Content Manager

Software Version 9.3

Content Manager Governance and Compliance SharePoint App: Installations Guide

Document Release Date: August 2018

Software Release Date: August 2018

Legal notices

Copyright notice

© Copyright 2008-2018 Micro Focus or one of its affiliates.

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

1 Introduction

1.1 Installation Guide

1.1.1 Scope

This document details the installation, enablement, and upgrade procedures for all versions in the 8.2.x and 9.x stream of Content Manager Integration for SharePoint releases. For guidance on the administrative features and functions of the integration software, please refer to the *Content Manager Integration for SharePoint User Guide*.

Consult the appropriate Content Manager or Microsoft documentation for details on Content Manager or Microsoft SharePoint Server 2013.

This document describes the currently supported configurations and features, anything not listed must be assumed to imply it is not supported.

1.1.2 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:

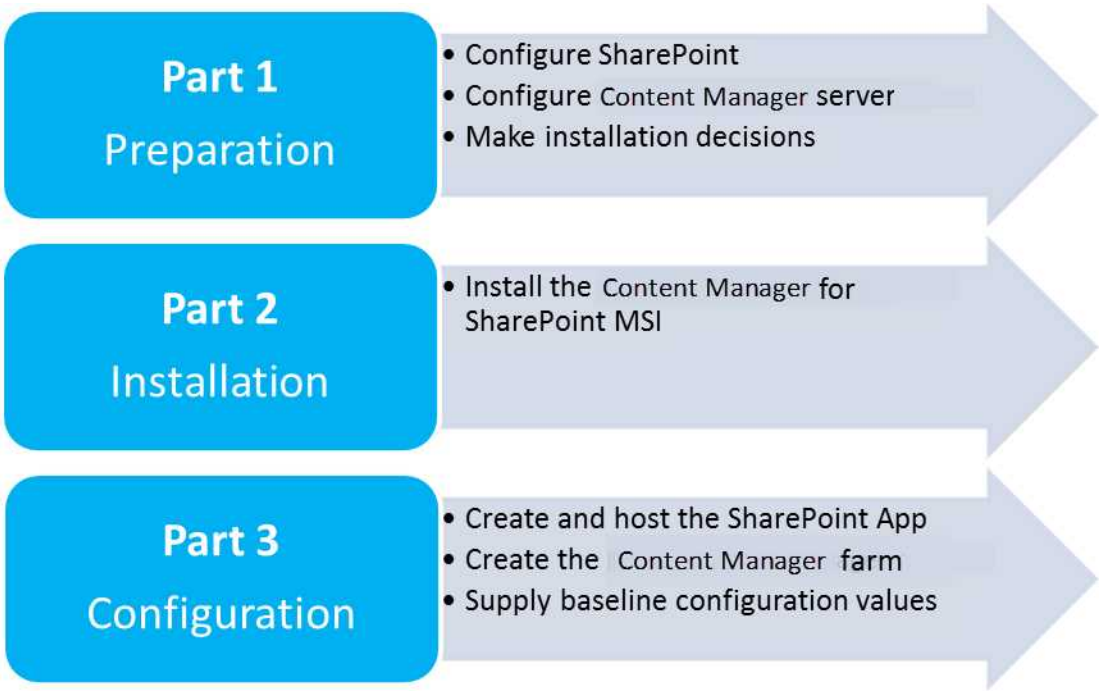
- Content Manager administration
- Microsoft SharePoint Server 2013 farm administration

To perform the installation or upgrade of the integration software, you **do not** need to be knowledgeable about records or information management principles or about working with Content Manager or SharePoint user content.

The person configuring the integration **will** need to understand your organization's information management requirements.

1.2 Overview of the installation process

In order to use Content Manager for governance and compliance of SharePoint information, the product needs to be firstly installed and configured. The overall process of taking your environment from its current state to one where Content Manager is ready to use can be summarized in three phases:



It is important that you follow the steps outlined in this document for each part of the process to ensure a successful implementation.

2 Preparation

2.1 Introduction

It is important to prepare your environment correctly for installation. Content Manager for SharePoint is an integration between Content Manager and Microsoft SharePoint. Both of these products are highly configurable with many optional components.

Preparing for the installation involves ensuring that any necessary configuration of these products has been performed prior to the installation occurring.

This section is also about understanding and making some installation choices prior to commencing installation.

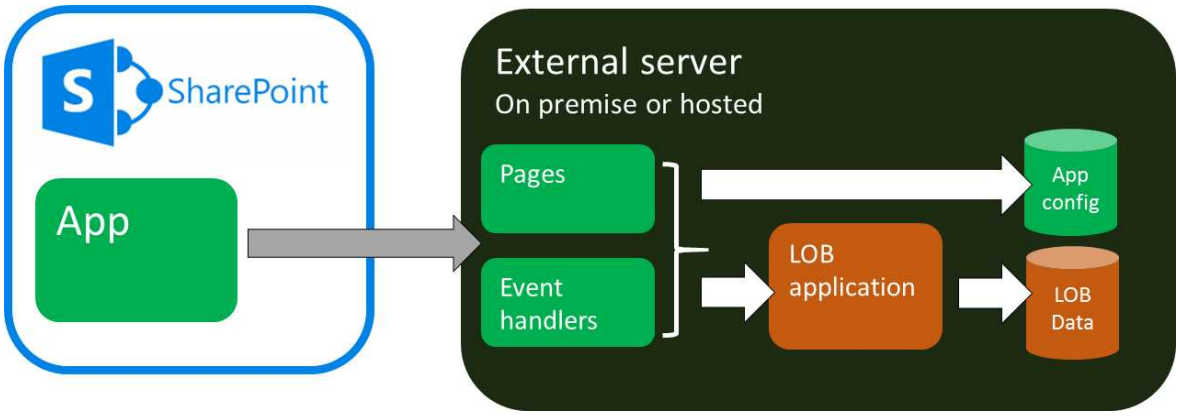
2.2 Understanding the product architecture

2.2.1 SharePoint apps

SharePoint 2013 introduced a new architecture for integrating/interacting with SharePoint. This architecture is known as the "App model".

The concept of a SharePoint app is that using only a small footprint on the SharePoint farm, it is able to configure UI components such as ribbon buttons. The actual processing provided by an app is performed on an external server, not on the SharePoint server.

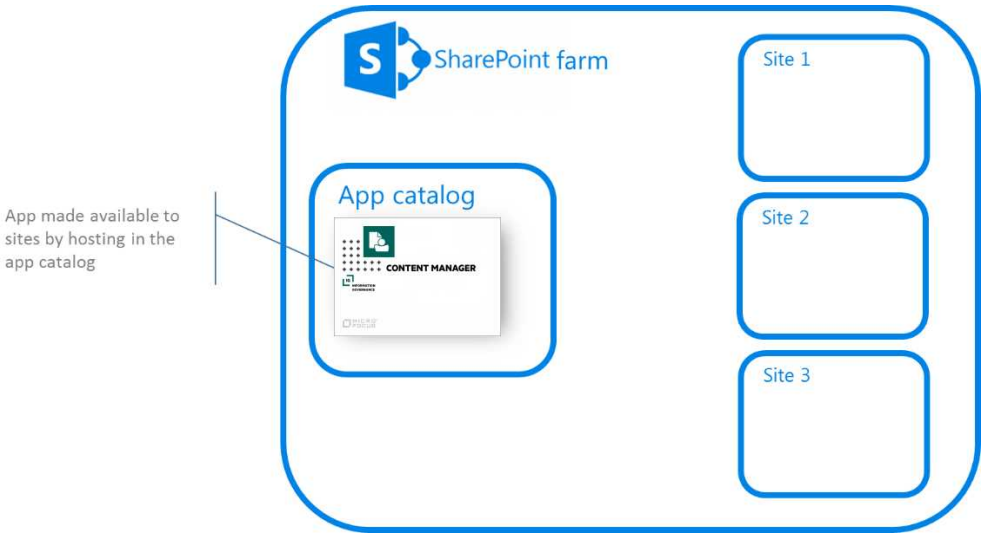
This type of SharePoint app is known as a "provider hosted app"



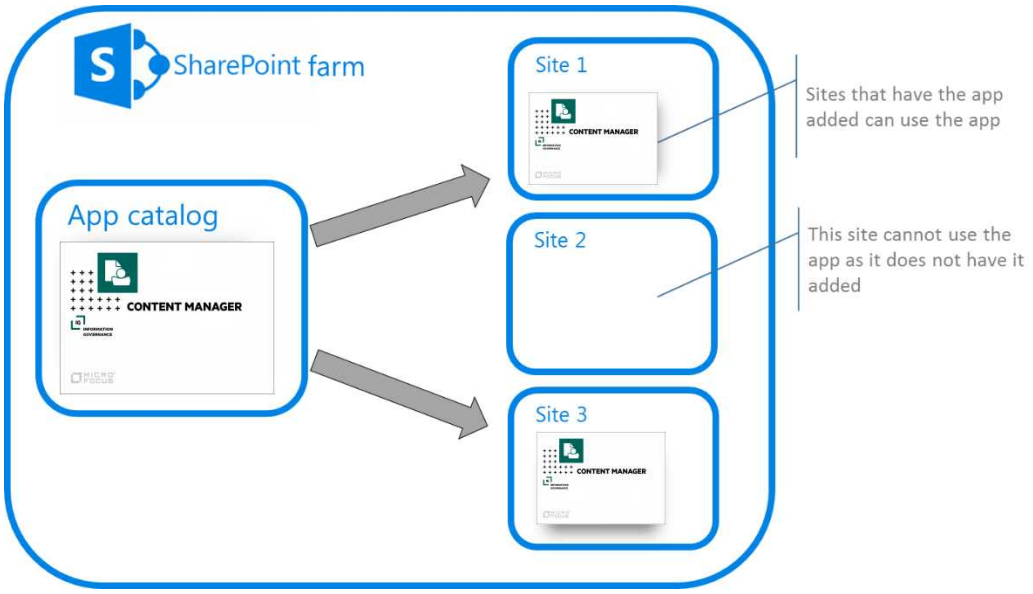
The external server typically provides:

- Any pages used by the app such as configuration pages
- A service for handling events raised by SharePoint that are relevant to the app.
- Access to the line of business (LOB) application that the app is using
- Storage of LOB data
- Storage of app configuration data

SharePoint apps are hosted in catalogs to make them available for use on a SharePoint site or site collection. The Microsoft corporate store is the catalog of publicly available apps that are available for purchase and use. SharePoint includes a corporate catalog that allows the hosting of apps that are only available for use in your organization.

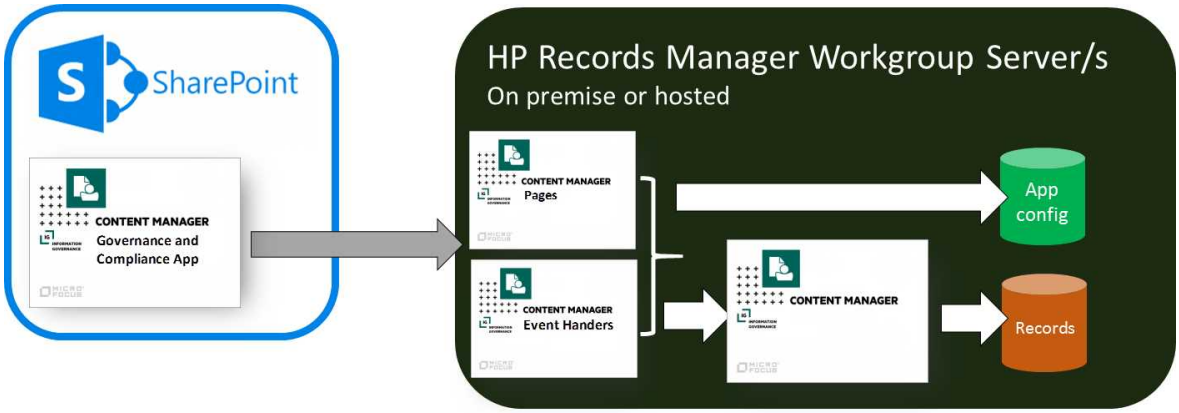


Once an app has been made available in the corporate catalog, it can be added to a site. It is at this point that the app functionality is available for use.



2.2.2 The Content Manager Governance and Compliance app

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.



Equating this to the explanation of SharePoint apps, it is Content Manager that is the LOB application with the LOB data being the records it stores.

The app configuration data for the app is stored in a dedicated SQL Server database. Although illustrated as residing on the workgroup server, this database can be hosted on an external SQL Server.

Installation of these components can be summarized as:

- The pages and event handlers are installed on the Content Manager Workgroup Server by a dedicated MSI

- The app is manually uploaded to the SharePoint app catalog in use by the SharePoint farm
- The app is manually added to sites and site collections where it is required

2.2.3 Job processing

Management tasks are performed asynchronously by jobs. When a job is requested it is added to a job queue. The job queue resides in the app configuration database. Workgroup servers in the Content Manager farm retrieve jobs from the job queue and process them when the server has the capacity to complete the job.

The retrieval and execution of jobs from the queue is performed by a Windows service called the "Content Manager SharePoint Service".

Processing jobs from the queue in this manner provides the following benefits:

- Failover: if a server in the Content Manager farm becomes unavailable, other servers can process the jobs
- Retry: if a job fails, it will be retried
- Restart: should a workgroup server become unavailable after it has commenced processing a job, when the server becomes available again, the job will recommence from the point that it was at when the server went offline.
- Throttling: jobs are processed in a throttled manner to ensure that the server processing does not consume more resources than it has available.

2.3 Determine Content Manager server topology

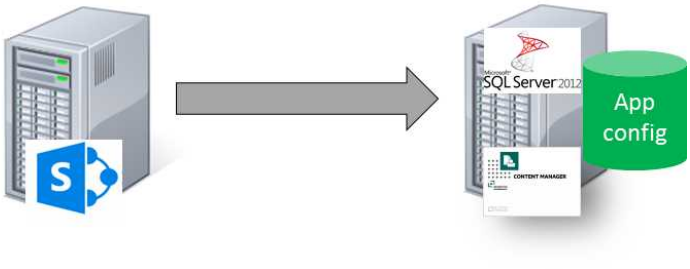
2.3.1 Overview

The size of your SharePoint farm, the number of users and the types of activities that these users perform will all be determining factors when deciding how to configure the server topology for Content Manager.

2.3.2 App configuration storage

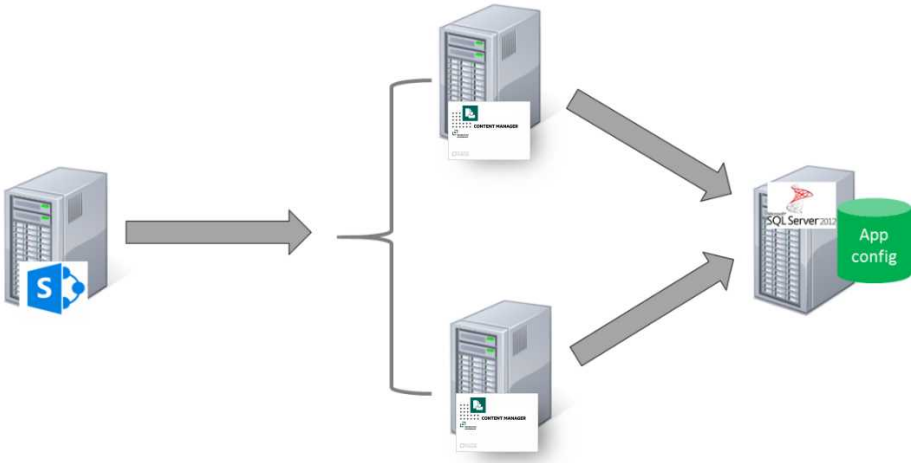
The app configuration is stored in a SQL Server database. This therefore requires a SQL Server instance to be available (see the Preparing SQL Server section later in this document for supported versions)

It is permitted to host SQL Server on the workgroup server. This is the simplest scenario.



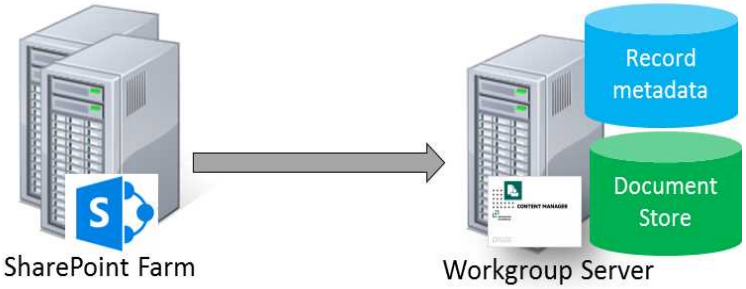
The app configuration database can be hosted on a separate dedicated SQL Server box if necessary.

In the scenario where multiple workgroup servers are used, only one instance of the app configuration database is required and will be shared by all workgroup servers in the farm.



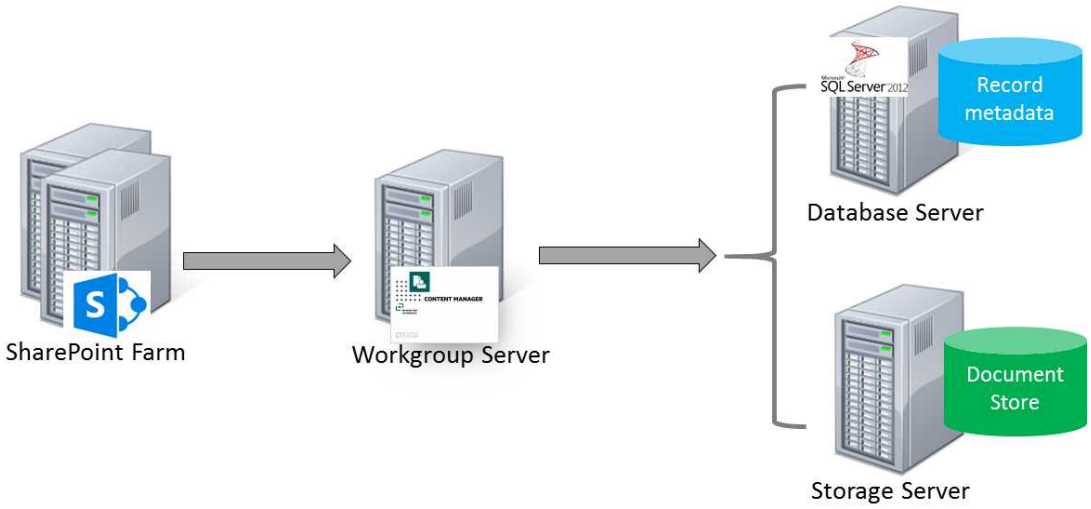
2.3.3 Workgroup servers

The simplest of server topologies will involve a single Content Manager workgroup server servicing the SharePoint farm.



Note that running the workgroup server on a SharePoint server is not currently supported.

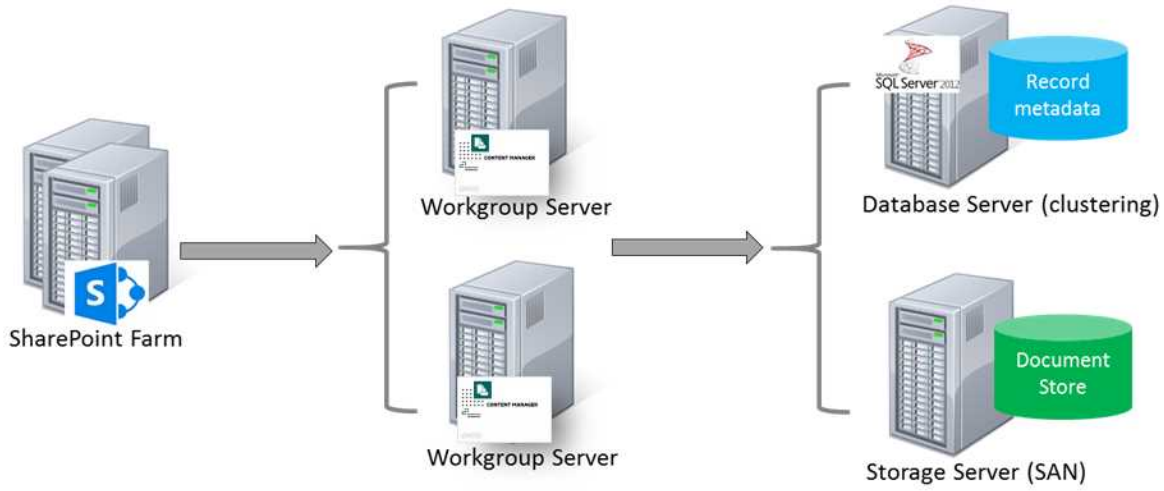
In a production environment, this architecture may in fact look as follows:



Depending on the performance of the workgroup server and the number and type of management tasks being performed for SharePoint content, this may satisfy the capability that is required by your organization.

However, what you lose by using only a single workgroup server is redundancy. Should the workgroup server become unavailable for any reason, information management will not be possible for SharePoint content.

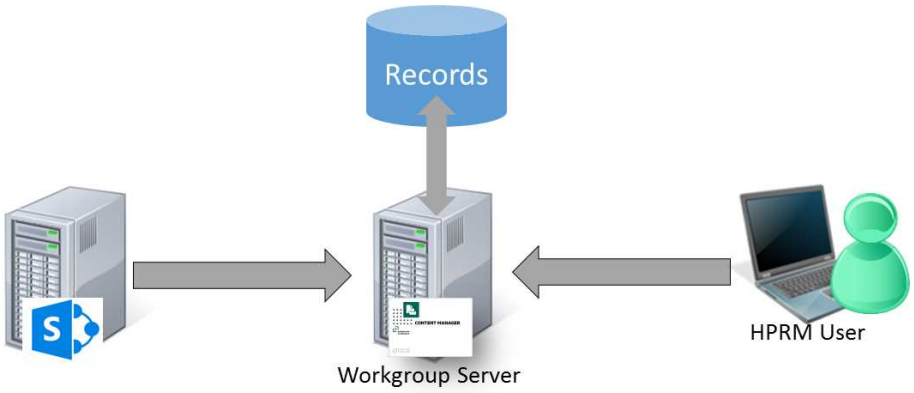
It is recommended that at least one other Content Manager workgroup server is made available to provide this redundancy. When multiple servers are used though, you must provide load balancing for these servers.



The collection of workgroup servers in use is referred to in the rest of this document as the ***"Content Manager Farm".***

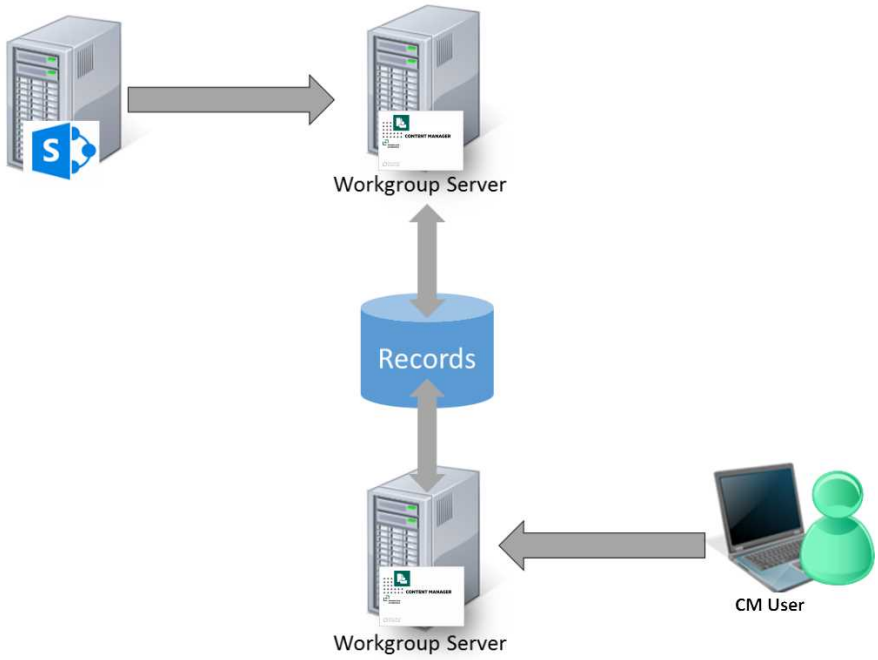
Considerations for using existing workgroup servers

Your organization may already have existing workgroup servers if it has an existing implementation of Content Manager. It is possible to use existing workgroup servers in lieu of dedicated servers used only by SharePoint.



In this scenario, SharePoint is utilizing a workgroup server (or collection of workgroup servers) that are already in use in the organization. Content Manager users can continue to use that workgroup server even though it is also being used for SharePoint management. This may be a suitable configuration in smaller deployments.

If using a dedicated workgroup server (or servers) explicitly for the management of SharePoint, your existing Content Manager users can continue to connect to Content Manager via the existing workgroup server.



In the illustrated scenario, records created from SharePoint content and records created by Content Manager users all reside in the same dataset. The records are simply accessed via different workgroup servers. In this example, the Content Manager user would be able to access records created from SharePoint, and SharePoint users would be able to access records created by the Content Manager user.

Using dedicated workgroup servers in this manner allows distributing much of the load to allow sufficient performance for both SharePoint and for Content Manager users.

These illustrations are simplified explanations of workgroup server architecture. Please consult the Content Manager documentation for a more detailed understanding.

Determining the number of workgroup servers

This section provides guidance for determining the number of workgroup servers to use in your Content Manager Farm. There are no hard and fast rules and the determination will be based on your organization's requirements and performance metrics.

As described in the section Job processing, workgroup servers in the farm retrieve jobs from the job queue in a throttled manner to prevent overcommitting resources on the server.

If on a regular basis, the list of jobs in the queue appears to be growing, for a sustained period, this can indicate that you have insufficient workgroup servers to satisfy the requirements of your SharePoint farm. In this scenario, users may experience delays in seeing requested jobs performed.

Depending on how your organization uses SharePoint and Content Manager, this may or may not be an issue. This is a decision that will be individual to each organization.

It is suggested that you define metrics identifying the maximum time that should be taken for a management task to be performed. For example:

When a user manually manages an item in SharePoint, that item should be managed within 60 seconds.

If you begin seeing this metric exceeded, it may be time to consider improving the performance of existing workgroup servers or adding additional workgroup servers.

SharePoint events are handled by the Content Manager servers. For example, when a managed item is modified by a user in SharePoint, the Content Manager server is called synchronously to confirm that the change is permitted and make any necessary updates to the record.

If users are regularly encountering noticeable delays when saving updated list items, this may also be an indication that the servers in the Content Manager farm have reached maximum capacity.

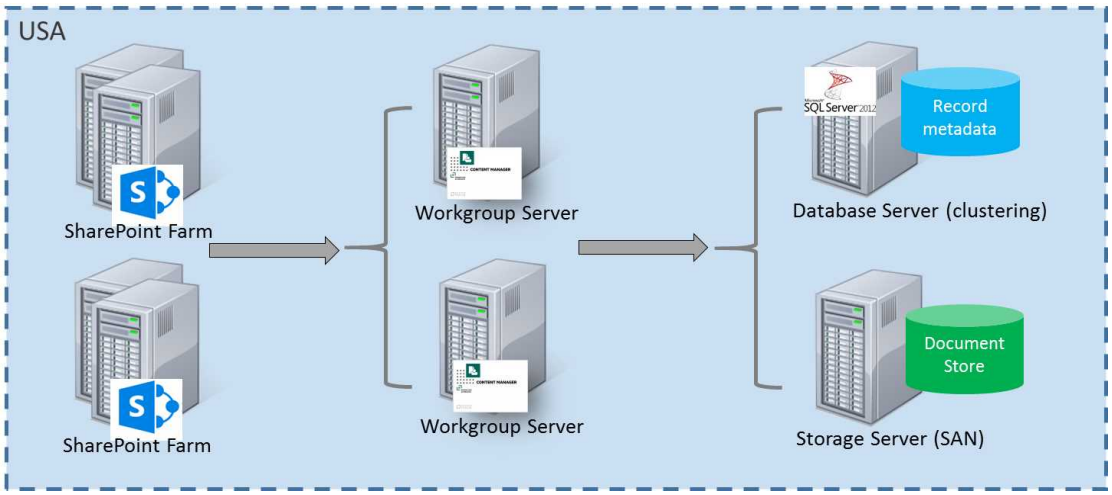
See Appendix: Performance planning for guidance around determining hardware requirements. Also see the ***Understanding the job queue*** section of the user guide for further details around how jobs are distributed.

2.3.4 Distributed architectures

This section covers common scenarios where an organization may have to geographically distribute system components and/or support multiple different SharePoint farms.

Multiple SharePoint farms - collocated

Multiple SharePoint farms can be supported by Content Manager. There are additional configuration steps required to support this covered in the section Supporting multiple SharePoint farms or multiple configuration databases

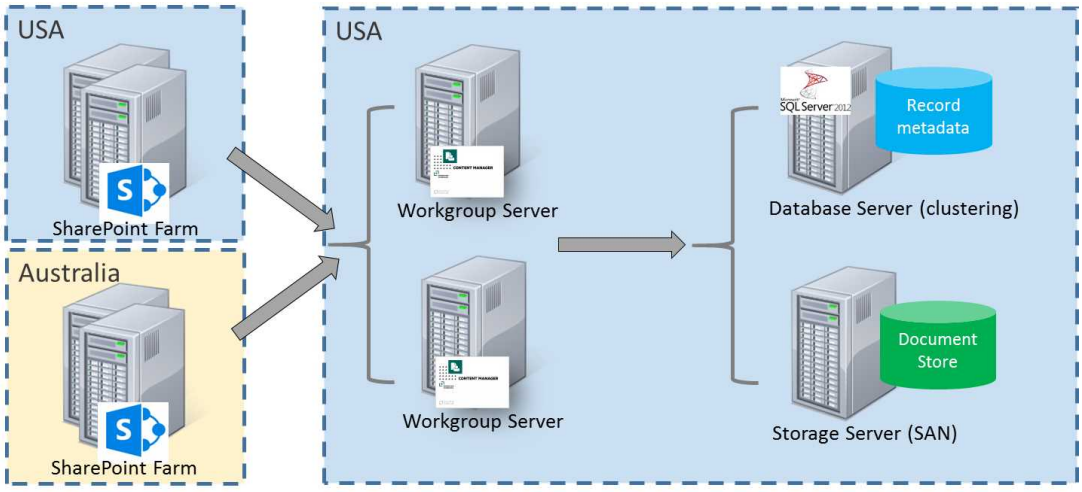


Multiple SharePoint farms – distributed

This scenario involves an organization with multiple SharePoint farms that are geographically distributed. For the examples, the farms are located in Australia and the USA and it is assumed there are network latency issues between the data centers.

Collocated workgroup server farm

An approach to service these farms is to use a single workgroup server farm collocated with one of the SharePoint farms. Both SharePoint farms connect to this workgroup server farm



This approach has the following considerations:

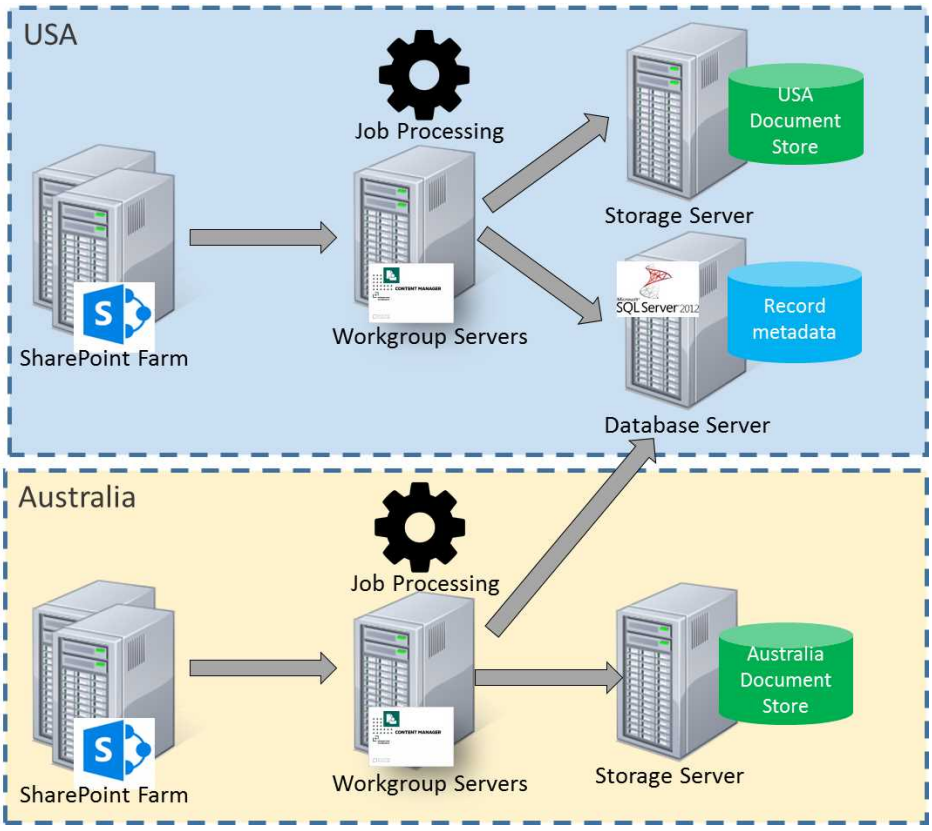
- Pros
  - Single location for maintenance and efficiency
  - Single dataset

- Single document store
- Simpler backup strategy
- Less infrastructure as both countries get redundancy from the same set of infrastructure
- IDOL indexing does not suffer from network latency for Australian content
- Retrieving Australian documents from USA no latency impact

- Cons
  - Editing managed list items in Australia would suffer from any Australia to USA latency (noting that we can accommodate up to 59 seconds latency but user's would probably only accept 4 seconds for a useability perspective).
  - Retrieving documents via search would be subject to Aus-US latency
  - Jobs running against Australia farm will take longer (but user does not see this)
  - Retrieving USA documents from Australia latency impact. Workgroup server caching and pre caching can minimize this impact.

Distributed workgroup server farm

An approach to service distributed SharePoint farms is to distribute the servers in the workgroup server farm across the two geographic locations. Each SharePoint farm connects to the workgroup server/s in its geographic location. Jobs for the region are processed on that regions workgroup server/s.

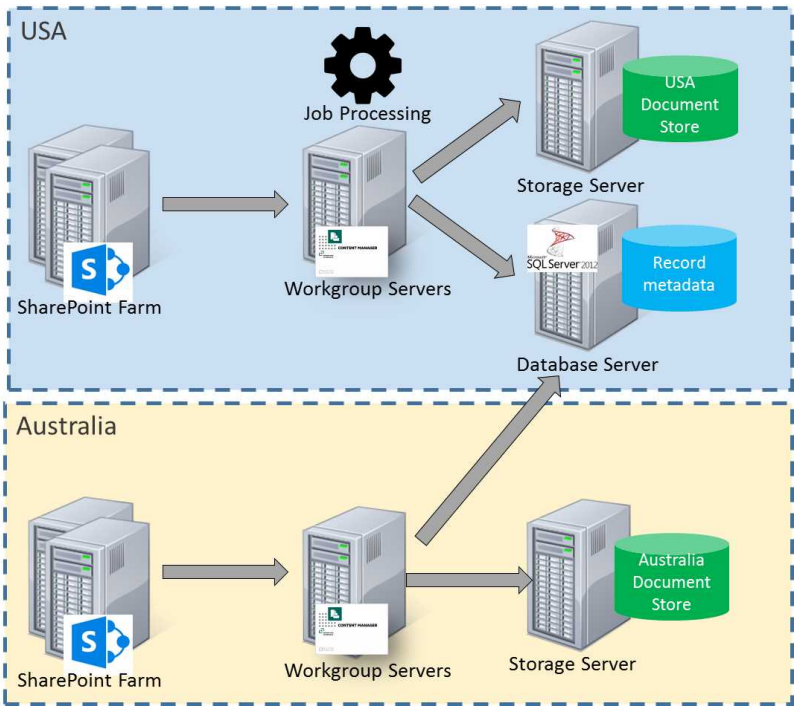


This approach has the following considerations:

- Pros
  - Shared database infrastructure – lower maintenance
  - Both regions share the database redundancy capabilities
  - Document retrieval through search fast
  - Can configure each region to only process their own jobs
- Cons
  - More infrastructure to provide workgroup server redundancy in each region
  - Multiple document stores
  - If IDOL indexing in USA will suffer latency for Australian documents
  - Retrieving Australian documents from USA (and vice versa) latency impact. Happens through search or during relocation.
  - Editing managed list items in Australia could suffer from any latency to database server.
  - Job processing on Australian server impacted by latency to database server.

Distributed workgroup server farm with central job processing

An approach to service distributed SharePoint farms is to distribute the servers in the workgroup server farm across the two geographic locations. Each SharePoint farm connects to the workgroup server/s in its geographic location. In this scenario, all jobs for all regions are processed by one of the workgroup server farms.

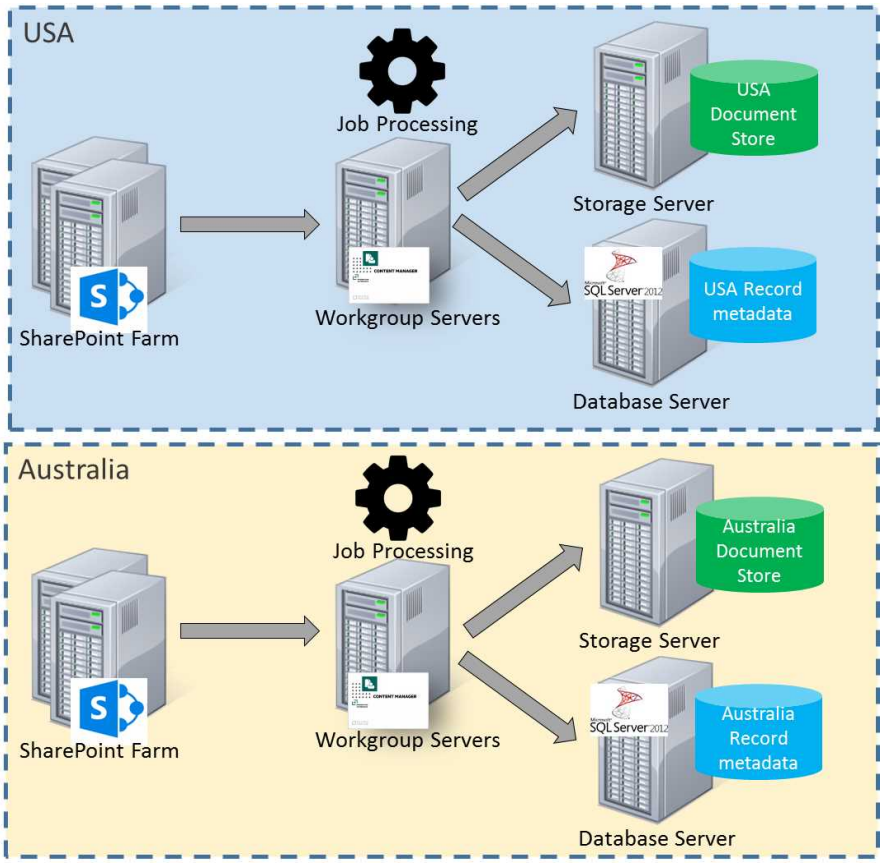


This approach has the following considerations:

- Pros
  - Can scale out in a central place rather than distributed as jobs are processed in a central place
  - Jobs are processed close to Content Manager so Content Manager interactions have no latency
- Cons
  - Workgroup servers in Australia are underutilized
  - Jobs for Australian content suffer latency reaching the Australian SharePoint farm

Separation of Content Manager

Another approach to management of geographically separated SharePoint farms is to have an entirely separate Content Manager infrastructure for each SharePoint farm.



