

opentext™

Content Manager and SharePoint Integration

White Paper

Contents

1	Introduction	3
1.1	Scope.....	3
1.1.1	<i>Target Audience</i>	3
2	Overview	4
2.1	Do's and Don'ts	4
2.1.1	<i>Do's</i>	4
2.1.2	<i>Don'ts</i>	5
3	Configure SharePoint Server.....	6
3.1	Create Site Collection	6
3.2	Service Installation.....	7
3.3	Creating an app catalog.....	8
3.3.1	<i>On Premise</i>	8
3.3.2	<i>SharePoint Online</i>	10
3.4	Configuring term set	10
4	Configure Content Manager Server	10
4.1	Server roles and features	10
4.2	Install SharePoint client components	11
4.3	Cache Installation and Configuration.....	12
4.3.1	<i>SharePoint On premise (AppFabric cache)</i>	12
4.3.2	<i>SharePoint Online (Azure cache)</i>	13
4.4	Enable Content Manager features.....	14
4.5	Configuring the account, permissions and granting access	15
4.6	Add trusted server accounts	16
4.7	Add to a SharePoint farm	17
4.8	Enable event processing	17
5	Install the Content Manger SharePoint MSI	18
5.1	Configuring the use of HTTPS.....	18
5.2	Modify the web config files.....	19
5.3	Additional steps for Windows Azure	20
5.4	Additional steps for use with SharePoint Online	20
6	Configuration	22
6.1	Using Configuration Wizard	22
6.1.1	<i>SharePoint On premise</i>	22
6.1.2	<i>SharePoint Online</i>	30
6.2	Using Configuration Tool	37
6.2.1	<i>Configuring a Tenant</i>	41
	About OpenText	46

1 Introduction

1.1 Scope

This document details the installation and enablement of Content Manager Integration with SharePoint.

1.1.1 Target Audience

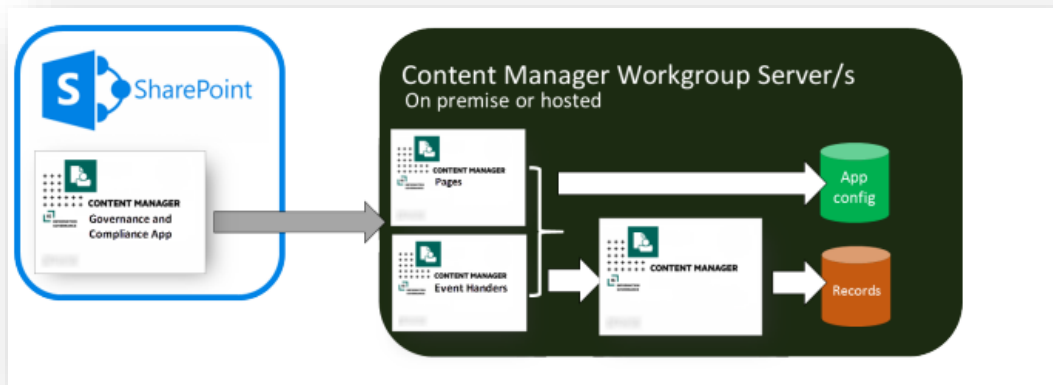
This document is for IT professionals responsible for installing, enabling, and upgrading the Content Manager Integration for SharePoint.

You should be knowledgeable about:

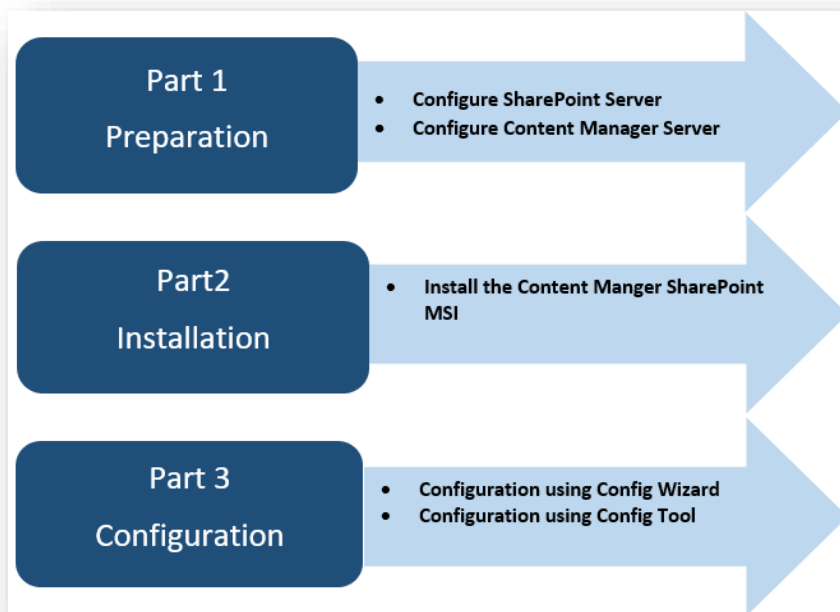
- Content Manager administration
- Microsoft SharePoint Server farm administration

2 Overview

Content Manager for SharePoint includes a SharePoint app. This app uses pages and event handlers that are installed on one or more Content Manager workgroup servers.



To use Content Manager for governance and compliance of SharePoint information, the product needs to be installed and configured.



2.1 Do's and Don'ts

2.1.1 Do's

- For On premise setup, the AppFabric Cache must be installed.
- SharePoint client components must be installed on the Content Manager server.

- The Service Accounts needs to be created in Content Manager dataset:
 - Job processing service account
 - Application pool account
- Viewing the log files – There are two log files containing information, which may help with fault finding an installation. Log files can be found in the “Logs” sub directory of the installation directory.
 - The log named **Configuration Tool.log** contains logging information created by the configuration tool.
 - The log named **SharePointIntegration.log** contains logging information created by the rest of the application.

For additional logging you can enable the Enterprise Library Configuration.

2.1.2 Don'ts

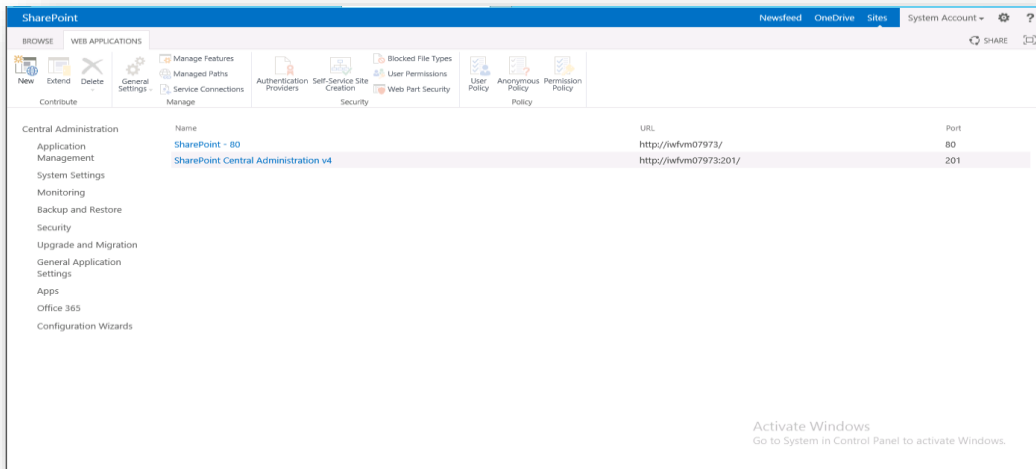
- Make sure not to install SharePoint server and Content Manager server on the same system.
- Make sure not to use System account as the Site Collection Administrator.

For detailed information, refer *Content Manager Governance and Compliance SharePoint App: Installations Guide* and *Content Manager Governance and Compliance SharePoint App: User Guide*.

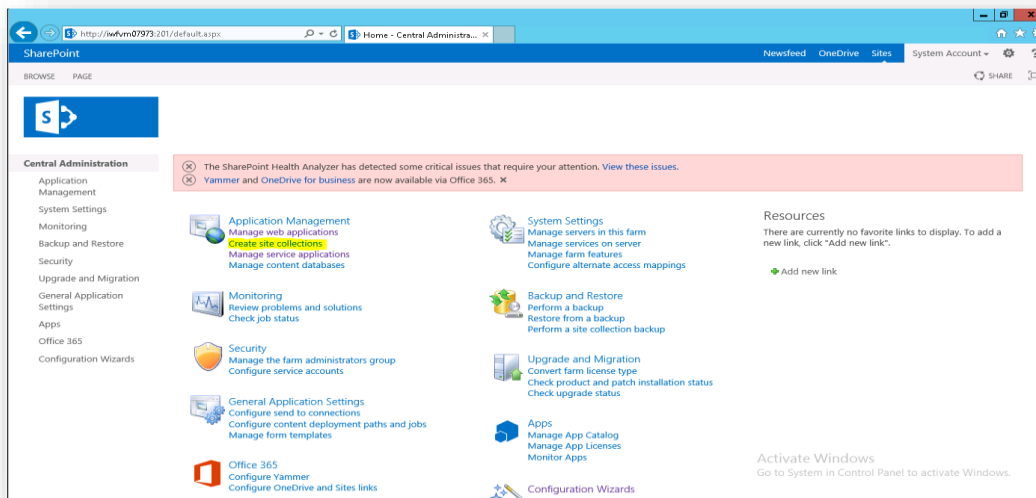
3 Configure SharePoint Server

3.1 Create Site Collection

1. Once you install SharePoint, the SharePoint Central Administration wizard will start. Follow the steps in the wizard to create default Web Applications. (Similar to web applications shown in the below image)



2. Click **Create site collection** and follow the steps to create the site collection. The newly created site collection will be available under the default Web Application created in the above step, for example, **SharePoint - 80**.



3.2 Service Installation

Microsoft SharePoint Foundation Subscription Settings Service:

Make sure you are logged in as a farm administrator, and that you run PowerShell as administrator, or else the script will not run correctly.

Execute the below commands:

```
Remove-PSSnapin Microsoft.SharePoint.PowerShell -erroraction SilentlyContinue

Add-PSSnapin Microsoft.SharePoint.PowerShell -erroraction SilentlyContinue

$accountName = Read-Host "Enter your timer service account in "domain\username" format"

$account = Get-SPManagedAccount $accountName

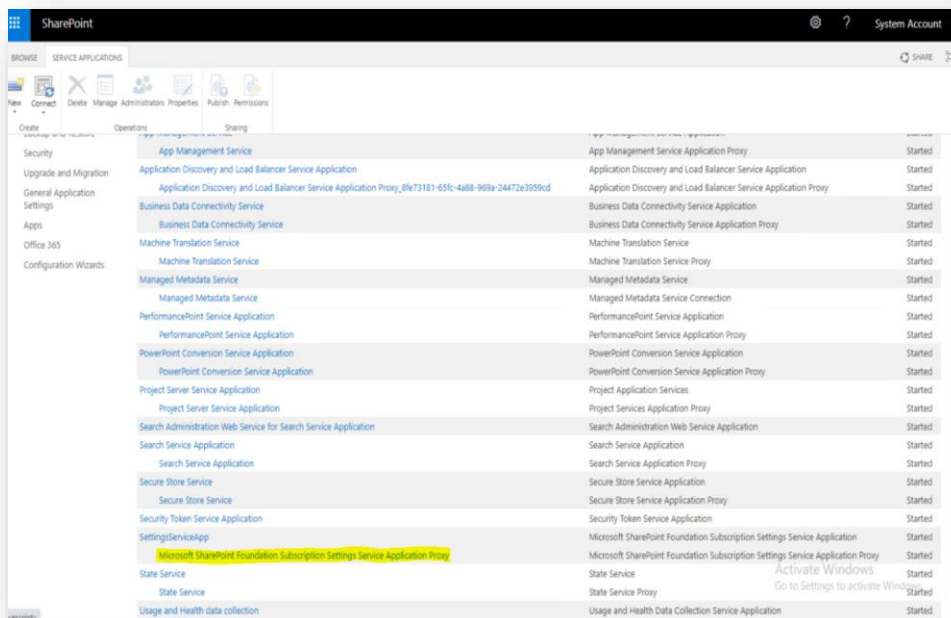
$appPoolSubSvc = New-SPServiceApplicationPool -Name SettingsServiceAppPool -Account $account

$appSubSvc = New-SPSubscriptionSettingsServiceApplication -ApplicationPool

$appPoolSubSvc -Name SettingsServiceApp -DatabaseName SP_2013_Subscriptions_Service_App

$proxySubSvc = New-SPSubscriptionSettingsServiceApplicationProxy -ServiceApplication $appSubSvc
```

