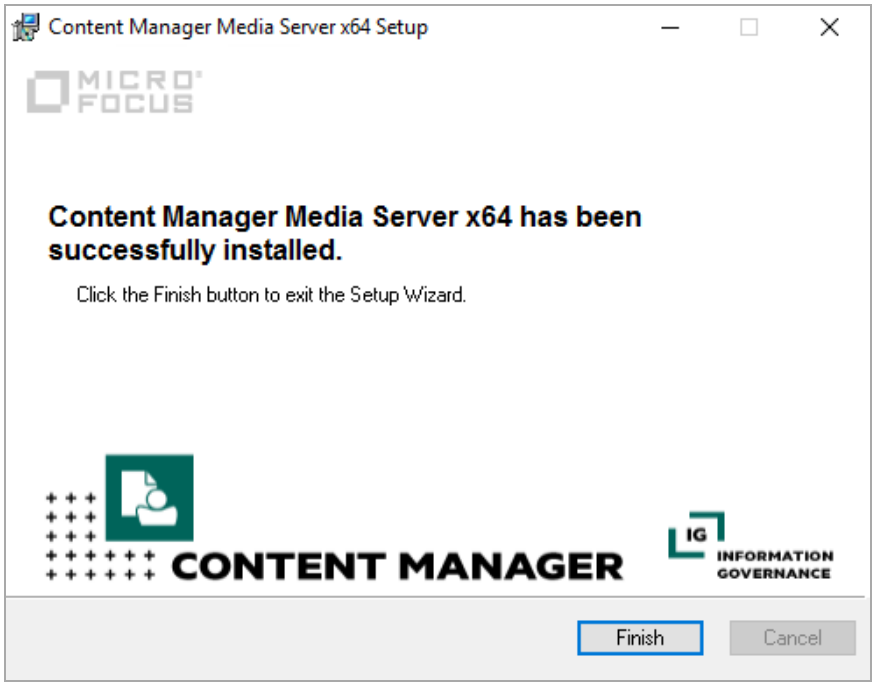
8. Click **Next**.

   The **Ready to Install the Application** dialog appears:



9. Click **Next**. The **Updating System** dialog appears.

   The **Media Server x64** successfully installed dialog appears:



10. Click **Finish**.

The installation of the Content Manager Media Server is complete.

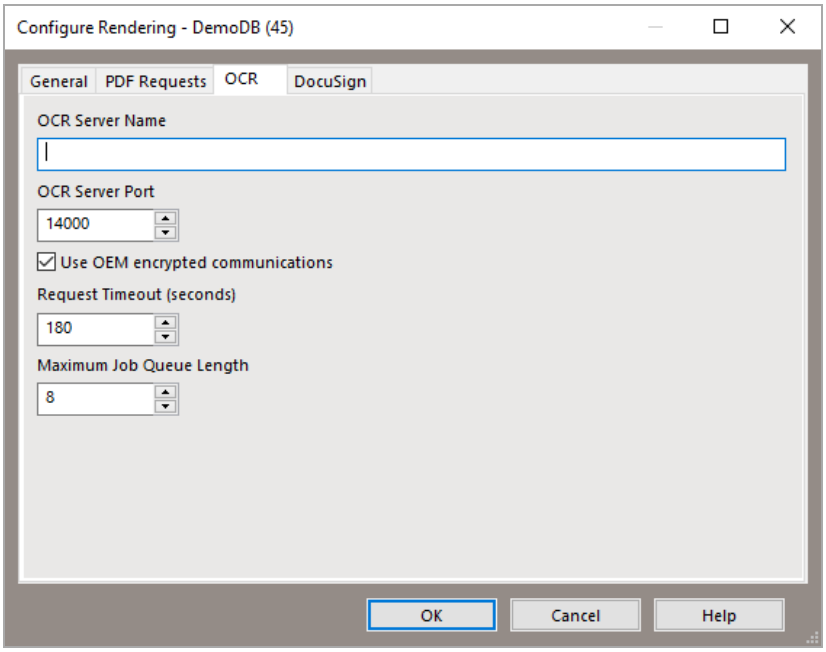
In the list of services on the computer, the service appears as **Content Manager Media Server Service**.