This approach has the following considerations:

- Pros
  - No latency
  - Can configure search across both datasets
- Cons
  - Silo-ed information
  - Maintenance of two separate infrastructures
  - May result in underutilized servers

2.4 Preparing Content Manager

2.4.1 Overview

The components used by the app to interact with Content Manager must be installed on all Content Manager servers that you have identified for your Content Manager Farm. There are various OS and Content Manager features that must be enabled in preparation for the installation to occur.

This section covers the preparation that must be performed to ensure your Content Manager farm is ready for installation to begin.

2.4.2 Supported environments

Content Manager servers that are used must have one of the following operating systems installed:

- Windows 2012
- Windows 2012 R2

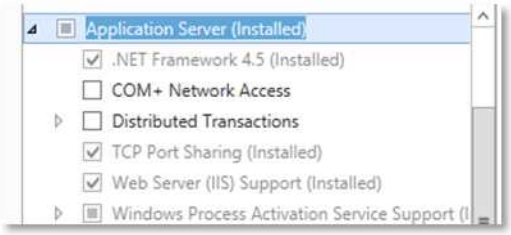
2.4.3 Server roles and features

All Content Manager servers must have a number of specific server roles and features enabled.

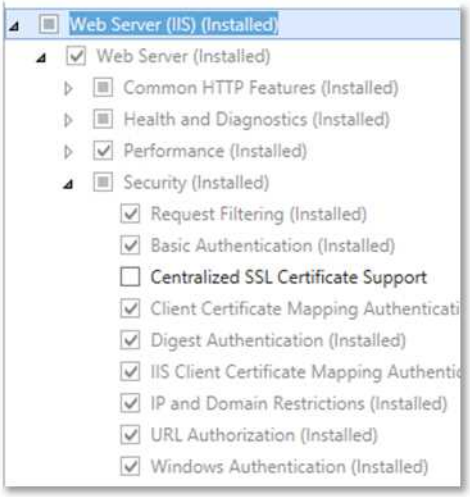
Server roles

Content Manager servers must have the following role and role elements enabled:

- Application Server role
  - .NET Framework 4.5
  - Web Server (IIS) Support



- Web Server (IIS) role
  - Web Server
    - Security
      - Windows Authentication



Server features

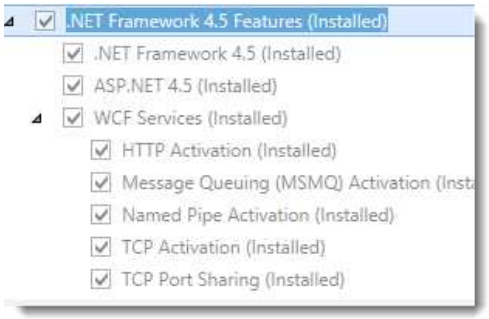
Content Manager servers must have the following features enabled:

- .NET Framework 3.5 Features
  - .NET Framework 3.5 (includes .NET2.0 and 3.0)

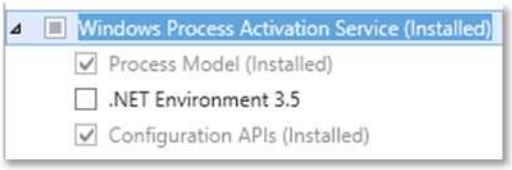
Not required for Azure environments

To install .NET 3.5 You will need the windows server DVD mounted in the dvd drive or else use the alternative path and point to the sources\sxs folder of the windows server dvd

- .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



The Windows Process Activation Service will be automatically activated as a result of activating the HTTP Activation feature.

2.4.4 Install and configure AppFabric

Overview

This section does not apply if your Content Manager servers are installed in a Windows Azure environment.

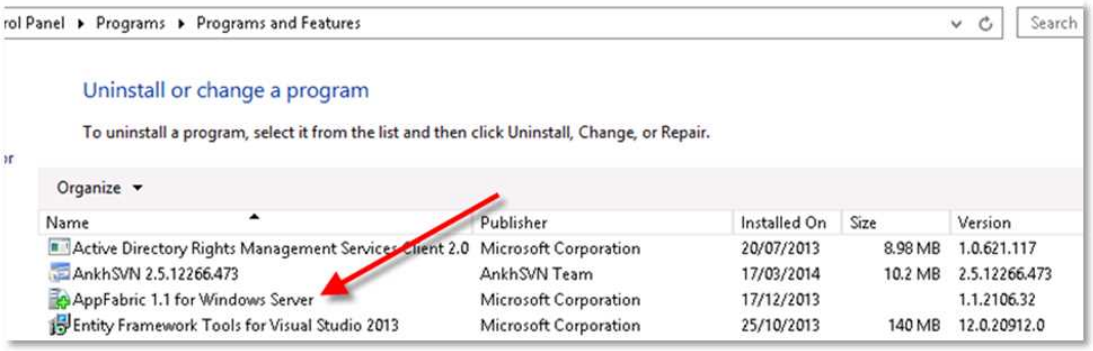
Configuration caching is used by the application to improve performance. The technology underpinning this configuration caching is Microsoft AppFabric.

All Content Manager servers in the farm must have AppFabric correctly installed and configured.

This section assumes that you have configured all server roles and features prior to beginning the installation.

Determining if already installed

Using the "Programs and Features" tool in Windows, you will see an entry for AppFabric in the installed programs if it has been previously installed.



The supported version is 1.1 x64.

Just because it has been installed does not mean that AppFabric has been configured. Be sure to follow the configuration instructions if you find that AppFabric is already installed

Installing and configuring

If it is necessary to install and configure AppFabric on your environment, please see the appendix Installing AppFabric and Configuring AppFabric for instructions. For troubleshooting issues with AppFabric see the Troubleshooting AppFabric appendix.

2.4.5 Configure Azure caching

Overview

If Content Manager is installed on a server hosted in Windows Azure, AppFabric cannot be used. Instead, Azure caching must be used.

Creating an Azure cache

It may be necessary to create an Azure cache if you have not already done so. For instructions on how to do this, please see the appendix Creating an Azure cache.

You will require the details of the cache endpoint and the primary cache key during configuration. You should note them down. See the appendices Obtaining the azure cache endpoint and Obtaining azure cache keys if you are unfamiliar with how to do this.

2.4.6 Install SQL Server pre-requisites

If the workgroup server does not have SQL Server installed on it, it will be necessary to install SQL components that are used by parts of the solution.

This step is only necessary on the server that you will run the configuration tool on.

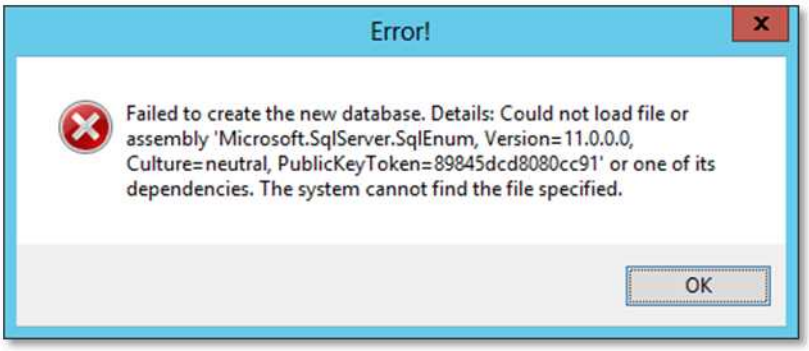
Install the Microsoft SQL Server 2012 SP1 feature pack from the following URL:

http://www.microsoft.com/en-au/download/details.aspx?id=35580

When prompted, it is necessary to download and install the following components:

- ENU\x64SQLSysClrTypes.msi
- ENU\x64\SharedManagementObjects.msi

Failure to install these on a workgroup server will result in an error similar to the one below when running the configuration tool:



2.4.7 Install SharePoint client components

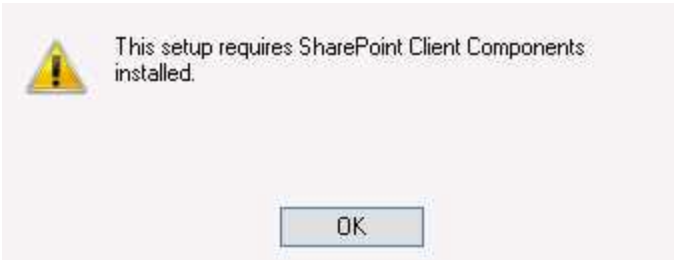
The connection to SharePoint is made from the Content Manager server using the SharePoint ***Client Side Object Model***, known as the ***CSOM***. It is a requirement to install these components to allow this communication to occur.

Versions earlier than 8.1.1 previously installed these components for you. From 8.1.1 onwards, this has been removed. This allows the updating of the CSOM to match changes and improvements in SharePoint. This can be particularly useful for SharePoint Online.

The CSOM is installed by the ***SharePoint Server 2013 Client Components SDK*** MSI available from Microsoft. You should download and install these components from here:
http://www.microsoft.com/en-us/download/details.aspx?id=35585

You must download and install the 64bit version of these components

If you do not install these components, during the installation of the Content Manager Governance and Compliance app you will encounter the following error.



2.4.8 Configure Content Manager

Workgroup server configured

All servers that will form part of the Content Manager farm must be configured to run as workgroup servers. Each server must have access to any Content Manager datasets that you intend to use when managing SharePoint content.

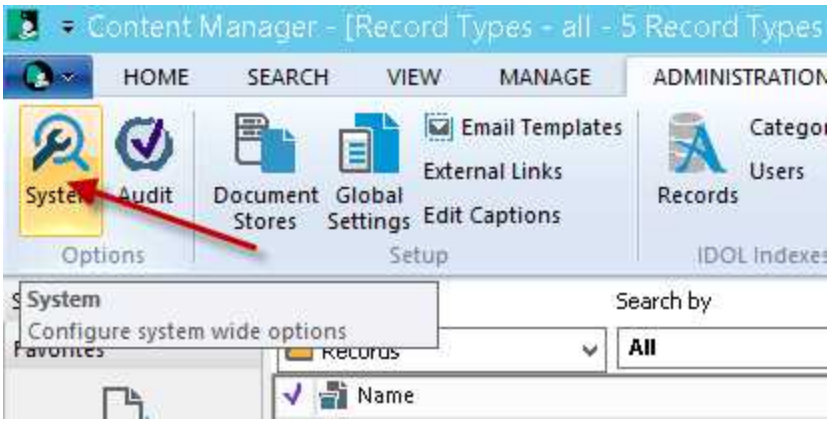
> *For details regarding how to configure a workgroup server, please see the Content Manager documentation.*

Enable Content Manager features

There are two Content Manager features that need to be enabled. To access feature enablement, follow these steps.

Using the Content Manager client as an administrator, connect to the dataset that will be used by SharePoint.

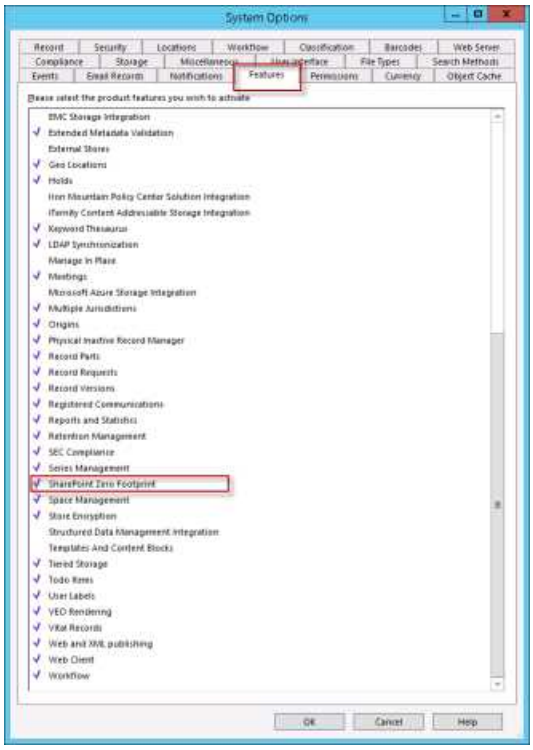
- From the **Options** section of the **Administration** ribbon, select **System**



Enable the SharePoint Zero Footprint feature

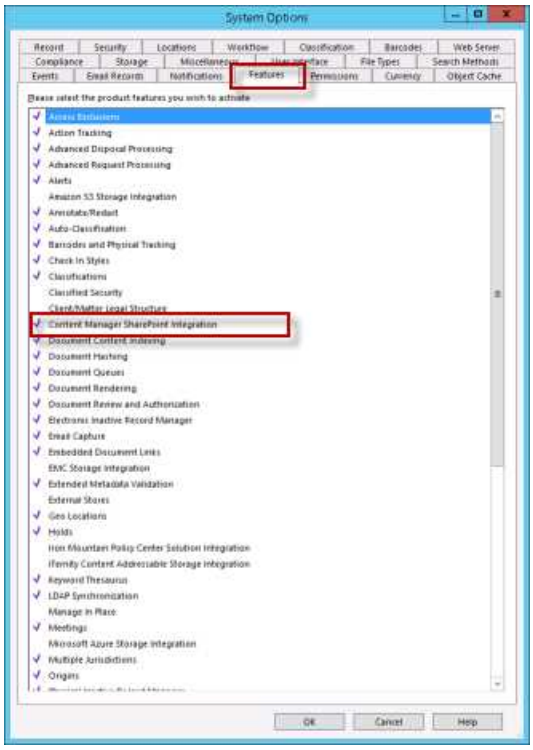
Version 8.1 of Content Manager introduces a new feature called “SharePoint zero footprint”. This feature must be enabled in Content Manager for the integration to work correctly.

- From the **Features** tab, ensure that the **SharePoint zero footprint** feature is enabled.



Enable the Content Manager SharePoint Integration feature

- From the **Features** tab, ensure that the **Content Manager SharePoint Integration** feature is enabled.



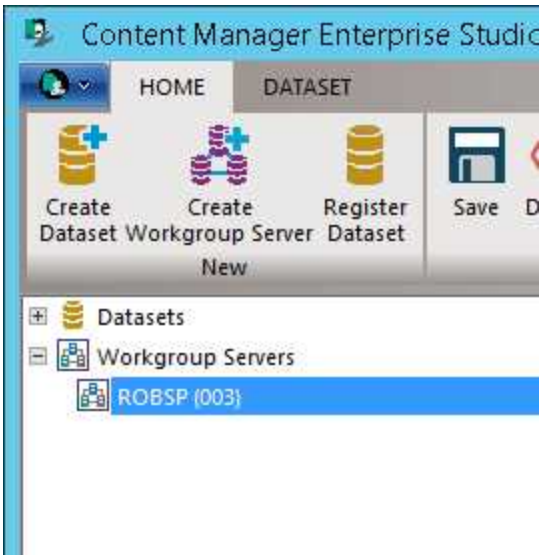
After enabling features, you should restart the Content Manager Workgroup Windows service for the settings to take effect.

Add to a SharePoint farm

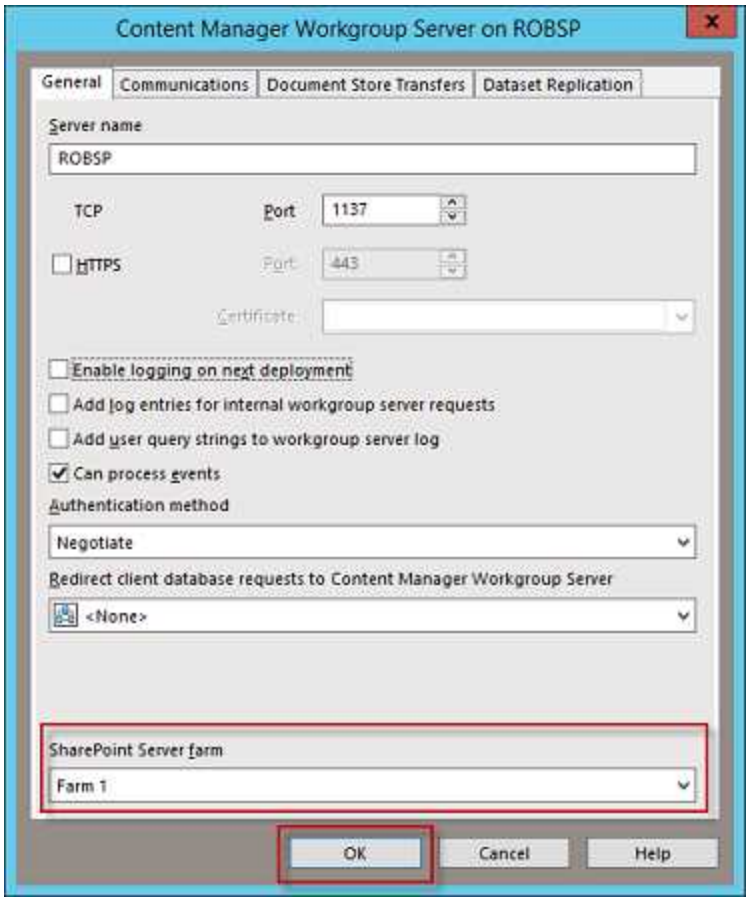
In order to assist with the routing of Content Manager events, it is necessary to indicate to Content Manager which SharePoint farm it will be servicing.

All servers in the Content Manager farm must be joined to the same SharePoint farm.

- Open the **Content Manager Enterprise Studio**
- Expand the **Workgroup Servers** node



- For each Workgroup server under this node (that you are using in your Content Manager farm):
  - Double-click the server to open the properties dialog
  - Choose a SharePoint server farm to join to. The value you choose is arbitrary however all servers that form part of the same Content Manager farm must use the same value
  - Click **OK**



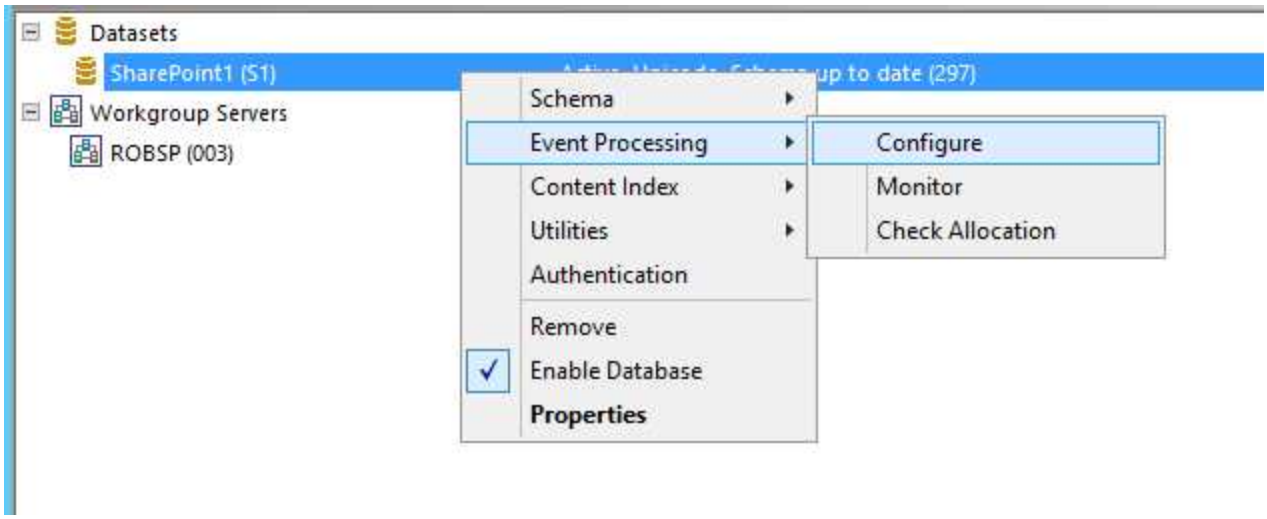
- Once all workgroup servers have been configured
  - Save the configuration
  - Deploy to all servers

  If you are unsure how to save and deploy, see the appendix "Saving and deploying Content Manager configuration settings"

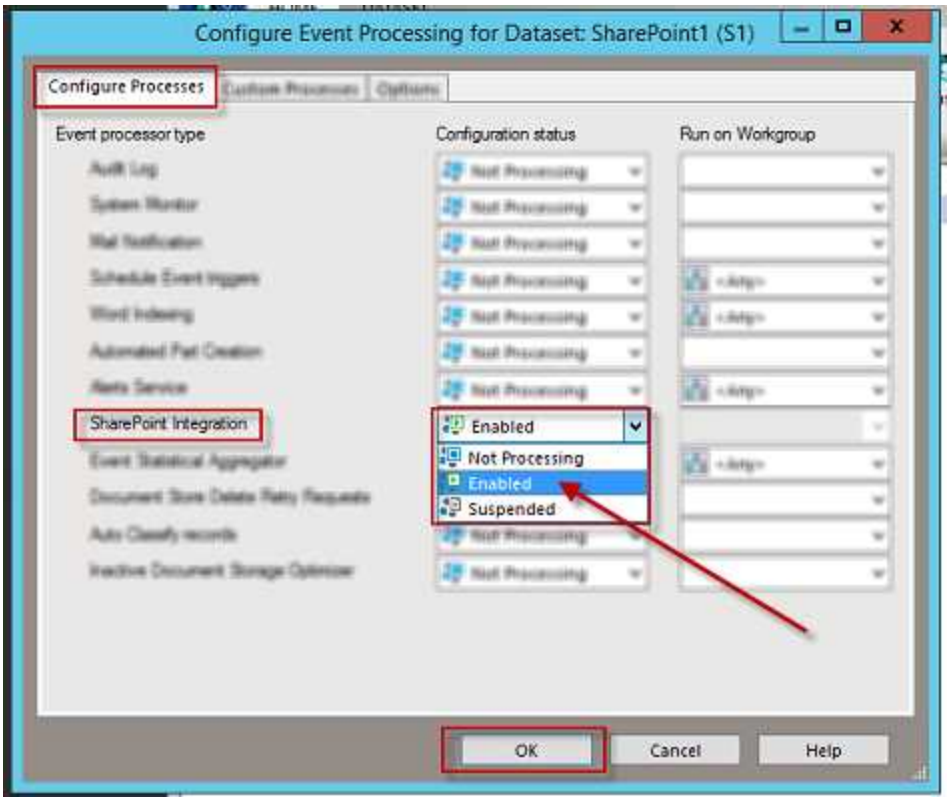
Configure event handling

For each dataset that will be used for managing SharePoint content, event processing must be enabled. Using "Content Manager Enterprise Studio", for each dataset perform the following steps:

- Expand the **Datasets** node
- Right-click on the dataset to be used and choose **Event Processing** then **Configure**



- Ensure that the **SharePoint Integration** event processor type is set to **Enabled** then click **OK**

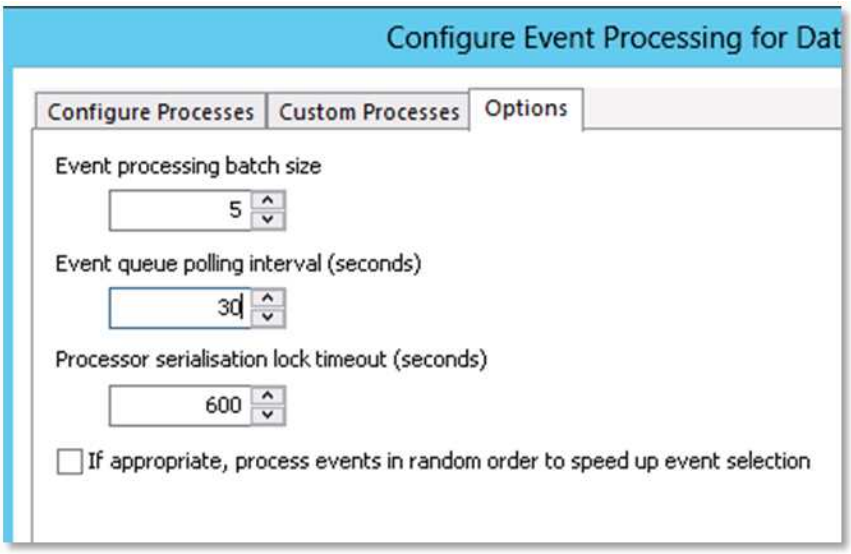


Reducing event handling time

The Content Manager event handler periodically examines the event queue to determine if there are events to be processed. By default, this polling of the event queue is performed every 120 seconds. This means that it may be up to 120 seconds before an event is processed. This may lead delays in processing Content Manager record changes.

It is recommended that you decrease this polling time to reduce the amount of time taken to process these types of changes.

On the event handling configuration dialog (see previous section), navigate to the ***Options*** tab. Change the ***Event queue polling interval*** to a lower time frame. It is recommended that you do not reduce this interval to less than 30 seconds as this can cause errors during document maintenance.



2.4.9 Prepare record types

Overview

It is necessary to identify and configure the record types that will be used in Content Manager for managing SharePoint content. This section describes the steps.

SharePoint site record type

When managing content, a record is created to represent the site that the content resides on. The record type that is used for creating this record is referred to as the "SharePoint site record type".

A suitable record type must be available to be used. During the configuration of the application, you will need to specify this record type.

Suitable record types must have a behavior in Content Manager of "SharePoint Site". If you are unfamiliar with how to determine the behavior of a record type, please see the appendix Determining the behavior of a record type

If there is currently no suitable record type to use for this purpose, then you must create this record type. For details on how to create a record type, please consult the Content Manager documentation.

SharePoint list record type

When managing content, a record is created to represent the list that the content resides on. The record type that is used for creating this record is referred to as the “SharePoint list record type”.

A suitable record type must be available to be used. During the configuration of the application, you will need to specify this record type.

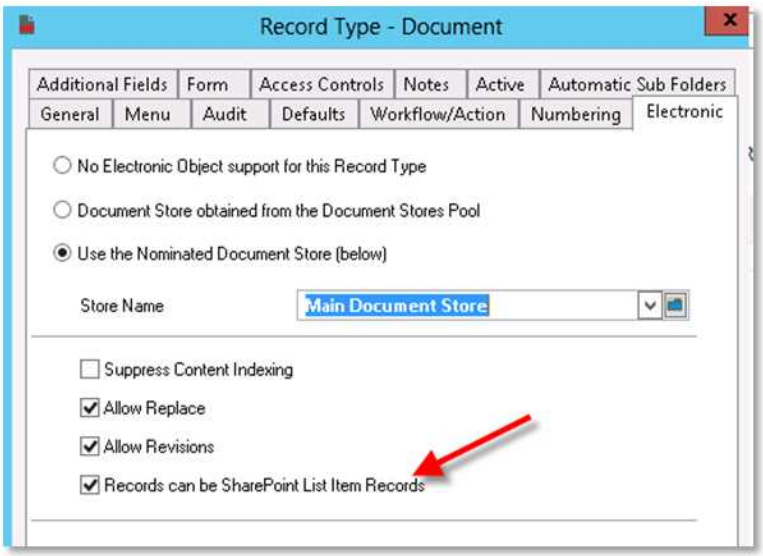
Suitable record types must have a behavior in Content Manager of “SharePoint List”. If you are unfamiliar with how to determine the behavior of a record type, please see the appendix Determining the behavior of a record type

If there is currently no suitable record type to use for this purpose, then you must create this record type. For details on how to create a record type, please consult the Content Manager documentation.

Mark record types as suitable

For a record type to be suitable for use when managing SharePoint content, it must be marked as being suitable. For each record type that is intended to be used to manage SharePoint content, you must do the following:

1. Access the **Electronic** tab of the record type
2. Ensure that this record type supports documents
3. Check the **Records can be SharePoint List Item Records** check box



For details on how to access the list of record types, see the appendix Accessing the list of record types

Ensure suitable numbering patterns

It is important that the numbering pattern you use for your record types will not clash with existing numbering. If the next available number for the record type has already been used, management will fail. Therefore, ensure that all record types that will be used for management of SharePoint content have unique numbering patterns and the next number to use is a number that is available.

This applies for record types that will be used to represent:

- List items
- Containers
- SharePoint lists
- SharePoint sites

For information regarding numbering patterns, see the Content Manager product documentation.

2.4.10 Prepare user locations

You must ensure that all users that will be performing management of content through SharePoint, have valid locations in Content Manager. These accounts must be active and must include the login details that this user will access SharePoint with.

You should note that when using SharePoint Online, the format of the accounts presented to Content Manager will use the format:

```
username@domain
```

For example

```
steven@acme.com
```

If using SharePoint online, ensure that the account details on the profile tab for a location use this format.

Note that this does not apply to the service accounts Job Processing service account and Application pool account. These will require the account name and domain fields on the profile tab to be completed separately regardless of whether you are using SharePoint Online or an on premise SharePoint farm.

For instructions on how to create a location in Content Manager that has access, see the appendix "Configuring the account, permissions and granting access for a location"

Permissions

Locations must be at least a ***Contributor*** in Content Manager to manage content. Locations that use the default ***Contributor*** or ***Knowledge Worker*** user types in Content Manager must have the ***Modify Record Additional Field Values*** permission enabled. This is not enabled by default.

It is suggested that you make this modification globally rather than on a location by location basis. See Setting the permissions granted to a user type section for instructions if you are unfamiliar with how to do this.

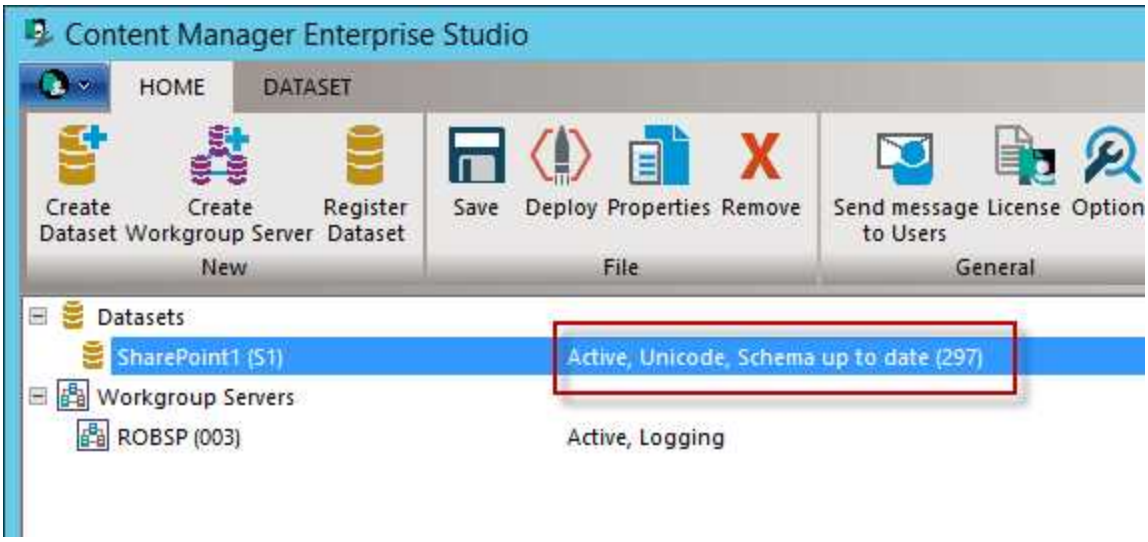
2.4.11 Prepare datasets

The Content Manager datasets that are to be used must be configured to support Unicode. To enable this support, run ***Content Manager Enterprise Studio*** as an **administrator**.

Please note, the process to enable Unicode has changed since previous versions.
Ensure you follow the steps below correctly in order to enable Unicode support on your datasets.

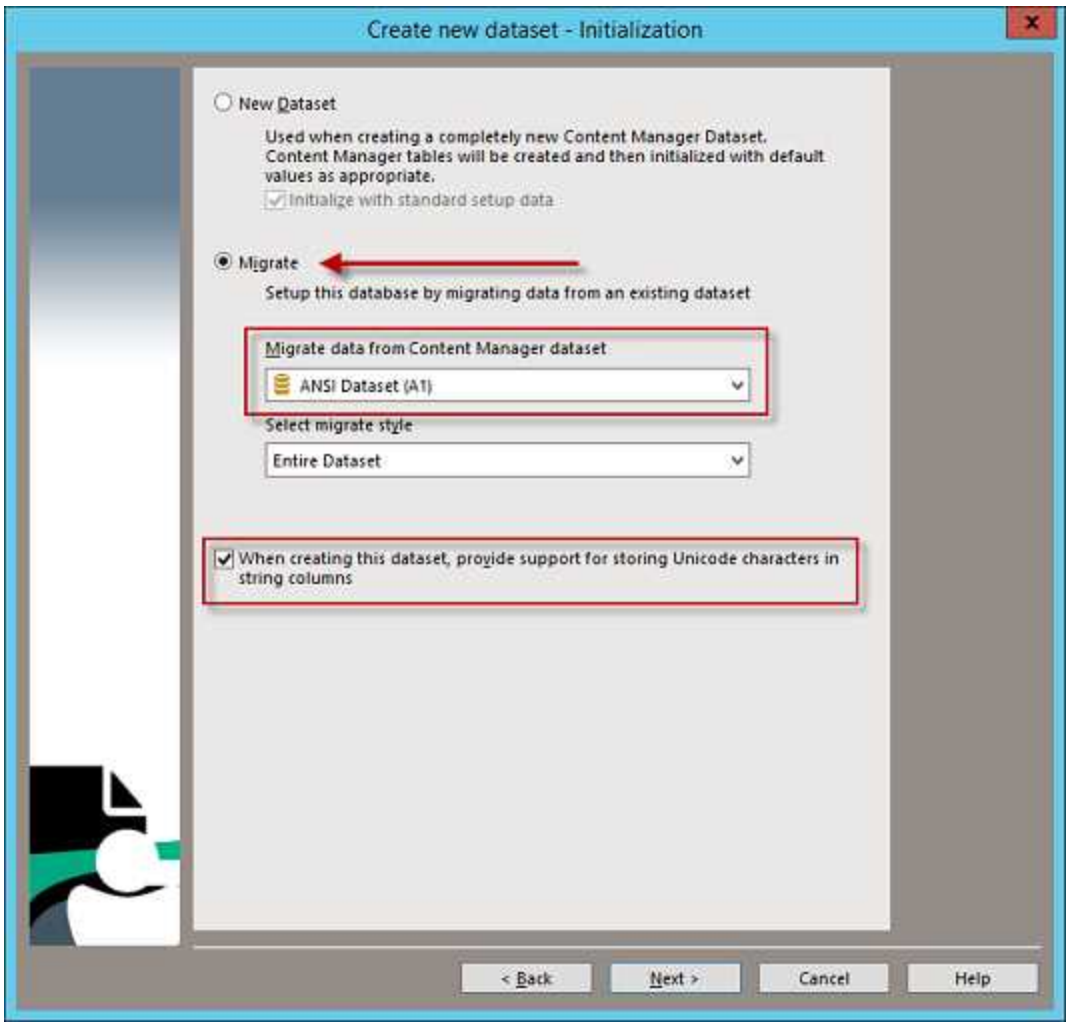
In Content Manager 9.0 you will be unable to do a direct conversion of your dataset from ANSI to Unidoce. You will need to create a new dataset, initializing it with Unicode support and then migrate your existing data over to it. The following section shows a brief overview of how to accomplish this. For more details, please consult the Content Manager documentation and notes.

Locate the dataset that is to be used and review the description. The description will include the term ***Unicode*** if Unicode has been enabled.



If this has not been enabled, select ***Create Dataset*** from the ribbon.

Follow the dataset creation steps as normal until you reach the Initialization wizard step. You will need to ensure you supply a bulk loading path during the creation process, otherwise the migration will not be able to run.

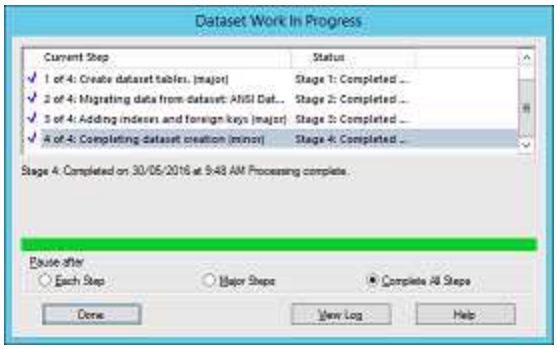


Select the ***Migrate*** option from the interface.

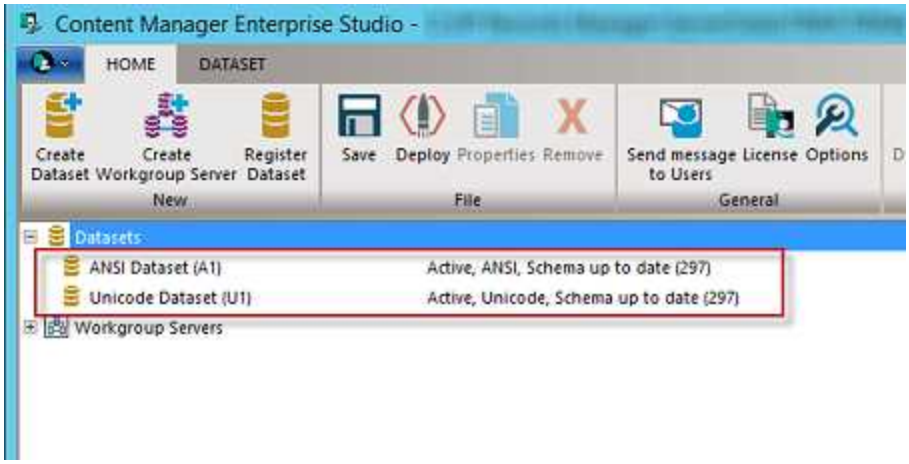
From the dropdown, select the dataset you wish to migrate data from.

To enable Unicode support for the new dataset, ensure the checkbox at the bottom of the page is checked.

Confirm the selection by pressing ***Next***. Follow the prompts to execute the dataset creation.



Upon completion of the tool you should be able to see the new dataset and the old, the new one showing Unicode support in the description.



2.5 Preparing SharePoint

2.5.1 Supported environments

Content Manager for SharePoint supports the following versions of SharePoint. You must ensure that your SharePoint environment adheres to these requirements.