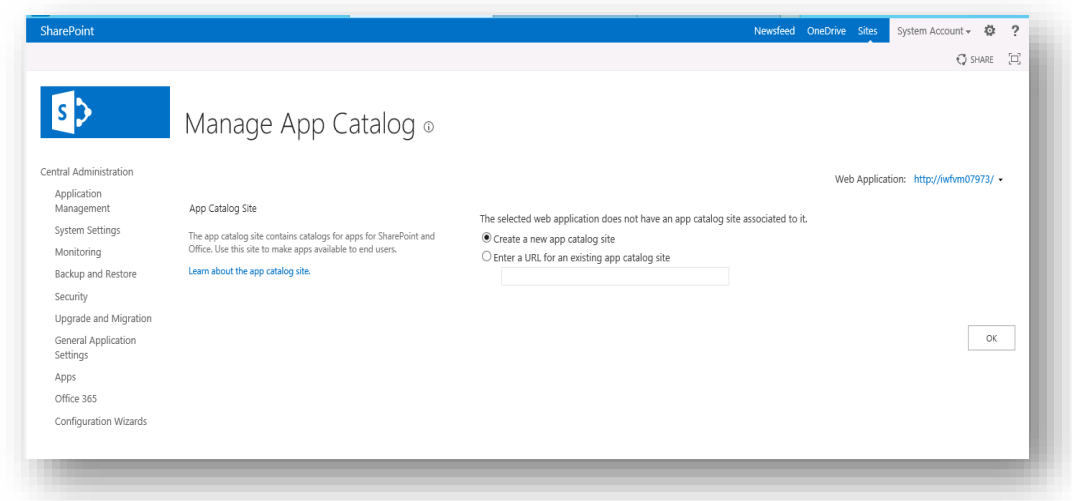
After you execute the above commands, the **Microsoft SharePoint Foundation Subscription Settings Service** gets created.



3.3 Creating an app catalog

3.3.1 On Premise

1. Go to SharePoint Central Administration and click on the **Apps** link in the navigation pane.
2. Click on the **Manage App Catalog** option.
3. On this page, select your content web application, select the **Create a new app catalog site** option, and click **OK**.



4. Then provide the values for **Title**, **URL**, **User name** (Site Collection Administrator) and click **OK**.

Create App Catalog

OK Cancel

Web Application
Select a web application.
Web Application: <http://spdev12013:4444/>

To create a new web application go to [New Web Application](#) page.

Title and Description
Type a title and description for your new site. The title will be displayed on each page in the site.
Title:
Description:

Web Site Address
Specify the URL name and URL path to create a new site, or choose to create a site at a specific path.
URL: <http://spdev12013:4444/>

To add a new URL Path go to the [Define Managed Paths](#) page.

Primary Site Collection Administrator
Specify the administrator for this site collection. Only one user login can be provided; security groups are not supported.
User name:

End Users
Specify the users or groups that should be able to see apps from the app catalog.
Users/Groups:

3.3.1.1 Configuring App URLs (On Premise only)

After creating an App Catalog, configure App URLs, which will be used by all the Apps that you add to the corporate catalog.

1. Go to SharePoint Central Administration and click on the **Apps** link in the navigation pane.
2. Click on the **App Management > Configure App URLs** link.
3. Enter your domain name and enter a prefix you would like to see to indicate app URLs. For example, 'app'. Then click **OK**.

Configure App URLs ⓘ

App URLs will be based on the following pattern: <app prefix> - <app id>.<app domain>

App domain
The app domain is the parent domain under which all apps will be hosted. You must already own this domain and have it configured in your DNS servers. It is recommended to use a unique domain for apps.
App domain:

App prefix
The app prefix will be prepended to the subdomain of the app URLs. Only letters and digits, no-hyphens or periods allowed.
App prefix:

3.3.2 SharePoint Online

1. Login as a tenant administrator, go to the Admin menu at the top right, and click SharePoint.
2. In the SharePoint admin center, you can see a list of site collections. On the left-hand menu, click on apps.
3. Click App Catalog, leave the default selection and click **OK** to create a new App Catalog. The app catalog is provisioned within its own site collection. Fill in details for the app catalog.
4. Click **OK** to provision the app catalog. This will take you back to the Admin Center.

3.4 Configuring term set

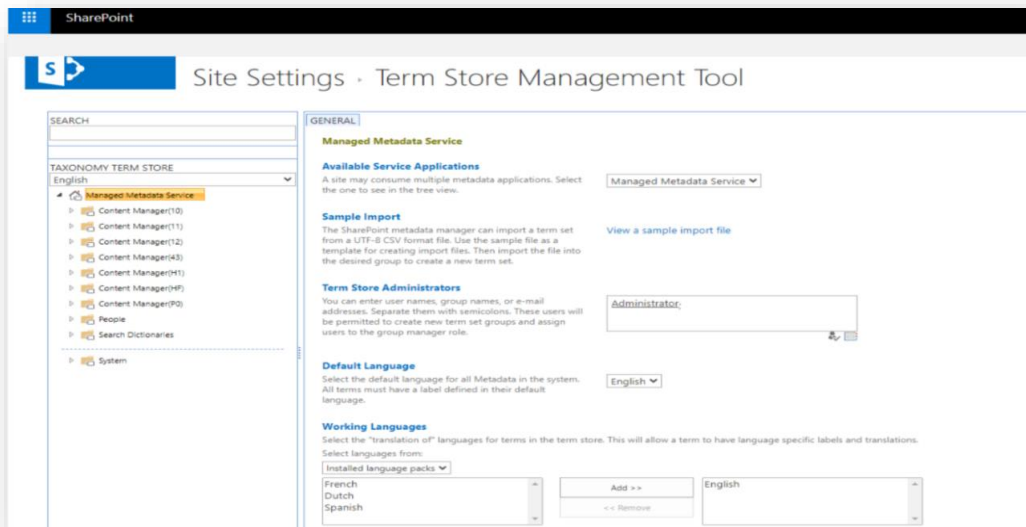
1. On Premise

- From the Central Administrator, go to **Application Management > Service Applications > Manage service applications > Managed Metadata Service**.

The Term Store Management Tool page is displayed.

2. SharePoint Online

- Login as a tenant administrator, click **Admin** at the top right and click on SharePoint.
- In the SharePoint admin center, you can see a list of site collections. On the left-hand menu, click on **term store**.



4 Configure Content Manager Server

4.1 Server roles and features

Content Manager servers must have the following server role and features enabled:

- Server roles:

- Application Server role
 - .NET Framework 4.5
 - Web Server (IIS) Support
- Web Server (IIS) role
 - Web Server
 - Security
 - Windows Authentication
- Server features
 - .NET Framework 3.5 Features
 - .NET Framework 3.5 (includes .NET2.0 and 3.0)
 - .NET Framework 4.5 Features
 - .NET Framework 4.5
 - ASP.Net 4.5
 - WCF Services
 - HTTP Activation
 - Message Queuing(MSMQ)Activation
 - Names Pipe Activation
 - TCP Activation
 - TCP Port Sharing
 - Windows Process Activation Service
 - Process Model
 - Configuration APIs

4.2 Install SharePoint client components

The connection to SharePoint is made from the Content Manager server using the SharePoint Client Side Object Model, known as the CSOM. These components are responsible for the communication between the Content Manager and SharePoint.

The CSOM is installed by the SharePoint Server 2013 Client Components SDK MSI available from Microsoft. Download and install the 64bit version of these components from here:

<http://www.microsoft.com/en-us/download/details.aspx?id=35585>.



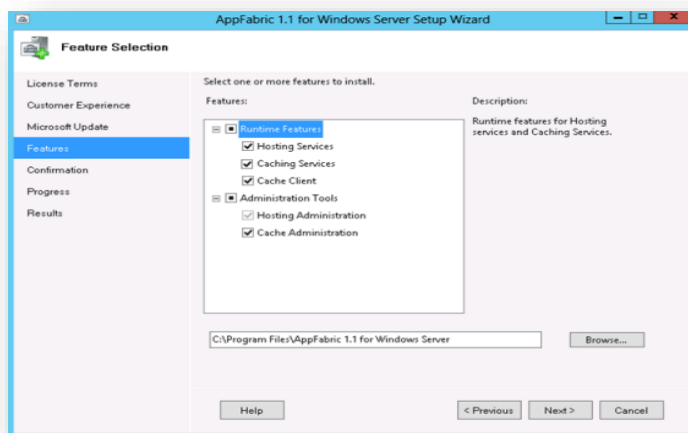
4.3 Cache Installation and Configuration

The Microsoft AppFabric framework must be installed on Content Manager Workgroup Servers, where the integration is installed (Content Manager Farm).

4.3.1 SharePoint On premise (AppFabric cache)

4.3.1.1 Installing AppFabric

1. Download AppFabric 1.1 directly from Microsoft.
2. Run the installer as Administrator. You can accept all the install wizard defaults, until you reach the **Features** page.
3. Select all the options and complete the rest of the wizard with default settings to install AppFabric.



4.3.1.2 Configuring AppFabric

1. Launch App fabric manually from the Start menu, right-click **Configure App Fabric** and click **Run as administrator**.
2. On the initial page, accept the wizard defaults and click **Next**.
3. On the Hosting Services page, accept the defaults and click **Next**.
4. On the Caching Services page, select the **Set Caching Service configuration** checkbox and click **Change**.
5. On the select user dialog, choose the **Custom account** option. Nominate a domain account for the AppFabric Caching Service, enter the relevant password and click **OK**.
6. Select a caching service configuration provider. Click on the **(Select a provider)** drop down, select **SQL Server AppFabric Caching Service Configuration Store Provider**, and click **Configure**.
7. On the AppFabric Server Caching Service Configuration Store dialog, select checkboxes for both:
 - Register AppFabric Caching Service configuration database
 - Create AppFabric Caching Service configuration database

8. Fill in your SQL Server name and provide a name for the caching configuration store database. This will create a new database in SQL Server. Click **OK**.
9. Click **Yes** in the following prompt.
10. Click **OK** in the confirmation dialog.
11. Select the option **New cluster** and the **Cluster size** (The cluster size depends on the number of Content Manager Workgroup Servers in your farm). Choose the appropriate option to match the number of servers. Click **Next**.
12. On the Configure AppFabric Cache Node page, if you have Windows Firewall enabled, select both checkboxes:
 - AppFabric Server AppFabric Caching Service
 - Remote Service ManagementIf the Windows Firewall is not enabled, click **Next**.
13. Click **Yes** in the configuration settings prompt.
14. A progress bar is displayed while the configuration settings are applied. Once this has completed, on the Application page, click **Finish**.

4.3.2 SharePoint Online (Azure cache)

There are two types of Azure caches that can be used:

- Managed
- Redis

The Redis cache is Microsoft's preferred cache to be used although both are still supported.

4.3.2.1 Creating a managed cache

Creating an **Azure Managed Cache** requires the use of Azure PowerShell. This is installed and configured on a local machine and can be used to remotely administer/configure Azure.