OCR rendering installation and configuration

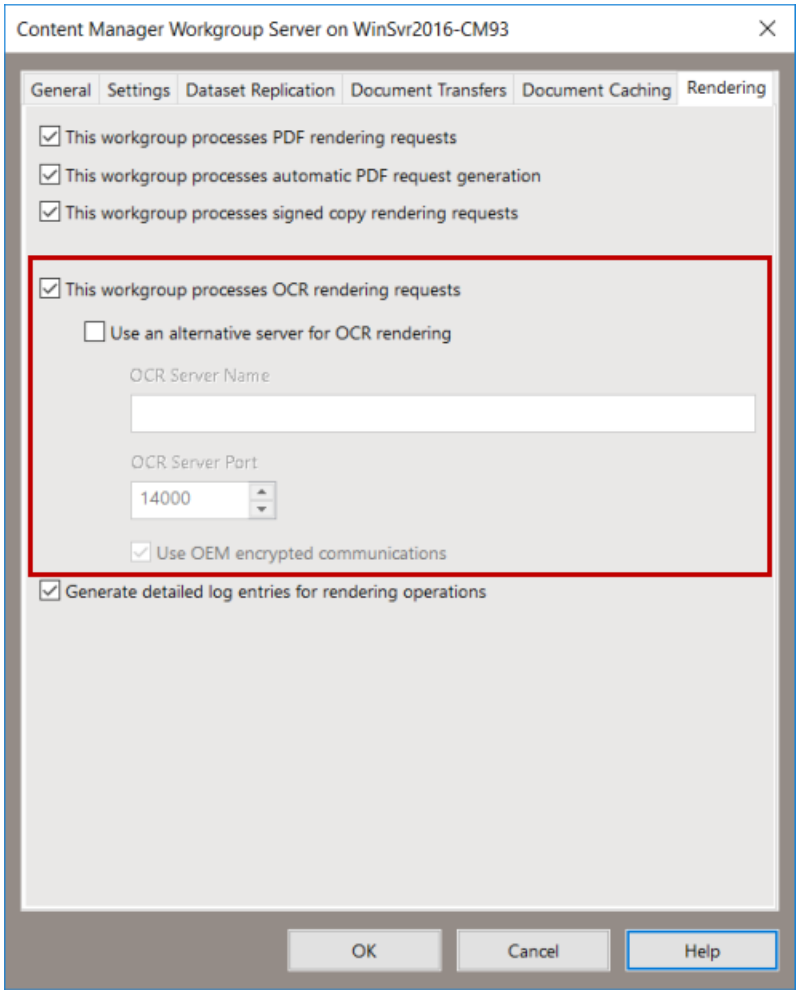
These instructions assume that you have a working Content Manager environment with clients, at least one Content Manager Workgroup Server and have the Document Rendering Event processing enabled and configured.

1. On the Media Server computer, use **CM_IDOLComponents_x64.msi** to install **Media Server**. See Installation Steps for details.
2. Ensure all the Content Manager services are started, including **Content Manager Media Server**.
3. In Content Manager Enterprise Studio on the **Home** tab, in the **General** group, click **License**. Apply the license file that you received from Software Support that enables OCR Image Processing functionality in Content Manager.
4. In the Content Manager client, on the **Administration** tab, in the **Options** group, click **System**. On the **Features** tab, enable **Document Rendering**. Click **OK**.
5. In Content Manager Enterprise Studio, expand the **Dataset** node and right-click on the dataset

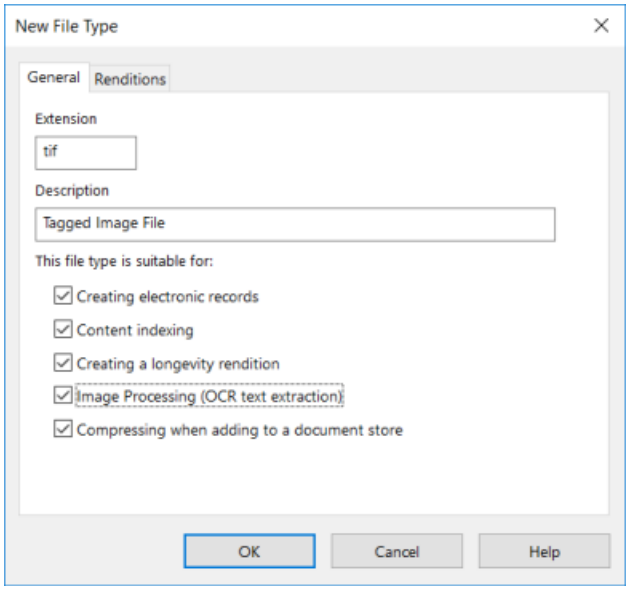
name, point to **Event Processing** and then click **Rendering**.
The **Configuring Rendering <datasetname>** dialog appears.