- SharePoint 2013 SP1
- SharePoint Online standard (2013)

On premise SharePoint

SharePoint farm severs must meet the following prerequisites in order to support the Content Manager Integration for SharePoint

- **Operating System:** Windows Server 2012 or Windows Server 2012 R2
- **SharePoint:** SharePoint 2013 SP1

SharePoint online

SharePoint Online 2013 multi tenanted is supported.

2.5.2 Prepare the corporate app store

The Content Manager Governance and Compliance app will be hosted in your corporate app store following installation. It is here that the app will be available for consumption by users. See the SharePoint Apps section in this document for further details.

In SharePoint Online, an app catalog is made available for you automatically. In an on premise installation though, an app catalog is not typically automatically provisioned for you. If you have an app catalog, you will need to know how to access it. If you don't already have an app catalog, then you will need to create one.

Enable the required services

This section is not applicable to SharePoint online

For installing and deploying apps the following services must be running on your farm

- App Management Service
- Micrsoft SharePoint Foundation Subscription Settings Service
- User Profile Service
- User Profile Synchronization service

If you are unfamiliar with how to start services on your farm, please see the Starting a service appendix.

Ensure you have a subscription settings service application

This section is not applicable to SharePoint online

A subscription settings service application must be available on your SharePoint farm. This is used by site collections to consume apps from the farm.

To identify if you already have one of these configured, examine the list of service applications installed on your farm and look for a service that has a type of ***Microsoft SharePoint Foundation Subscription Settings Service Application***. If you are unfamiliar with how to see the list of service application see the Access service applications appendix.

If there is not one of these services in your farm, it will be necessary to create one. See the Creating a Subscription Settings Service Application appendix.

If a service exists, ensure that it is started.

Do not confuse this service with the "Microsoft SharePoint Foundation Subscription Settings Service". Note the inclusion of the word "Application" at the end.

Identifying the app catalog in use

During installation, you will need to be able to access the corporate app catalog to upload the Content Manager Governance and Compliance app as part of the configuration process.

For an on premise installation of SharePoint, it is possible to identify the app catalog in use using central administration. For SharePoint Online, the SharePoint admin center provides access.

If you are unfamiliar with how to do this, please see the appendix Identifying the app catalog in use.

You will need the URL of your app catalog during the configuration stage.

Creating an app catalog

If an app catalog does not already exist, then a new one must be created. If you are unfamiliar with how to do this, please see the Creating an app catalog appendix.

Configure the app URL

This section is not applicable to SharePoint online

Configure a suitable app URL to use with apps added to the corporate catalog. See the Configuring an app URL appendix for details about this task if you are unfamiliar.

2.5.3 Prepare environment for high trust apps

This entire section is not applicable to SharePoint Online

Overview

High trust apps are apps that require access to SharePoint information. The Content Manager app is a high trust app. When using high trust apps in an on premise environment, it is necessary to configure this trust.

In order to configure your environment to allow high trust apps, it is necessary to provide a certificate that is used by SharePoint and the Content Manager server to create the necessary trust.

For further reading about high trust apps, you can read the following article:
http://msdn.microsoft.com/library/office/fp179901.aspx

Obtain a certificate

It will be necessary to obtain a certificate to use in the high trust environment. This could be purchased from a third party, obtained from your corporate certificate service (if you have one), or for testing and

POC purpose, you can use a self-signed certificate.

For instructions regarding how to create a self-signed certificate, see the appendix Creating a self-signed certificate.

The following is an extract from the MSDN article: http://msdn.microsoft.com/en-au/library/office/jj860570.aspx

The third party can be a commercial Certificate Authority (CA) or an on-premises CA. In regard to commercial CAs, note that the industry is phasing out "intranet-only" certificates for web servers. They can still be purchased, but all such certificates will expire in November, 2016, or sooner. It is not necessary to have this kind of certificate for a high-trust app for SharePoint, because certificates that can be used for internet-facing web servers can also be used for intranet web servers, but the latter generally cost more.

The certificate should be in two formats, Personal Information Exchange (pfx) and Security Certificate (cer). If it is not in either of these formats when originally obtained, the customer can convert it using a utility.

> *Note that this article also provides guidance for conversion of certificate types to the pfx and cer formats.*

Distribute the certificate to all Content Manager servers in the Content Manager farm

The certificate used for high trust must also be available on every server in the SharePoint farm.

It is important to place the certificate in the same location on every server in the Content Manager farm.

- Identify a folder on the Content Manager server that will be used to hold the certificate.
- Ensure that the following accounts have at least read rights to this location:
  - Any user who will run the configuration tool
  - The job processing service account
  - The application pool account
- Copy the ".cer" file to this location
- Add the certificate to the "Trusted Root Certification Authorities" (see the appendix "Adding a certificate to the Trusted Root Certification Authorities for a machine")

> *Note that the final step is omitted in a number of Microsoft articles regarding high trust apps but has been found to be necessary.*

Record the path that the certificate is located as this will be required during configuration.

Distribute the certificate to all SharePoint servers in the SharePoint farm

The certificate used for high trust must also be available on every server in the SharePoint farm.

It is important to place the certificate in the same location on every server in the SharePoint farm.

- Identify a folder on the SharePoint server that will be used to hold the certificate.
- Ensure that the following accounts have at least read rights to this location:
  - the app pool identity for the IIS app pool “SecurityTokenServiceApplicationPool”
  - the app pool identities used by any SharePoint web application that will use the Content Manager Governance and Compliance app
- Copy the “.cer” file to this location
- Add the certificate to the “Trusted Root Certification Authorities” (see the appendix “Adding a certificate to the Trusted Root Certification Authorities for a machine”)

Note that the final step is omitted in a number of Microsoft articles regarding high trust apps but has been found to be necessary.

Configure SharePoint 2013 to use certificates and configure trust for your app

The following procedure configures the certificate as a trusted token issuer in SharePoint. It is performed just once and can be done on any SharePoint server in the farm.

This is done by registering the certificate with SharePoint with what is known as a “Trusted token issuer”.

Using ***PowerShell ISE*** (running as administrator) on any SharePoint server in the farm, run the script later in this section.

If you don’t use Powershell ISE, you will need to run the script line by line.

You must only run this script once!

When this script runs, it will prompt you for the full path to the certificate file that is being used to establish high trust (this is the path used in the Distribute the certificate to all SharePoint servers in the SharePoint farm step) . The console will display the issuer ID that has been allocated.

You must be sure to record the issuer ID as you will require this during installation and configuration.

SharePoint 2013 does not normally accept self-signed certificates. The script provided in this section includes the following entry that allows you to use a self-signed certificate. If you are not using a self-signed certificate then you should remove the following line from the script before running it:

```
$serviceConfig.AllowOAuthOverHttp = $true
```

You should remove this entry before running the script except when one or more of the following is true:

- The certificate used to configure high trust is a self-signed certificate
- You intend to use http as the protocol for connection with Content Manager.
- You intend to use http as the protocol for SharePoint

The registration of the certificate as a token issuer is not effective immediately. It may take as long as 24 hours before all the SharePoint servers recognize the new token issuer. Running an iisreset on all the SharePoint servers, if you can do that without disturbing SharePoint users, would cause them to immediately recognize the issuer. The script includes an IISReset call. If this will cause issues, you may remove this line in the script.

The following is the token issuer script to run to configure the trust:

```
Remove-PSSnapin Microsoft.SharePoint.PowerShell -erroraction SilentlyContinue
Add-PSSnapin Microsoft.SharePoint.PowerShell -erroraction SilentlyContinue
#Create a new issuer id
$issuerId = [System.Guid]::NewGuid().ToString()
$realm = Get-SPAuthenticationRealm
$confirm = Read-Host "Caution!!! Run this script once only. Do you want to
continue? (Y/N)"
if(($confirm -eq 'Y')  -or ($confirm -eq 'y'))
{
     #Get the certificate path
     $certificatePath = Read-Host "Enter the full path (including file name) to the
certificate(.cer)"
     $certificate = New-Object
System.Security.Cryptography.X509Certificates.X509Certificate2($certificatePath)

     #Set this certificate as the root authority
     New-SPTrustedRootAuthority -Name “HPRecordsManagerTrust” -Certificate
$certificate

     #Construct the full Issuer ID
     $fullIssuerIdentifier = $issuerId + ‘@’ + $realm

     #Register the certificate as a trusted token issuer
     New-SPTrustedSecurityTokenIssuer -Name "HPE Content Manager High Trust App" -
Certificate $certificate -RegisteredIssuerName $fullIssuerIdentifier –IsTrustBroker


     Write-Host "Use this issuer id" + $issuerId + "in your App Manager"

     #Turn on OAuth over HTTP
     $serviceConfig = Get-SPSecurityTokenServiceConfig
     $serviceConfig.AllowOAuthOverHttp = $true
     $serviceConfig.Update()
     IISreset
}
```

If you run this script more than once, you will see an error message indicating that the **HPRecordsManagerTrust** already exists.

Should this situation arise, it will be necessary to delete the **HPRecordsManagerTrust**, and the corresponding **Trusted Security Token Issuer** that was created.

To do this, carry out the following steps:

1. In PowerShell ISE (As Administrator) run the following command:

   ```
   Remove-SPTrustedRootAuthority -Identity "HPRecordsManagerTrust"
   ```

2. Now identify the RegisteredIssuerName for the HPE Content Manager High Trust App, by running the following command:

   ```
   Get-SPTrustedSecurityTokenIssuer | select Name,RegisteredIssuerName | fl
   ```

3. This will list any Trusted Security Token Issuer registered on the farm, including the HPE Content Manager High Trust App:

   ```
   Name                 : HPE Content Manager High Trust App
   RegisteredIssuerName : 85298320-b8a1-4ca6-9057-6407fea6fe49@ab9d84e2-0d92-
   4e4e-8b36-40bbc4004a7e
   ```

4. Copy the **RegisteredIssuerName** value to the clipboard, and then run the following command, inserting the value you just copied:

   ```
   Get-SPTrustedSecurityTokenIssuer | ?{$_.RegisteredIssuerName -eq
   "<RegisteredIssuerName value goes here>"} | Remove-
   SPTrustedSecurityTokenIssuer
   ```

5. For example, to remove the HPE Content Manager High Trust App listed above, you would run the following command:

   ```
   Get-SPTrustedSecurityTokenIssuer | ?{$_.RegisteredIssuerName -eq "85298320-
   b8a1-4ca6-9057-6407fea6fe49@ab9d84e2-0d92-4e4e-8b36-40bbc4004a7e"} |
   Remove-SPTrustedSecurityTokenIssuer
   ```

You can then rerun the token issuer script again to reissue the issuer ID for the HPRecordsManagerTrust.

> *If you do run the script a second time in this scenario, the issuer ID will change so it will be necessary for you to update any record you have of it.*

Should you at any stage forget the issuer ID, you can run the following script to list out the issuer IDs in your system:

```
Get-SPTrustedSecurityTokenIssuer | select Name,RegisteredIssuerName | fl
```

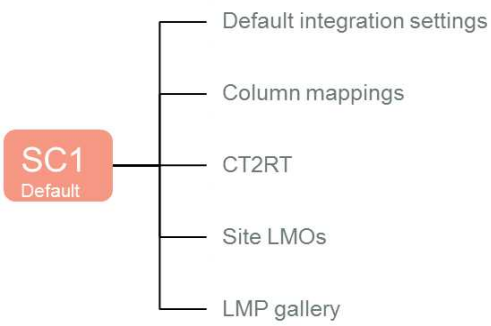
This will list all trusts configured in your SharePoint farm. Locate the entry with the name "HPE Content Manager High Trust App". The "RegisteredIssuerName" contains a string with the "@" symbol half way along. The characters before the "@" symbol are the issuer ID.

2.5.4 Identify the default site collection

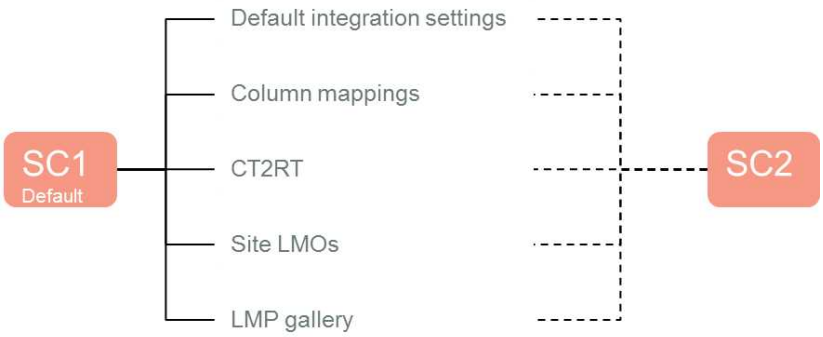
Overview

During configuration, you will be required to identify a site collection that will act as the default site collection. The default site collection is used as the provider of default configuration values for other site collections.

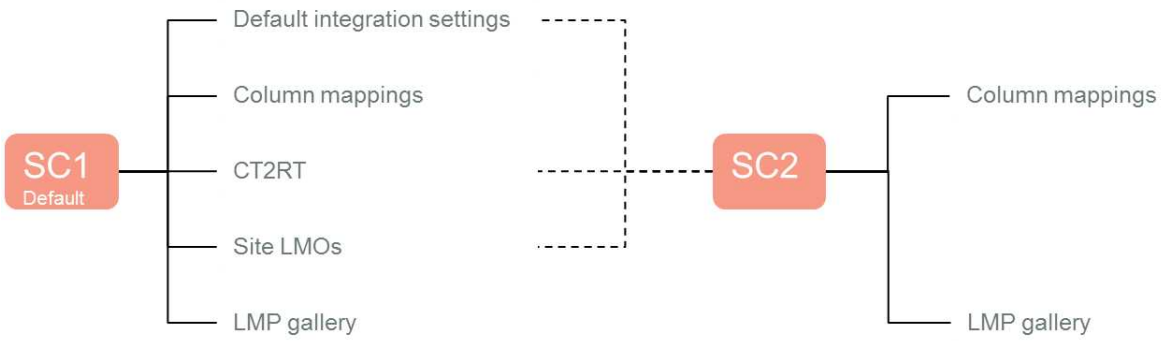
On the default site collection you can define the configuration settings that will be used by that site collection.



Other site collections can then elect to use the configuration that is specified on the default site collection.



It is even possible to indicate that a site collection will only use some of the default site collection values, and provide values itself for other configuration.



Considerations for choosing the default site collection

If you are using a site collection as a content type hub, this site collection would make a good candidate for the default site collection as it is already used to provide information to other site collections in your farm. It therefore may be logical to extend it to provide the Content Manager default configuration as well.

2.6 Preparing SQL Server

As described in the App configuration storage section of this document, it is necessary to provide access to a SQL Server instance. This SQL Server instance will be used to host the app configuration database.

2.6.1 Supported environments

The SQL server instance must be one of the following versions:

- SQL Server 2012
- SQL Server 2012 R2
- SQL Server 2014

Express editions of these versions of SQL Server are suitable.

2.7 Identify and configure accounts

Overview

There are several key accounts that are used by the product. These accounts must have specific permissions to the Content Manager Server, to Content Manager datasets and also to SharePoint. This section describes the permissions that these accounts must have.

It is advisable to identify and configure these accounts prior to installation and configuration as you will be asked for them during that process.

For instructions how to configure Content Manager location details, see the appendix Configuring the account and permissions for a location.

Installing user

The installing user is the account that will be used to:

- Install the Content Manager for SharePoint MSI
- Configure the app using the configuration tool
- Provision the app in the app catalog
- Add the app to site collections that require it

This user must have the following permissions:

- Have **dbcreator** permissions in the SQL Server instance in use
- Contribute permissions to the Apps for SharePoint list in the corporate app catalog
- Site collection administrator for the site collection that will be used as the default site collection
- A term store administrator for the managed metadata service used by the default site collection.
- Have a location in Content Manager with a user type of **Records Co-ordinator** or higher.
- Read access (or higher) to the location that the high trust certificate is installed on every server in the Content Manager farm

Job processing service account

The job processing service account is used to run the "Content Manager SharePoint Service" Windows service. During installation you will be asked for the account to use for this service. You will need to provide an account that has the following specific permissions:

- Have a location in Content Manager with a user type of **Administrator** and a security level and security caveats at least as high as any records that will be managed. The preference is to grant "<Highest>" security.
- Annotated in Content Manager Enterprise Studio that it can impersonate other accounts (see the appendix "Indicating that an account can impersonate" in the Content Manager tasks section)
- Granted the "log on as a service" right on the machine (the installation process will grant this permission for you)
- Member of the "Performance Monitor Users" group on every server in the Content Manager farm (this is not required in Windows Azure environments)

- A site collection administrator on all site collections that will be managed (required for necessary document access)
- Read access (or higher) to the location that the high trust certificate is installed on every server in the Content Manager farm

Application pool account

An account is required to be used as the identity of the application pool that will run the IIS site created by the installer. During installation you will be asked for the account to use for the application pool. You will need to provide an account that has the following specific permissions:

- Have a location in Content Manager with a user type of **Administrator** and a security level and security caveats at least as high as any records that will be managed. The preference is to grant "<Highest>" security.
- Annotated in Content Manager Enterprise Studio that it can impersonate other accounts (see the appendix "Indicating that an account can impersonate" in the Content Manager tasks section)
- Be a member of the local **IIS_USRS** group on every server in the Content Manager farm.
- Read and write permission to the installation directory (the installation process will grant this permission for you)
- Be a member of the **Performance Monitor Users** group on every server in the Content Manager farm (this is not required in Windows Azure environments)
- Read access (or higher) to the location that the high trust certificate is installed on every server in the Content Manager farm

Note that whilst it is preferable to have separate accounts for the application pool and job processing service, it is acceptable to make them the same account.

Document viewers group/user

When documents that have been managed are viewed from Content Manager, the document is retrieved from SharePoint in order to display to the user. This document retrieval is performed by the **Content Manager Workgroup Service** and is therefore performed as the identity that is used by that service.

During configuration you will be asked to specify a group or user who is permitted to perform this document retrieval. This is known as the document viewers group or user.

Ensure that this group has the following members:

- The identity used to run the "Content Manager Workgroup" windows service (see the appendix "Identifying the account that a Windows service is running as")

Job queue administrators

Tasks and requests are performed by jobs in the job queue. Any user can view their own jobs but only members of the job administrators group can view all jobs from all users.

During configuration you will be asked to specify a group that contains the users who are considered job administrators. You should identify a group that has only those who are required to view all jobs.

Ensure that this group has the following members:

- All users that will need access to see all jobs in the job queue

If an AD group is not suitable for your environment needs, you can specify a list of users who should have this permission instead.

Search administrators group

When a federated search is executed, the result source is configured to attempt the search as a specific user. Although the identity of the request will be presented as this user, it is the interactive user that the search will be performed as.

In order to prevent malicious users attempting to perform searches on behalf of others, the identity of the request must be confirmed as a trusted identity. Trusted identities are indicated by their inclusion in a particular AD group. This group is known as the ***Search Administrators*** group. During configuration you will be asked for the group to use. You should identify an AD group that only has the search identity in it.

Ensure that this group has the following members:

- All users that will be used as the NTLM credentials for a result source that access Content Manager records

The user guide covers in depth the process of creating a result source.

Default search location

There are situations where it is not possible to configure a result source to use a particular NTLM account. In those scenarios, the request will be presented as an anonymous. In this scenario, if a value is specified for ***the Default Search Location***, the search will be performed as this user, regardless of who the interactive user is.

You will be asked during configuration for an account to use. Ensure that this user cannot see any records that are not considered available to all Content Manager users.

This feature is optional and this value can be left blank to render this feature inoperative.

SharePoint\System location

This section only applies if you intend to use the SharePoint Content Organizer feature.

If you plan to use the SharePoint ***Content Organizer*** feature, tasks performed by the content organizer present to Content Manager as a user with the account name: ***SharePoint\System***

A location must exist in Content Manager for this account. This location must:

- Have a user type of **Contributor** or higher (and have correc permissions as described in the Permissions section)
- Have the domain specified as ***SharePoint*** and the account name specified as ***System*** on the profile tab.
- Be allowed to login to Content Manager

2.8 Determining if HTTPS or HTTP should be used

The installation creates an IIS site used by the Content Manager Governance and Compliance app. This contains pages, services and resources used by the app as well as all the components that interact with Content Manager.

This site is initially configured to use the HTTP protocol. This protocol is only considered suitable for testing and proof of concept.

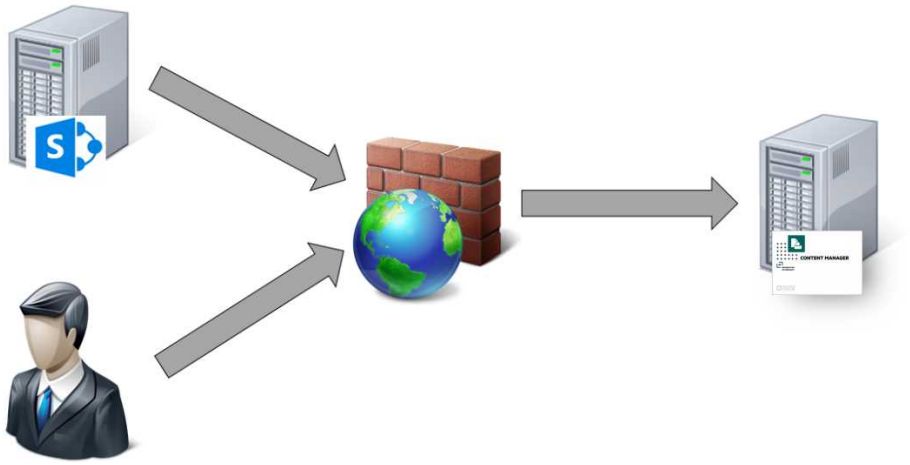
For production installations, it is important that you use the HTTPS protocol on the app service site. For SharePoint Online installations, the only supported protocol is HTTPS.

There are additional configuration steps required to enable HTTPS. You should determine if HTTPS will be required prior to beginning the configuration process.

2.9 Selecting a suitable http port

During installation, you will be asked to specify a port that the app service will be installed on. This port must:

- Not already be in use by IIS (see appendix Determining ports in use)
- Not be in use by another application (see appendix Determining ports in use)
- Be open on any firewalls that are between the SharePoint farm and the Content Manager farm
- Be open on any firewalls that are between end users and the Content Manager farm.



If you intend to use HTTPS, then the importance of this port is reduced as part of configuration, the site will be switched to port 443. You will still be required to enter a port during installation however.

3 Installation

3.1 Installing the Content Manager components

3.1.1 Overview

The installation of the Content Manager components is required on each workgroup server in the Content Manager farm. For each workgroup server that has been identified, you must ensure that the necessary preparation described earlier in this document has been performed, prior to installing the product MSI.

If you have not followed the steps in the preparation chapter, installation will not be successful.

3.1.2 Installation

The components that are required to be installed on a Content Manager workgroup server can be installed using the "Content Manager_SharePoint2013AppIntegration_x64.msi" MSI found on the installation media.

It is assumed that the use of an MSI is something that is familiar to the reader. Based on this assumption, this document deliberately does not document each step in the installation process.

Run the MSI, during the installation process, you will be asked to provide the following information:

Access site details

The details of the IIS web site are required to be entered.

See the Selecting a suitable http port section of this document for the details of this value. Enter a numeric value only that represents the port that has been selected.

See the Application pool account section of this document for details of this account. Enter the selected account in the format domain\account e.g. *acmecorp\AppPool*

Job processing service identify

The details of the job processing identity are required to be entered during installation.

See the Job processing service account section of this document for details of this account. Enter the selected account in the format domain\account e.g. *acmecorp\JobService*

3.1.3 Configuring the use of HTTPS

Overview

If you have elected to use the HTTPS protocol, there are several manual steps that you must perform following the installation process to convert the app service site to use this protocol.

See the Determining if https or http should be used section for guidance as to how to make this selection.

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.

Enable HTTPS for this site. If you are unfamiliar with how to do this, see the Enabling HTTPS for a site appendix.

> *Note that using a self-signed certificate will not be suitable for https on the Content Manager SharePoint Server website. You will need to use an existing SSL certificate, or obtain one through a certificate request in IIS.*

Disable HTTP for this site. If you are unfamiliar with how to do this, see the Disabling http for a site appendix.

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)
2. Locate all the following nodes (there should be 3):

   ```
   <security mode=”TransportCredentialOnly”>
   ```

3. Modify all nodes to read:

   ```
   <security mode=”Transport”>
   ```

4. Now locate the node:

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

5. Modify the node to read:

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

6. Save the changes to the web.config file.

Testing that HTTPS is correctly configured

If HTTPS is configured correctly, it should be possible to successfully browse to a number of key URLs (replace "YourURL" with the machine name of the Content Manager server or the load balanced URL used for accessing the Content Manager farm.

- https://YourURL/Pages/DialogLoader.html (will display the text "working on it")
- https://YourURL/EventReceivers/remoteevents.svc (displays a default service description page)
- https://YourURL/SecureServices/DataStoreService.svc (displays a default service description page)

3.1.4 Additional steps for Windows Azure

If installing on a server hosted in Windows Azure, the following additional steps are required.

These steps are applicable if using a Windows Azure Managed Cache or a Redis cache.

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 (dependant on whether using managed or Redis):
   a. <CacheType>WindowsAzureManaged</CacheType>
   b. <CacheType>WindowsAzureRedis</CacheType>
5. Save the file.

Note that in some cases it has been found that after publishing using the configuration tool that this value reverts to AppFabric. If this happens, you will be able to access the app start page but no other pages. You may also see errors in the SharePointIntegration.log file stating **Failed to access app fabric cache.**

If this occurs, repeat the steps above to correct the file.

Replace AppFabric assemblies

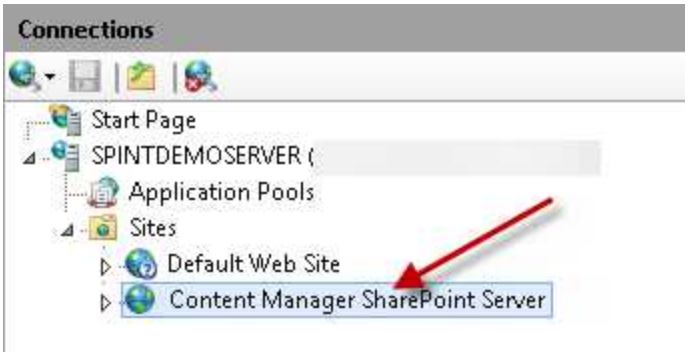
1. Stop the Windows service: ***Content Manager SharePoint Service***
2. In the installation directory, locate the folder: ***WindowsAzure***
3. Copy all files that are in this directory
4. In the installation directory, locate the folder: ***bin***
5. Paste the copied assemblies into this directory, overwriting any existing assemblies already in that directory.
6. Start the Windows service after completion of Publish: ***Content Manager SharePoint Service***

Note that if you mistakenly perform this step and need to revert to the app fabric assemblies, they are available in the AppFabric folder in the installation directory.

3.1.5 Additional steps for use with SharePoint Online

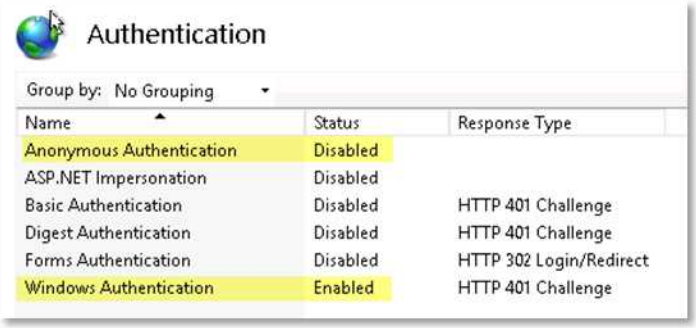
Authentication used by SharePoint Online differs to the authentication used by a high trust app used with an on premise instance of SharePoint. The installation process assumes that an on premise instance of SharePoint will be used, so IIS authentication must be re-configured. Carry out the following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

1. Open **IIS Manager** and select the site: **Content Manager SharePoint Server**

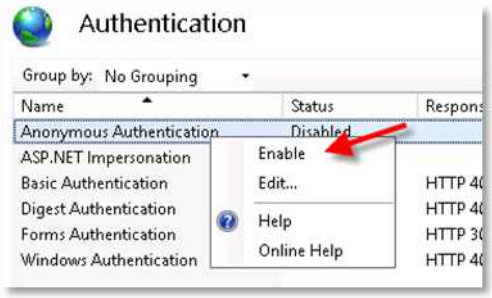


2. In the right hand pane using the “Features view” locate and double click the “Authentication” icon

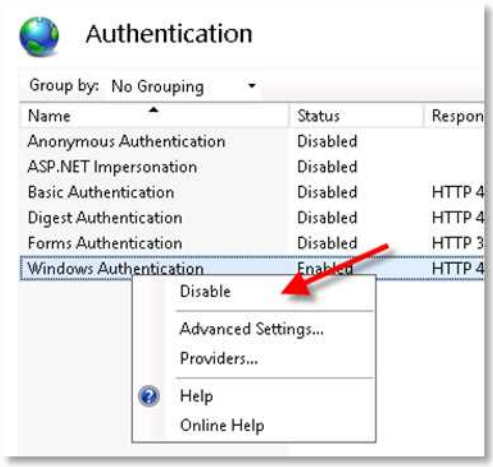
3. Authentication will initially show “Anonymous Authentication” as “Disabled” and “Windows Authentication” as “Enabled”



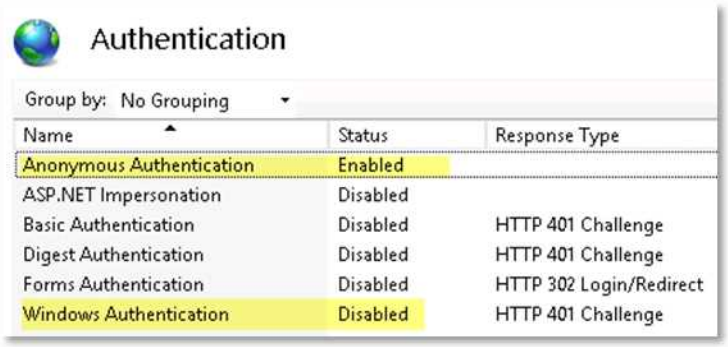
4. Right click on “Anonymous Authentication” and select “Enable”



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



6. The authentication should now be set as follows



Note that authentication is still performed by the app before granting access to resources.

3.2 Installing the auditing components

In order to capture document view events through SharePoint, a separate SharePoint solution must be installed on the SharePoint farm. This section describes how to install this solution.

It is not possible to install the auditing components in Office 365.

3.2.1 Adding the solution to the farm solutions

The solution must be added to the collection of solutions available on the farm before it can be used.

Locate the solution file on the machine where the Content Manager Governance and Compliance app installation package was run in the earlier step. The solution file can be found at:

```
[Program Files]\Micro Focus\Content Manager\Content Manager SharePoint
Integration\Audit\ HPEContentManagerGovernanceAndCompliance.wsp
```

Copy this file to a web server in your SharePoint farm.

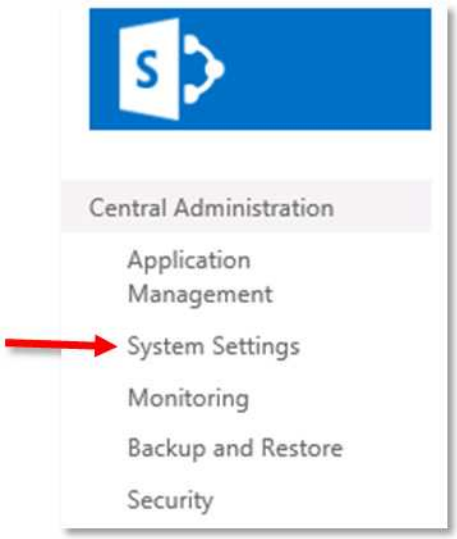
On the web server, open an instance of SharePoint Management Shell as administrator and execute the following command replacing [source] with the full path to the copied wsp file. This script will add the solution to the solution store.

```
Add-SPSolution -LiteralPath "[Source]\HPEContentManagerGovernanceAndCompliance.wsp"
```

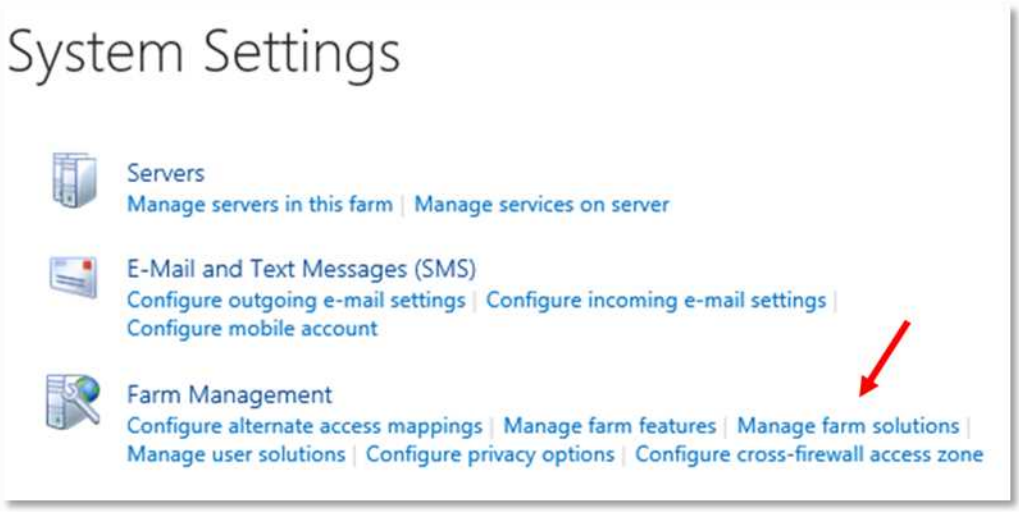
3.2.2 Deploying the solution

The solution must be deployed to any web applications that intend to use it.

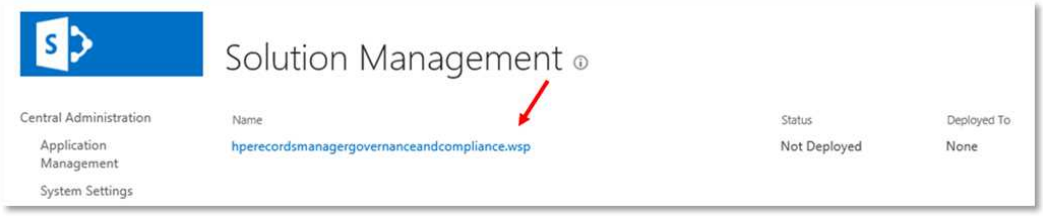
Browse to the ***Central Administration*** site for the SharePoint farm. Click on the ***System Settings*** link.



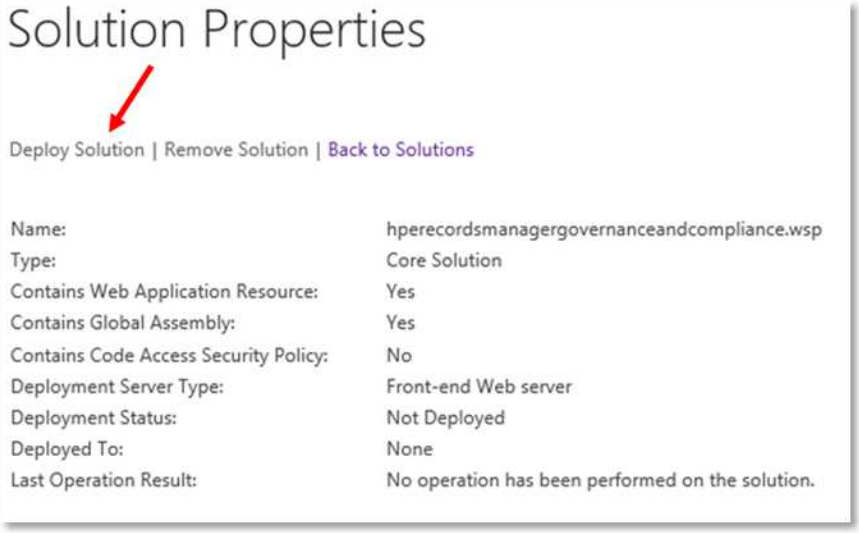
Click the ***Manage farm solutions*** link



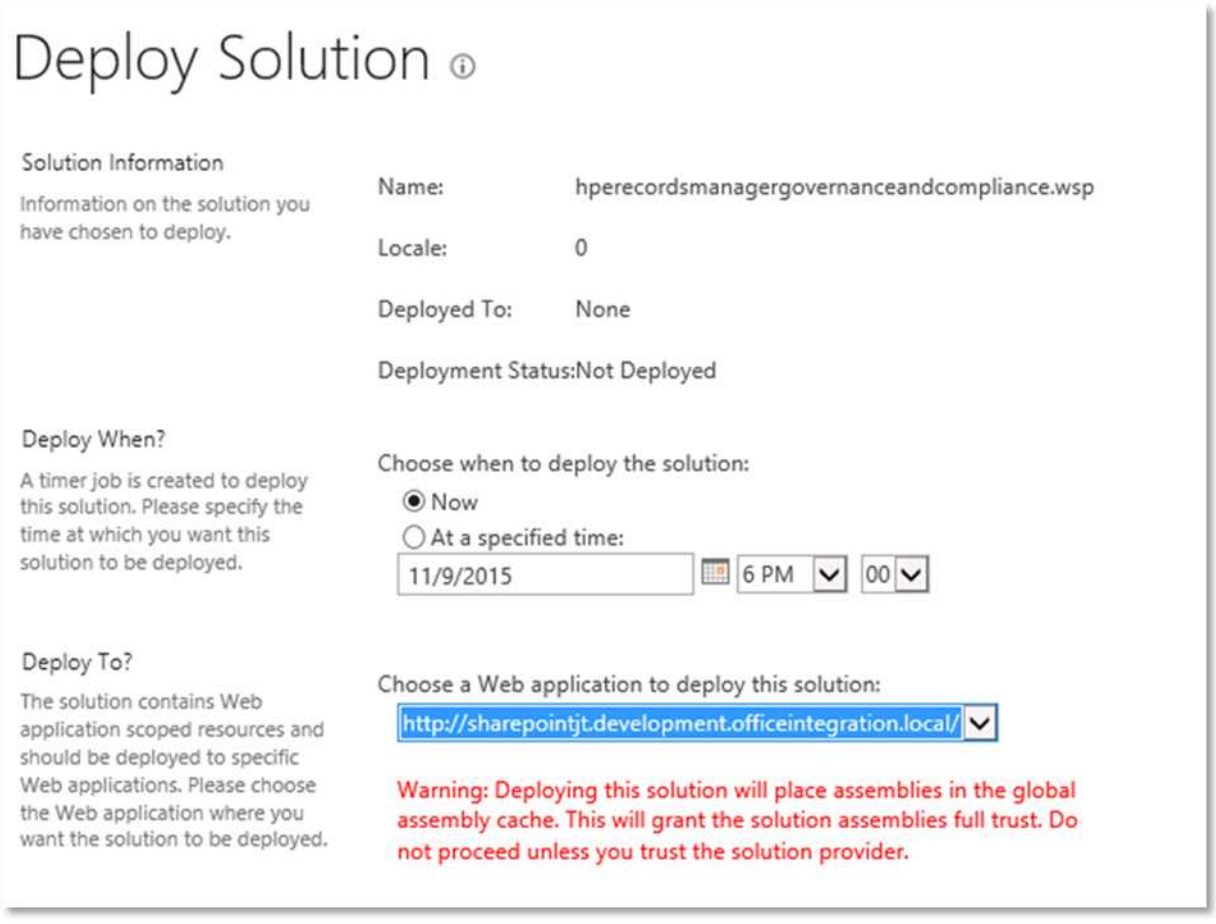
The HPEContentManagerGovernanceAndCompliance.wsp solution should appear in the list of solutions. Click on this solution.