1. To install Windows Azure PowerShell, go to <http://azure.microsoft.com/en-us/downloads/> and under the Windows PowerShell section, click on Install.
2. Once installed, run Windows Azure PowerShell and connect to your subscription. This is beyond the scope of this document, but this article describes the process of installation and configuration:

<http://azure.microsoft.com/en-us/documentation/articles/install-configure-powershell/>

To create an Azure cache for use by the integration, follow these steps:

1. Start **Windows Azure PowerShell** and connect to the appropriate subscription.
2. Run the following commands:

```
New-AzureManagedCache -Name cmcache -Location "East Asia" -Sku Basic -  
Memory 128MB  
  
Get-AzureManagedCache
```

3. This creates a cachename 'cmcache', in the region that you define, and once created returns the details of caches in the current subscription.
4. Once created, the cache can be managed from the Azure Management Portal.

Obtaining access keys

1. Select the cache you just created and click on the **MANAGE KEYS** option in the bottom toolbar.
2. On the **Manage Access Keys** dialog, Click **Copy to Clipboard** next to the PRIMARY ACCESS KEY.
3. On the clipboard prompt, click **Allow access**.

4.3.2.2 Creating a Redis cache

To create an Azure Redis cache, navigate to the Azure portal. At the time of writing, you must use the preview version of the portal to perform this task.

1. Log in to Azure portal and select **Create a resource**.
2. On the new page, select **Databases** and then select **Azure Cache for Redis**.
3. Complete the requested details to create the cache.

Obtaining endpoint and access keys

1. Log in to Azure portal and navigate to **All Resources > Redis cache > Overview** page.

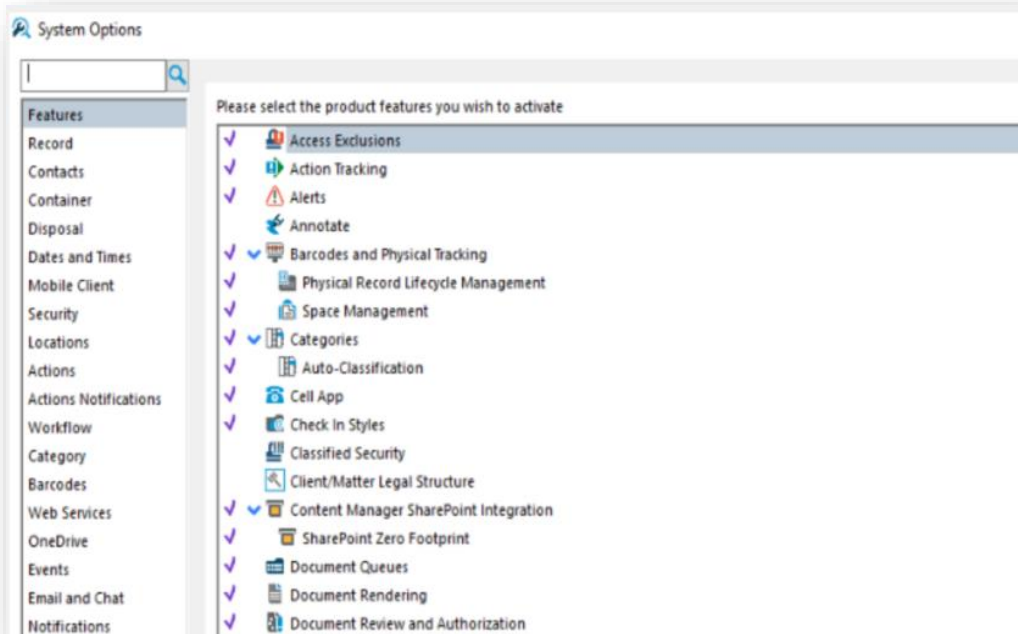


- **Endpoint:** The **Host name** is the Azure cache endpoint. Select and copy the value.
- **Primary access key:** Click the **Show access keys** link to reveal the keys in use.
- **Configured to use SSL:** To determine if Redis cache is configured to use SSL, under the
- **Ports** section the value of **Allow access only via SSL** will indicate if the cache is configured to only use SSL.

4.4 Enable Content Manager features

There are two Content Manager features that need to be enabled. Perform the following steps to enable them:

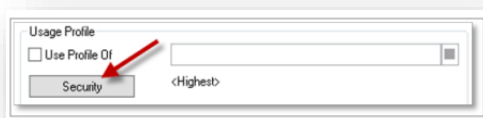
1. Run the Content Manager as an administrator. Go to **Administration > System**. The System Options window is displayed.
2. Click **Features**.
3. Enable the **Content Manager SharePoint Integration** and **SharePoint Zero Footprint** options.



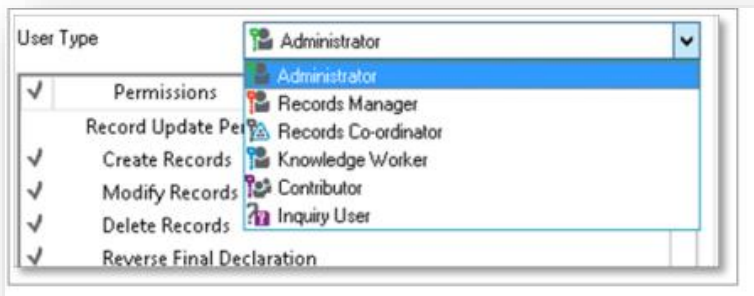
4.5 Configuring the account, permissions and granting access

The following steps assume that a Content Manager Internal Location of type “Person” has already been created for the applicable account.

1. Logged into the Content Manager client as an Administrator. Open the location properties page and enable network login.
2. In the Profile tab, to provide a security level of to a Location, click **Security** and in the resulting dialog, select the **Highest level**. Click **OK**.

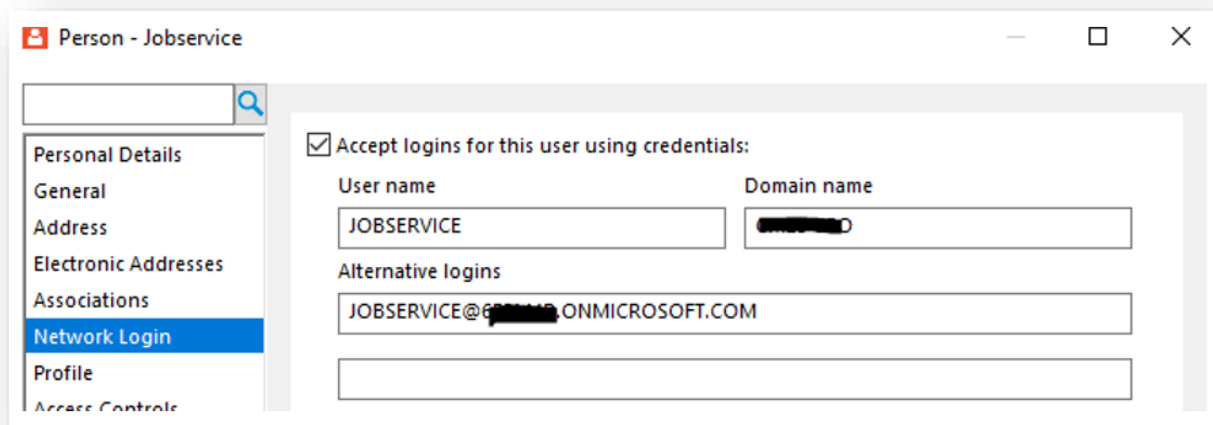


3. To set the User Type of the Location, select the applicable option from the **User Type** drop-down menu.



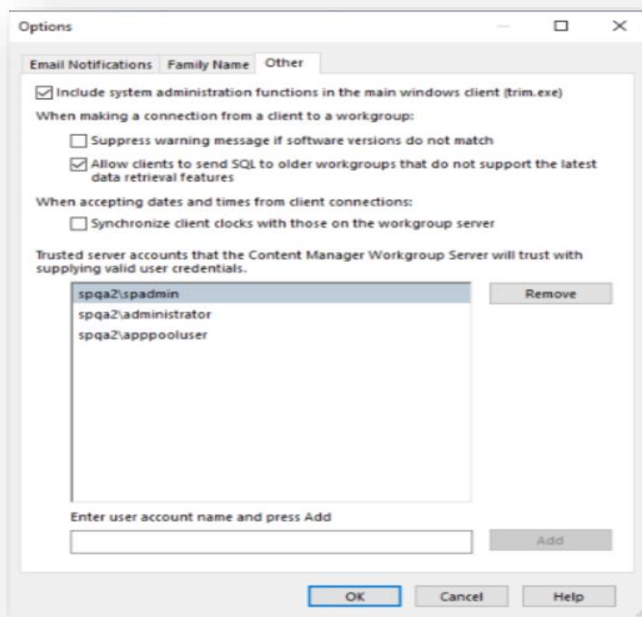
4. Click **OK** on the properties dialog to save settings.
5. Locations must be at least a Contributor in Content Manager to manage content.

For SharePoint online, the Job Service and AppPool locations in Content Manager need to have alternative login definitions.



4.6 Add trusted server accounts

1. Log into the Content Manager Enterprise Studio as a system administrator. Select the Dataset used for SharePoint and Content Manager integration. Go to, **Home > General > Options**. The Options window is displayed. Click **Other** tab.
2. In the field captioned **Enter user account name and press Add**, enter the name of the job service account in the format domain\username and click **Add**.



3. With the job service account added to the trusted server accounts list, click **OK** to close the dialog.
4. **Save** and **deploy** your changes in the Content Manager Enterprise Studio.

4.7 Add to a SharePoint farm

All the servers in the Content Manager farm must join the same SharePoint farm.

1. Open the Content Manager Enterprise Studio.
2. Expand the Workgroup Servers node.
3. Open Workgroup server properties dialog and choose a **SharePoint server farm** to join to. Click **OK**.

4.8 Enable event processing

You must enable event processing for each dataset used for managing SharePoint content. In the Content Manager Enterprise Studio, for each dataset, perform the following steps:

1. Expand the Datasets node.
2. Right-click on the dataset to be used and choose **Event Processing > Configure**.
3. Ensure that the SharePoint Integration event processor type is set to **Enabled** and then click **OK**.

5 Install the Content Manger SharePoint MSI

The installation of the Content Manager components is required on each workgroup server in the Content Manager farm. Run the MSI and provide the following information:

1. Double-click on **CM_SharePointIntegration_x64** msi to install the Content Manager components. A welcome screen is displayed.
2. Click **Next**. The License screen is displayed.
3. Accept the license and click **Next**. The Destination folder screen is displayed.
4. Click **Next** to display the Access Site Details.
5. Enter the port number, app pool user account information and the password. Enter the selected account in the format domain\account. Click **Next**. The job processing service identity screen is displayed.
6. Enter the job service username and password. Enter the selected account in the format domain\account. Click **Next**.
7. Click **Next**. The update system is displayed.
8. Click **Finish** once the installation is complete.

The Content Manager SharePoint Configuration tool icon appears on your desktop.

5.1 Configuring the use of HTTPS

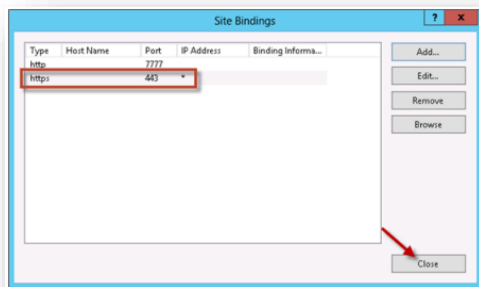
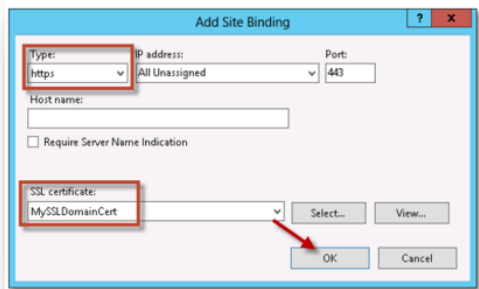
Enabling https for the site The installation process creates a web site in IIS with the name “Content Manager SharePoint Server”. By default, this site is configured to use HTTP.