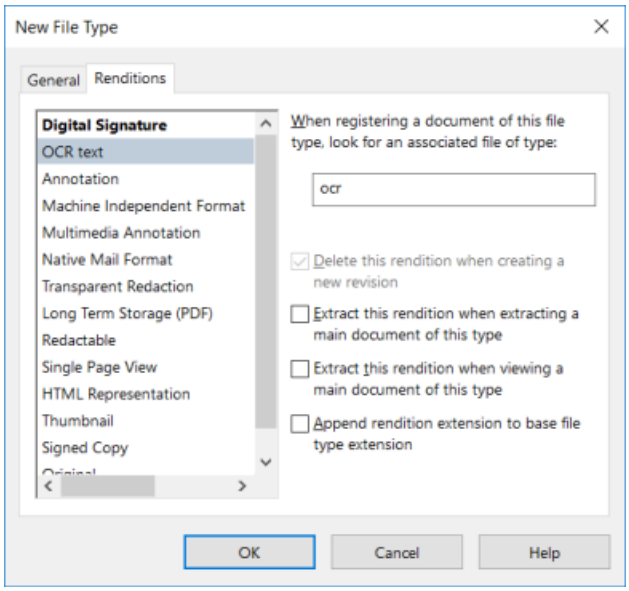
6. On the **OCR** tab, set **OCR Server Name** to point to where the Media Server was installed. The default port is 14000.
   - **Use OEM encrypted communications** - default: enabled with the OEM IDOL license. Disable if you are using Enterprise IDOL and require communications outside of Content Manager.
   - **Request Timeout (seconds)** - The duration in seconds before a request that has been submitted to the Media Server is automatically canceled by Content Manager. Once the timeout period has elapsed, Content Manager will mark the request as failed.
   - **Maximum Job Queue Length** - The maximum number of concurrent jobs that can be submitted to the Media Server.
7. Click **OK**.
8. In Content Manager Enterprise Studio, expand the **Workgroup Servers** node, right-click on the Workgroup Server name that is to process OCR rendering requests and then click **Properties**.
   The **Content Manager Workgroup Server <WGS name>** dialog appears.



9. On the **Rendering** tab, select **This workgroup processes OCR rendering requests**. If there is an alternative server processing OCR requests, the properties of this server can be defined using the **Use an alternative server for OCR rendering** option.
10. Ensure all Workgroup servers that are processing OCR rendition requests have this option enabled. Click **OK**.
11. In Content Manager Enterprise Studio, **Save** and **Deploy** your configuration changes to the Workgroup Servers.
12. In Content Manager, on the **Administration** tab, in the **Options** group, click **System**.
13. On the **File Types** tab, click **Add** and add an appropriate file type for OCR, e.g. TIF or JPG and select **Content Indexing and Image Processing (OCR text extraction)**.



14. On the **Renditions** tab, select **OCR text**. On the right for the field **When cataloging a document of this file type…**, type **ocr**.
15. If not enabled, select **Delete this rendition when creating a new revision** and click **OK** twice.



16. To automatically create OCR Renditions when records of a suitable type are checked into Content Manager, in the Content Manager client, on the **Manage** tab, in the Records group, click **Record Types**.
17. On the Record Type name, right-click and click **Properties**. On the **Record Type Properties** dialog, on the **Electronic** tab, select **Automatically create OCR rendition (for tif, jpg, etc.)** and then click **OK**.

Make sure that the services are running:

- **Content Manager Media Server**
- **Content Manager Workgroup Service**

The setup is complete.

Now, when you check in an electronic document to Content Manager, for example, a .tif file, a text rendition will automatically be created and will be attached to the record, where it becomes visible in the record **Properties - Renditions** tab.

The rendering processing queue can be monitored within the Content Manager client. From the **Administration** tab, in the **Other** group, click **Monitor Render Queue**. The **Monitor Render Queue** dialog appears displaying all documents that are in the render queue. See the Content Manager Help file for additional information.