Select the Deploy Solution link



Select the web application to deploy to and click OK to begin the deployment



Confirm that the solution has been deployed correctly.


Solution Management
Name
Status
hperecordsmanagergovernanceandcompliance.wsp
Deployed

4 Configuration

4.1 Overview of the configuration process

Following installation of the product, there are various configuration options that must be set before SharePoint content can be managed. The steps in this section take the environment from one where the product is simply installed, to one where the basic configuration of the environment is complete.

There are two ways of configuring SharePoint Integration:

- **Using the Configuration Wizard** - The Configuration Wizard will guide the user through the various configuration steps required to correctly configure the SharePoint Integration. *The Configuration Wizard is not supported for upgrades.*
- **Using the Configuration Tool** - The Configuration Tool allows modification to existing configuration data and should be used once the Wizard has been used to create the initial configuration

To select a configuration option log into the machine as the installing user, right click this tool and select **Run as Administrator**.

*The associated **CM9.3_ SharePointIntegrationUserGuide.pdf** for this product provides information on more advanced configuration options.*

CAUTION: The use of system accounts to configure the SharePoint Configuration Wizard is prohibited, as the tool cannot override the admin/system accounts. Use the job account to login into the system, and then run the SharePoint Configuration Tool as run an administrator. Note that, this restriction is applicable only when running the Configuration Wizard only. When running the Configuration Tool, an admin/system account can be used.

When configuring using the Wizard there is a specific order that configuration must be performed. This can be summarized as:

- Establish the Content Manager farm by
  a. creating and connecting to an app configuration database
  b. specifying the URL of the Content Manager farm
- Specify caching options to use
- Create the app
- Add the app to the app catalog
- Add the app to the default site collection
- Specify the default site collection
- Specify the workgroup servers in the Content Manager farm
- Configure permission groups

- Configure email settings
- Publish the settings to all servers in the the Content Manager farm
- Create SharePoint term sets
- Specifying the default integration settings
- Create Content Manager columns in SharePoint if required

This section describes how to perform these configuration steps.

> *Note that a number of steps require use of the configuration tool. Keep the configuration tool open between steps unless it is explicitly mentioned that you can close the tool.*

4.2 Establish the Content Manager farm

4.2.1 Open the Content Manager SharePoint Configuration tool

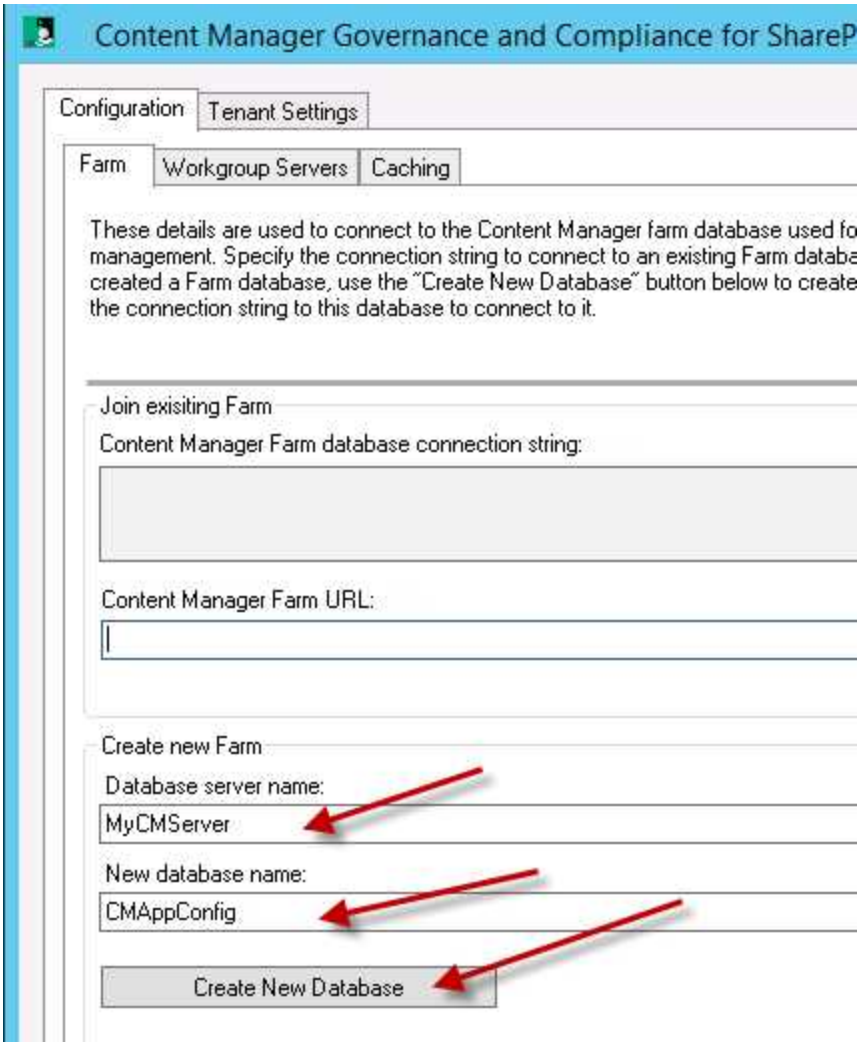
The Content Manager SharePoint Configuration tool (referred to as the configuration tool) is used to perform core configuration for Content Manager for SharePoint. This tool can be accessed from the desktop shortcut installed by the MSI, or from the Windows start menu.

Logged into the machine as the installing user, right click this tool and select **Run as Administrator**.

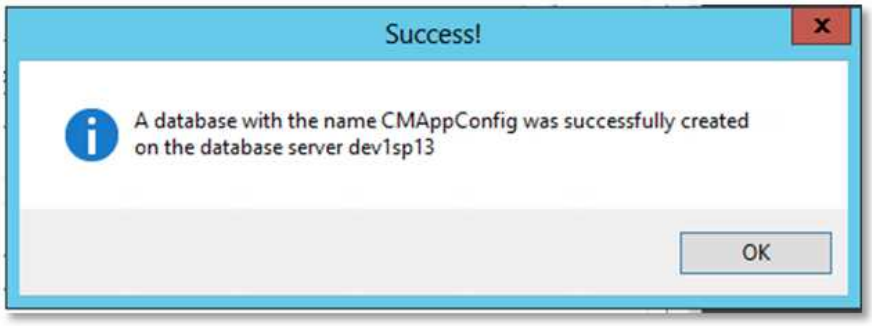
4.2.2 Creating a new app configuration database

For a new Content Manager farm, you will need to create an app configuration database. If not already selected, choose the **Farm** tab on the configuration tool.

Locate the **Create new farm** group. Enter the name of the SQL Server instance to be used, and provide a name for the database that will be created.



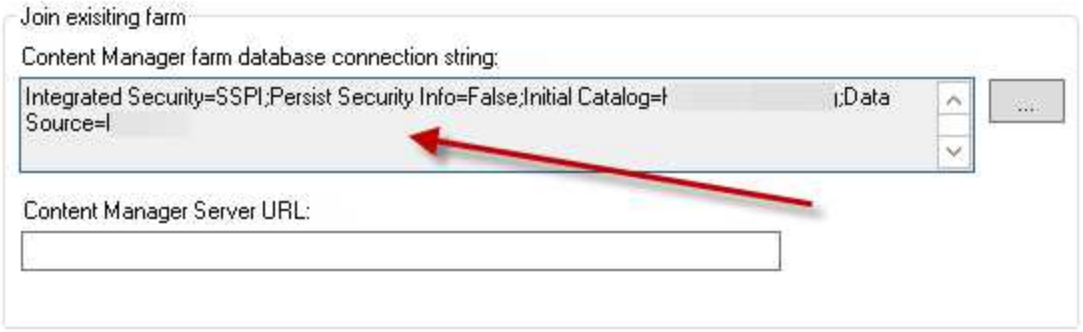
Click **Create New Database** to begin the creation of the database. A success message indicates that the database was created.



4.2.3 Connecting to an existing configuration database

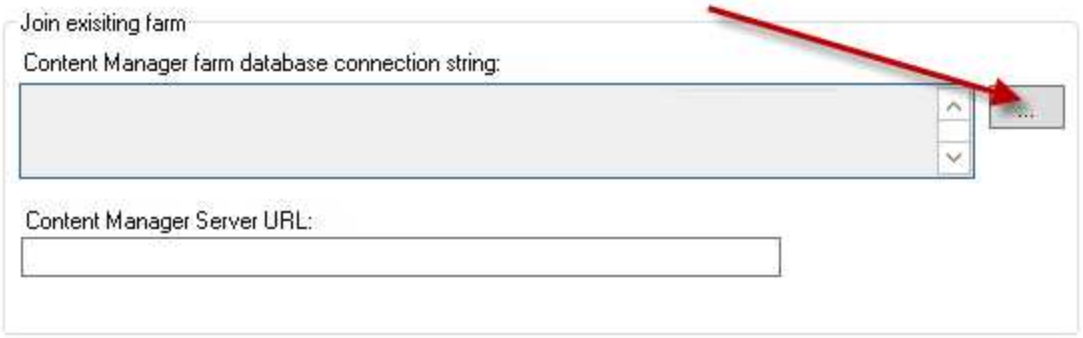
Once an Content Manager Farm configuration database exists, it is necessary to connect to that database. In the J**oin existing farm** group, the **Content Manager farm database connection string** allows specifying the connection string to use to connect to the correct database.

If you created a new database using the steps in the previous section, the connection string will have been automatically populated.



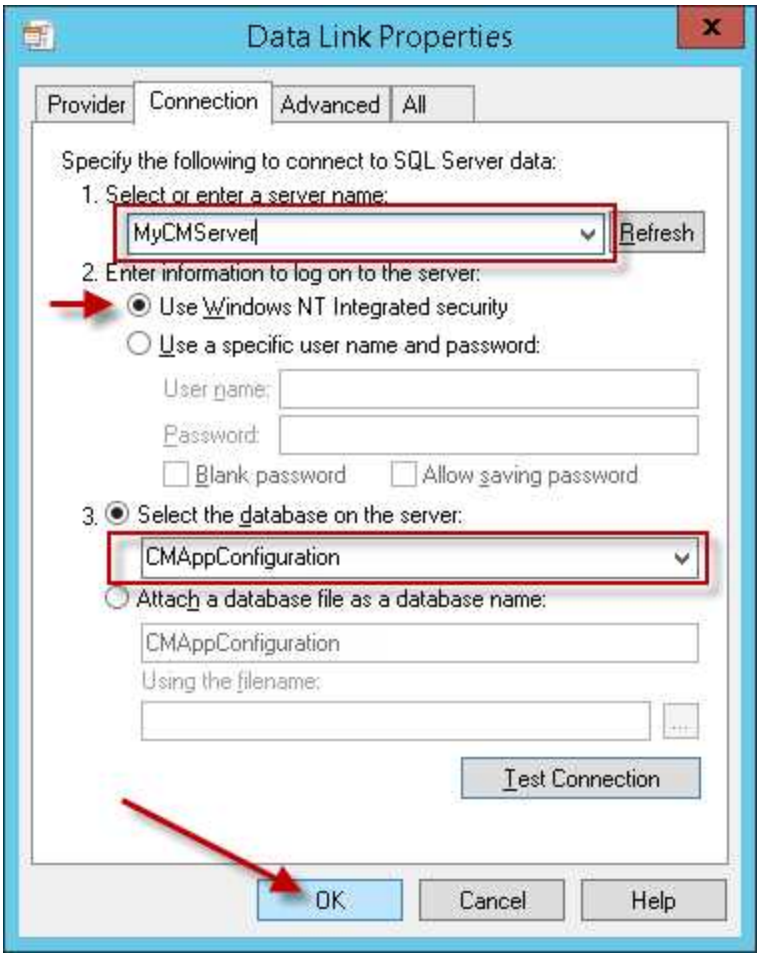
If you are connecting to a database that has been established by another means, then it is necessary to construct the connection string.

Click the ellipse button next to the **Content Manager farm database connection string** text box



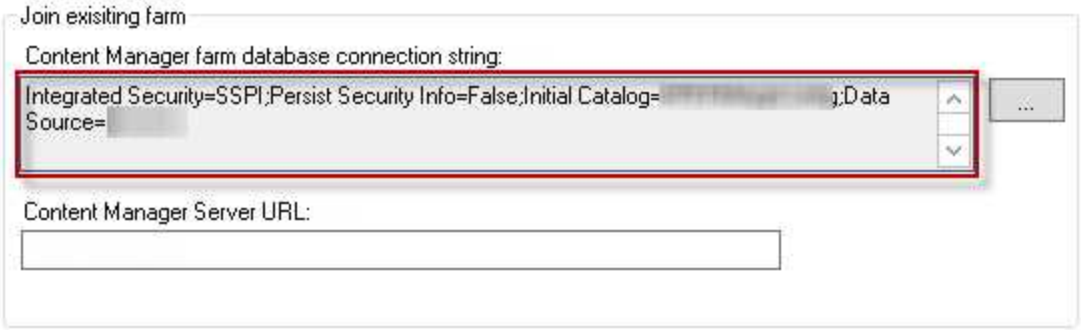
Using the **Data Link Properties** dialog that shows:

- Specify the name of the SQL Server instance that the database resides on
- Choose **Use Windows NT Integrated security**
- Select the database from the **Select the database on the server** dropdown



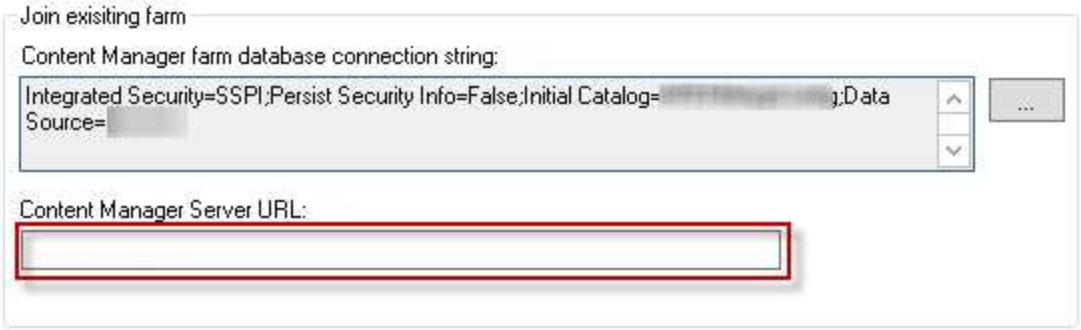
Warning: the app configuration database is not the database that Content Manager uses for record storage. Do not attempt to connect to the Content Manager records database in this step.

- Click **OK** to construct the connection string



4.2.4 Specifying the Content Manager farm URL

Under the connection string details is a text box that allows the entry of the URL to use when interacting with the Content Manager farm.



If your farm has only a single server, this is the URL of that server. In the case where HTTP is being used, the URL will be:

```
http://MachineName:port
```

Where "MachineName" is the name of the Content Manager server and "port" is the port that you selected during installation. For example, if the machine name was "CM1" and you elected to use port 200, the URL would be:

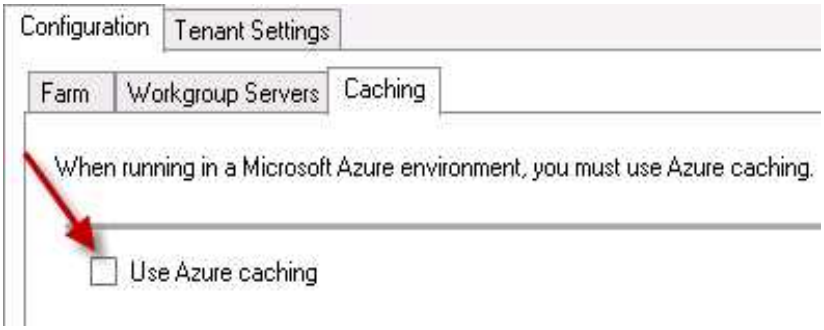
```
http://CM1:200
```

If you Content Manager farm contains multiple servers though, this URL must be the load balanced URL for the Content Manager farm.

4.3 Set caching options

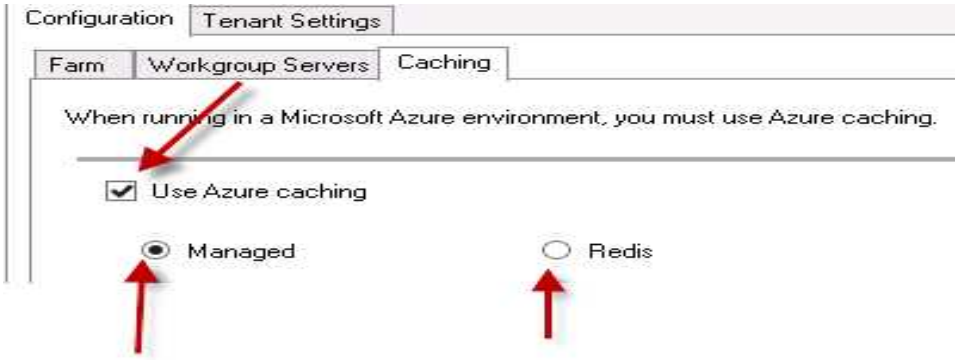
If your Content Manager servers are hosted in a Windows Azure environment, it is necessary to use a different caching mechanism. The "Caching" tab of the configuration tool allows specifying the cache to use.

If the servers are not on Windows Azure, ensure that ***Use Azure caching*** is not checked:

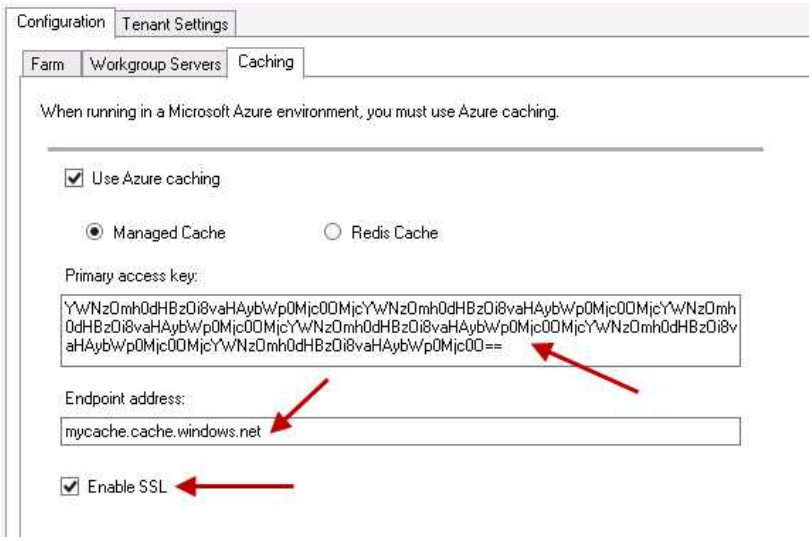


If Windows Azure is used, ensure that ***Use Azure caching*** is checked.

Select the type of Azure cache that is being used, ***Managed*** or ***Redis***.



Enter the details of the Azure cache into the Primary access key and Endpoint address fields.



If the cache is configured so that access if only via SSL, then you must also check the ***Enable SSL*** check box. To determine if this value is required see Determining if the Azure cache is configured to use SSL

4.4 Adding the app to SharePoint

4.4.1 Register the app in SharePoint

Before uploading an app to the corporate app catalog, it must be registered with SharePoint first. This process provides an “App ID” that will be used later in the configuration process.

Registration is performed using the SharePoint “appregnew.aspx” page. To access this page, navigate to the following URL where [site collection URL] is the full URL to the root of your default site collection:

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

For example, if the site collection URL was http://SharePoint, then the URL of the appregnew page would be:

```
http://SharePoint/_layouts/15/appregnew.aspx
```

On premise SharePoint

This section only applies to on premise SharePoint installations

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

Take a copy of the generated **App Id**, as this will be required in a later step.

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

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
```

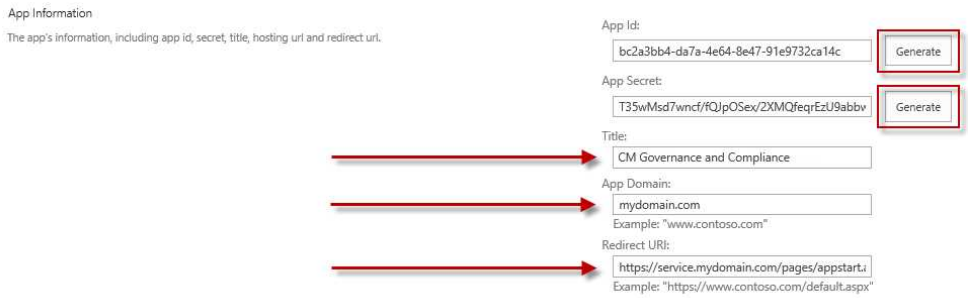
For example, if the Content Manager farm URL is:

```
https://service.mydomain.com
```

Then the full URL to specify in the Redirect URL will be :

https://service.mydomain.com/pages/appstart.aspx

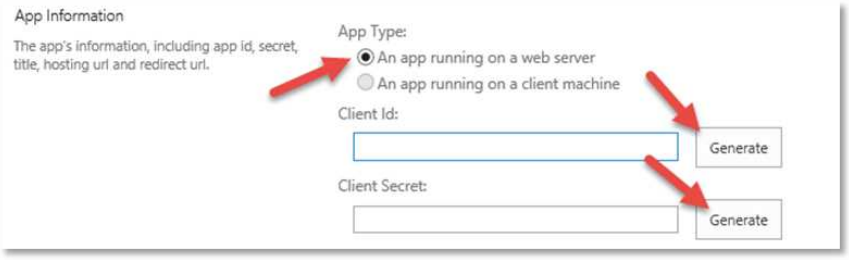
Entering these details will register the app in your environment.



SharePoint Online

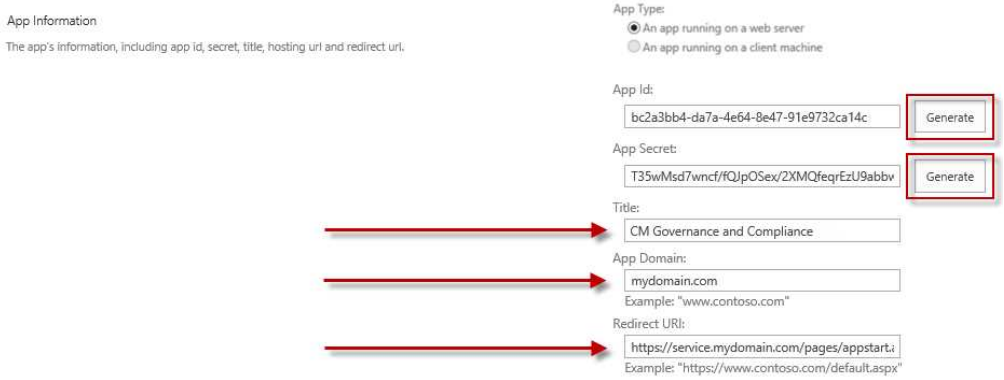
This section only applies to SharePoint Online

Using the appregnew page, specify and **App Type** of **An app running on a web server**. Generate a **Client Id** and **Client Secret** by clicking on the **Generate** buttons.



Take a copy of both the **Client Id** and **Client Secret** generated, as these will be required in a later step.

Specify ***Content Manager Governance and Compliance*** for the title. Specify your app domain i.e. the domain that the app will be used in and click Create. This will register the app in your environment.



4.4.2 Configure a Tenant

A tenant is a logical group of site collections that share the same configuration. In an on premise SharePoint deployment, a tenant represents a SharePoint farm or a SharePoint web application. A tenant represents a SharePoint tenant in SharePoint online. In previous versions, to support these configurations, a separate configuration database was needed. As of 9.1 a single configuration database is used to support these configurations. These changes are introduced as part of SaaS support. Managed Service Providers can now use the configuration tool to support multiple customers

Managed Service Providers (MSPs)

Adding a Tenant

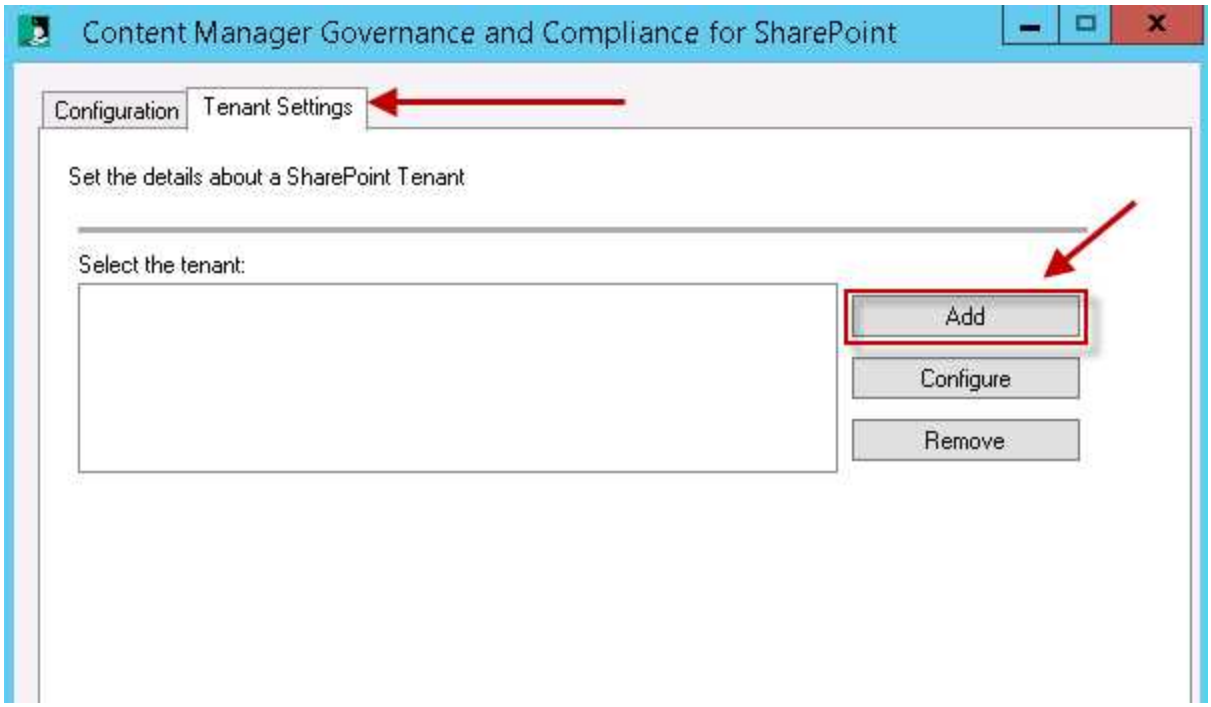
A Tenant can be added by selecting the Add or Configure buttons on the Tenant Settings tab.

The first tab on the Tenant Settings dialog is the "Tenants" tab. You need to save a tenant before you can continue with the rest of the configuration. From the Tenant Settings tab a tenant can be added, configured or removed.

Add - Will add a new Tenant

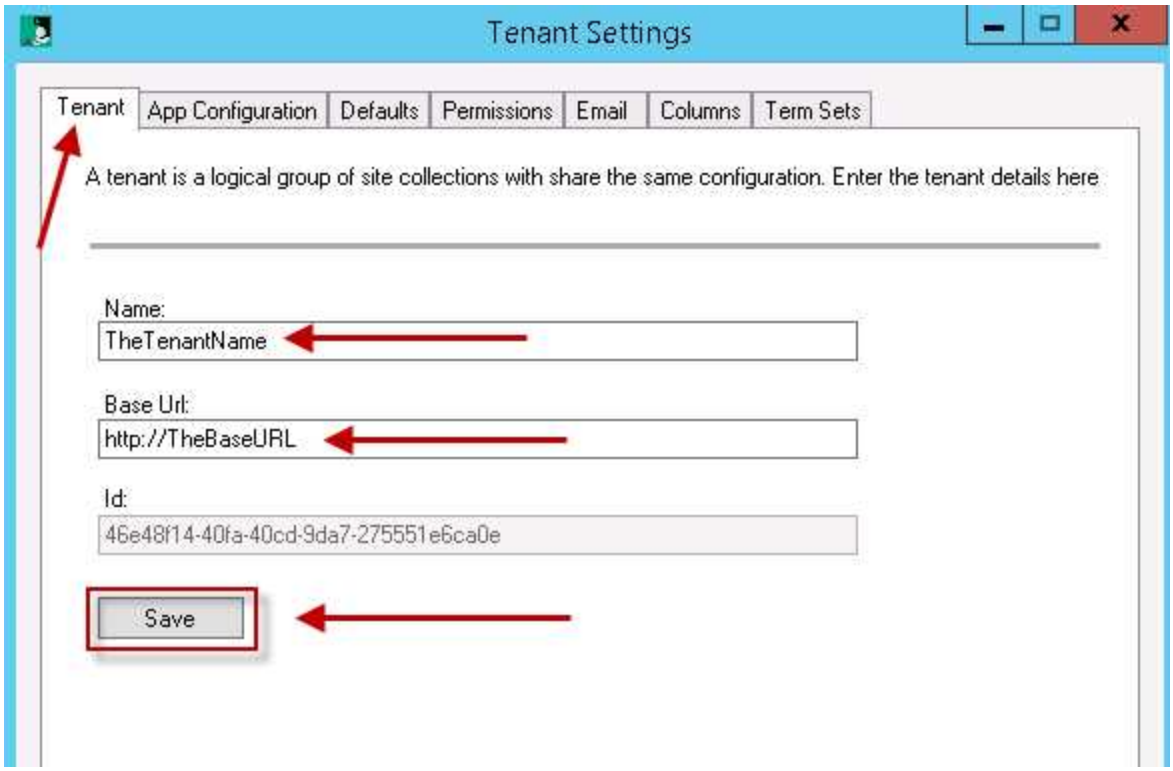
Configure - Select an existing Tenant and then click 'Configure' This will display the tenant for modifying

Remove - Select the existing Tenant and then click remove, this will the Tenant. When a Tenant is removed all the jobs and configuration related to that particular tenant will be removed from the configuration database.



Configuring a Tenant

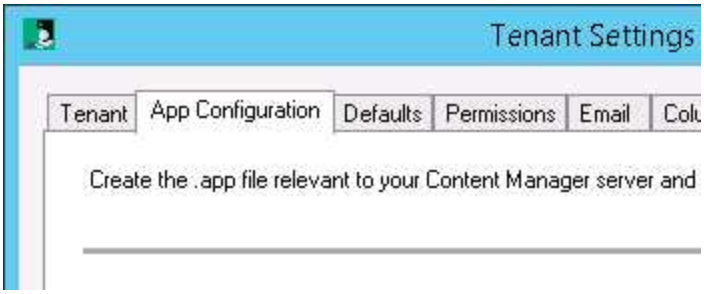
To configure a Tenant select **Add** from the **Tenant Settings** tab. A Tenants settings dialog will display, the Name and base URL need to be populated before the save button is selected. The "Base Url" is your web application url in an on premise scenario, whereas it is your SharePoint online tenant root url in case of SharePoint onlineThe Id is a read only field that is automatically populated with a Tenant ID.



4.4.3 Create the .app file

Before you can add the app to the corporate app store, it is necessary to generate the .app file first. The .app file contains the details of the Content Manager Governance and Compliance app. It must be generated uniquely for each organization as it contains the unique URL of the Content Manager Server URL.

Using the configuration tool, navigate to the **Tenants** tab then select the **App configuration** tab.



Determining the template to use

When the Content Manager Governance and Compliance app is added to a site, the items ribbon will include the following buttons:

- Manage with Content Manager
- Finalize with Content Manager
- Relocate to Content Manager
- Archive to Content Manager
- Management Details
- Security Details

It may be required in your organization to prevent one or more of these buttons being made available to end users. In the next steps, the app file will be generated based on a template. By default, the template used contains all menu items.

Should you require one or more items to not be included, then you must change the template that is being used. Firstly, identify which template is applicable:

Template file name	Included menu items
ContentManagerGovernanceComplianceTemplate.app	Manage with Content Manager Finalize with Content Manager Relocate to Content Manager Archive to Content Manager Management Details Security Details
AppTemplate2.app	Finalize with Content Manager Archive to Content Manager Management Details Security Details
AppTemplate3.app	Archive to Content Manager
AppTemplate4.app	None
AppTemplate5.app	None (including configuration menu options)

All templates except AppTemplate5 include configuration menu options such as RMOs and exposure settings.

If a template other than the first one is required, you must perform the following steps before proceeding.

Navigate to the directory the templates are installed to. This is the Templates directory under the install directory.

Change the name of the ***ContentManagerGovernanceComplianceTemplate.app*** file to ***ContentManagerGovernanceComplianceTemplate1.app***.

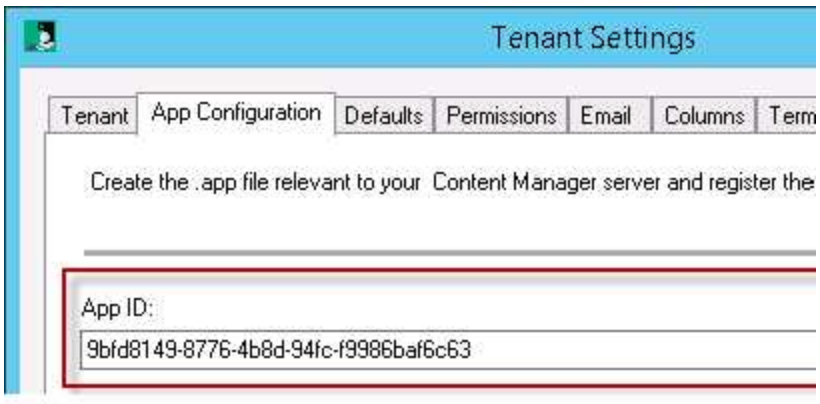
Locate the file that is the template to be used. Copy this template and change the name of it to:

```
ContentManagerGovernanceComplianceTemplate.app
```

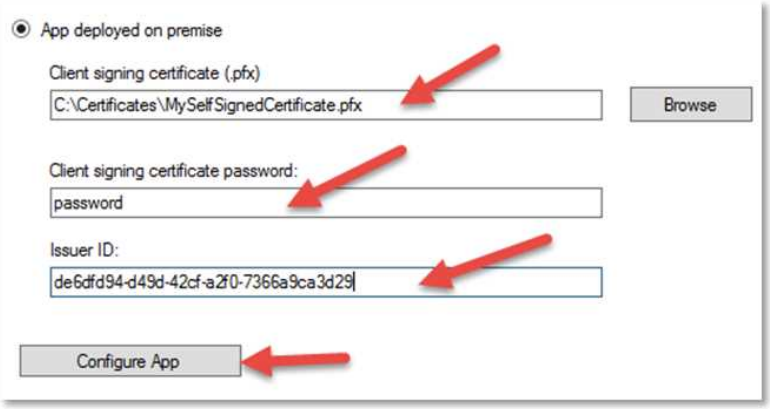
On premise SharePoint

This section only applies to on premise SharePoint

1. Enter the **App ID** captured while registering the app.



2. Select the **App deployed on premise** radio button to enable the on premise controls.
3. Choose the client signing certificate that was used when preparing the Content Manager server for high trust apps.
4. Enter the password used with the selected certificate.
5. Enter the issuer ID obtained while configuring trust for your app.

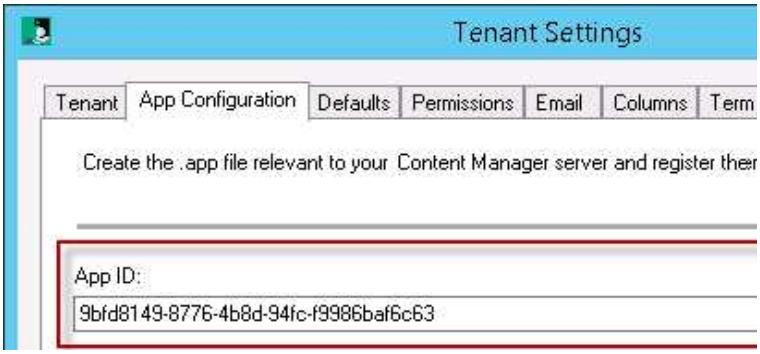


6. Click **Configure App**. If successful you will be presented with a success message.

SharePoint Online

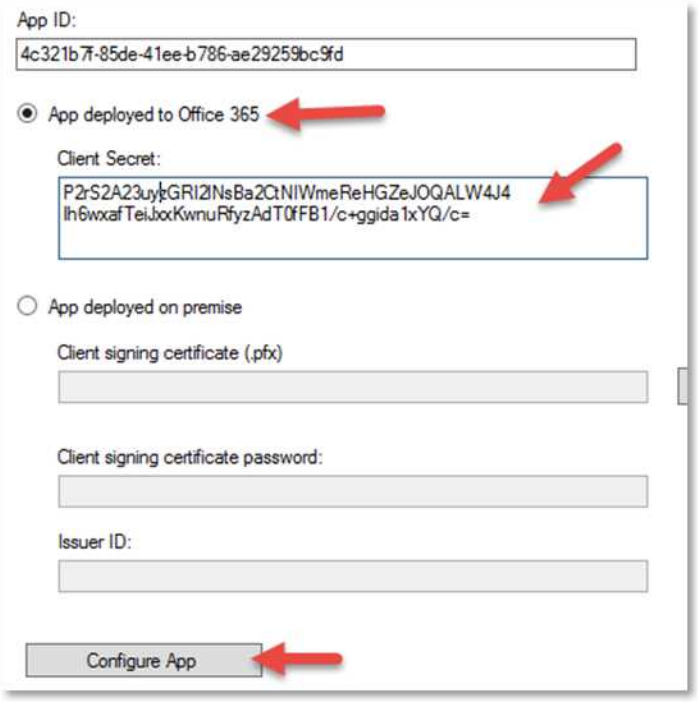
This section only applies to SharePoint Online

Enter the **Client ID** captured while registering the app as the **App ID.**



Select the **App deployed to Office 365** radio button to enable the relevant controls.

Enter the **Client Secret** captured while registering the app.

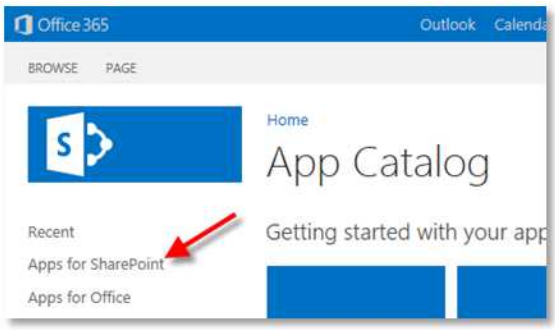


Click **Configure App.** If successful you will be presented with a success message.

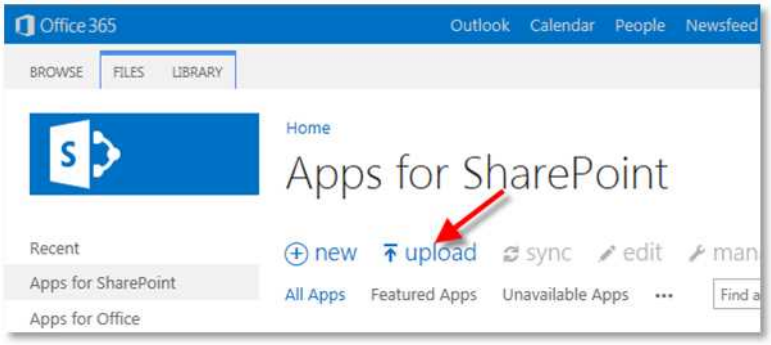
4.4.4 Add the app to the corporate catalog

These steps describe how to add the Content Manager Governance and Compliance app to the corporate app catalog.

- Navigate to the corporate app catalog used by your SharePoint farm.
- Click the “Apps for SharePoint” link



- Click the “upload” link



When prompted, select the app file to upload. 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
```

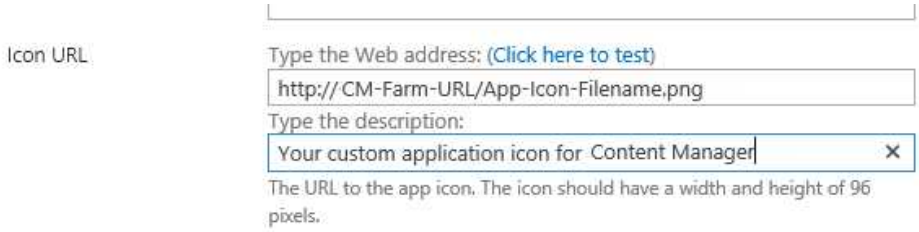
The app file name is:

```
HPRMGovernanceCompliance.app
```

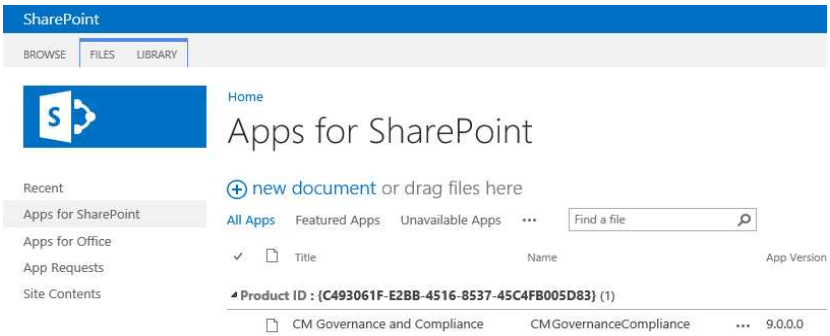
During upload, you will be prompted to enter metadata for the app. Entry of this information is optional, however, entering the URL of the image to display for the app is recommended.