To enable HTTPS for the Content Manager SharePoint Server website, you will first need to have obtained an SSL certificate, or use an existing SSL certificate for your internal domain

Certificate Type	Notes	Suitable For
Commercial SSL Certificate	Obtained from a commercial SSL vendor such as GoDaddy, Thawte, Verisign, Digicert etc. These have an annual cost associated, but ARE required to secure communication with SharePoint Online environments	On premise, and SharePoint Online
Domain Certificate	Issued from an internal Active Directory Certification Authority, these can be used (at no cost) to secure internal sites on premise	On premise only
Self-signed Certificate	Created within IIS, can be used in some scenarios (SharePoint High-Trust) for testing/development	Not suitable

The following steps assume you have a valid SSL certificate added to IIS Server Certificates, available for use.

1. Open IIS Manager and navigate to the Content Manager SharePoint Server website.
2. Right-click on the site name in the **Connections** pane and choose **Edit Bindings**.
3. On the Site Bindings dialog, click **Add**.
4. On the Add Site Binding dialog, change the **Type** to https and then select your certificate in the **SSL certificate** drop-down. Click **OK**.



5. The https entry has been added. Close the Site Bindings dialog.

To test, open a browser and navigate to `https://pages/dialogloader.html` where yourURL is your load balanced URL, or the name of the Content Manager server, or configured host header. You should see the 'Working on it' page, without any certificate errors.

5.2 Modify the web config files

The web.config file used by the Content Manager SharePoint Server site is by default configured for http.

1. Navigate to the installation directory and open the file called **web.config** (notepad is a suitable program for opening this file) Locate all the following nodes (there should be 3):

```
<security mode="TransportCredentialOnly">
```

2. Modify all nodes to read:

```
<security mode="Transport">
```

3. Now locate the node:

```
<add binding="basicHttpBinding" scheme="http"
```

```
bindingConfiguration="secureBinding" />
```

4. Modify the node to read:

```
<add binding="basicHttpBinding" scheme="https"
bindingConfiguration="secureBinding" />
```

5. Save the changes to the **web.config** file.

5.3 Additional steps for Windows Azure

If installing on a server hosted in Windows Azure, the following additional steps are required to update the caching configuration:

1. In the installation directory, locate the file: **CacheConfiguration.xml**
2. Open this file (notepad is a suitable application).
3. In the file, locate the following node:

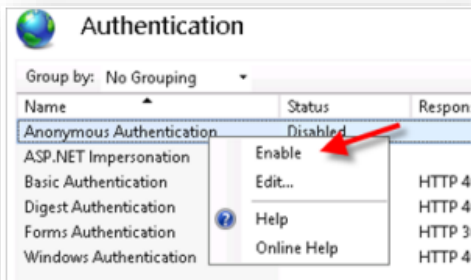
```
<CacheType>AppFabric</CacheType>
```

4. Modify this node to read (dependent on whether using managed or Redis):
 - `<CacheType>WindowsAzureManaged</CacheType>`
 - `<CacheType>WindowsAzureRedis</CacheType>`
5. Save the file.

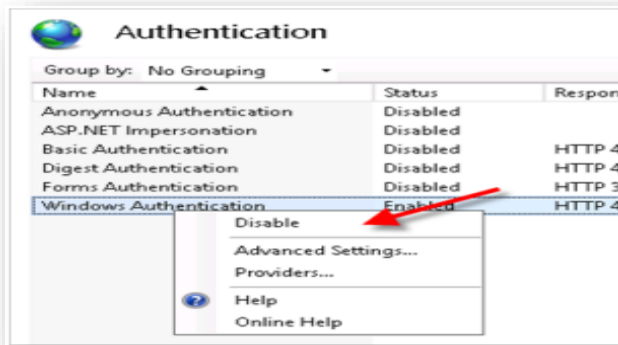
5.4 Additional steps for use with SharePoint Online

Authentication used by SharePoint Online differs to the authentication used by a high trust app used with an on-premise instance of SharePoint. The installation process assumes that an on-premise instance of SharePoint will be used, so IIS authentication must be re-configured. Perform the following steps:

1. Open IIS Manager and select the site: **Content Manager SharePoint Server**.
2. In the right-hand pane using the **Features** view locate and double click **Authentication** icon.
Authentication will initially show **Anonymous Authentication** as Disabled and **Windows Authentication** as **Enabled**.
3. Right click on Anonymous Authentication and select **Enable**.



4. Right click Windows Authentication and select **Disable**.



6 Configuration

To select a configuration option log into the machine as the installing user, right click **Content Manager SharePoint Configuration** tool available on your desktop and select **Run as Administrator**. Configuration selection window is displayed.



There are two ways of configuring SharePoint Integration:

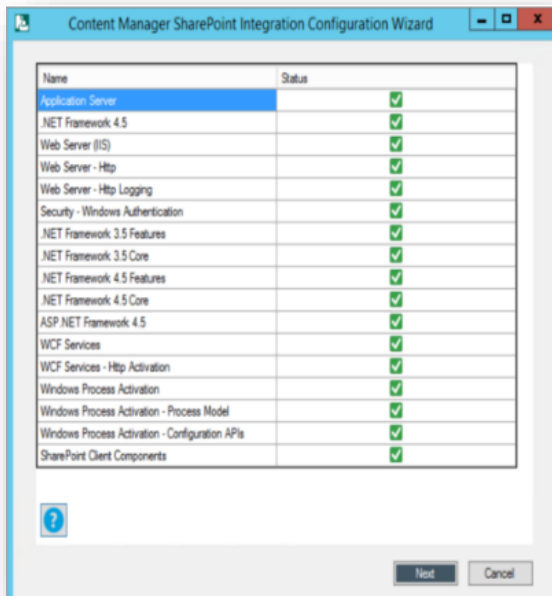
1. Using the Configuration Wizard
2. Using the Configuration Tool

6.1 Using Configuration Wizard

The Configuration Wizard will guide you through the configuration steps required to correctly configure the SharePoint Integration. For fresh installation it is always recommended to use Configuration Wizard.

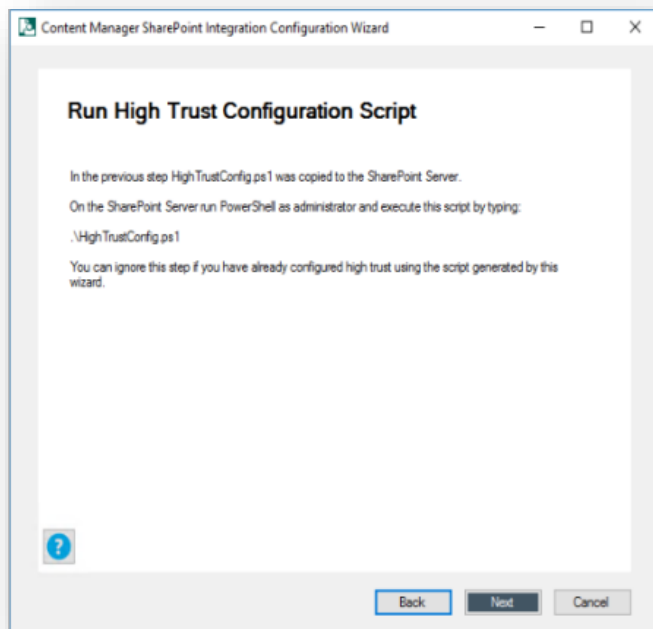
6.1.1 SharePoint On premise

1. Run the Content Manager SharePoint Configuration tool as Administrator and click **Launch Configuration Wizard** in the selection window. The welcome screen is displayed.
2. Click **Next**. The Pre check window is displayed listing all the prerequisites for the integration.

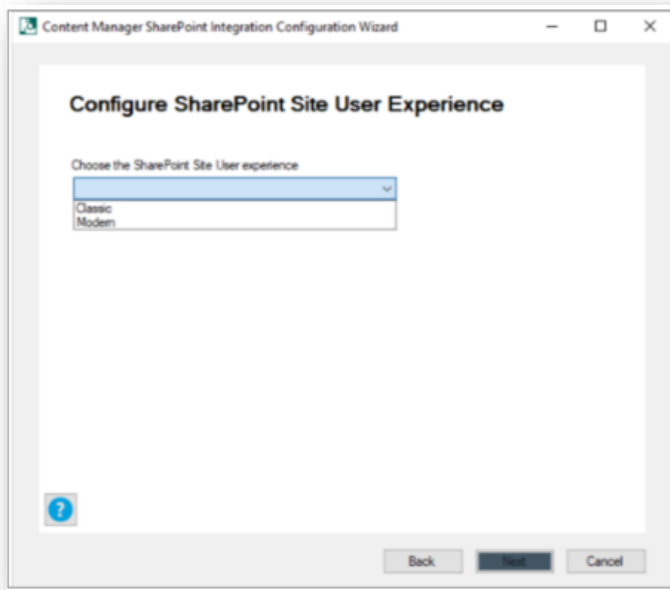


3. Click **Next**. The Content Manager Farm details window is displayed.
4. Select from the drop down whether you want to create a new Content Manager farm or join existing one or use the current farm.
 - a) If you are creating new Content Manager farm, enter the SQL Server Instance and name for the Content Manager farm database in the Create a new Content Manager Farm window.
Click **Next**. The Cache Details window is displayed.
 - b) if you are joining the existing farm, enter the server name, database details and test the connection in the Join an Existing Content Manager Farm > Data Link Properties window.
 - c) Click **OK** and then click **Next**. The Cache Details window is displayed.
 - d) If you are using the current farm, the Cache Details window is displayed.
5. Select the type of cache (AppFabric) that will be used by Content Manager farm from the drop down and click **Next**.
6. Select the SharePoint instance (On premise) being configured from the drop down and click **Next**. The Tenant Information window is displayed.
7. You can add a new tenant or edit existing one based on whether you have created a new Content Manager farm or using the existing / current farm.
 - a) **For new Content Manager farm** If you have created a new Content Manager farm in step 4, then in the Tenant Information window, you get option only to add a new tenant.
Select **Add new Tenant** from the drop-down and click **Next**. The Content Manager Farm URL window is displayed. Go to step 8.
 - b) **For existing farm or using current farm** If you have joined an existing farm or using a current farm, then in the Tenant Information windows, you also get an option to **Edit** an existing tenant information. Perform one of the following steps:
 - i. **Add new Tenant** - If you select this option from the drop-down, click **Next**. The Content Manager Farm URL window is displayed.

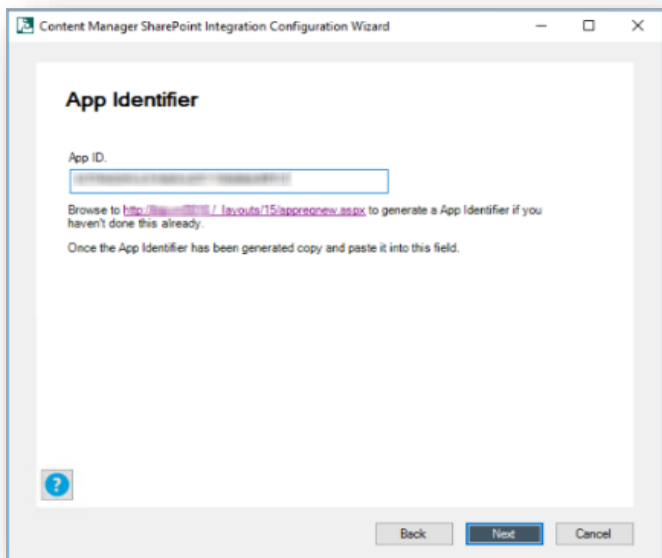
- ii. **Edit existing Tenant** - If you select this option from the drop-down, the Choose Tenant window is displayed. Select an existing tenant from the drop-down and click **Next**. The Content Manager Farm URL window is displayed.
8. Enter the Content Manager load balanced URL and click **Next**. The Configure SharePoint for Apps window is displayed.
9. Select **Yes** or **No** based on whether the SharePoint instance has already been configured or not and click **Next**. The Default Site Collection window is displayed.
10. Enter the default site collection URL and click **Next**.
11. Ensure the following manual steps are completed:
 - a) Copy the script and certificate files from Content Manager to a folder on the SharePoint server. Click **Next** if you have already copied the files.
 - b) On the SharePoint server, run the script copied from Content Manager. This script generates a **.xml** file. Click **Next**.