After that, Content Manager indexes the document content, which makes it retrievable by using a document content search.

> **NOTE:** There is a delay before the document content is available for searches. This is because by default, the delay is set to be 600 seconds in the content service configuration files, using the parameter MaxSyncDelay. For testing purposes, you could change this value to 30 temporarily by editing the configuration files.
>
> For advanced OCR configuration details (including the OCRing of rotated text or other languages), please refer to the Media Server Admin guide (which can be downloaded as a ZIP file from http://h30359.www3.hpe.com/online_help/IDOL/Servers/Media%20Server/12.0/Packages/MediaServer_12.0_Documentation.zip).

Troubleshooting OCR Rendering

File types

Ensure that the file types for the target documents have been configured correctly in Content Manager **System Options** - **File Types** tab as the file type extension, and not with a leading asterisk (*).

For example, the file type should be entered as **JPG** and not ***.JPG** - this would appear in the **File Types** dialog in Enterprise Studio as ***.*.JPG** instead of ***.JPG**.

Media Server log files

The Media Server log files, **TRIMRender.log**, can be used to check on how files are progressing through the Media Server. These logs can be useful for determining if files are being sent to the Media Server, and if the problem is occurring before, during or after the Media Server steps.

Appendix I
Upgrading SQL Server Connection Strings

After upgrading the software and running Enterprise Studio, on the primary Workgroup Server, all SQL Server datasets registered in the system will report 'Could not connect'.

This is because we have removed our dependence on OLE DB driver for talking to databases and replaced it with ODBC driver. The system, however, does not automatically update the connection strings. This needs to be done manually.

As per these Installation instructions you should have noted down the connection settings for your SQL Server datasets prior to upgrading.

1. Open each dataset's Properties.
2. Change to the **Connection** tab.
3. Click the KwikSelect button.
4. Enter the values noted into the appropriate fields in the new **Connection Settings** dialog for SQL Server.
5. Click **Test Connection** to make sure the database connection string works.
6. Click **OK** to save changes.
7. Click **OK** to save dataset settings.
8. Deploy these changes to all Workgroup Servers as normal.

See **Content Manager Enterprise Studio Help – Connection Settings dialog box for SQL Server** for further information.

Appendix J
Special Database Configurations

For SQL Server's AlwaysOn Availability groups

Content Manager now supports SQL Server's AlwaysOn Availability groups. Please refer to the following link on how to install and configure this setup: https://docs.microsoft.com/enus/sql/database-engine/availability-groups/windows/overview-of-always-on-availability-groups-sqlserver

> **NOTE:** Content Manager does not support read-only routing.

To facilitate this for Content Manager, the administrators will need to modify the dataset **Database Connection String** properties in Content Manager Enterprise Studio for each of their datasets.

On the dataset **Properties - Connection** tab, click the KwikSelect on the **Database Connection String** field, the S**QL Server Connection Settings** dialog will appear. The following changes are required to be made and saved:

- The Server Name field will need to be changed to be the IP address or name of the AlwaysOn Availability group's Listener.
- The Database Name field will need to match one of the AlwaysOn Availability group's synchronized databases.
- Select the Use AlwaysOn Availability Groups option.

For Microsoft Azure's SQL Database

Content Manager now supports Microsoft Azure's SQL Database. Please refer to the following link on how to create your account and configure a database: https://azure.microsoft.com/en-us/services/sqldatabase/

To facilitate this for Content Manager, the administrators will need to perform the following steps:

- In Content Manager Enterprise Studio, from the **Home** tab, in the **New** group, click **Create Dataset** to display the **Create new dataset - Identification** dialog. Complete this page to create a Microsoft SQL Server dataset and click **Next**.
- Copy the ODBC connection string provided by the Azure site for the database created on the Microsoft Azure website.
- In Content Manager Enterprise Studio, on the **Create new dataset - Connection** dialog, paste the string into the **Database Connection String** field for the new dataset.

- Click the KwikSelect on the **Database Connection String** field, the **SQL Server Connection Settings** dialog will appear, make the following changes before saving:

1. Type in the correct password for the login as it would not have been provided.
2. Click the drop-down on the Database Name field, it should retrieve the correct list of databases available on the server. This is a login test.
3. Select the correct database (if it is not already selected) and click OK to continue with the dataset creation.