The URL will be:

```
Content Manager Farm URL + "/Images/AppIcon.png"
```



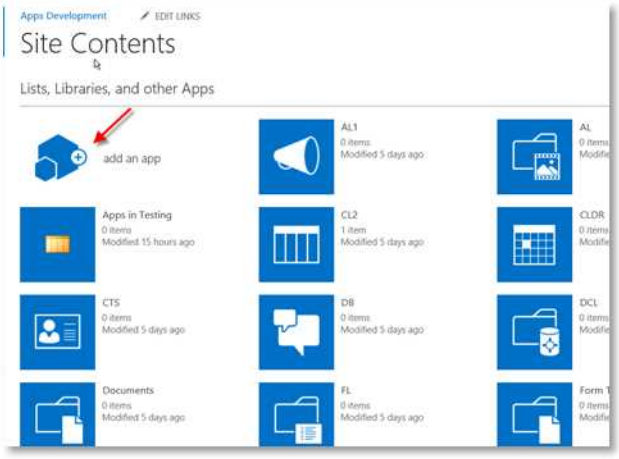
Clicking **Save** on this form will complete the addition of the app into the app catalog.



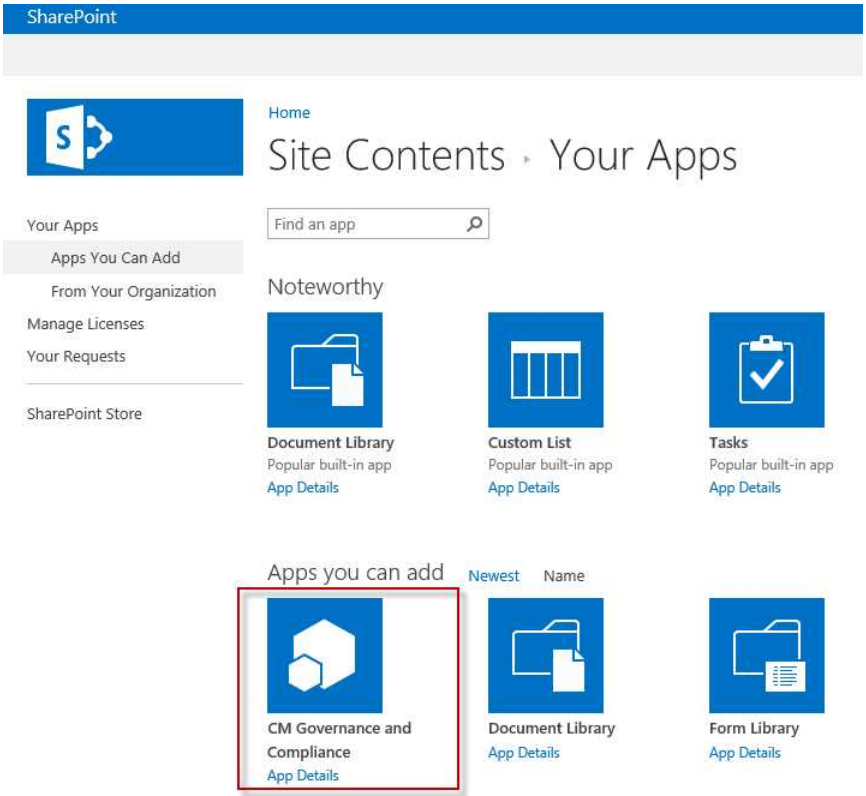
4.4.5 Add the app to the default site collection

The app must be added to the site collection that has been selected as the default site collection.

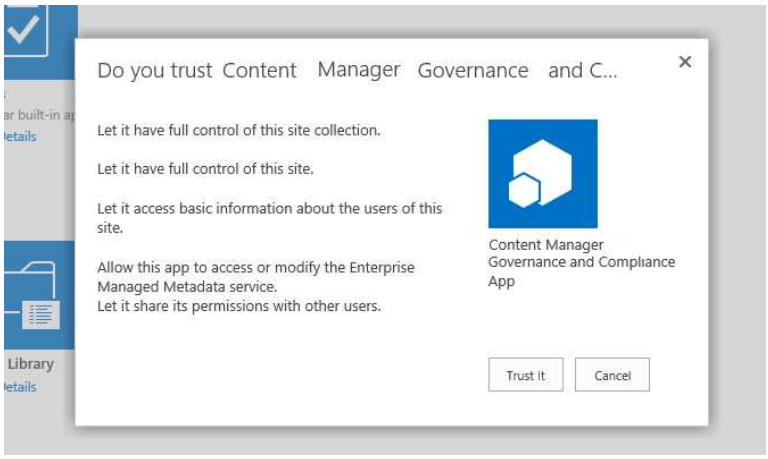
Navigate to the root of the default site collection, then to **Site Contents** for the site collection. On this page choose the **add an app** link.



On the apps page, choose either of the links **Apps You can Add** or **Apps from your Organization** and select the ***Content Manager Governance and Compliance*** app from the list.



Click the **Trust It** button to allow the app to be added.



You will see the app added to the site contents and initially in a state where it is being installed. Once installed it will appear as follows on the site contents page.

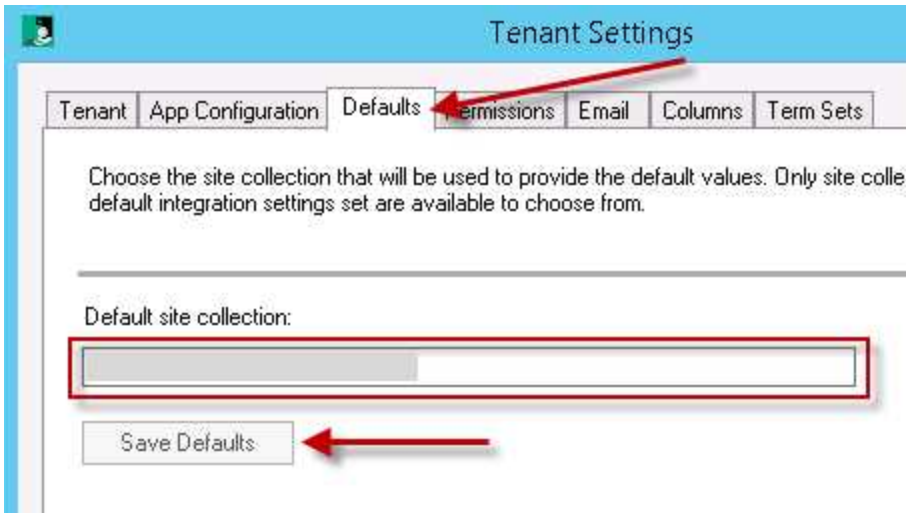
For troubleshooting the addition of apps, see the **troubleshooting app issues** *appendix.*

4.5 Set the default site collection

4.5.1 Setting the default site collection

As part of configuration, the default site collection must be nominated. Using the configuration tool, navigate to the **Tenants Defaults** tab.

Enter the full URL of the root of the default site collection and click the **Save Defaults** button.



During the save, the location that has been entered will be validated. This validation requires:

- The URL is a valid SharePoint site collection URL
- The URL is accessible from the Content Manager server
- The Content Manager Governance and Compliance app has been added to the root site

You must have a valid default site collection saved in order to complete the configuration.

> *If the configuration tool will not allow you to save the default site collection, check that the app has been added to that site collection and that the issuer ID entered on the app configuration tab is correct.*

When saving the defaults, you may receive an error indicating that The App Id entered is not valid.

This error can occur in two known scenarios. The first is that the app ID entered is actually incorrect. You can test that the app ID entered is correct by navigating to:

```
[your site collection] /_layouts/15/appinv.aspx
```

In the “App ID” text box put in what you think the app ID is and use the “lookup” button. If the app ID is valid, it will find your app.

If it doesn't find your app, then the app ID is actually wrong and the error is telling you the right thing.

Another scenario where this will occur is if the configuration tool can't communicate with the site collection. This can occur if SharePoint is using https but you have disabled the use of https when configuring SharePoint 2013 to use certificates and configure trust for your app.

Double check the guidance earlier in this document regarding configuring trust for the app, particularly in regards to:

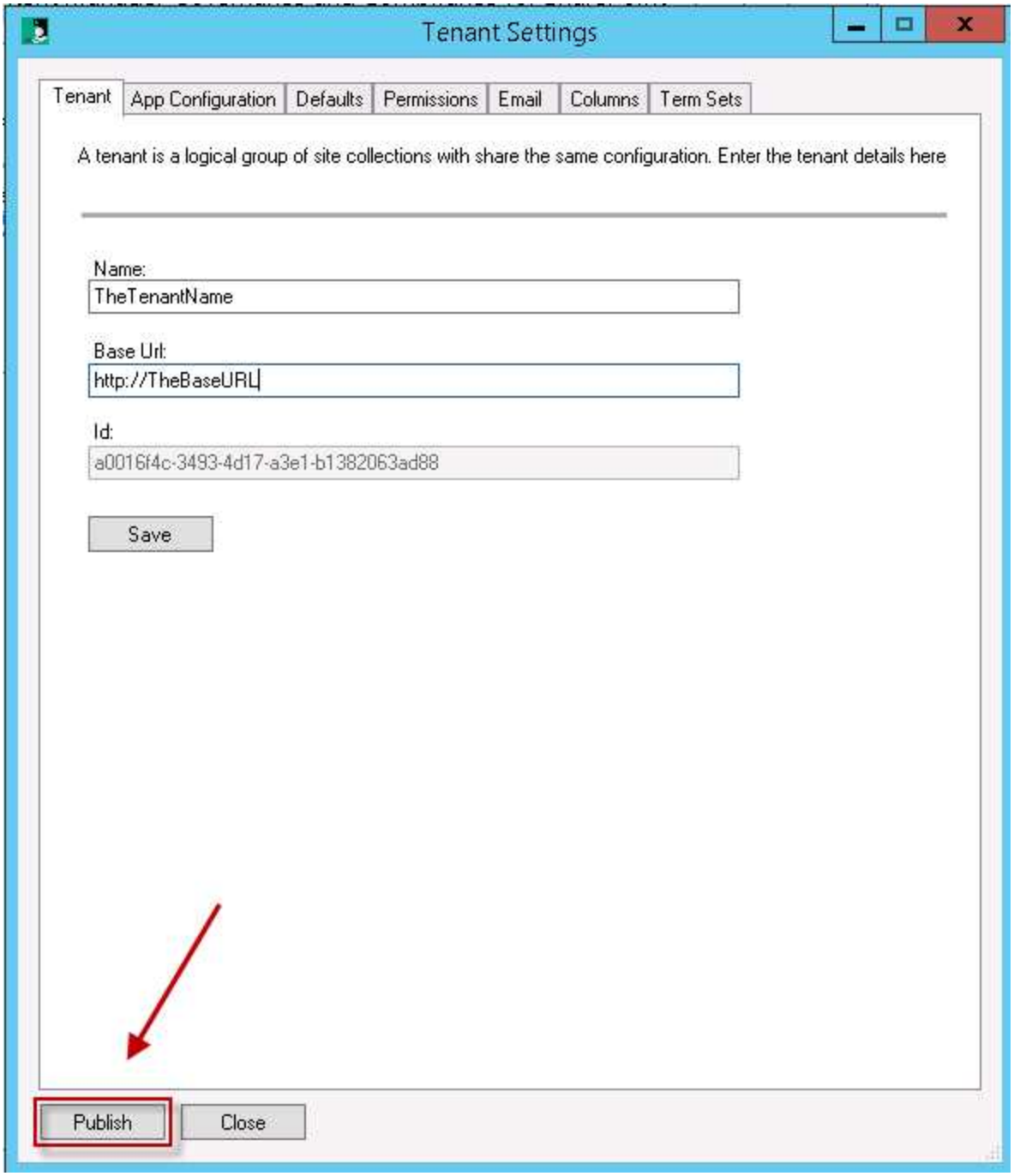
```
$serviceConfig.AllowOAuthOverHttp = $true
```

4.6 Publishing basic settings

4.6.1 Tenants

It is necessary for the Tenant settings be published from within the tenant settings before the rest of the configuration can be continued.

Using the configuration tool, navigate to the**Tenant Settings** tab, select the **Tenant**, click**Configure**and then**Publish**

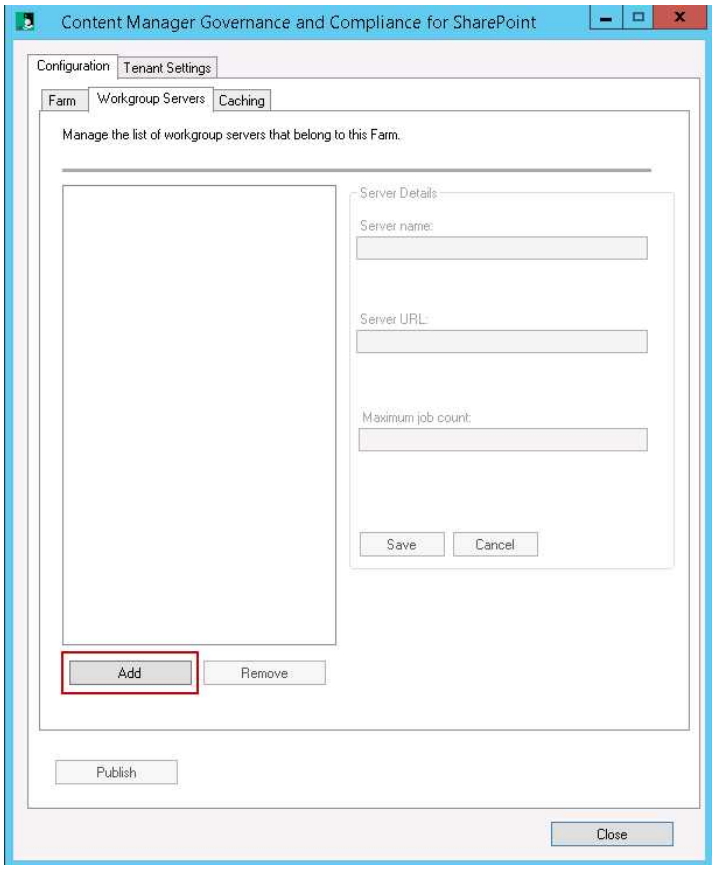


4.6.2 Workgroup servers

It is necessary to identify the workgroup servers that will be used in the Content Manager farm.

Using the configuration tool, navigate to the **Configuration** tab then navigate to the **Workgroup Servers** tab.

Each Content Manager farm must have at least one workgroup server. To add a workgroup server, click the **Add** button.



Enter the machine name of the workgroup server as the **Server name**. This must be the **exact name** of the machine.

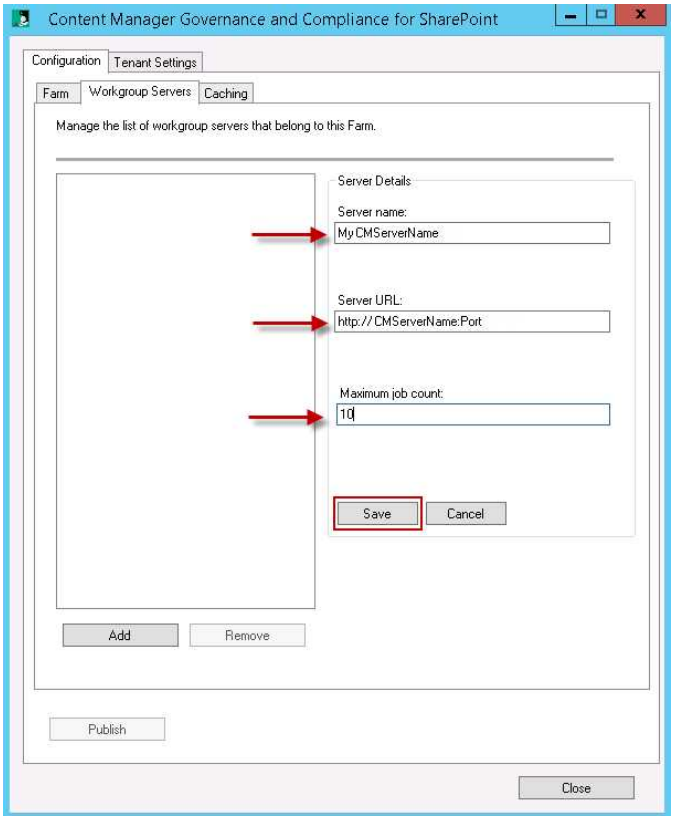
Enter the URL of the server. In the case where HTTP is being used, the URL will be:

```
http://MachineName:port
```

Where “MachineName” is the name of the Content Manager server and “port” is the port that you selected during installation. For example, if the machine name was “CM1” and you elected to use port 200, the URL would be:

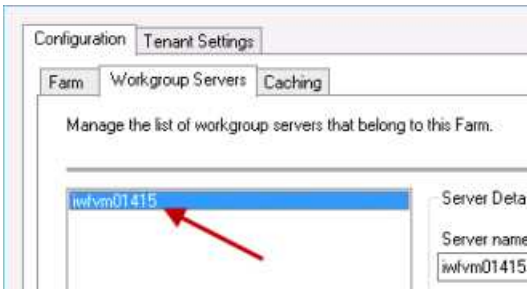
```
http://CM1:200
```

Enter the Maximum job count. This is the number of jobs that this server will process simultaneously. The default value is 10.



Once these details have been entered, click the **Save** button. During the save, the URL specified will be validated to confirm that the server is available on that URL.

Once validated, the URL will appear in the list of workgroup servers,



Continue adding workgroup servers until all workgroup servers in the Content Manager farm have been added.

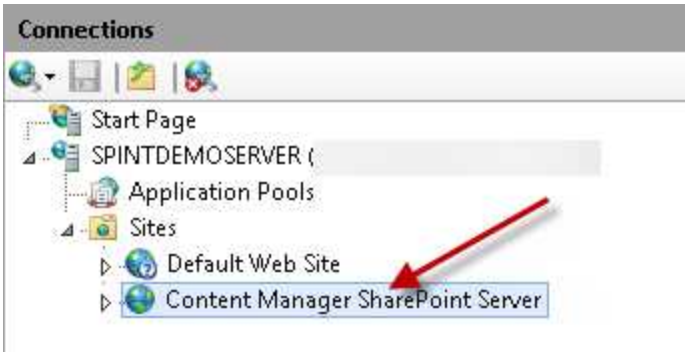
Unable to add server – https issue

If you have configured the Content Manager farm for SharePoint Online or you are using HTTPS there is a known issue that prevents adding a workgroup server to the list. The symptoms are:

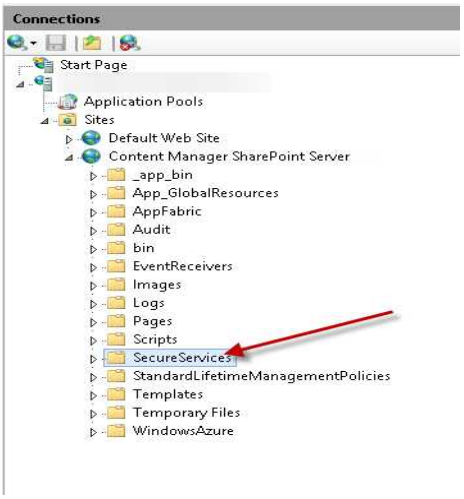
- When you try to add a server to the server list, a validation error states “A valid server cannot be reached on this URL”
- If you browse to the URL *https://YourUrl/SecureServices/DataStoreService.svc* you receive an authentication prompt. Regardless of entering the correct credentials, you are not permitted to view the page.
- If you have configured HTTPS to be used, you have tested that this is working correctly.

If you encounter this issue, this will also prevent the publishing of configuration data. It is likely that you will need to utilize the following workaround on the machine that you are running the configuration tool (and only on that machine):

Open **IIS Manager** and select the site: **Content Manager SharePoint Server**

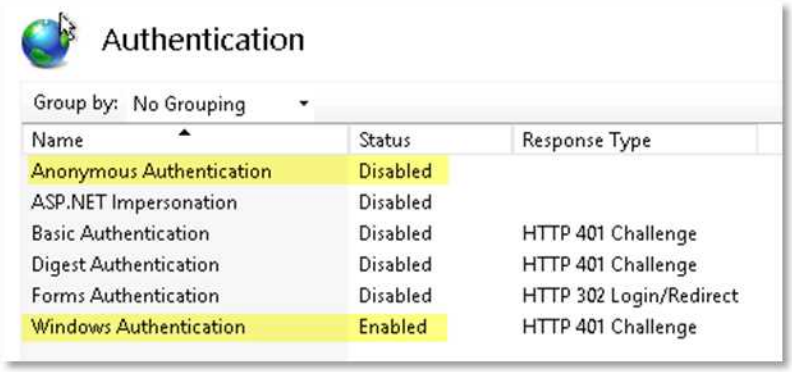


Expand the site and select **SecureServices**

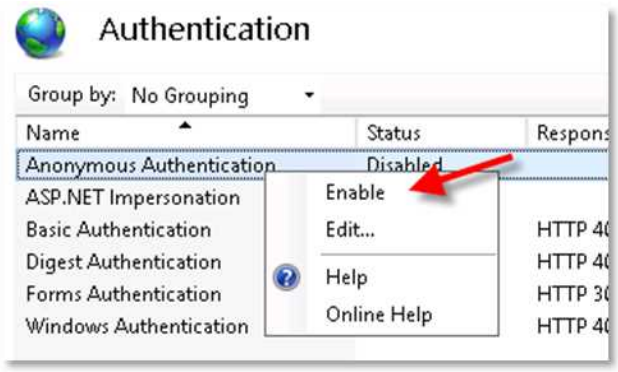


In the right hand pane using the “Features view” locate and double click the **Authentication** icon

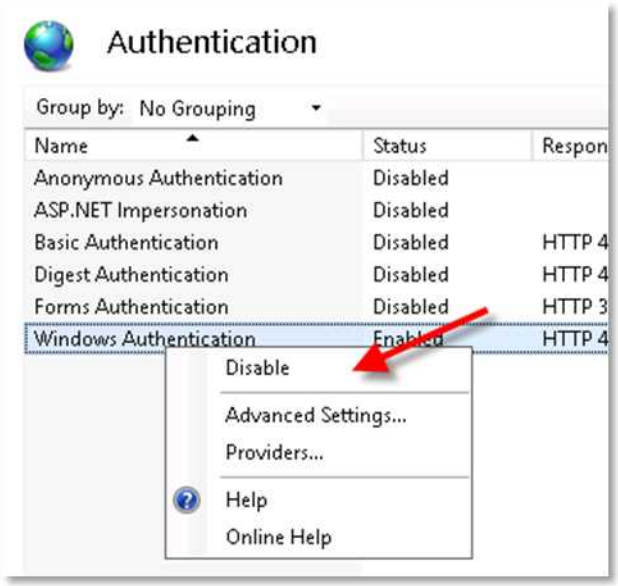
Authentication will initially show **Anonymous Authentication** as **Disabled** and **Windows Authentication** as **Enabled**



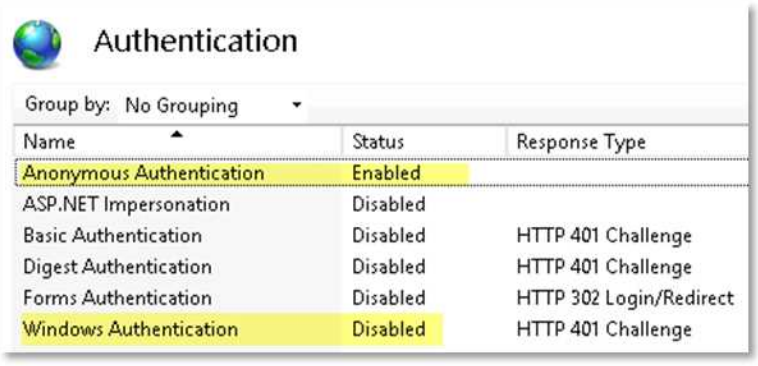
Right click on A**nonymous Authentication** and select **Enable**



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



The authentication should now be set as follows



You will also need to temporarily update the web.config file for the site.

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

```
<transport clientCredentialType="Windows"/>
```

Modify this node to read:

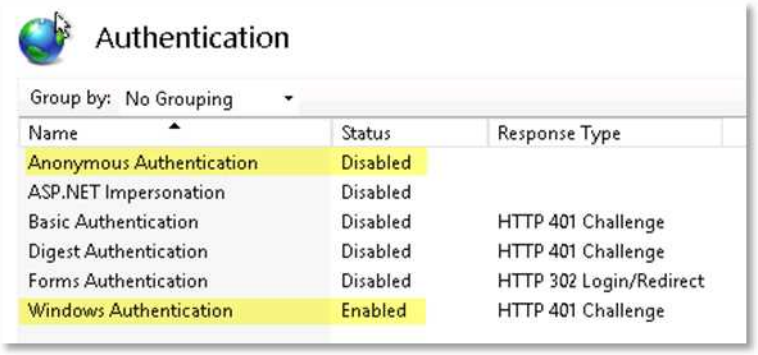
```
<transport clientCredentialType="None"/>
```

Save the web.config file.

Confirm that you can browse to the *URL https://YourUrl/SecureServices/DataStoreService.svc*

You should now be able to add your workgroup servers to the list.

Once you have finished publishing, you must change the authentication back to:



You must revert the web.config node that was modified back to read:

```
<transport clientCredentialType="Windows"/>
```

Unable to add server – code access security issue

If you have configured code access security at machine level, there is a known issue that prevents adding a workgroup server to the list. The symptoms are:

- When you try to add a server to the server list, a validation error states “A valid server cannot be reached on this URL”
- If you browse to the URL *https://YourUrl/SecureServices/DataStoreService.svc* you receive an error. If you turn off custom errors in the web.config file, the error mentions code access security.

If you encounter this issue, this will also prevent the publishing of configuration data and use of the Content Manager Governance and Compliance app. You will need to make the following changes on all machines in your Content Manager farm.

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 node

```
<system.web>
```

Insert the following node before the closing tag:

```
<trust level="Full"/>
```

The full node should look similar to this when complete:

```
<system.web>
     <customErrors mode="On"/>
  <compilation debug="false" targetFramework="4.5" />
  <httpRuntime requestValidationMode="4.5" executionTimeout="60" />
  <pages controlRenderingCompatibilityVersion="3.5" clientIDMode="AutoID" />
  <identity impersonate="false" />
     <trust level="Full"/>
</system.web>
```

Save the web.config file.

Confirm that you can browse to the URL *https://YourUrl/SecureServices/DataStoreService.svc*

You should now be able to add your workgroup servers to the list.

Note that there are security considerations with setting the trust level to full. It is not recommended that this approach be taken if your server is internet facing. You should consider modifying the CAS policies instead.

4.6.3 Permissions

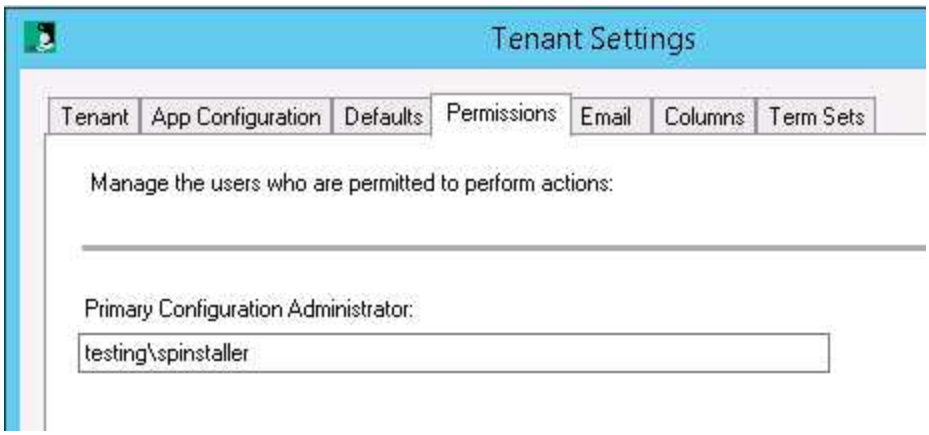
The groups used for determining permissions must be set. Using the configuration tool, navigate to the **Tenant Settings** tab, select the **Tenant**, click**Configure** then the **Permissions** tab.

Using the format:

```
Domain\groupname
```

Enter the following details:

Primary Configuration Administrator - Manages the users who are permitted to perform actions



For information about permissions, please see section 14.5 "Configuration Access Controls" of the Content Manager Governance and Compliance SharePoint App: User Guide.

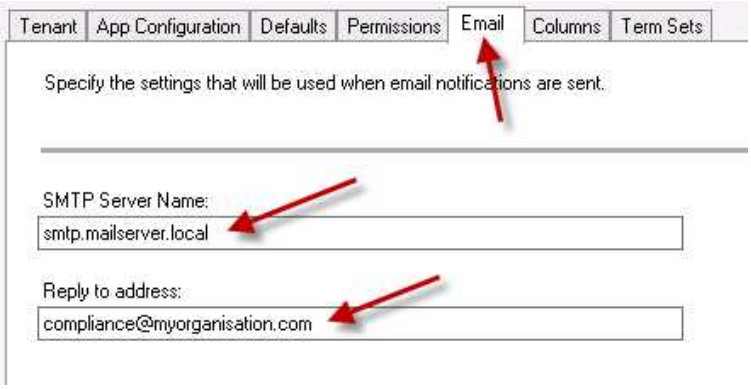
4.6.4 Email

If email notifications are required, it is necessary to provide the details required for these notifications.

Using the configuration tool, navigate to the **Tenant Settings** tab, select the **Tenant**, click**Configure** and than the **Email** tab.

Provide the full name of the SMTP Server that should be used for sending email notifications.

Enter a reply to address that email notifications will appear to come from.



Email settings are not validated by the configuration tool.

4.6.4 Publish

Once all settings have been entered, they must be published to all servers in the Content Manager farm.

Using the configuration tool, navigate to the **Configuration** tab and click the **Publish** button at the bottom of the dialog.

4.6.5 Restart the Content Manager SharePoint Service (Azure only)

This section is only applicable for machines using Windows Azure caching

Restart the Windows service named:

```
Content Manager SharePoint Service
```

This is required to complete the configuration of Azure caching.

4.7 Additional configuration to support ADFS

4.7.1 Overview

If your environment uses Active Directory Federation Services (ADFS), there are additional steps that you must perform before proceeding further. These steps involve:

- Adding a relying party trust
- Modifying the web.config file used by the Content Manager SharePoint

4.7.2 Enable HTTPS

The ***Content Manager SharePoint Server*** IIS site installed on Content Manager server must use HTTPS as the communication protocol. ADFS configuration will not be possible if this is not done.

See Configuring the use of HTTPS for instructions regarding this step. Note that if you have not already configured HTTPS, you will need to redo the previous configuration steps in this chapter to reflect the updated workgroup server HTTPS based URL.

4.7.3 Add relying party trust

A relying party trust is required in ADFS referring to the Content Manager farm URL.

For instructions to perform this task, see the following URL:

https://technet.microsoft.com/en-us/library/adfs2-help-how-to-add-a-relying-party-trust(v=ws.10).aspx

The following are the values to enter during the wizard this article describes:

- Select Data Source
  - Choose “Enter data about the relying party manually
- Specify Display Name
  - Display name: enter the Content Manager farm URL

- Choose Profile
  - Choose “AD FS 2.0 profile”
- Configure URL:
  - Check “Enable support for the WS-Federation Passive protocol”
  - Relying party WS-Federation Passive protocol URL: enter the full HRPM farm URL
- Configure Identifiers
  - Relying party trust identifier: enter “uri:sharepoint:hprm”
- Choose Issuance Authorization Rules
  - Choose “Permit all users to access this relying party”

4.7.4 Update the web.config file

The web.config file for the ***Content Manager SharePoint Server*** IIS site must have some modifications made to support ADFS.

Locate the following file located in the installation directory:

`ConfigureSTS.ps1`

Run this script using PowerShell. This will perform modifications on the web.config file.

Locate the following file located in the installation directory:

`Web.config`

Open this file and modify the following highlighted text to reflect the correct values (as found in your AD FS Management console)

```
 <system.identityModel>
    <identityConfiguration>
      <audienceUris>
        <add value="uri:sharepoint:hprm" />
      </audienceUris>
      <certificateValidation certificateValidationMode="None" />
      <issuerNameRegistry
type="System.IdentityModel.Tokens.ConfigurationBasedIssuerNameRegistry,
System.IdentityModel, Version=4.0.0.0, Culture=neutral,
PublicKeyToken=b77a5c561934e089">
        <trustedIssuers>
          <add thumbprint="[Enter your token issuer certificate thumbprint here]"
name="[Enter your STS name here]" />
        </trustedIssuers>
```

```
      </issuerNameRegistry>
    </identityConfiguration>
  </system.identityModel>
  <system.identityModel.services>
    <federationConfiguration>
      <cookieHandler requireSsl="false" />
      <wsFederation passiveRedirectEnabled="true" issuer="[Enter the full url to
the SAML2.0/WS-Federation here (relative url is adfs/ls)]"
realm="uri:sharepoint:hprm" reply="uri:sharepoint:hprm" requireHttps="false" />
    </federationConfiguration>
  </system.identityModel.services>
  <appSettings>
    <add key="ClaimProviderType" value="SAML" />
    <add key="TrustedProviderName" value="[Enter your STS name here]" />
    <add key="IdentityClaimType" value="SMTP" />
  </appSettings>
```

Save the updated web.config file when the changes are complete.

4.7.5 Ensure Content Manager locations are configured

Any user locations in Content Manager that will be used via SharePoint must have the ***Alternate Identifier*** of the location set to the primary claim that will be presented by ADFS. In most cases this is the email address.

4.7.6 Ensure SharePoint user profiles include the SharePoint primary claim

When authenticating to SharePoint a user may present a number of claims. During the configuration of ADFS with SharePoint, it is necessary to nominate what is the ***primary*** claim to be used to authenticate the user. This is the claim that SharePoint will look for to determine who the user is.

If this primary claim does not exist on the user's SharePoint profile, then a user will not be able to access SharePoint.

If you have not configured the profile with the primary claim and the user can access SharePoint, you have probably left integrated authentication enabled therefore the user is being authenticated by SharePoint using AD credentials.

Typically the primary claim will be the user's email address. Consult SharePoint documentation for how to determine the primary claim.

To manage the properties configured for a user profile, see the section Accessing a user profile

4.7.7 Restricting Access based on custom group claims

To better provide for custom authentication, we are allowing users to customize the authentication of users by enabling the use of custom group claims. This functionality is enabled by default and is only triggered when the application detects a custom claim during the authentication process.

In order to leverage this feature, you will be required to write and build a custom assembly. A more technical description of what is required to use this feature can be found in the Appendix - Custom Claims Implementation

4.7.8 To view managed documents in Content Manager

Additional configuration steps need to be undertake to be able to view a managed document in Content Manager:

a. Browse to the installation directory and edit the DocumentViewDetails.xml.

b. Set the value of the LoadBalancedUrl to the URL of new SearchAndViewSite and save it.

c. Restart the jobprocessing service.