- c) Copy the .xml file to the Content Manager system. Click **Next** if you have already copied the files. The Configure SharePoint Site User Experience window is displayed.
12. Select the SharePoint Site User experience (**Classic** or **Modern**) from the drop down and click **Next**. The App Identifier window is displayed.



13. Generate the App ID using the link and copy paste the ID in App ID field. Click **Next**.



Registration is performed using the SharePoint "appregnew.aspx" page. To access this page, navigate to the following URL :

[site collection URL]/_layouts/15/appregnew.aspx

Entering all the details will register the app in your environment, as shown below:

App Information
The app's information, including app id, secret, title, hosting url and redirect url.

Client Id:
2afaf018-5249-4b34-a572-9fa69c22484a

Client Secret:
U7hxs91sThRX+C1o0UQKG8Ot4fw/r/FPpx5vc

Title:
CM Governance and Compliance

App Domain:
www.spqa2.com
Example: "www.contoso.com"

Redirect URI:
https://btpvm07298221/pages/appstart.aspx
Example: "https://www.contoso.com/default.aspx"

The SharePoint Configuration Results window is displayed.

14. Enter the full path to the .xml file you copied on to the Content Manager system and click **Next**.

The Set the Protocol to use window is displayed.

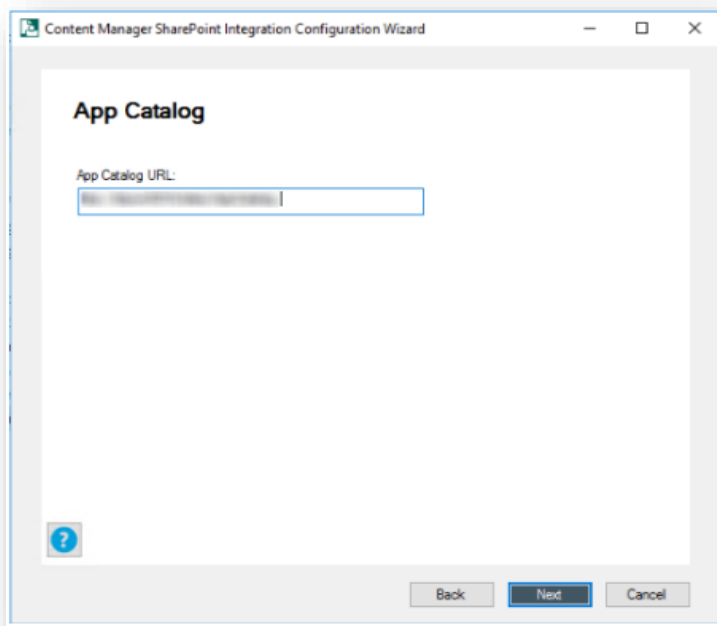
15. Select the type of protocol (HTTPS) to use for communication between Content Manager and SharePoint and click **Next**.

The Auto Install App window is displayed.

16. Select **Yes** from the drop down to automatically install the Content Manager Governance and Compliance App to the default site collection and click **Next**.

If you have already installed the Content Manager Governance and Compliance App, select **No** from the drop down and click Next.

17. Enter the app catalog URL and click **Next**.



If you have selected **No** in Step 16, proceed with next step. Else, go to Step 19.

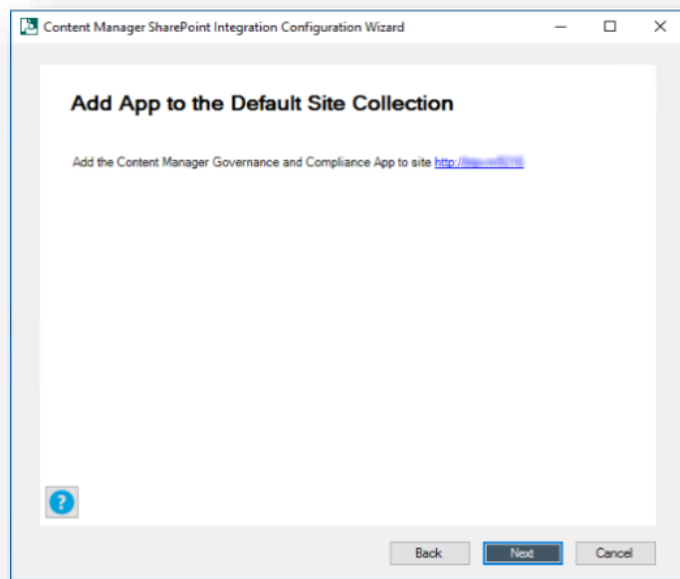
18. On the SharePoint System, manually, upload the Content Manager Governance and Compliance App. Click **Next**.

Upload the app to the corporate catalog in SharePoint system.

- a) Navigate to the corporate app catalog used by your SharePoint farm.
- b) Click the **Apps for SharePoint** link.
- c) Click the **upload** link.

The app file created in the previous step can be found in the installation directory of Content Manager for SharePoint. By default, this directory is: [Program Files]\Micro Focus\Content Manager\Content Manager SharePoint Integration The app file name is: HPRMGovernanceCompliance.app

- d) Clicking **Save** on this form will complete the addition of the app into the app catalog.
19. Add the **Content Manager Governance and Compliance App** to the Default site collection. Click **Next**.



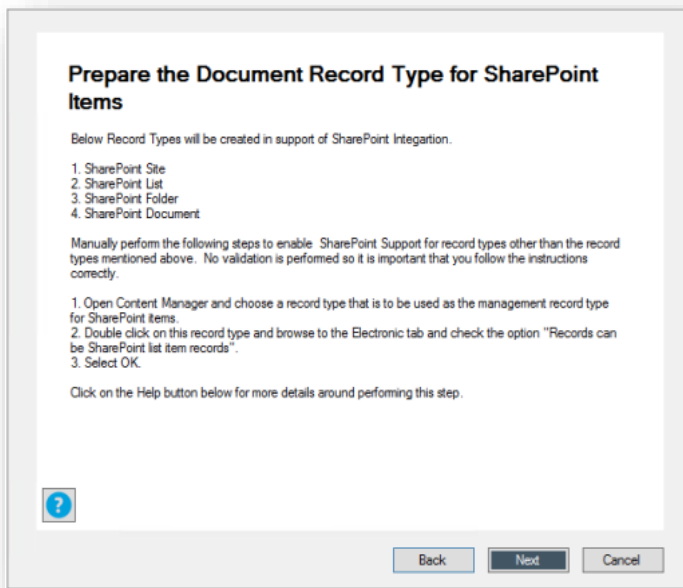
The Content Manager Governance and Compliance App installation is validated.

20. Once the installation and validation of Content Manager Governance and Compliance App are complete, you may choose to enter email settings.

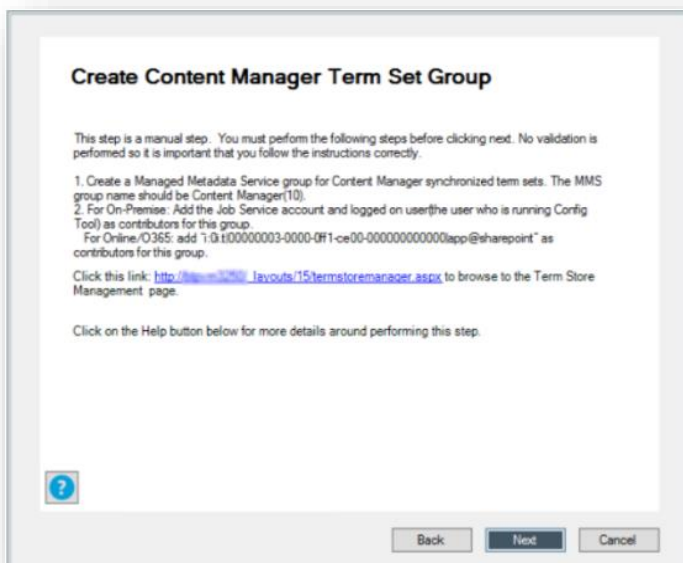
If you are going to configure email at later stage, select No in the drop down, click Next and proceed to next step. Otherwise, continue by entering the SMTP server name and Reply to address. Click **Next**.

The Primary Configuration Administrator window is displayed.

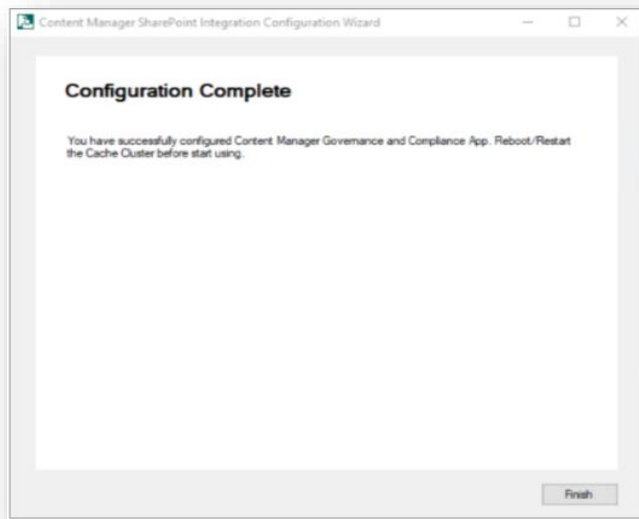
21. Enter an account to use as the primary configuration administrator and click Next. The settings are published. Click **Next**.
22. Enter the Content Manager dataset ID and click **Next**.
23. Ensure the following manual steps are completed: If you have already performed these manual steps, click **Next**.
 - a) Add the App Pool User account and the Administrator account as trusted server accounts in Content Manager system.
 - b) Enable the event processing in Content Manager.
 - c) Join a SharePoint farm.
 - d) Enable the Content Manager SharePoint integration and SharePoint Zero FootPrint features.
 - e) Prepare the document record type for SharePoint items.



f) Create Content Manager term set group.

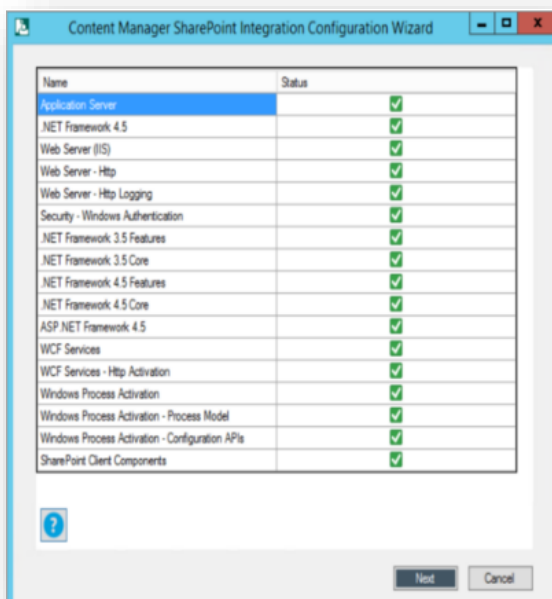


24. Click **Next**. The Do not Create Classification terms window is displayed.
25. Select the check box if you do not want to create classification terms. Click **Next**.
26. This step to choose the record type is automated. By default, the standard SharePoint record type gets configured.
27. The Configuration Complete window is displayed with a status message. Click **Finish**.



6.1.2 SharePoint Online

1. Run the Content Manager SharePoint Configuration tool as Administrator and click **Launch Configuration Wizard** in the selection window. The welcome screen is displayed.
2. Click **Next**. The Pre check window is displayed listing all the prerequisites for the integration.