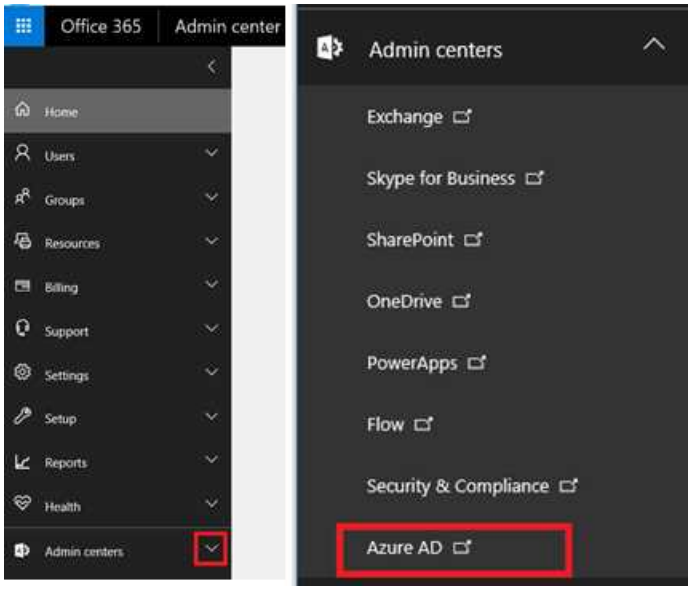
4.8 Configuring the Content Manager Integration for SharePoint Online - Azure AD authentication

The additional configuration steps described in this chapter need to be carried out before you can choose the record types on the Default Integration settings page while you are in a SharePoint Online environment.

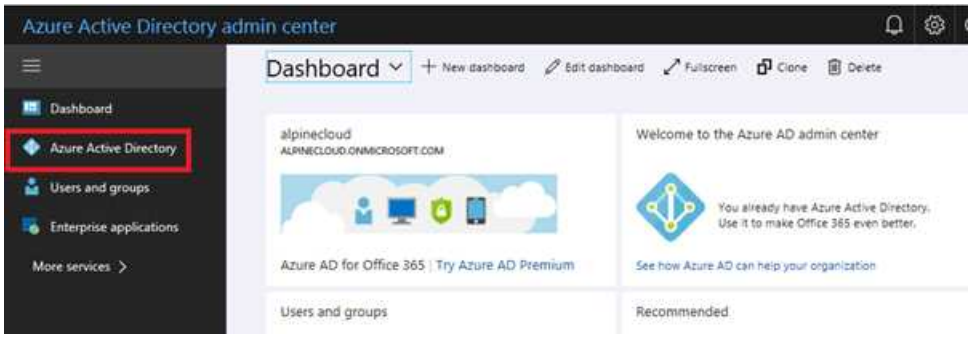
Azure AD Configuration

Browse to the Office 365 Admin site by clicking on the Admin button on the app launcher

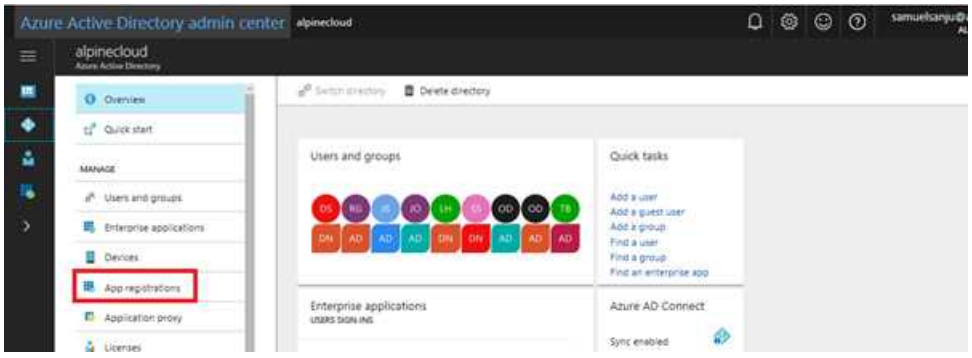
Expand the Admin centers and select Azure AD from the list



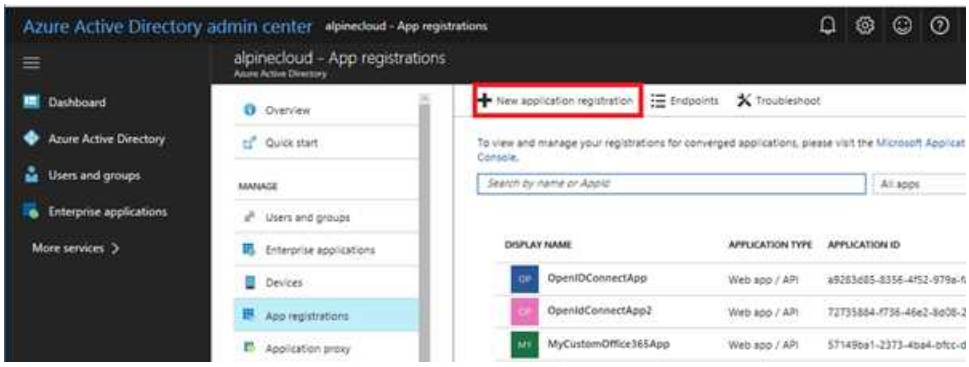
On the Microsoft Azure portal, select the Azure Active Directory menu



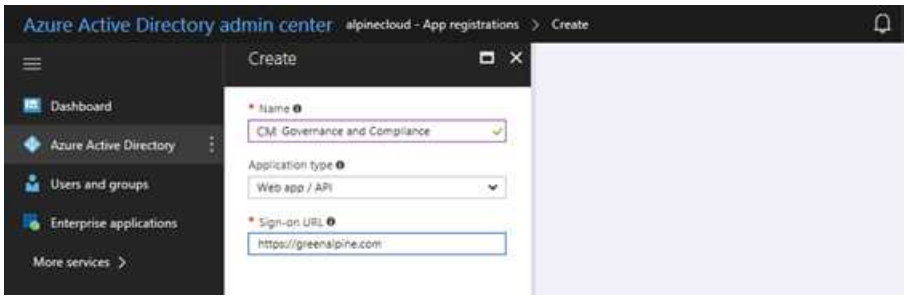
Once in your active directory, click on the App registrations tab



Click the “New application registration” option

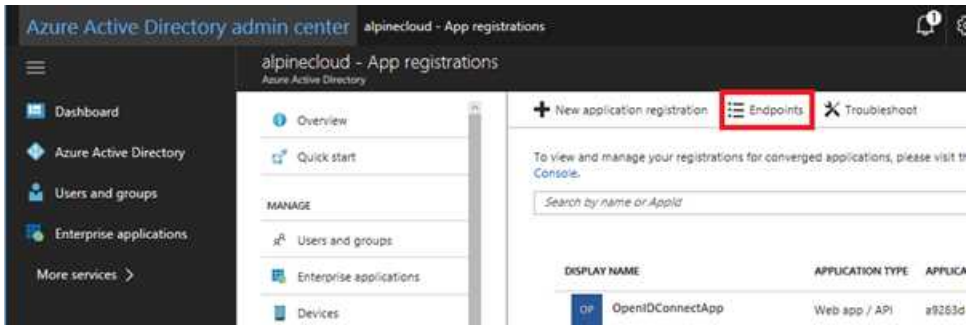


On the create page, type in “CM Governance and Compliance” leave the Application type as “Web app/API” and click next



For the Sign-on URL specify the root URL of your CM SharePoint Integration SharePoint Server IIS site and press “Create”

Once the app registration is complete, you will be taken back to the “App Registrations” page. On this page, click on the “EndPoints”

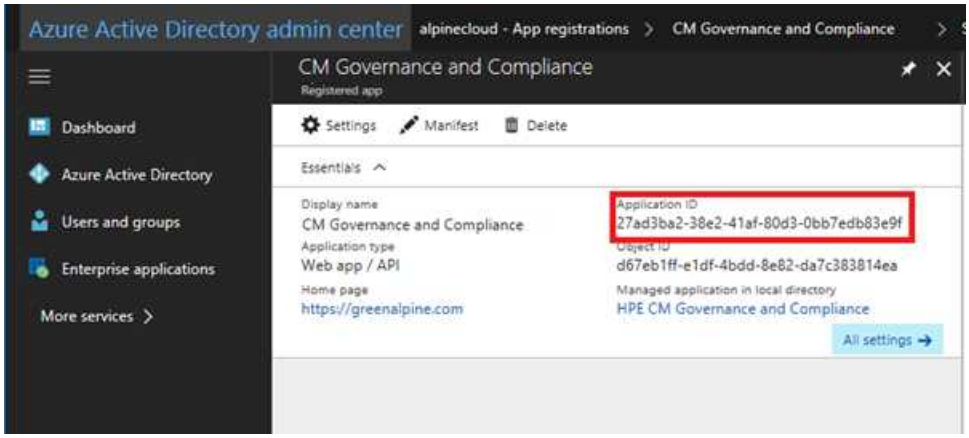


Copy the **FEDERATION METADATA DOCUMENT** to clipboard. The copied value will look like the one below:

https://login.microsoftonline.com/a55c1bb7-ba79-4ebd-89e2-a1355ac043b9/federationmetadata/2007-06/federationmetadata.xml

> **NOTE:** The highlighted ID is your Tenant Id.

Now go back to the App registrations page and click on the Content Manager Governance and Compliance app you created.



Copy the “Application Id”. You need to enter these values in the Configuration Wizard to complete your configuration.

4.9 Creating Content Manager term sets

4.9.1 Overview

SharePoint has a concept of defining a set of terms, possibly hierarchical in nature, which can be used in many places across your SharePoint farm. This allows definition and maintenance of this set of terms in one central location.

These sets of terms are known as “term sets”.

Content Manager for SharePoint utilizes term sets to represent the following types of Content Manager data:

- Record types
- Classifications
- Security levels
- Security caveats

These terms must be created in SharePoint using the tools provided.

> *Creating term sets must be separately instigated. If you fail to do this, you will not be able to complete configuration of the product.*

Currently only single SharePoint farm Managed Metadata Services are supported. There is no support for sharing services across multiple SharePoint farms. It is possible to share services across farms

and it may work for the creating and using the Content Manager term sets, however no support will be provided in case there are problems encountered.

Create a group for the Content Manager database

Term sets are created in "Term Stores" that reside in a "Managed Metadata Services" (MMS). In a term store you can define a group that is used to logically group related term sets. In order to create the Content Manager term sets, a dedicated group must be created for each Content Manager dataset that terms are required for.

To create this group, ***you must be a term store administrator***. For instructions on how to add a user as a term store administrator, see the appendix *Adding a term store administrator*.

For each MMS that is used by your SharePoint farm to provide term sets, you must create a new group in the term store (see the *Creating a term store group* appendix for details if required).

The name that you give to your group is very important. It must be in the format:

```
Content Manager(database ID)
```

Replace the term "database ID" with the 2 character identifier of your Content Manager dataset. For example, if your dataset ID was "45" then the name of your group would be:

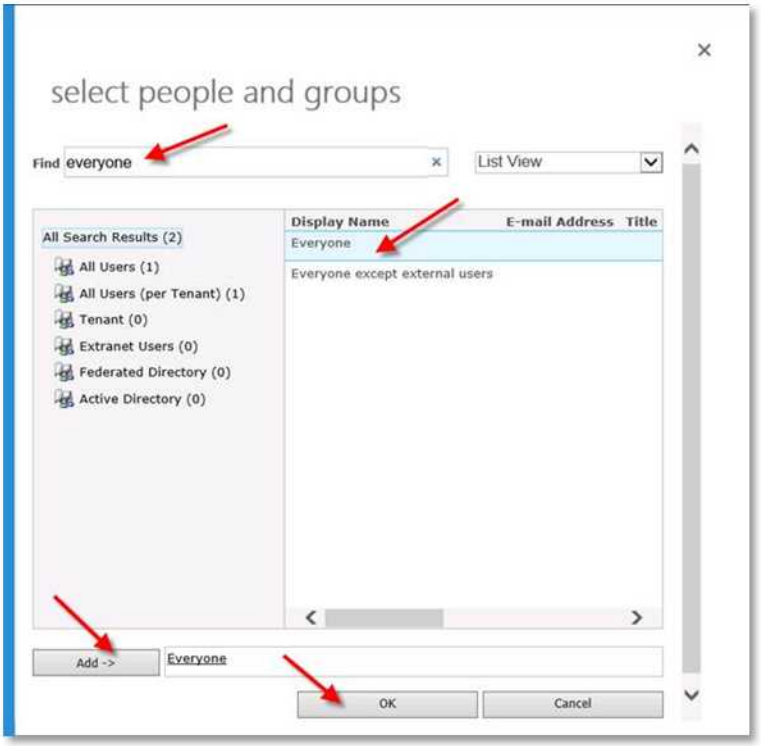
```
Content Manager(45)
```

Note that there is no space between "Manager" and the opening bracket.

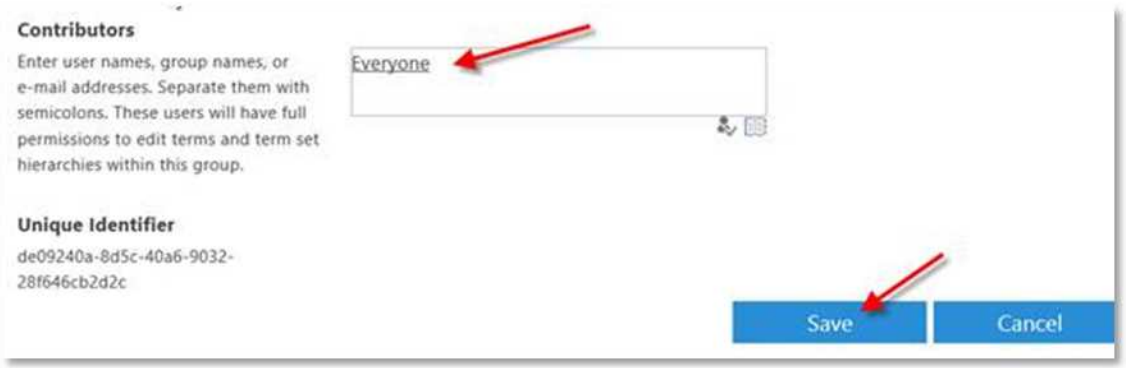
Once the group has been created, you must give sufficient permission to allow the creation of the terms. Locate the **Contributors** section for the group just created. Click the directory button.

On the **select people and groups** dialog, type the word "everyone" in the search box and click on the search button.

Select "Everyone" from the search result and click on the **Add** button followed by the **OK** button.



Click the **Save** button to commit the permissions.



This permission may seem excessive but is a current limitation of SharePoint.

> *Note that there is an issue in SharePoint currently that will show this value as "true" instead of "Everyone" following the save. This is currently expected behavior.*

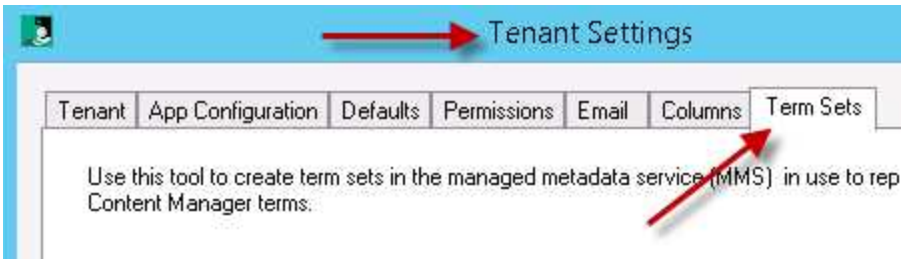
Instigating term set creation

The creation of term sets is performed using the configuration tool.

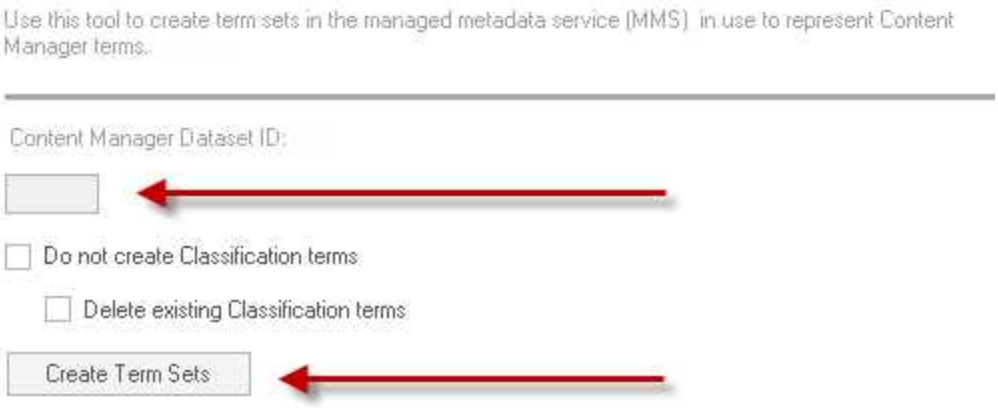
Note: It is advised to stop the SharePoint service when undertaking tern set creation or maintenance.

Open the configuration tool.

Navigate to the **Tools** tab then the **Term Sets** tab:



Enter the **ID** of the Content Manager dataset that the term sets should be created to represent then click the **Create Term Sets** button.



This will instigate the process of creating term sets. Note that the term sets will be created in every term store that you have created the Content Manager group.

If no groups have been created, this tool will not fail. Term sets will just not be created.

You can repeat use of this tool for as many datasets as you intend to use.

Creation of terms sets without using Classification terms

A term set can be created without leveraging the Classifications within Content Manager by selecting the "Do not create Classification terms" check box on the term sets tab. Doing so will also allow you to remove any existing Classification terms (see below)

Removal of existing term sets

If your installation has existing Classification terms, you can remove all of the existing entries by ensuring the "Delete existing Classification terms" check box is selected when creating term sets without using Classification terms (see above).

Maintenance of term sets

From time to time, new terms will be added to Content Manager and existing terms will be modified or even removed entirely. Because of this, it is necessary to maintain the values of the term sets.

A maintenance process executes every hour to update the terms.

Alternatively, if a change is required more immediately than this, run the term sets tool again. This will correct any term set changes almost instantly.

Supported Configuration

The Term Set should only be created on the same SharePoint farm that the SharePoint Integration is configured on.

4.10 Set default integration settings

4.10.1 Overview

The **Default Integration Settings** are used to determine how content in SharePoint is managed by Content Manager. The **CM9.3_ SharePoint2013IntegrationUserGuide.pdf** describes more advanced configuration options but in the absence of this advanced configuration, it is the **Default Integration Settings** that are used during the management process.

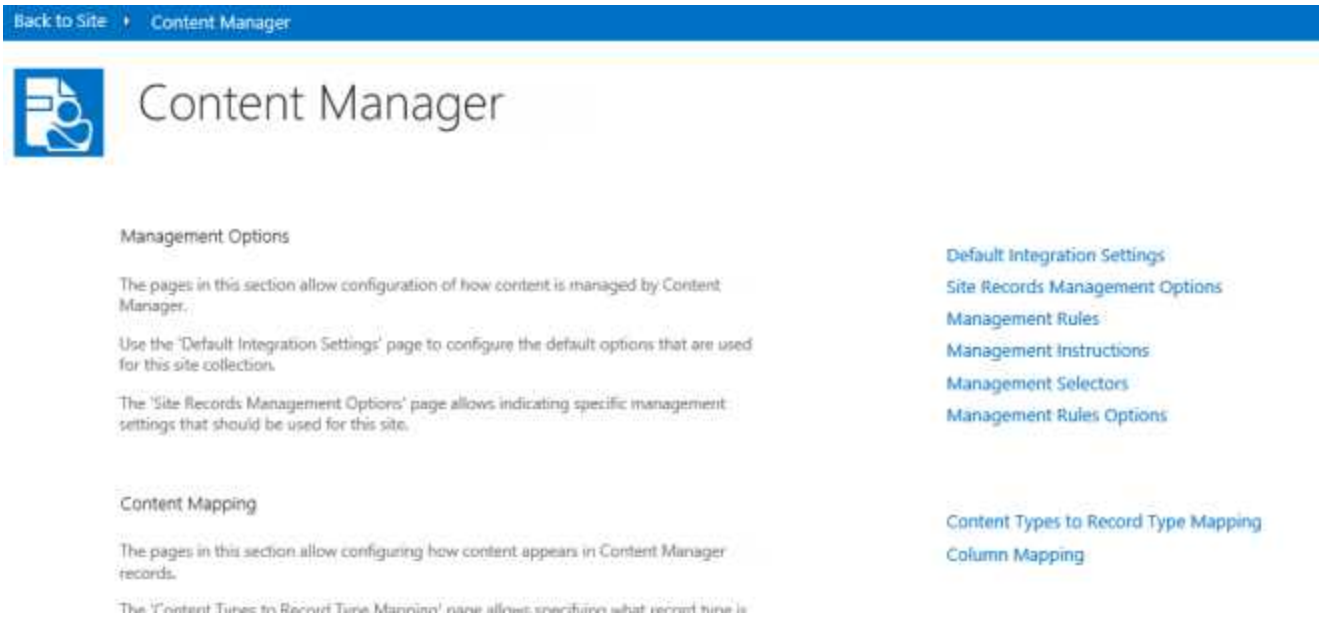
> *For initial configuration, you should set the default integration settings used by the default site collection as these will be used by other site collections. If performing initial configuration, in the following sections, use the default site collection.*

Accessing app configuration pages

A number of app configuration pages are accessed from a page referred to as the “app start page”. To access the app start page for the Content Manager Governance and Compliance app, navigate to the site contents page of the site collection.

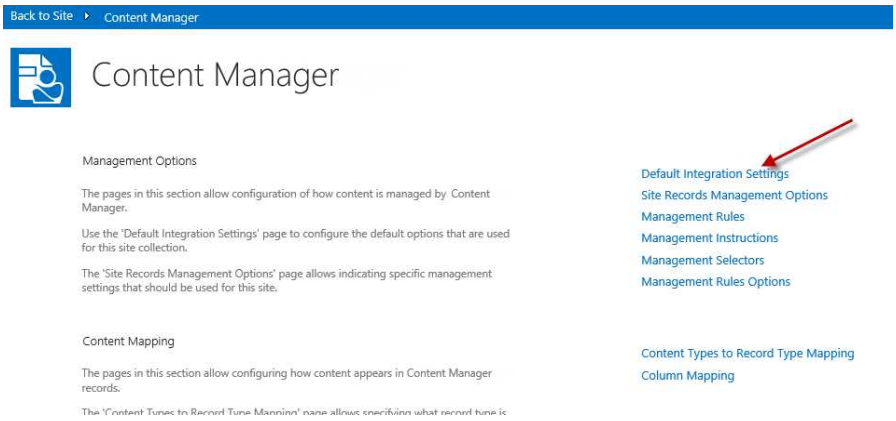
Locate the **Content Manager Governance and Compliance** app and click on it.

This will take you to the app start page:



4.10.2 Setting the default integration settings

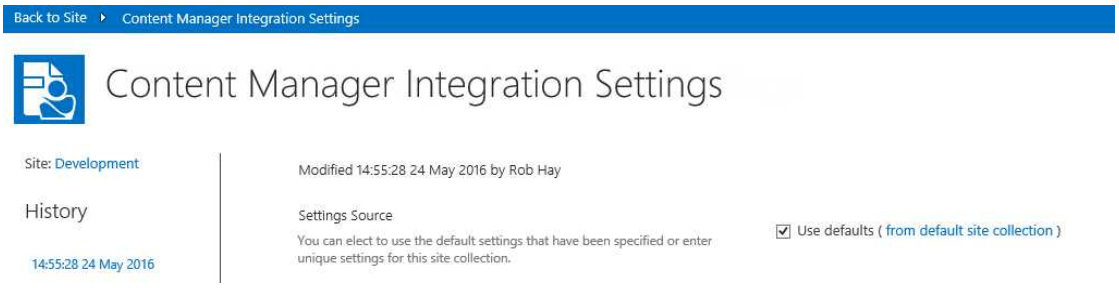
From the app start page click the **Default Integration Settings** link. You must be a site collection administrator to access this page.



Settings source

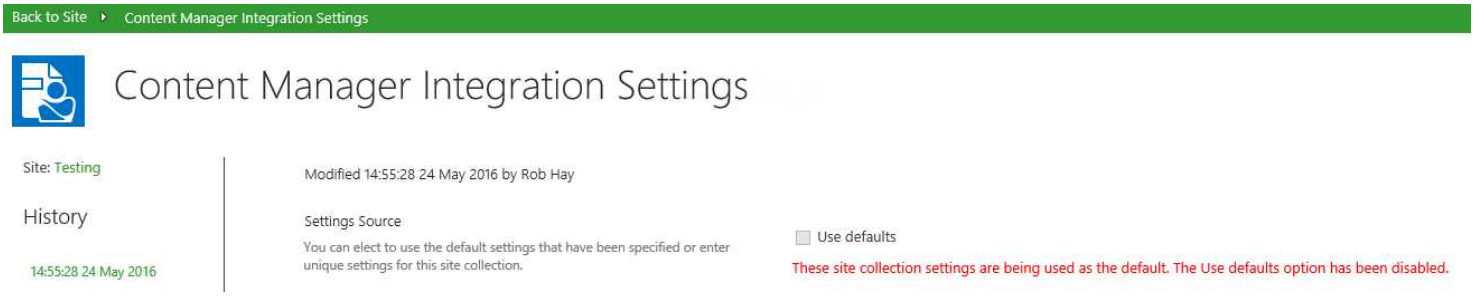
The settings source section allows you to specify if the values used for this page should come from the default site collection, or whether this site collection specifies its own values.

In the following scenario, the default site collection settings are used and it is not possible to enter values on this page.



If the **Use defaults** check box is unchecked, then specific values for this site collection can be entered.

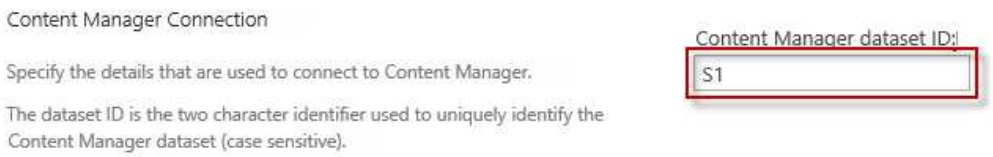
If this site collection is the nominated default site collection, then the **Use defaults** check box is disabled.



Content Manager Connection

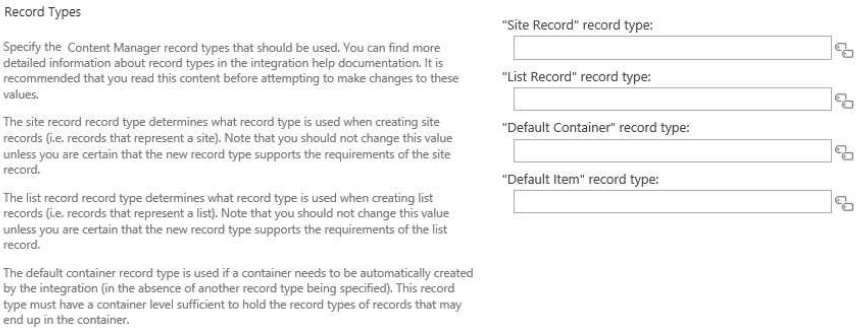
The Content Manager Connection section of the page allows specifying the ID of the Content Manager dataset to be used.

Enter the two character identifier of the Content Manager dataset ID to use noting that this value is case sensitive.



Record Types

The record types section of this page allows specifying the Content Manager record types that should be used by default during management.



The **Site Record** control will allow you to select any record type that has a behavior of **SharePoint site**.

The **List Record** control will allow you to select any record type that has a behavior of **SharePoint list**.

The **Default Container** control will allow you to select any record type that has a behavior of **Folder** and is marked as suitable for being a list item record.

The **Default Item** record type will allow you to select any record type that has a behavior of **Document** and is marked as suitable for being a list item record.

> *You must specify a value for all four record types before the page will allow you to save.*

For details regarding record type requirements see the Prepare record types section earlier in this document.

> *Only record types that existed prior to creating term sets or a term set maintenance job running will be available for selection.*
>
> *You must have specified a dataset ID prior to selecting record types or the selection dialog will not show any values.*

*The remaining settings on this page are covered in the **CM9.3_ SharePoint2013IntegrationUserGuide.pdf** and can be left default for the initial setup*

4.11 Creating columns

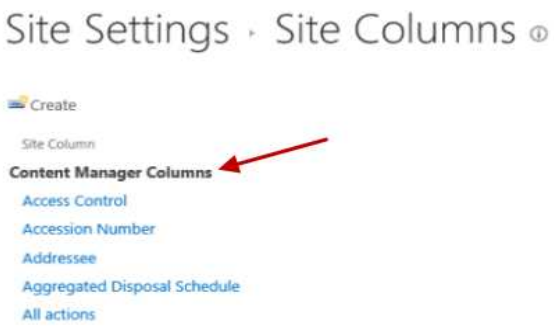
4.11.1 Overview

When working with managed SharePoint content, often there is a requirement to see values for the corresponding Content Manager record in the SharePoint list item itself. For example, it may be important to your organization that the record number for the record is easily identified. In this scenario, a “record number” column could be added to the list. Using column mapping (described in more detail in the **CM9.3_ SharePoint2013IntegrationUserGuide.pdf**)this column can be mapped such that it shows the value of the record number from Content Manager.

Rather than require your organization to create SharePoint columns then map them to Content Manager fields, the configuration tool includes a column creation tool. This tool creates a collection of site columns that represent most of the fields in Content Manager. These columns are automatically mapped to the relevant Content Manager field during creation.

Once created, these fields appear in the "Content Manager Columns" group and can be used throughout the site collection they exist on.

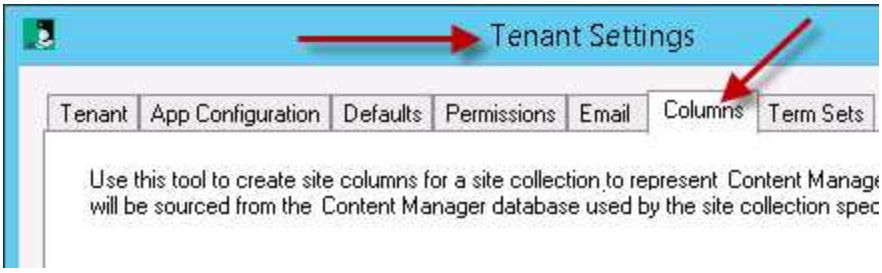
Creating columns requires that the 4.10 Set default integration settings, on page 110 section has been completed first.



Note that the creation of columns is optional. It is not required by the application.

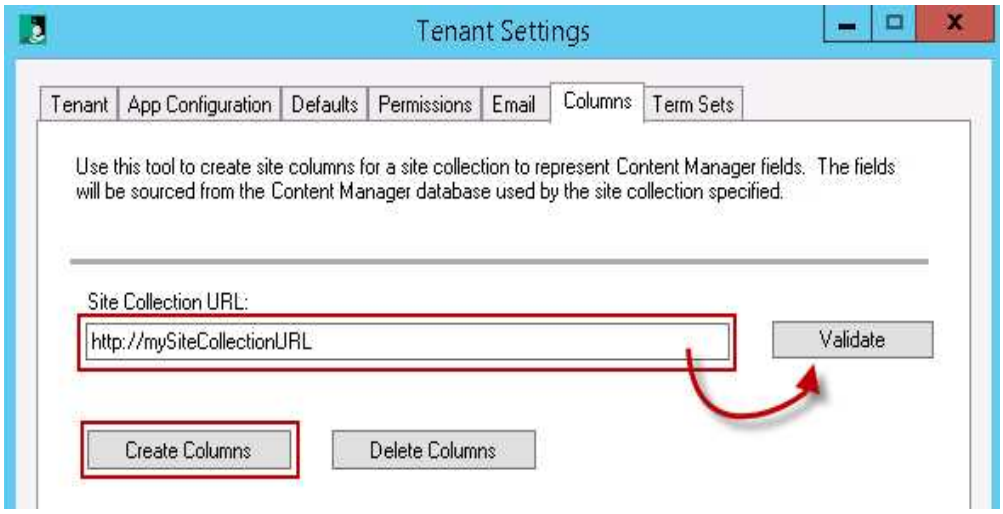
Creating columns

Column creation is performed using the configuration tool. Navigate to the **Tools** then **Columns** tab.



Enter the full URL of the site collection that the site columns should be created on. The **Validate** button will confirm that the URL entered is a suitable SharePoint site collection.

Click the **Create Columns** button to start the column creation.



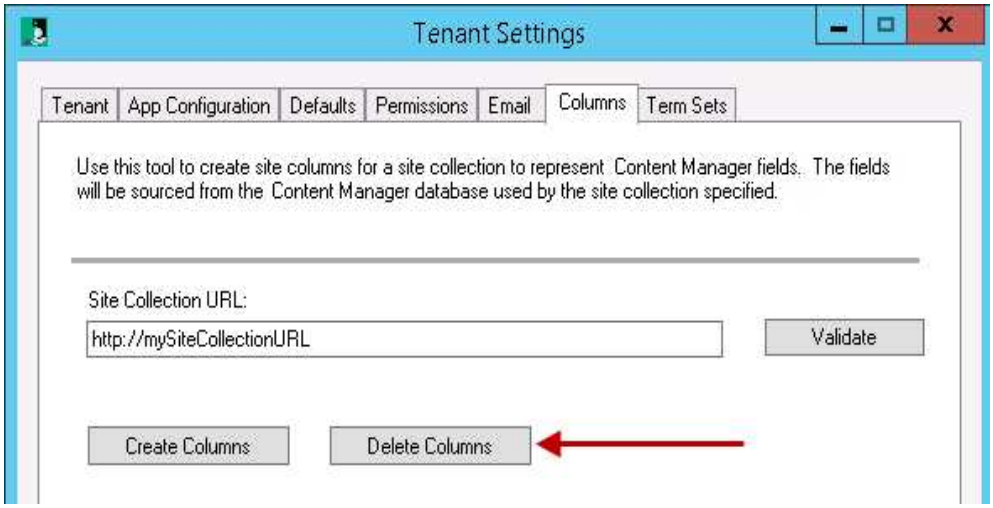
Maintenance of columns

Unlike term sets, there is no process to maintain the columns should a new one be added or an existing one be modified or removed.

If column maintenance is required, simply run the create columns tool again.

Deleting columns

To remove all columns that have been created by the tool, enter the URL of the site collection to remove them from, then click the **Delete Columns** button.



This will delete all columns in the "Content Manager Columns group, including any that have been added manually.

If a column is being used by a content type, it will not be deleted. When all columns cannot be deleted, the log file will indicate which columns were not removed.

Recommendations for location of columns

If your SharePoint farm is using a content type hub, rather than create columns on all site collections create columns only on the content type hub. Use the hub to propagate columns to other site collections.

If using a content type hub and you do not follow this recommendation, it is likely that errors will occur with the hub as it tries to create the Content Manager columns on other site collections that already have them.

4.12 Setting up subsequent site collections

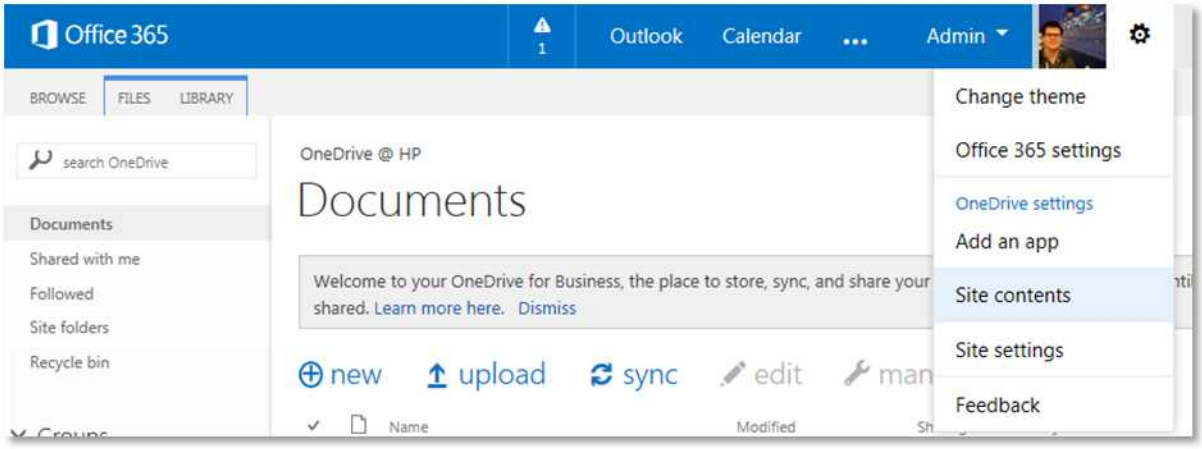
Following configuration of the initial, default site collection, all that is required to configure subsequent site collections is to add the app.

If the default values configured on the default site collection are suitable for this subsequent site collection, then there are no further steps required.

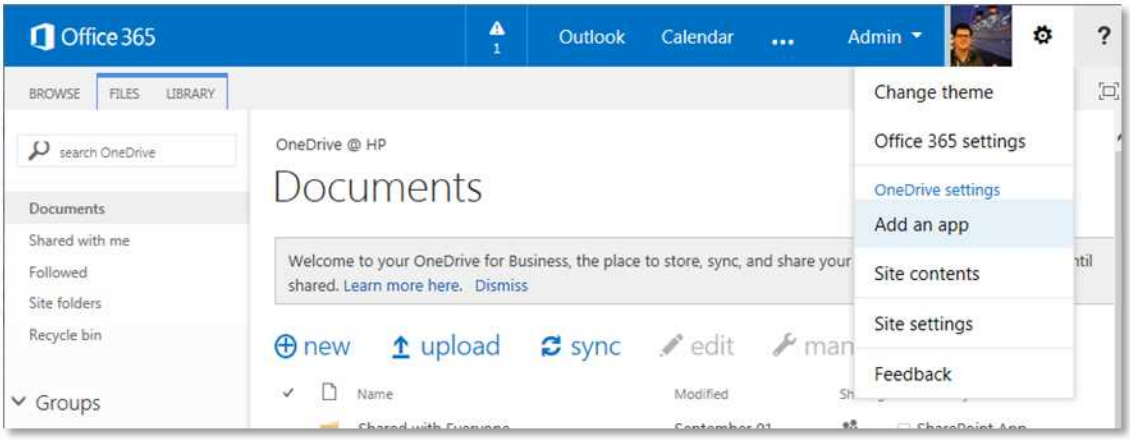
4.13 Setting up One Drive for Business

One Drive for Business (ODB) provides cloud file storage for business users. The underpinning technology is SharePoint 2013. A user's drive in ODB is in fact nothing more than a document library. The Content Manager Governance and Compliance app is fully compatible with ODB.

To utilize the app with ODB involves adding the app as is required for any other site or site collection. This can be done by accessing the Site contents and then add the app.



Alternatively, the Add an app link can be used to navigate directly to apps page.



4.14 Supporting multiple SharePoint farms or multiple configuration databases

A configuration database used by a Content Manager farm is only designed to support a single SharePoint farm. In the scenario where your organization has multiple SharePoint farms, you will need to plan for this accordingly.

A similar scenario that requires the same planning in the case where multiple configuration databases are required. Consider the scenario where you have 20 site collections. Ten of these site collections will require one set of configuration while the other 10 use a different set of oconfiguration.

With a single configuration database, the first ten could use the default site collection settings to obtain configuration values. The other ten though would have be set individually as the default values are not the ones required. This requires setting the same values ten time.

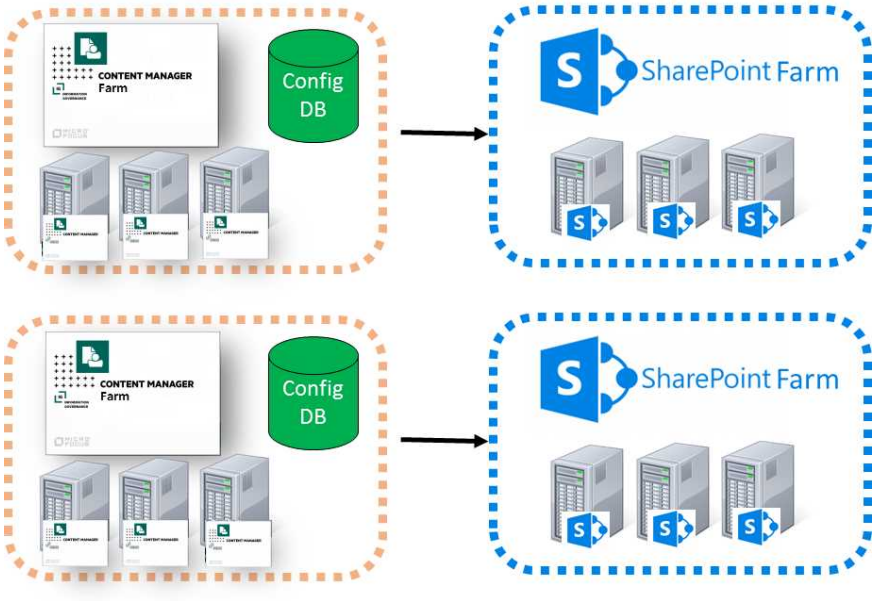
If the second lot of ten site collections used an independent configuration database, a default site collection could be defined and the other nine site collections consume the values from it.

There are two primary options available to support these scenarios.

The explanation in this section describes the separation of SharePoint farms. The same approach is required if a set of site collections need to be separated on the same farm.

4.14.1 Paired SharePoint and Content Manager farms

A Content Manager farm has a single configuration database. In the “paired” approach, for each SharePoint farm, a dedicated Content Manager farm is configured each with a single configuration database.

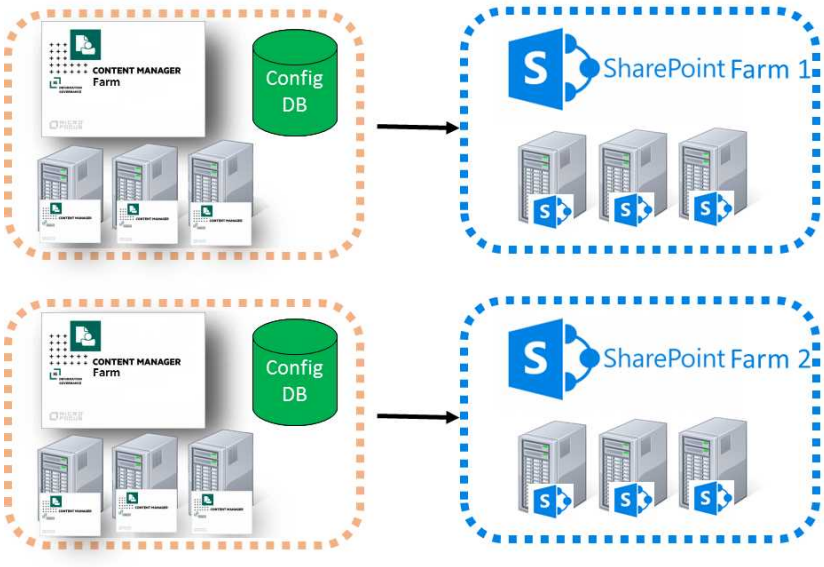


The advantage of this approach is that it is simple to understand and configure as everything for a particular SharePoint farm is logically separated.

The disadvantage of this approach though is that you may end up with underutilized workgroup servers. Consider the scenario where your organization has two SharePoint farms. It has been determined that the number of workgroup servers required to service the load of each farm is as follows:

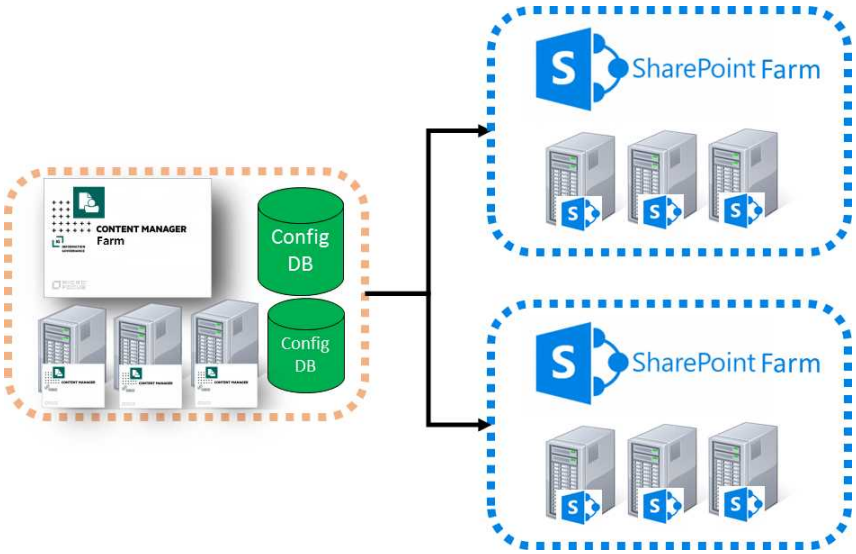
- SharePoint farm 1: 1.5 workgroup servers
- SharePoint farm 2: .5 work group servers

Although a sum total of two workgroup servers is required to address the total load, using the paired approach, three servers would be required.



4.14.2 Shared Content Manager farm

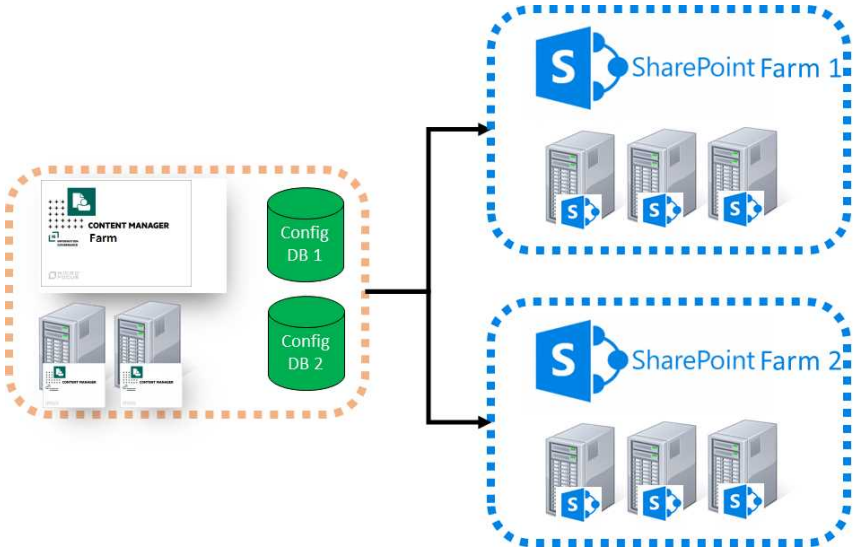
The second approach to supporting multiple SharePoint farms is to “share” a Content Manager farm with a number of SharePoint farms. In this approach, one Content Manager farm is created, however, the farm contains multiple configuration databases (one for each SharePoint farm)



The disadvantage of this approach is that it is more difficult to configure than the paired approach. The advantage though can be illustrated by considering the scenario where your organization has two SharePoint farms and it has been determined that the number of workgroup servers required to service the load of each farm is as follows:

- SharePoint farm 1: 1.5 workgroup servers
- SharePoint farm 2: .5 work group servers

Using the shared approach, the requirements can be serviced with two workgroup servers as against the three that are required in the paired approach.



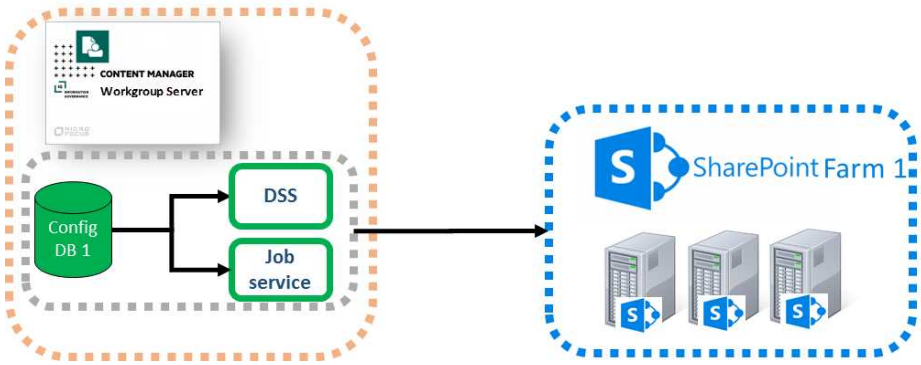
Architecture of a shared Content Manager farm

For the explanation of a shared Content Manager farm, the farm will be considered to only have a single workgroup server. When using multiple servers in a Content Manager farm, the architecture and configuration must be repeated on each server in the farm.

When the Content Manager Governance and Compliance app server components are installed on a workgroup server, two key components are created:

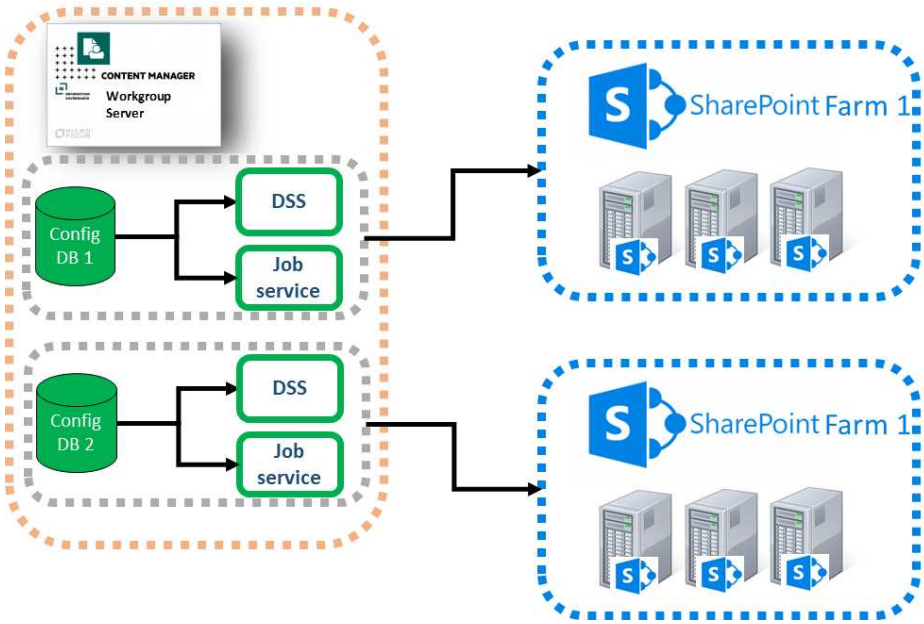
1. An IIS site referred to as the Data Store Server (DSS)
2. The Content Manager SharePoint Windows service (referred to as the job service)

These components interact with the configuration database used by the farm.



In this diagram the config database is illustrated as residing on the workgroup server. It is important to recognize that this database could reside on a dedicated SQL server farm. It has been drawn this way for convenience.

The shared Content Manager farm approach involves duplicating the core components to allow them to interact separately with the relevant config database.



When duplicated in this way, the DSS must be placed on a different IIS port or use a different host header to allow the Content Manager Governance and Compliance app on each farm to access the correct configuration database.

Creating a shared Content Manager farm

This section assumes that you have correctly installed and configured this Content Manager farm for one SharePoint farm already.

A script is installed with the server components that performs most of the configuration effort for you.

Modifying the execution policy on the machine

In order to run this script, a temporary change to the execution policy may be required.

Run an instance of Powershell as an administrator

Determine the current execution policy in use by running the following script:

```
Get-executionpolicy
```

Note down the name of the current policy so it can be used to revert to it.

Set the execution policy to RemoteSigned using the following script:

```
set-executionpolicy RemoteSigned
```

After running the script to create the shared Content Manager farm, revert your policy back to the original by running the following script where [Your original policy] is the name of the policy determine by running the get script:

```
set-executionpolicy [Your original policy]
```

Running the farm configuration script

Run Powershell ISE as an administrator. Using Powershell ISE open the file ***FarmConfiguration.ps1*** from the installation directory used when installing the Content Manager Governance and Compliance app server components

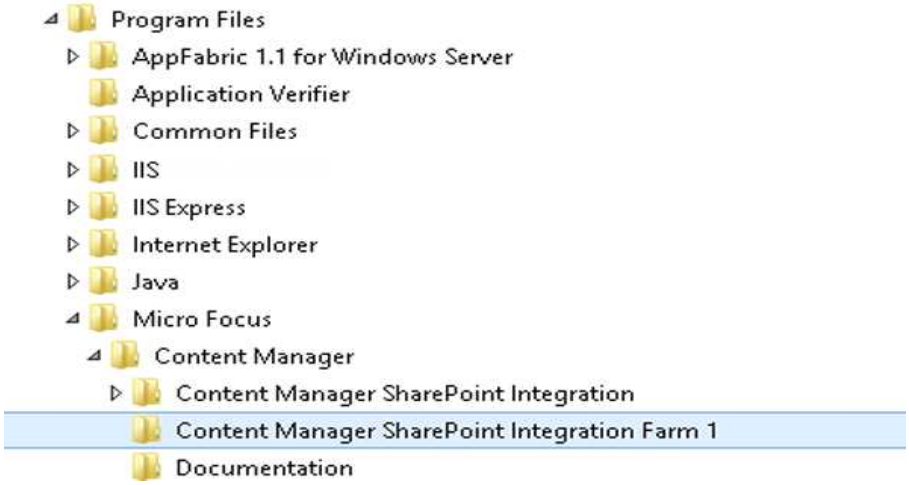
Run this script.

This script will prompt you for the following details:

- The port number to use for the IIS site – ensure you choose one that is not already in use
- Whether to enable SSL for the site – this will add a https binding to the site
- The identity of the application pool in the format ***domain\name***
- The password for the application pool
- The identity of the job processing service in the format ***domain\name***
- The password for the job processing service

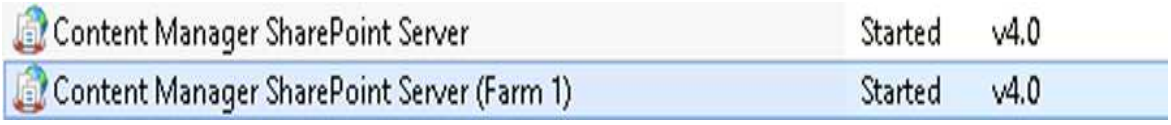
Following the execution of the script, you can verify that it succeeded by confirming the following steps. The name of the components will have the number of your farm appended. The first additional farm you create will be 1, the next 2 and so on. In the following section, the term ***Farm x*** has been used to represent the farm number:

- A new directory has been created at the same level as the installation directory named ***Content Manager SharePoint Integration (Farm x)***



- In IIS a new site has been created named ***Content Manager SharePoint Server (Farm x)***

- In IIS a new application pool has been created named ***Content Manager SharePoint Server (Farm x)***



- A new windows service has been created named ***Content Manager SharePoint Service (Farm x)***

This script should be run for every additional farm that is to be created.

Configuring a shared Content Manager farm

After running the script to create the shared Content Manager farm, each new instance must be configured.

Post installation steps

Essentially, running the farm configuration script installs a new instance of the server components. You must complete (for each farm you have created), all steps in chapter 3 after the installation chapter (3.1.2).

Configuration

For each farm that has been created using the farm configuration script, you must complete the configuration for the farm just as you did for the first installed farm.

You must run the right instance of the configuration tool though. The shortcut installed for the configuration tool by the MSI is the instance used by the first farm created by the MSI. To locate the correct instance of the configuration tool to run, navigate to the directory that was created by the farm configuration script. Locate the following file:

```
HP.Integration.SharePoint.JobProcessing.exe
```

Right click and run as administrator. This is the instance of the configuration tool that applies to that farm.

It is also important to understand that you must follow the steps to generate a new app file. The new app file generated will contain the correct URL to the shared Content Manager farm instance to use. This is the app file that must be used on the SharePoint farm managed by this shared instance.

Removing a shared Content Manager farm

If a shared Content Manager farm is no longer required, it can be removed as follows:

- Ensure that the job processing service applicable to the farm is stopped
- Open Powershell ISE as an administrator
- Run the following script replacing “x” with the number of the farm to remove. This will delete the job processing service for the farm:

```
$service = Get-WmiObject -Class Win32_Service -Filter "Name='Content Manager
SharePoint Service (Farm x)'"
$service.delete();
```

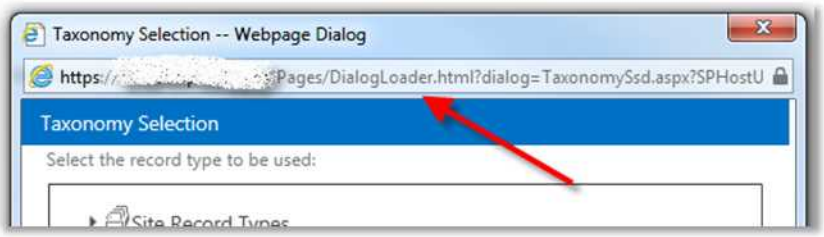
- From IIS delete the site created for the farm
- From IIS delete the app pool created for the farm
- Delete the directory created for this farm

Note that uninstalling the MSI will not remove any shared farms that have been created. You must use this manual process.

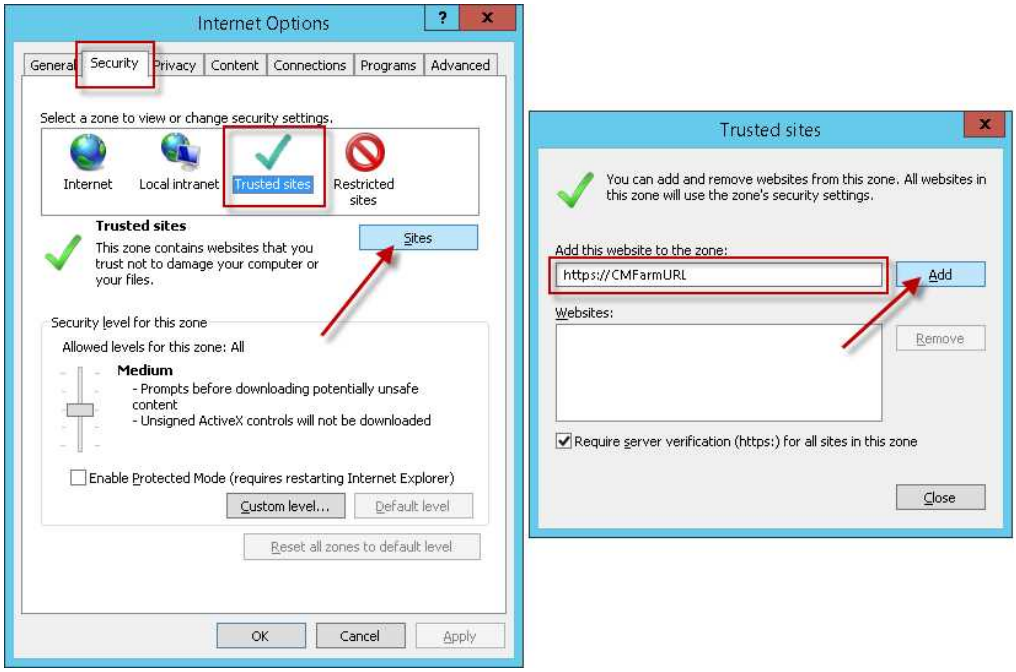
4.15 Other configuration tasks

Trusted sites

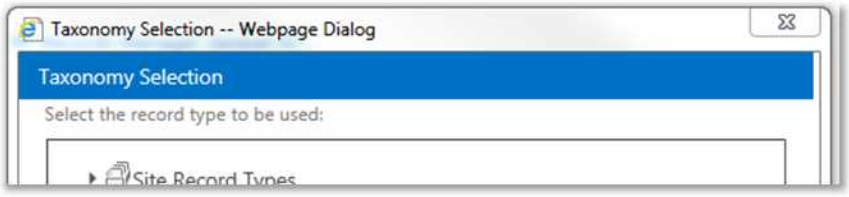
The integration includes a number of dialogs that are shown to the user. These dialogs may include address bars along top of the dialogs. Although these do not hinder the functionality of the product, they may be aesthetically incorrect.



Adding the URL specified as the load balanced URL for the Content Manager farm to trusted sites in Internet Explorer settings will prevent this address bar from being shown.



Once added to the trusted sites, the address bar will no longer show.



This configuration task is best suited to group policy rather than setting on individual machines.

5 Upgrading the Content Manager Governance and Compliance App in SharePoint 2013 or 2016

5.1 Overview

This section is about upgrading an existing installation of version 8.1 to a later build. This involves upgrading the Content Manager components, and possibly upgrading the app. It will not always be necessary to update the app and therefore it should only be updated if it is specifically mentioned that it should be done.

5.2 Upgrading 8.3 Records Manager

Version 9.2 of the Content Manager Governance and Compliance app will only work with version 8.3 of Records Manager. You must upgrade to version 8.3 of Records Manager before upgrading the Content Manager Governance and Compliance App for SharePoint.

5.3 Upgrading the Content Manager components

5.3.1 Considerations

Repeating configuration steps

The upgrade process will overwrite any IIS configuration settings made following the previous settings. This will require you to reapply the following:

- Configuring the use of https (if the Content Manager server is configured to use https)
- Additional steps for Windows Azure (if the Content Manager server is in that environment)
- Additional steps for use with SharePoint Online (if the app if hosted in SharePoint Online)

Unavailability of the Content Manager farm

During the upgrade, the Content Manager farm (even if only a single machine) will at times be in a state that will not be useable by SharePoint. This could result in issues managing content. It is recommended that you follow these steps to render the Content Manager farm unavailable during this time.

Stop the service: ***Content Manager SharePoint Service*** on each server in the Content Manager farm. This will ensure that any pending jobs will not get processed during the upgrade.

Upgrade one workgroup server at a time, first making it unavailable to the load balancer in use. This will ensure that events being raised by SharePoint can still be handled by the remaining servers in the Content Manager farm.

Perform any configuration tool work once the last server has been upgraded. This will ensure that any database upgrades are not performed until the latest time.

5.3.2 Performing the upgrade

Upgrading from 8.3

If upgrading from 8.3 a tool has been provided to prepare the existing configuration for the 9.2 upgrade. To upgrade the 8.3 Records Manager Farm database see 15_Appendix-8.3 Upgrade the Records Manager Farm database

Install the SharePoint client components

When upgrading to version 8.3, it may be necessary to install the SharePoint client components. If upgrading from 8.1.1 then this step will already have been done. If upgrading from 8.1 then this must be done prior to attempting to upgrade the Content Manager server components.

Upgrade the server components

The components that are required to be installed on a Content Manager workgroup server can be installed using the ***CM_SharePointIntegration_x64.msi*** MSI found on the installation media.

You must perform this upgrade on each workgroup server used in the Content Manager farm.

On every server in the Content Manager farm, run the MSI to upgrade the components.

Repeat any steps determined to be applicable in the preceding considerations section.

5.4 Upgrading the app configuration database

These steps only need to be performed on one server in the Content Manager farm

If upgrading from 8.3

5.4.1 Reconnect to the app configuration database

Following upgrade, it will be necessary to connect to the app configuration database again using the configuration tool. See the section Connecting to an existing configuration database for details.

5.4.2 Upgrade the app configuration database

Using the configuration tool, perform a publish. This will perform any upgrades required on the app configuration database for 9.0 and beyond.

5.5 Upgrading the SharePoint app

These steps only need to be performed on one server in the Content Manager farm

5.5.1 Rerun the app configuration tool

Regardless of whether the app was updated or not, following an upgrade the app configuration tool must be rerun. It is not necessary to publish again.

5.5.2 Update the app in the app catalog

It will not always be necessary to update the app and therefore it should only be updated if it is specifically mentioned that it should be done.

Upgrading to version 8.3 release requires the app to be upgraded. The upgraded app will be version 8.3.0.0

Should the app require updating, ensure that you have generated the updated app file before proceeding.

There is a known issue in SharePoint that in some scenarios causes the app upgrade process described below to not work correctly. If the upgrade process does not work correctly, an alternative set of steps are included. It is permissible to simply follow the alternative upgrade procedure described without attempting the upgrade first.

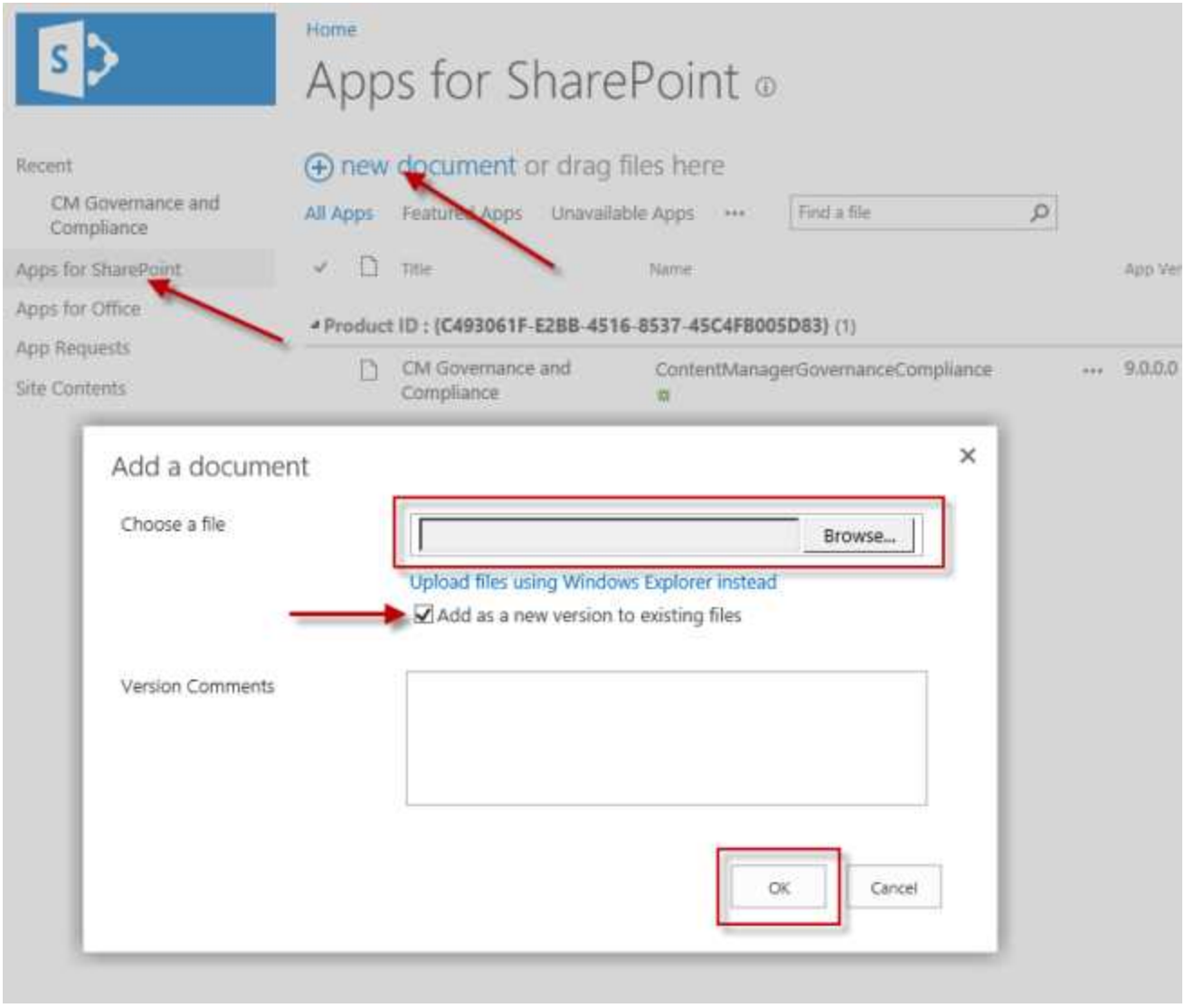
Standard app upgrade procedure

Navigate to the app catalog. See the appendix Identifying the app catalog in use for guidance.

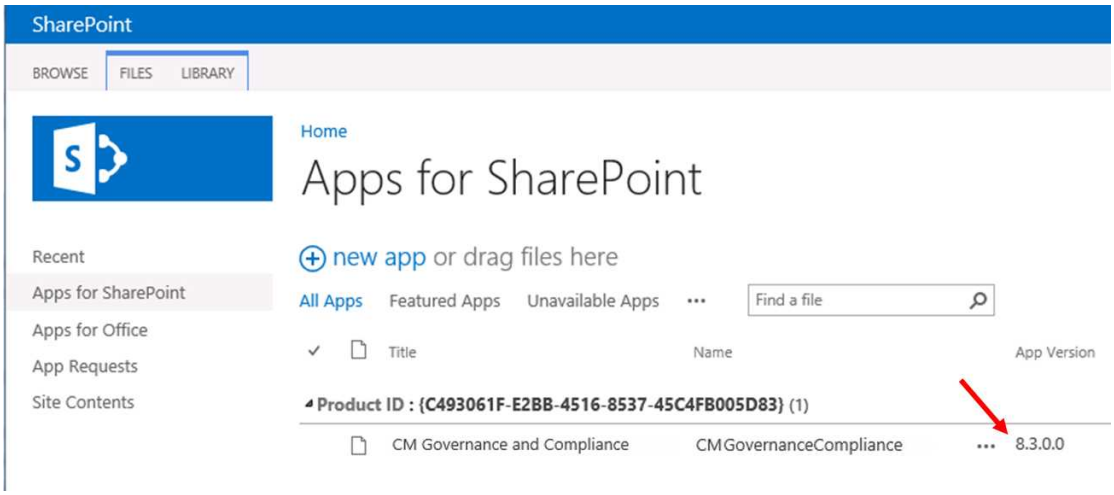
Navigate to the **Apps for SharePoint** section.

Click the **new app** button.

When prompted, choose the updated .app file ensuring that **Add as a new version to existing files** is checked.



This will add the updated app as a new version to the existing app. You can see the app version in the app catalog:

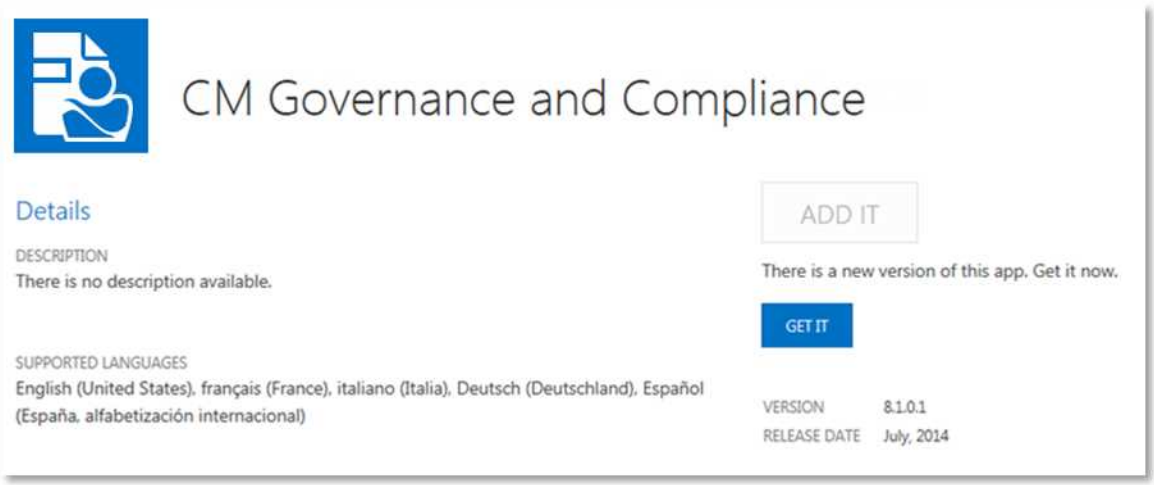


When updating the app, any time you add the app from that point on, the new version of the app will be used. For existing places where the app has been added, you will need to elect to update the app.

Navigate to the site that the app is added to and then to the site contents for that site. The app will indicate that an update is available:

The availability of the update may not appear immediately.

Click on the "update" link. This will show the details of the update (similar to below):



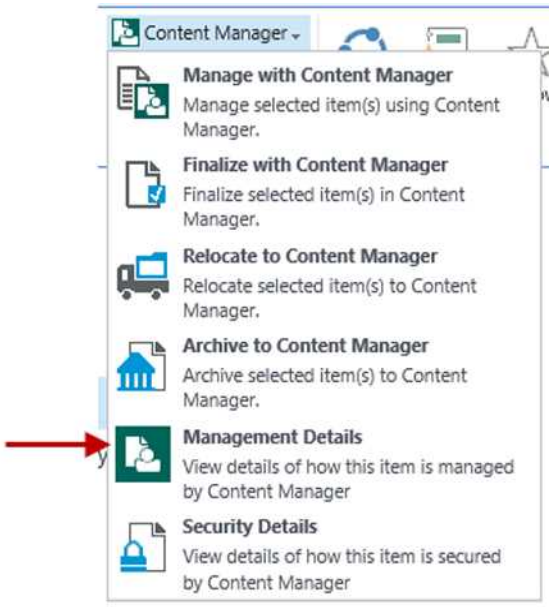
The version displayed in this screenshot is for illustrative purposes only. The version will be the one described at the beginning of this section.

Click the ***GET IT*** button to begin the update.

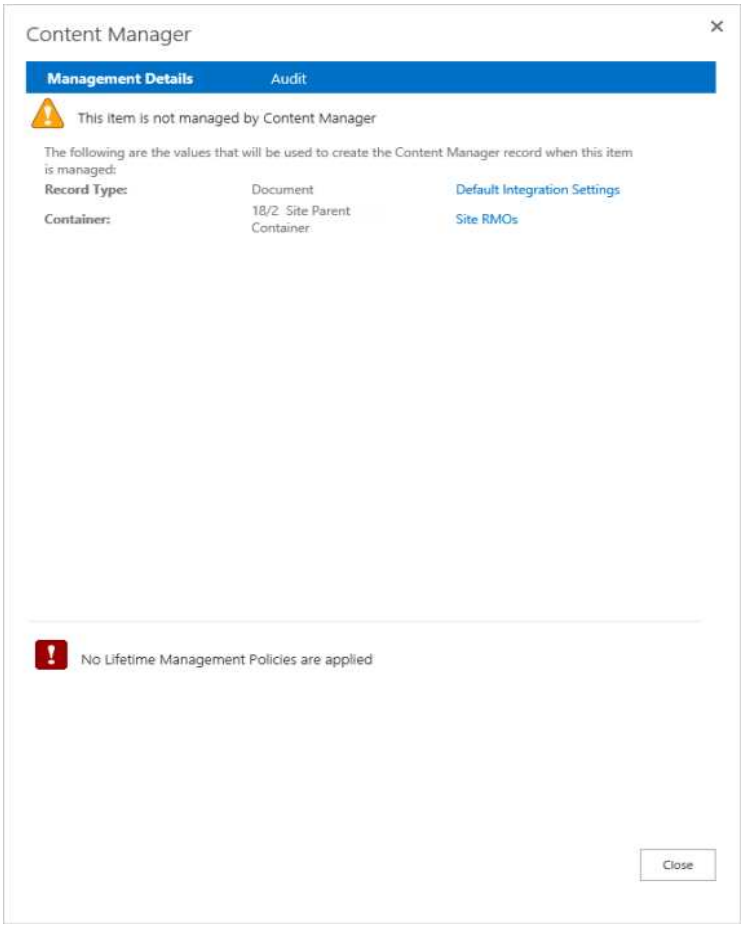
A quick way to test that the app has upgraded successfully is to navigate to the ribbon for a list or library. From the ***List*** or ***Library*** tab, drop down the ***Content Manager button*** next to the list or library settings. Confirm that the ***Audit Histor*** option appears and that the ribbon button is Content Manager and uses the new green background logo.

It may take up to an hour for SharePoint to begin displaying the new images and menu options.

Select an item in a list or library and from the Items of Files tab, choose the Management Details option.



The size of the dialog should be taller than it is wide. If it is almost square, then the app has not updated correctly.



There is a SharePoint issue that can result in the size of this dialog being correct on some lists but not on others. Removing the app from the site and re-adding it generally corrects this issue.

Alternative app upgrade procedure

Should the app upgrade fail then the following steps provide an alternative upgrade path. These steps involve removing the app wherever it has been added, removing it from the app catalog then re-adding it to the catalog and all required sites.

Note that removing the app will not remove the configuration that has been performed. Configuration such as mappings, RMOs, LMPs and management rules will all still remain in the configuration database. Removing the app does not delete this configuration. When the app is re-added after updating, all of the previous configuration data will remain unchanged.

Start by removing the app wherever it has been added. It is important to ensure you remove all instances of it or this will cause issues.

Follow the steps in the Removing the SharePoint app section to remove the app.

Follow the steps in the Add the app to the corporate catalog section to re-add the app to the catalog.

Follow the steps in the Add the app to the default site collection to re-add the app to the sites that require it.

5.6 Upgrading Content Manager columns

Version 8.1.1 introduces changes to columns created by the column creation tool. These will not apply to any columns that you have previously created with an earlier version. If upgrading from a version earlier than 8.1.1 you must use the column creation tool to remove all columns, then use the tool to create the columns again.

6 Upgrading from SharePoint 2010 Integration Solution

6.1 Supported upgrade path

The Content Manager Governance and Compliance app for SharePoint 2013 was introduced in version 8.1. Although much of the functionality is similar to the Content Manager SharePoint Integration for SharePoint 2010, it must be thought of as an entirely new product.

There is currently no supported true upgrade path. To move from a version of the Content Manager SharePoint Integration for SharePoint 2010 to the Content Manager Governance and Compliance app for SharePoint 2013 requires a complete removal and clean-up of the legacy Integration, performing the steps outlined in the Microsoft guides for upgrading SharePoint 2010 to SharePoint 2013, and finally following the steps in this guide for preparing SharePoint 2013 for Apps.