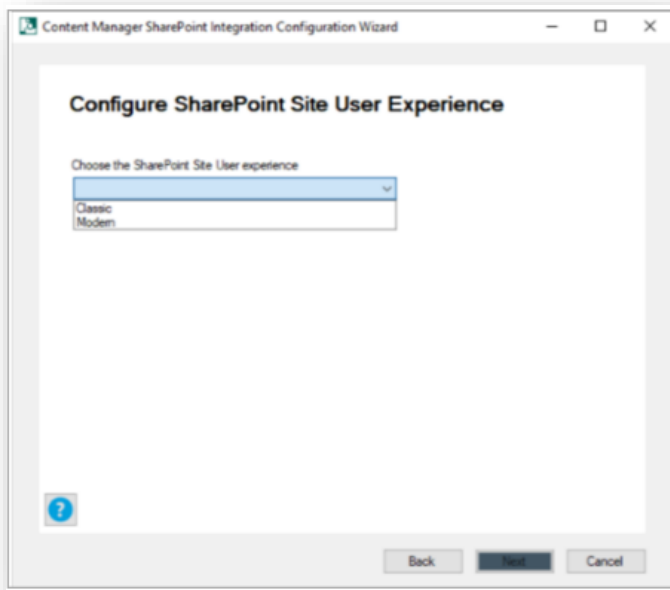


3. Click **Next**. The Content Manager Farm details window is displayed.
4. Select from the drop down whether you want to create a new Content Manager farm or join existing one or use the current farm.
 - a) If you are creating new Content Manager farm, enter the SQL Server Instance and name for the Content Manager farm database in the Create a new Content Manager Farm window.

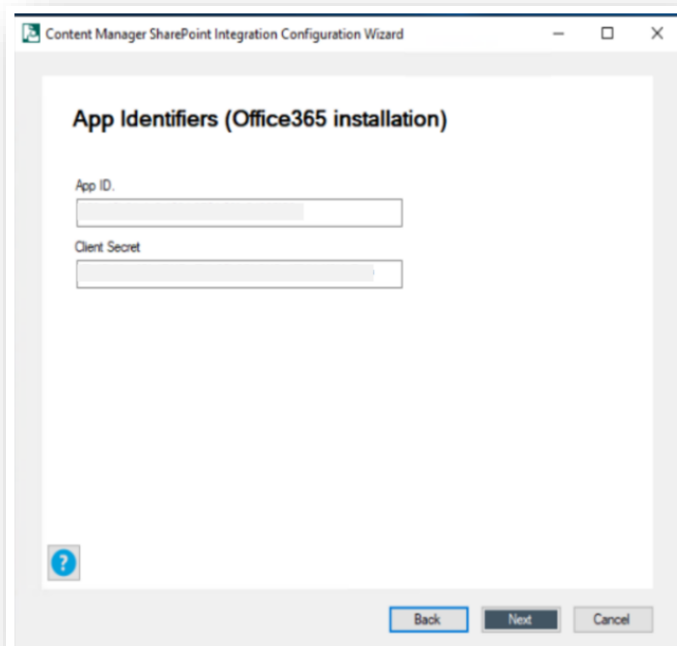
Click **Next**. The Cache Details window is displayed.

- b) if you are joining the existing farm, enter the server name, database details and test the connection in the Join an Existing Content Manager Farm > Data Link Properties window.
 - c) Click **OK** and then click **Next**. The Cache Details window is displayed.
 - d) If you are using the current farm, the Cache Details window is displayed.
5. Select the type of cache (Azure cache) that will be used by Content Manager farm from the drop down and click **Next**.
 6. Select the SharePoint instance (Office365) being configured from the drop down and click **Next**. The Tenant Information window is displayed.
 7. You can add a new tenant or edit existing one based on whether you have created a new Content Manager farm or using the existing / current farm.
 - a) **For new Content Manager farm** If you have created a new Content Manager farm in step 4, then in the Tenant Information window, you get option only to add a new tenant.

Select **Add new Tenant** from the drop-down and click **Next**. The Content Manager Farm URL window is displayed. Go to step 8.
 - b) **For existing farm or using current farm** If you have joined an existing farm or using a current farm, then in the Tenant Information windows, you also get an option to **Edit** an existing tenant information. Perform one of the following steps:
 - i. **Add new Tenant** - If you select this option from the drop-down, click **Next**. The Content Manager Farm URL window is displayed.
 - ii. **Edit existing Tenant** - If you select this option from the drop-down, the Choose Tenant window is displayed. Select an existing tenant from the drop-down and click **Next**. The Content Manager Farm URL window is displayed.
 8. Enter the Content Manager load balanced URL and click **Next**. The Configure SharePoint for Apps window is displayed.
 9. Select **Yes** or **No** based on whether the SharePoint instance has already been configured or not and click **Next**. The Default Site Collection window is displayed.
 10. Enter the default site collection URL and click **Next**.
 11. Select the SharePoint Site User experience (**Classic** or **Modern**) from the drop down and click **Next**. The App Identifier window is displayed.



12. Enter the App identifiers – App ID and Client Secret. Click **Next**.



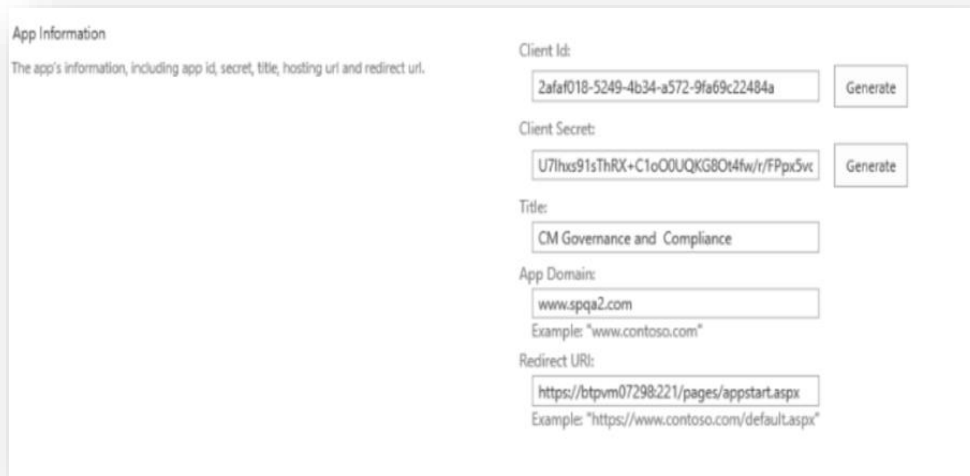
Generating the Client ID (App ID) and Client secret

Registration is performed using the SharePoint “appregnew.aspx” page. To access this page, navigate to the following URL :

[site collection URL]/_layouts/15/appregnew.aspx

For example, https://xxxxx.sharepoint.com/_layouts/15/appinv.aspx

Entering all the details will register the app in your environment, as shown below:



Using the appregnew page, generate a **Client Id** and **Client Secret** by clicking on the **Generate** buttons.

Specify “Content Manager Governance and Compliance” for the **Title**. Specify your **Appdomain** i.e. the domain that the app will be used in.

For the **Redirect URI**, you must specify the full URL of the app start page. This will be the Content Manager farm URL with the following appended:
/pages/appstart.aspx

Then the full URL to specify in the Redirect URL will be: *[farmURL]/pages/appstart.aspx*

After entering all the details, click **Create** to register the app in your environment.

The SharePoint Configuration Results window is displayed.

13. Enter the Username and password for the Office365 Tenant administrator details and click **Next**.

The Set the Protocol to use window is displayed.

14. Select the type of protocol (HTTPS) to use for communication between Content Manager and SharePoint and click **Next**.

The IIS certificate installation window is displayed.

15. Click **Next**.

The IIS certificate selection window is displayed.

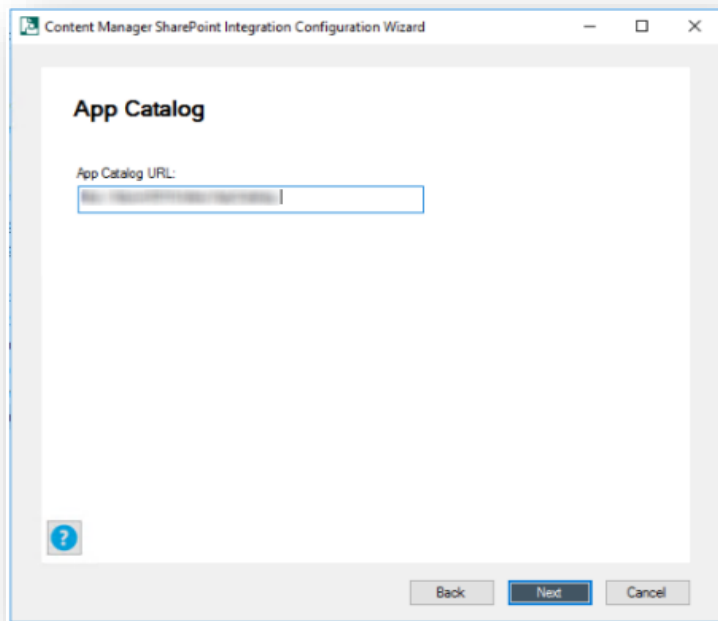
16. Click **Next**.

The Auto Install App window is displayed.

17. Select **Yes** from the drop down to automatically install the Content Manager Governance and Compliance App to the default site collection and click **Next**.

If you have already installed the Content Manager Governance and Compliance App, select **No** from the drop down and click **Next**.

18. Enter the app catalog URL and click **Next**.



If you have selected **No** in Step 17, proceed with next step. Else, go to Step 21.

19. On the SharePoint System, manually, upload the Content Manager Governance and Compliance App. Click **Next**.

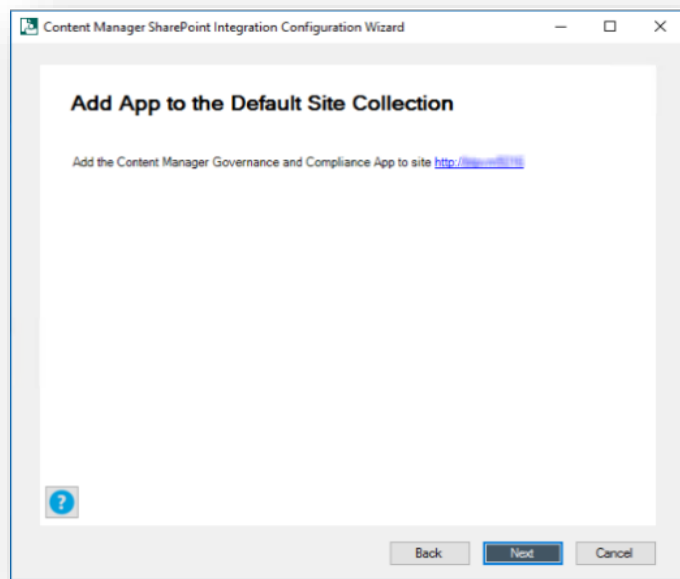
Upload the app to the corporate catalog in SharePoint system.

- a) Navigate to the corporate app catalog used by your SharePoint farm.
- b) Click the **Apps for SharePoint** link.
- c) Click the **upload** link.

The app file created in the previous step can be found in the installation directory of Content Manager for SharePoint. By default, this directory is: [Program Files]\Micro Focus\Content Manager\Content Manager SharePoint Integration The app file name is:
HPRMGovernanceCompliance.app

- d) Clicking **Save** on this form will complete the addition of the app into the app catalog.

20. Add the **Content Manager Governance and Compliance App** to the Default site collection. Click **Next**.



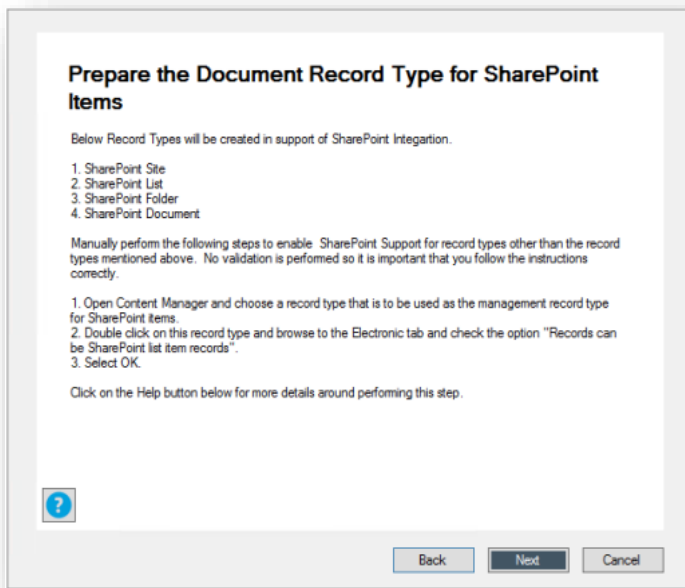
The Content Manager Governance and Compliance App installation is validated.

21. Once the installation and validation of Content Manager Governance and Compliance App are complete, you may choose to enter email settings.

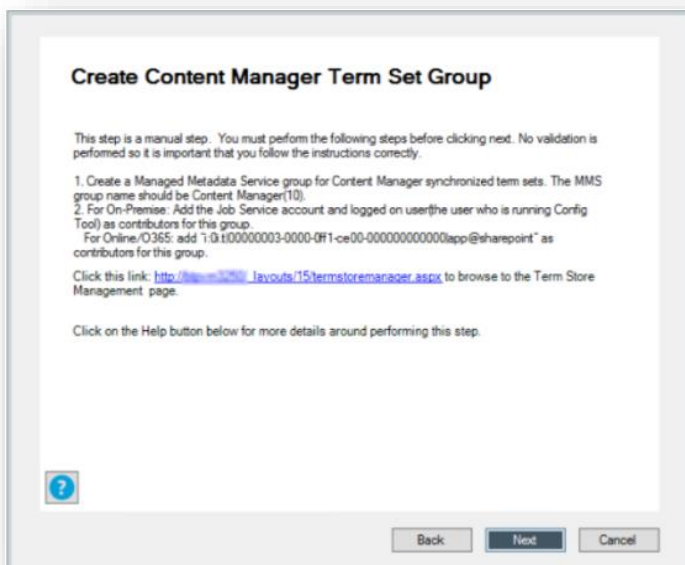
If you are going to configure email at later stage, select No in the drop down, click Next and proceed to next step. Otherwise, continue by entering the SMTP server name and Reply to address. Click **Next**.

The Primary Configuration Administrator window is displayed.

22. Enter an account to use as the primary configuration administrator and click Next. The settings are published. Click **Next**.
23. Enter the Content Manager dataset ID and click **Next**.
24. Ensure the following manual steps are completed: If you have already performed these manual steps, click **Next**.
 - a) Add the App Pool User account and the Administrator account as trusted server accounts in Content Manager system.
 - b) Enable the event processing in Content Manager.
 - c) Join a SharePoint farm.
 - d) Enable the Content Manager SharePoint integration and SharePoint Zero FootPrint features.
 - e) Prepare the document record type for SharePoint items.



f) Create Content Manager term set group.



25. Click **Next**. The Do not Create Classification terms window is displayed.

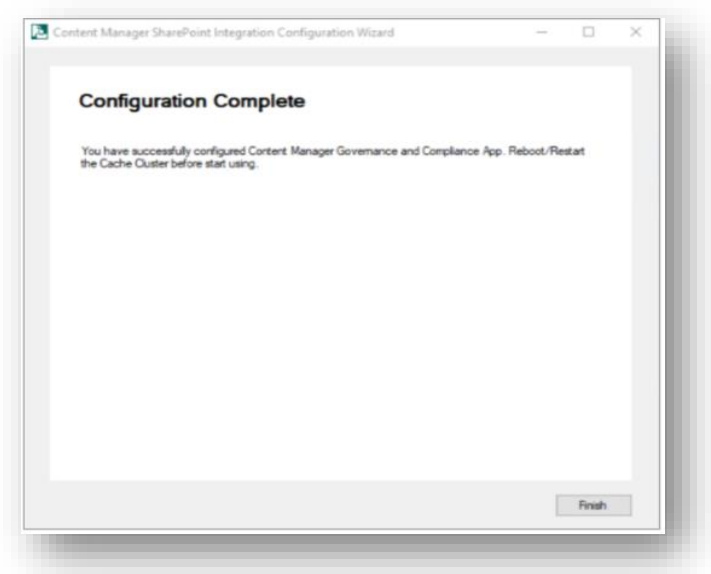
26. Select the check box if you do not want to create classification terms. Click **Next**.

The Azure AD Application Details window is displayed.

To Configure the Content Manager Integration with Azure AD authentication, see section *Configuring the Content Manager Integration for SharePoint Online - Azure AD authentication* in Content Manager Governance and Compliance SharePoint App: Installation Guide.

27. Enter the Application Id and the Tenant Id and click **Next**.

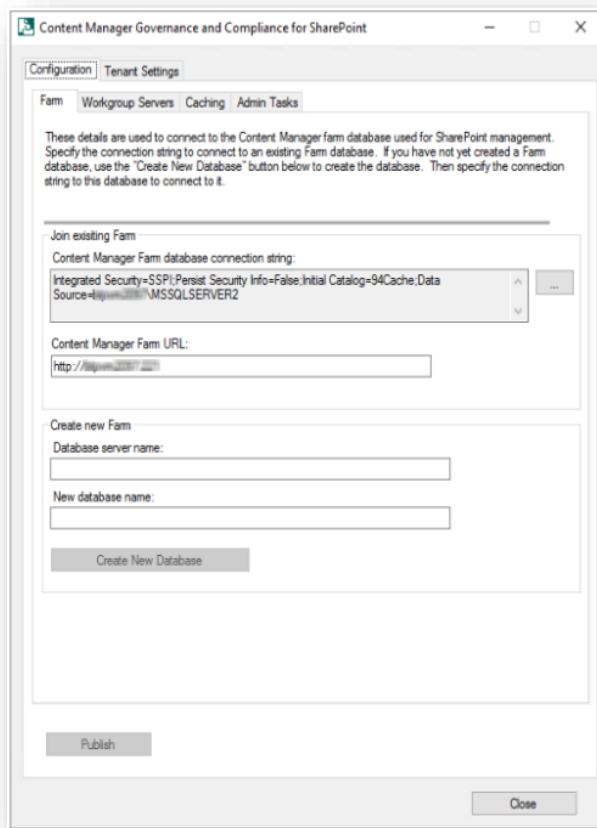
28. This step to choose the record type is automated. By default, the standard SharePoint record type gets configured.
29. The Configuration Complete window is displayed with a status message. Click **Finish**.



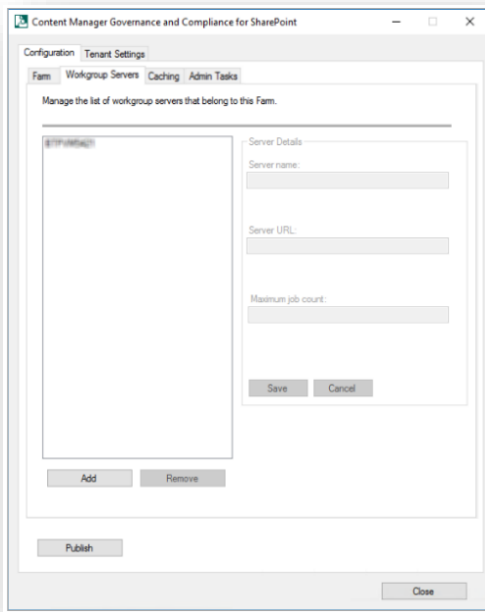
6.2 Using Configuration Tool

The Configuration Tool allows modification to existing configuration data and should be used once the Configuration Wizard has been used to create the initial configuration.

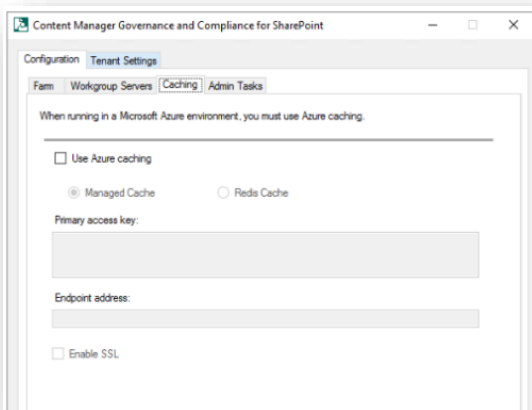
1. **Configuration tab:** includes Farm, Workgroup, Caching and Admin Tasks tabs.



- a) **Farm tab:** This tab includes the details of Content Manager farm database used for SharePoint management.
- b) **Workgroup Servers tab:** This tab lists the details of workgroup servers in the farm. In this tab, you can add new workgroup servers to the farm, modify server details of the existing workgroup servers in the farm or remove the workgroup servers from the farm.



c) **Caching tab:** In this tab, you can modify the caching settings.



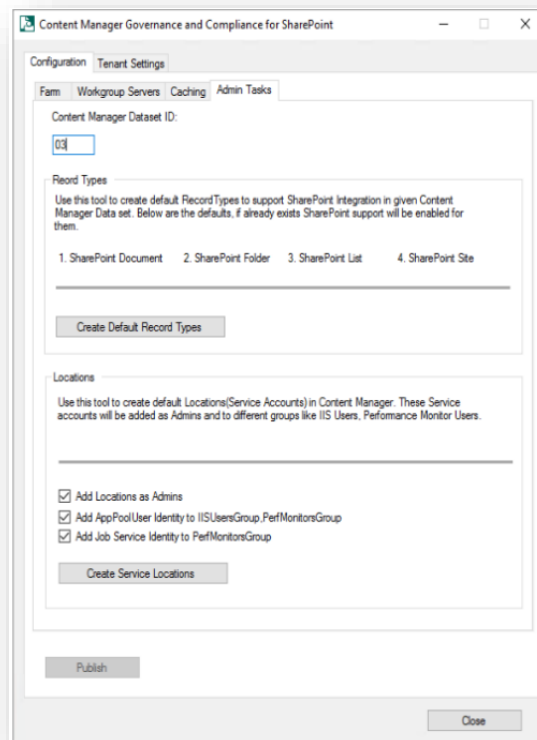
If Content Manager is hosted on Windows Azure environment, then set the caching option in the Caching tab.

- Check the **Use Azure caching** check box and select the type of Azure caching: - Managed or Redis.
- Check the **Enable SSL** check box if the cache is configured to be accessed through SSL.
- Enter the details of the Azure cache into the **Primary access key** and **Endpoint address** fields.

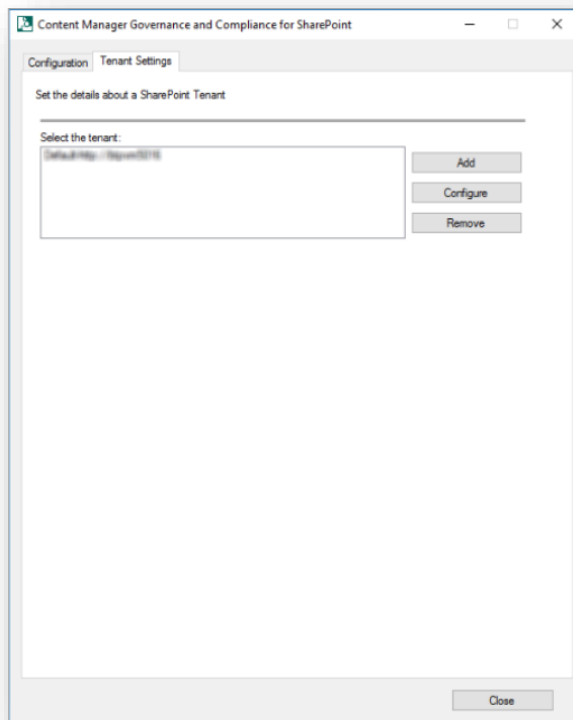
d) **Admin Tasks Tab:** This tab lets you create default Record Type and locations for the given Dataset ID.

- **Record Types** - SharePoint Document, SharePoint Folder, SharePoint List, and SharePoint Site are the default record types that will be created. If the record types already created, then they will be enabled to support SharePoint list item records.

- **Locations** - The service accounts will be added as Administrator in Content Manager. The AppPoolUser and Job Service accounts will be added to different groups like, IIS users and Performance monitor users groups.



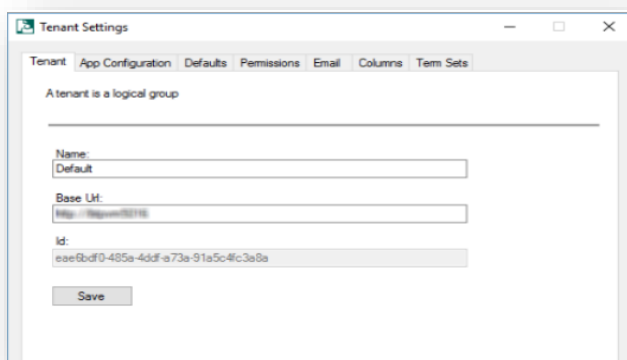
2. **Tenant Settings tab:** This tab allows you to add, configure or remove the tenant settings.



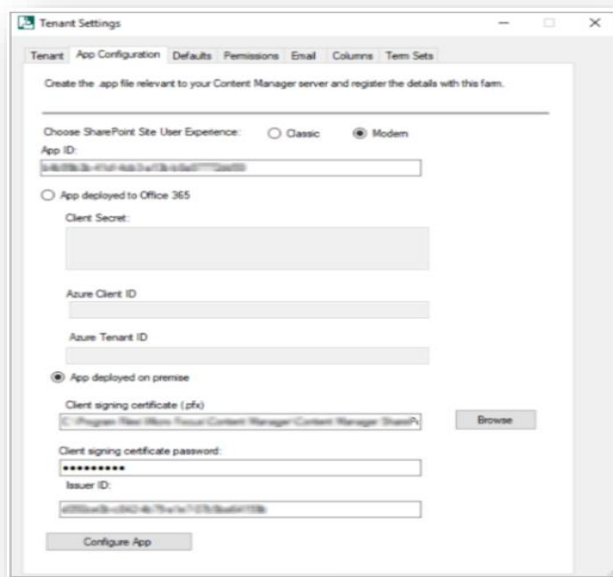
- **Add** - adds a new Tenant.
- **Configure** - Select an existing Tenant and then click **Configure** This will display the tenant for modifying.
- **Remove** - Select the existing Tenant and then click **remove**, this will remove the Tenant. When a Tenant is removed all the jobs and configuration related to that tenant will be removed from the configuration database.

6.2.1 Configuring a Tenant

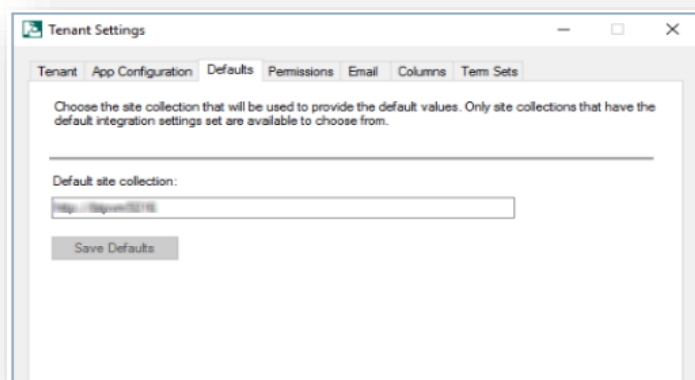
1. **Tenant tab:** To configure a Tenant select **Add** from the Tenant Settings tab.



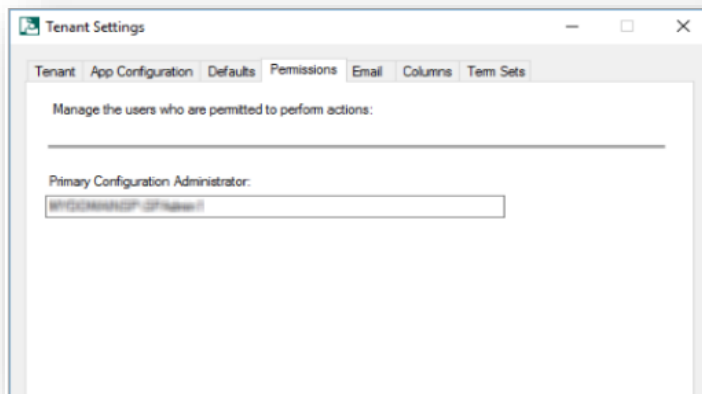
2. **App Configuration tab:** This tab includes information on SharePoint Site User experience, App ID, whether App is deployed on SharePoint online or OnPremise, path to certificate file, and Issuer ID.



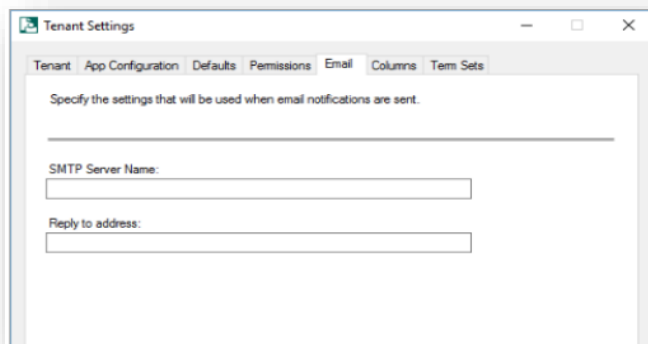
3. **Defaults tab:** This tab contains information about the default site collection.



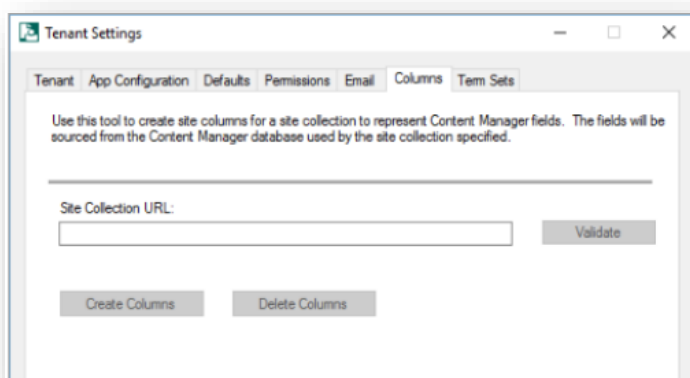
4. **Permissions tab:** This tab includes information about the Primary Configuration Administrator, the user who is permitted to perform actions.



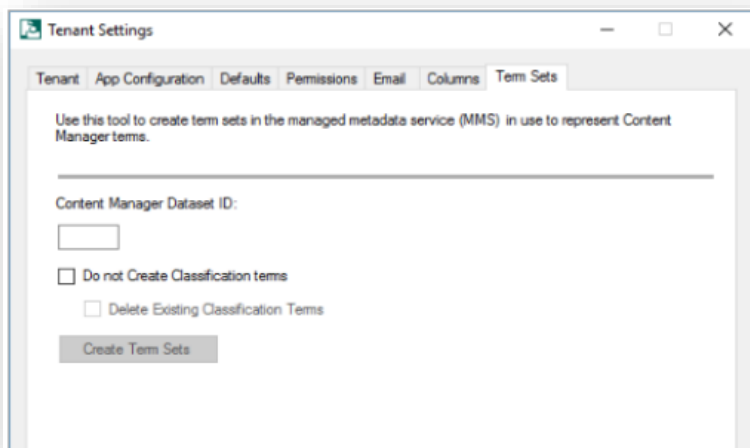
- 5. **Email tab:** This tab contains details of email notification settings, such as, SMTP Server Name and Reply to address.



- 6. **Columns tab:** This tab contains information about site columns for site collection that represent fields in the Content Manager.




- 7. **Term Sets tab:** This tab includes information about Content Manager Dataset ID and term sets.



8. Publish

Once all the settings have been entered, they must be published to all the servers in the Content Manager farm. Click **Publish** at the bottom of the dialog to reflect the changes to all the servers in the Content Manager farm.

Once all the installation and Configuration done successfully, you will able to open the below page from SharePoint site collection.



Content Manager

Management Options

The pages in this section allow configuration of how content is managed by Content Manager.

Use the 'Default Integration Settings' page to configure the default options that are used for this site collection.

The 'Site Records Management Options' page allows indicating specific management settings that should be used for this site.

Content Mapping

The pages in this section allow configuring how content appears in Content Manager records.

The 'Content Types to Record Type Mapping' page allows specifying what record type is used to create the record in Content Manager based on the content type that it has in SharePoint. If a content type is not mapped, then the record type used will be the one specified in the 'Default Integration Settings' page.

The 'Column Mapping' page allows configuring which fields on the Content Manager record contain the values from particular SharePoint columns.

Lifetime Management

The pages in this section allow creating and applying Lifetime Management Policies that are used to control the lifetime of content in SharePoint. Policies can determine when content is managed by Content Manager and when it is removed from SharePoint.

The 'Lifetime Management Policies' page shows a gallery of all lifetime management policies that have been defined for this site collection. From the gallery you can define new policies and edit existing ones.

The 'Lifetime Management Options' page allows configuring the lifetime management policies that apply to this site.

Use the 'Reapply Policies Now' link to force the reapplication of applicable lifetime management policies to this site and all children. This will not stop or restart policies already under way and can be useful to start new policies have been added to the default site UMOI.

Search

The pages in this section allow configuring how searches of Content Manager behave.

Security

The pages in this section allow configuring and reviewing how Content Manager security is applied to content on this site.

The 'Security Settings' page allows enabling and disabling the various security options.

The 'Group Membership' page allows you to easily identify the SharePoint groups that a user belongs to and can be useful for fault finding security challenges.

The 'Security Claims' page allows viewing of all security combinations that are currently in use on this site collection. This can also be useful for fault finding security challenges.

Site Management

Manage, finalize, relocate and archive actions apply to all content on this site. In the case of relocate and archive, they also apply to all child sites. For example, if you choose to relocate this site, any child sites (and their children) will be relocated as well.

Monitoring

The pages in this section can be used to monitor the management of content by Content Manager.

The 'Job Queue' allows access to pending, running, failed and historical jobs.

The 'Job Queue Settings' allows to configure Job Queue related settings.

Site auditing allows viewing the audit history for this site.

Site Collection auditing allows viewing the audit history for the whole site collection.

CM Statistics Overview allows viewing total number of documents processed in to Content Manager.

[Default Integration Settings](#)

[Site Records Management Options](#)

[Management Rules](#)

[Management Instructions](#)

[Management Selectors](#)

[Management Rules Options](#)

[Content Types to Record Type Mapping](#)

[Column Mapping](#)

[Lifetime Management Policies](#)

[Lifetime Management Options](#)

[Reapply Policies Now](#)

[Federated Search Settings](#)

[Security Settings](#)

[Group Membership](#)

[Security Claims](#)

[Configuration Access Controls](#)

[Manage this site](#)

[Finalize this site](#)

[Relocate this site](#)

[Archive this site](#)

[Job Queue](#)

[Job Queue Settings](#)

[Notification Settings](#)

[Site Auditing](#)

[Site Collection Auditing](#)

[CM Statistics Overview](#)

About OpenText

OpenText enables the digital world, creating a better way for organizations to work with information, on-premises or in the cloud. For more information about OpenText (NASDAQ/TSX: OTEX), visit opentext.com.

Connect with us:

[OpenText CEO Mark Barrenechea's blog](#)

[Twitter](#) | [LinkedIn](#)