6.1.1 SharePoint 2010

The Content Manager SharePoint Integration for SharePoint 2010 is a legacy product. It is not possible to use the Content Manager Governance and Compliance app in SharePoint 2010, only 2013 and 2016.

If the intention is to upgrade to SharePoint 2013 you must:

1. Read this blog article for latest information on how to remove the legacy Content Manager SharePoint Integration from SharePoint 2010: http://www.imsharepoint.net/blog/2017/6/21/how-to-upgrade-from-sharepoint-2010-integration-solution-to-sharepoint-2013-integration-app

2. Upgrade SharePoint 2010 to SharePoint 2013

3. Install the Content Manager Governance and Compliance app

6.2 Configuration data

As the process of moving from the legacy Integration to the Integration app version is not a true upgrade, any configuration that has been made in an existing installation will be lost and will need to be recreated once the Integration app has been successfully installed.

If configuration data needs to be replicated in the Integration app version then you will need to document the existing configuration data. This includes:

- Site collection integration settings
- Records management options that are not default values
- Custom lifetime management policies

- Lifetime management options
- Content type to record type mappings
- Custom column mappings (the default ones will be created automatically) ● Exposure settings for lists that expose Content Manager content

Note that record type to content type mappings are not supported in the Integration app version.

6.3 Removing the legacy SharePoint 2010 Integration

Before making any changes to the deployed Integration solution please read this blog article for latest information required to perform the removal and clean up steps: http://www.imsharepoint.net/blog/2017/6/21/how-to-upgrade-from-sharepoint-2010-integration-solution-to-sharepoint-2013-integration-app

Do not deactivate any features or retract the solution from SharePoint web app

6.3.1 Identify where the Content Manager solution is deployed

Make a list of the full URLs of every web application in the farm that the Content Manager SharePoint 2010 Integration has been deployed to.

In SharePoint 2010 this solution is hprecordsmanager.14.wsp.

In SharePoint 2013 this solution is hprecordsmanager.15.wsp

You will need to read this blog article for latest information and execute the steps against every web application that has the solution deployed: http://www.imsharepoint.net/blog/2017/6/21/how-to-upgrade-from-sharepoint-2010-integration-solution-to-sharepoint-2013-integration-app

6.4 Upgrade SharePoint

If moving from SharePoint 2010, perform the necessary steps to upgrade to SharePoint 2013 SP1.

6.5 Installing the new version

Follow this document to install the Content Manager Governance and Compliance app.

7 Removing the integration components

7.1 Overview

Removal of the integration requires the following steps:

- Remove the app for every site it is currently being used
- Remove the app from the app catalog
- Uninstall the Content Manager components
- Manual removal of any remaining files
- Uninstallation of AppFabric (if it was installed as part of the installation process)

7.2 Removing the SharePoint app

7.2.1 Remove from all sites

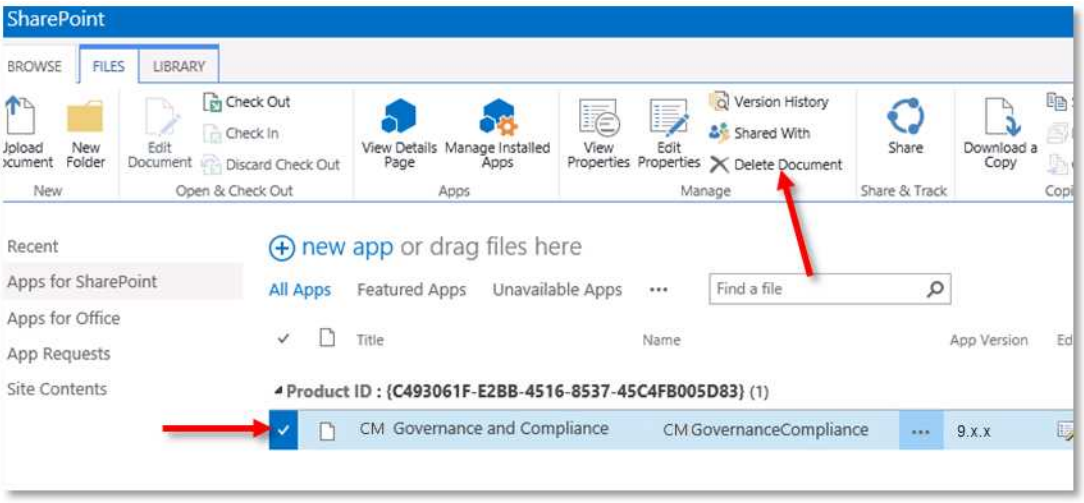
For every site that the Content Manager Governance and Compliance app is added to, it must be removed.

You can either do this manually, navigating to each site, to site contents, and then removing the Content Manager Governance and Compliance app, or you can use PowerShell to automate removal.

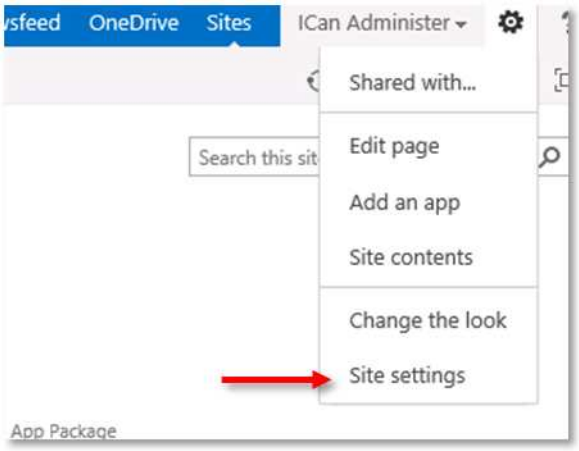
See the Remove Content Manager app from all sites and site collections in a web application section for an example script. This script will write a list of all locations that the app was removed from.

7.2.2 Remove from the corporate app catalog

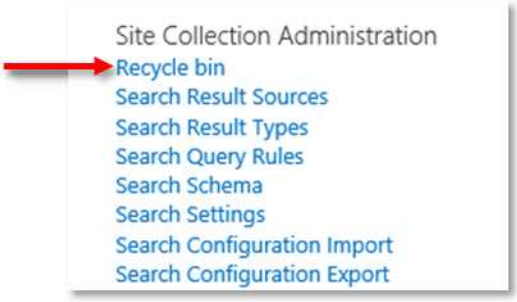
Navigate to the app catalog in use, select the app and delete it.



You must ensure the app has been removed from the first and second stage recycle bins. From the app catalog navigate to ***Site Settings***

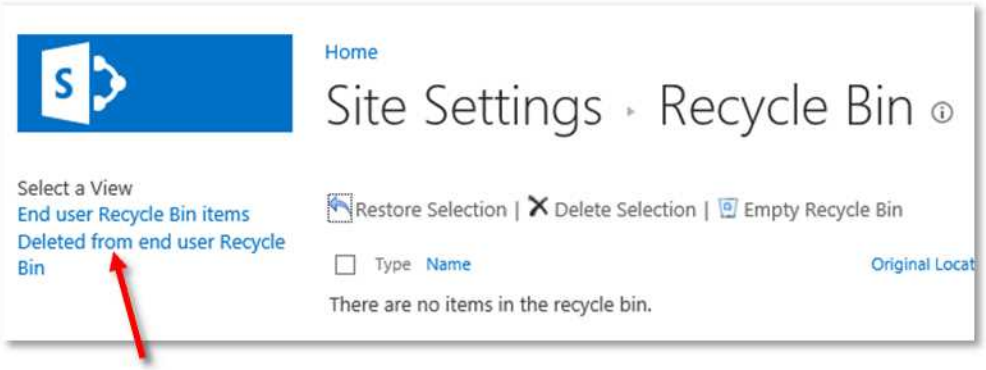


Click the ***Recycle bin*** link



If the recycle bin contains an instance of the app, either select it and use the ***Delete Selection*** button or simply use the ***Empty Recycle Bin*** link.

Navigate to the second stage recycle bin.



If the recycle bin contains an instance of the app, select it and use the ***Delete Selection*** button.

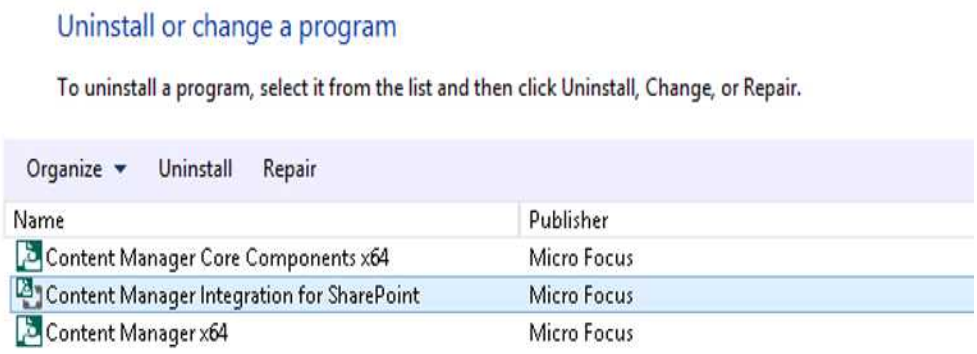
7.3 Removing the Content Manager Components

The removal of Content Manager SharePoint components must be performed on every server in the Content Manager farm.

7.3.1 Uninstallation

The removal of the components installed on the Content Manager workgroup server can be instigated through the machine **Add or remove programs** feature

Select the **Content Manager Integration for SharePoint 2013** entry in the **Add or remove programs** and click the **Uninstall** button.



7.3.2 Manual removal of remaining files

In some cases, there will be files remaining after the installation has completed.

To remove them, navigate to the installation directory. By default this is:

```
[Program Files]\Micro Focus\Content Manager\Content Manager SharePoint Integration
```

Delete this directory to remove all remaining files.

7.3.3 Removal of any shared Content Manager farms

Any shared Content Manager farms created must be manually removed. See the Removing a shared Content Manager farm section for details.

8 Appendix: Performance planning

This section provides information that will allow you to calculate hardware requirements for Content Manager as well as performance configuration requirements for SharePoint itself.

8.1 How the app performs work

The Content Manager Governance and Compliance app uses a centralized job queue, to manage and action requests from multiple web applications and site collections. The benefits of using a queue are:

- Improved user experience - A virtual elimination of waiting times for users performing management and configuration actions. Even though an action may impact thousands of SharePoint items, the user will not have to wait for that action to complete, and can carry on working. The action itself is carried out asynchronously in the background.
- Failover protection – With multiple servers in the Content Manager farm, if one server goes down, the other will continue to process jobs, with no interruption in service.
- Robustness – If jobs fail for any reason, an automatic mechanism retries the job a number of times.
- Scalable – Jobs are processed as resources become available. Scale up and out are both supported to manage workload.

8.1.1 What is a job?

A job is raised for a number of different actions performed in day-to-day interaction with the ***Content Manager Governance and Compliance*** app. When a job is raised, it is added to the job queue in a pending state. The job service takes jobs in a pending state and processes them. A job can either perform a single, or multiple tasks, and includes actual management of content along with configuration tasks (Applying Lifetime Management Policies, Content Type mappings etc.)

Single instance jobs

Single instance jobs are jobs that are raised to perform a job that only needs to be performed once. For example, a request to manage an item is carried out by a single instance job.

These types of jobs form the bulk of the jobs raised in day-to-day operation.

Recurring jobs

Recurring jobs are jobs that perform actions that need to be repeatedly run automatically at a pre-defined interval. These jobs will always have instances in the scheduled view, and do not require any manual intervention. Once a recurring job runs, it automatically adds another instance of itself in a pending state, to be run at a scheduled time. The job queue

8.1.2 What is the job queue

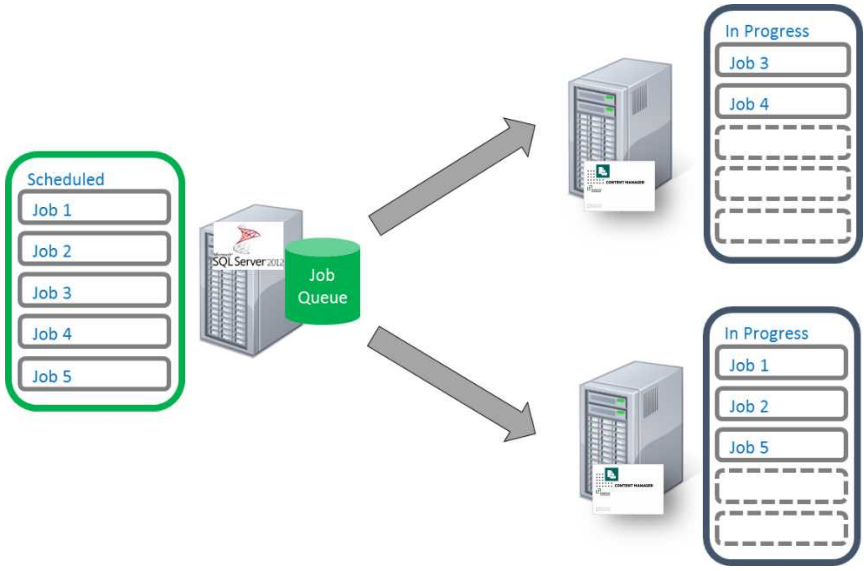
The job queue is a centralized list of all jobs in the Content Manager Farm, it includes all jobs that are due to be processed, are currently running, have completed or have failed. The queue is also a useful area to identify any issues with the ***Content Manager Governance and Compliance*** app, information from the queue can help administrators and Content Manager Support to understand the nature of the problem. It can also be used to understand how the app is being used, where content in SharePoint is being managed, and who is raising manual management actions. It is only possible to see jobs for the particular tenant's job queue.

8.1.3 How are jobs distributed from the queue

The job queue is accessible by all the servers in the Content Manager farm. That is, all workgroup servers that have the ***Content Manager integration for SharePoint*** installed and configured on them.

Each server runs the ***Content Manager SharePoint Service***, as a local Windows service. This is responsible for coordinating the job queue. The number of jobs that a server can run concurrently is based on the value entered in the configuration tool for the server's ***Maximum job count*** property. If a server is not currently processing its maximum number of jobs, it will take jobs from the job queue to process.

In the following example, both servers are configured with a ***Maximum job count*** of 5.



This means that the maximum number of concurrent running jobs equal to the sum of the ***Maximum job count*** for all servers you have configured in the Content Manager farm.

Job prioritization

Jobs are predominantly processed in the order that they are added to the queue, however, some types of jobs are given priority over other jobs. The following are the general guidelines that are used to determine the priority of a job.

1. Respond to direct management requests or changes that trigger LMPs as soon as possible
2. Correct anything that affects security as soon as possible
3. Perform administration style jobs when resources permit but ahead of backlog jobs
4. Perform backlog jobs (ie processing LMPs on existing content at the time of application of a LMP) when resources permit

8.1.4 Increasing the number of jobs that are processed

In the example above, because both servers are configured with a Maximum job count of 5, the maximum number of jobs that will ever be processed simultaneously is 10.

Adding workgroup servers to the farm

Adding additional workgroup servers to the farm provides a simple mechanism for scaling out the job queue processing capacity. In the previous example, adding a third workgroup server would result in a total of 15 jobs that could be processed simultaneously.

Increasing the number of jobs a server can process

The configuration tool used for the Content Manager Governance and Compliance app allows specifying how many jobs each workgroup server should process simultaneously. It is possible to specify varying numbers for each server to accommodate the individual capacity of each.

Of course the number of jobs that a workgroup server can process will be limited by the resources of that machine. There will come a point where processor and memory use is at capacity for that machine. Increasing the number of jobs processed by that machine beyond that point will not result in any performance gain as all jobs will simply take longer resulting in the same throughput.

As a guide, the number of jobs being processed should not cause the resource usage to be consistently more than 80% of machine capacity.

Considering SharePoint's capacity

The number of requests that SharePoint can accept for a particular app is deliberately limited using a process called ***throttling***. Throttling prevents one particular app from consuming too many SharePoint resources.

When throttling occurs, SharePoint will deny access to the app for a period of time. During this time it returns the following errors:

```
HTTP/1.1 429 Too Many Requests
```

Additionally, in the ULS logs, the following messages are included:

```
ResourceBudgetExceeded, sending throttled status code.
Exception=Microsoft.SharePoint.SPResourceBudgetExceededException:
ResourceBudgetExceeded at
Microsoft.SharePoint.SPResourceTally.Check(Int32 value) at
Microsoft.SharePoint.SPAggregateResourceTally.Check(SPResourceKind kind, Int32
value) at Microsoft.SharePoint.Client.SPClientServiceHost.OnBeginRequest()
```

Throttling is performed at a web application level. This means that if an app is being throttled on one site collection, all other site collections on that web app are also subject to throttling.

When the number of jobs being processed by the Content Manager Governance and Compliance app is high, SharePoint throttling can be encountered.

Modifying SharePoint's throttling level

It is possible to increase the point at which SharePoint will throttle requests. The involves modifying the amount of time that a sustained number of app requests can access SharePoint before throttling occurs. By default this value is 150000ms.

For on premise installations, you can increase this value using the following Powershell script (this example will increase to 450000ms)

```
$webapp = Get-SPWebApplication -Identity http://< web app url>
$webapp.AppResourceTrackingSettings.Rules.Add(
[Microsoft.SharePoint.SPResourceKind]::ClientServiceRequestDuration, 450000,
450000)
```

Increasing this value may be helpful in situations where job processing is not consistently high and only have periods of high workload.

Where SharePoint throttling becomes an issue due to consistently high numbers of jobs, throttling can be disabled altogether using the following script.

```
$webapp = Get-SPWebApplication -Identity http://<web app url>
$rule = $webapp.AppResourceTrackingSettings.Rules.Get(
[Microsoft.SharePoint.SPResourceKind]::ClientServiceRequestDuration)
rule.Remove()
```

It is not possible to modify throttling in SharePoint Online. The following article describes SharePoint Online throttling: https://msdn.microsoft.com/en-us/library/office/dn889829.aspx

Adding servers to the SharePoint farm

During peak job processing periods, the resource usage of SharePoint servers will be increased. Should the resources be found to be consistently over 80% utilization, the addition of more servers to the SharePoint farm will result in the ability to process jobs faster.

Automatic job throttling

The processing of jobs will automatically throttle the number of jobs being processed when SharePoint throttling is encountered. Jobs will pause for a period of time while waiting for SharePoint to finish the throttling period.

If after restarting, SharePoint throttling is encountered again, the number of jobs being processed simultaneously is reduced by 20%. This change will be reflected in the value of simultaneous jobs configured in the configuration tool.

If throttling is continually encountered, the number of processing jobs will continue to be reduced by 20% down to a minimum of 10 simultaneous jobs.

8.1.5 Job removal

When a Tenant is removed from the Configuration Tool Tenant Settings or a trial period expires all pending jobs for that customer will be removed and no new jobs will be created.

8.2 Phases of implementation

Implementation of the Content Manager Governance and Compliance app usually occurs on an already established SharePoint implementation. The implementation can be considered to occur in three phases.

8.2.1 Backlog phase

An existing SharePoint farm will have existing content. Usually the Content Manager governance and compliance app is being implemented not only to provide governance to future content but also for existing content. During initial implementation there may be a large amount of content that needs to be governed that is disproportionate to the typical amount of content to be dealt with.

For example, at implementation time, an organization may have 1 Million items that need to be managed however, on average they only expect 250k new items to be created every year.

The period of time where this existing content is being managed is referred to as the ***Backlog phase***.

It is important to separate this phase as a significant number of additional servers may be required during this time to complete the backlog phase in the time expected by the organization.

For new SharePoint implementations, there is no backlog phase.

8.2.2 Ongoing phase

Once the backlog of existing content has been completed, the phase that refers to the "business as usual" management of content being created on a day to day basis is referred to as the ***Ongoing phase***.

8.2.3 Crossover phase

There is usually a period where both the backlog and the ongoing phase are concurrent. During initial implementation, whilst the existing content is being governed, users are still in a "business as usual" stage where new content is being created. This period is referred to as the ***Crossover phase***.

For new SharePoint implementations, there is no crossover phase.

8.3 Hardware calculations

The size of the necessary hardware will vary significantly from organization to organization. It is dependent on a number of factors. This section provides guidance for how to determine the number of servers that are necessary.

Regardless of the number of servers calculated using these metrics, it is strongly recommended that a minimum of two Content Manager servers are always employed to provide failover protection should one server become unavailable.

8.3.1 Machine specifications

Figures quoted in this section are based on servers with the following specifications:

Processor	Quad core 2.6Ghz
RAM	16Gb

8.3.2 Required timeframes

It is important to understand what metrics need to be achieved. The following are the key ones that should be understood:

Backlog phase duration: how long can be allocated for the backlog phase to complete

Management delay: during the ongoing phase, how long is acceptable as a duration from the point where an item becomes eligible to be managed (either via LMP or manually) till it is actually managed.

8.3.3 Content sizing

Understanding the size of the amount of content both initially and ongoing is key to determining the resource requirements. You will need to know the following information, even if only approximately, in order to determine hardware requirements.

8.3.4 Content sizing – backlog phase

Total content sizing

The details in this section are about the size of the current SharePoint implementation. This is all current content, regardless of whether the content is to become a record or not.

	Value
Number of SharePoint farms	
Total number of site collections	
Total number of documents	
Total number of metadata items	

Managed content sizing

The details in this section describe the portion of the total content sizing that is expected to become a record during the backlog phase.

	Value
Total number of documents	
Total number of metadata items	

Relocated content sizing

The details in this section describe the portion of the total content sizing that is expected to be relocated or archived during the backlog phase.

	Value
Total number of documents	
Average document size	

8.3.5 Content sizing – ongoing phase

Total content sizing

The details in this section describe the expected amount of content to be created during the ongoing phase, regardless of whether it is to become a record or not.

	Value
Total documents added per day	
Total metadata items added per day	

Managed content sizing

The details in this section describe the expected amount of content to be created during the ongoing phase, that will become a record.

	Value
Total number of documents per day	
Total number of metadata items per day	

Relocated content sizing

The details in this section describe the portion of the total content sizing that is expected to be relocated or archived during the backlog phase.

	Value
Total number of documents	
Average document size	

8.3.6 Performance metrics used

The following describe the rate of processing by the Content Manager Governance and Compliance app for various tasks. All values are based on one server only.

Application of LMPs

This is the application of LMPs to existing content. This does not include the time taken to apply management to the item. Management processes must be considered in addition to the application of LMPs.

Items per minute	200
Items per hour	12000
Items per day	288000

In place manage/finalize (no security)

This is the management or finalization of an item where security is not turned on for the site.

Items per minute	33
Items per hour	1980
Items per day	47520

In place manage/finalize (with security)

This is the management or finalization of an item where security is turned on for the site.

Items per minute	23
Items per hour	1411
Items per day	33864

Relocate/archive documents

This is the relocation or archiving of an item that has a 500Kb document associated with it.

Items per minute	24
Items per hour	1440
Items per day	34560

Relocate/archive metadata items

This is the relocation or archiving of an item that does not have a document associated with it.

Items per minute	29
Items per hour	1777
Items per day	42648

8.3.7 Backlog phase calculations

Calculating the required number of servers to complete the backlog requires determining the requirements for applying LMPs and the requirements for processing actions from the LMP. Using the performance metrics, it can be calculated how many days a single server would take to perform each task.

Once this duration has been calculated, then it is divided by the number days that the backlog duration should take to determine the number of servers. In the examples below, a backlog duration of 30 days has been used.

All tables in the following sections contain example figures. Items per day has been calculated using the metrics in the Performance metrics used section.

Application of LMPs to all items

Total items	42M document + 2.3M metadata = 44.3M
Items per day	288000
Single server time	154 days
Servers required to meet backlog duration	5.2

Management/finalization of non secure items

Total items	242k document + 13k metadata = 255k
Items per day	47520
Single server time	6
Servers required to meet backlog duration	.2

Management/finalization of secure items

Total items	100k document + 20k metadata = 120k
Items per day	33864
Single server time	4
Servers required to meet backlog duration	.2

Relocate/archive documents

Total items	350k
Items per day	34560
Single server time	11
Servers required to meet backlog duration	.4

Relocate/archive metadata items

Total items	50k
Items per day	42648
Single server time	2
Servers required to meet backlog duration	.1

Total number of servers

Application of LMPs to all items	5.2
Management/finalization of non secure items	.2
Management/finalization of secure items	.2
Relocate/archive documents	.4
Relocate/archive metadata items	.1
Total Servers required to meet backlog duration	**7 (rounded up from 6.1)**

8.3.8 Ongoing phase calculations

The ongoing phase calculations are based on calculating how many items per minute require processing then dividing it by the per minute rate that is achievable by a single server. Then dividing that figure by the number of minutes that are acceptable for the management duration.

In the examples below, the management duration used is of 1 minute has been used.

All tables in the following sections contain example figures.

Application of LMPs to all items

Total items per month	16040000
Items per day	517419
Items per hour	21559
Items per minute	359
Single server rate/min	200
Servers required to meet metrics	1.8

Management/finalization of non secure items

Total items per month	273250
Items per day	8814
Items per hour	367
Items per minute	6
Single server rate/min	33
Servers required to meet metrics	.2

Management/finalization of secure items

Total items per month	273250

Items per day	8814
Items per hour	367
Items per minute	6
Single server rate/min	33
Servers required to meet metrics	.2

Relocate/archive documents

Total items per month	500000
Items per day	16129
Items per hour	672
Items per minute	11
Single server rate/min	24
Servers required to meet metrics	.5

Relocate/archive metadata items

Total items per month	26000
Items per day	838
Items per hour	34
Items per minute	1
Single server rate/min	29
Servers required to meet metrics	.1

Total number of servers

Application of LMPs to all items	1.8
Management/finalization of non secure items	.2

Management/finalization of secure items	.2
Relocate/archive documents	.5
Relocate/archive metadata items	.1
Total Servers required to meet metrics	**3 (rounded up from 2.8)**

8.3.9 Crossover phase calculations

The total number of servers required during the cross over phase is the number calculated for the backlog phase plus the number required for the ongoing phase.

Using the examples in the previous sections, this organization would require 10 servers during the crossover phase.

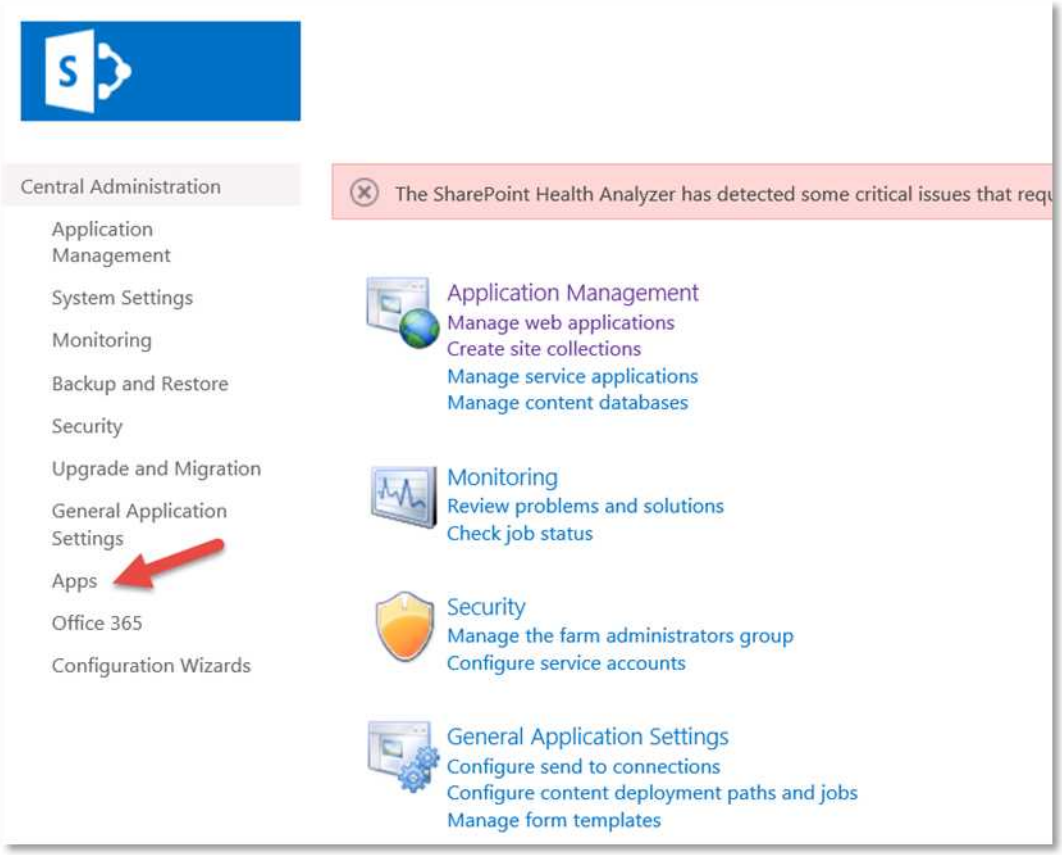
Note that the example figures used are for a large organization creating a significant amount of content.

9 Appendix: SharePoint administration tasks

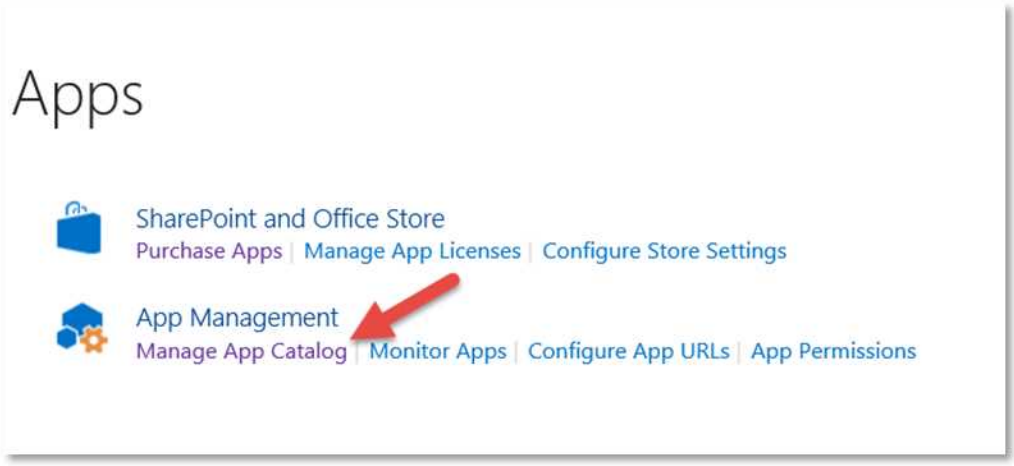
9.1 Identifying the app catalog in use

9.1.1 On premise installations

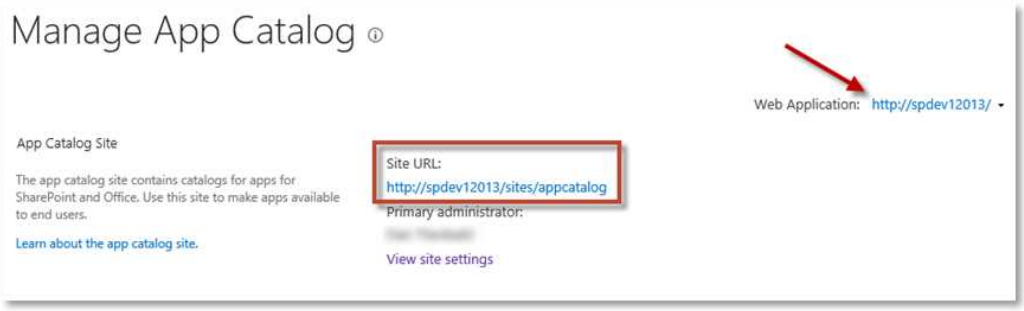
Go to SharePoint Central Administration, and click on the **Apps** link in the navigation pane



Click on the **Manage App Catalog** option



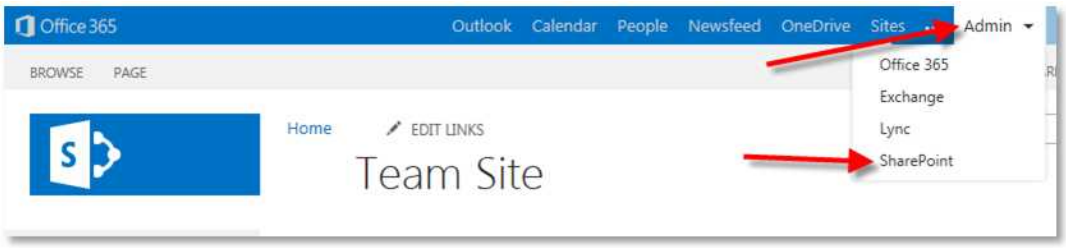
Ensure you have the correct web application selected, and note the Site URL, this is your app catalog.



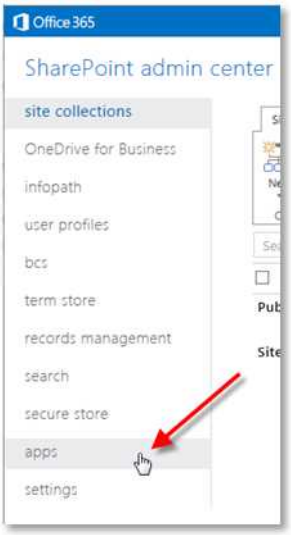
If you select the correct web application but do not see a site URL, then you do not have an app catalog configured for this web application. Go to the section below *'Creating an app catalog – On Premise'*

9.1.2 SharePoint Online

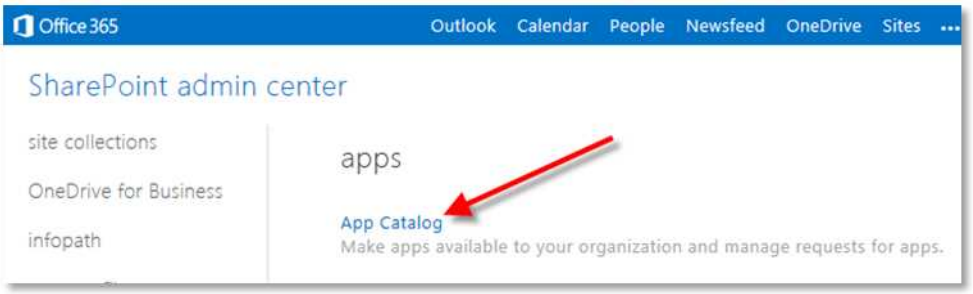
Login to your Office 365/SharePoint Online portal, as a tenant administrator, and click on the **Admin → SharePoint** menu item.



From the left-hand navigation pane, click on **Apps**.



Click on the **App Catalog** link.

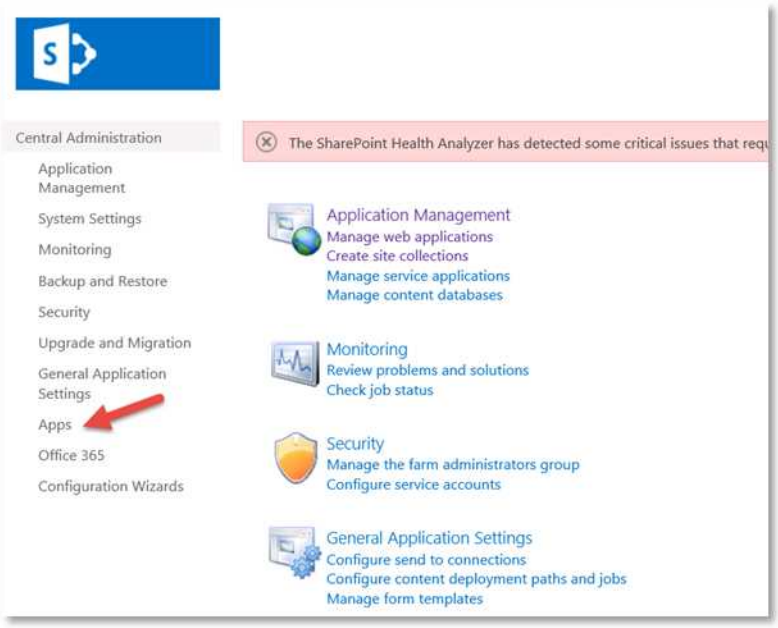


9.2 Creating an app catalog

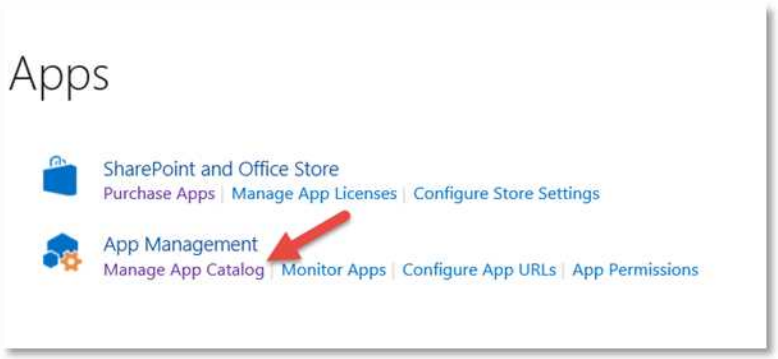
9.2.1 On Premise

If you do not already have a corporate app catalog within your SharePoint content web application, then you need to create one. Understanding apps, and the general app architecture, is outside the scope of this document, but here are some basic steps to create an app catalog suitable for testing/proof-of-concept work.

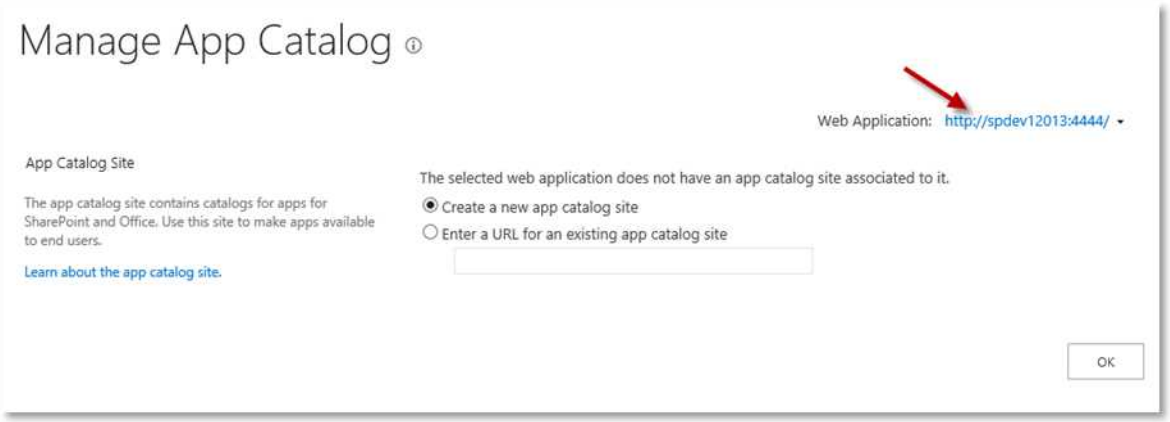
Go to SharePoint Central Administration, and click on the **Apps** link in the navigation pane



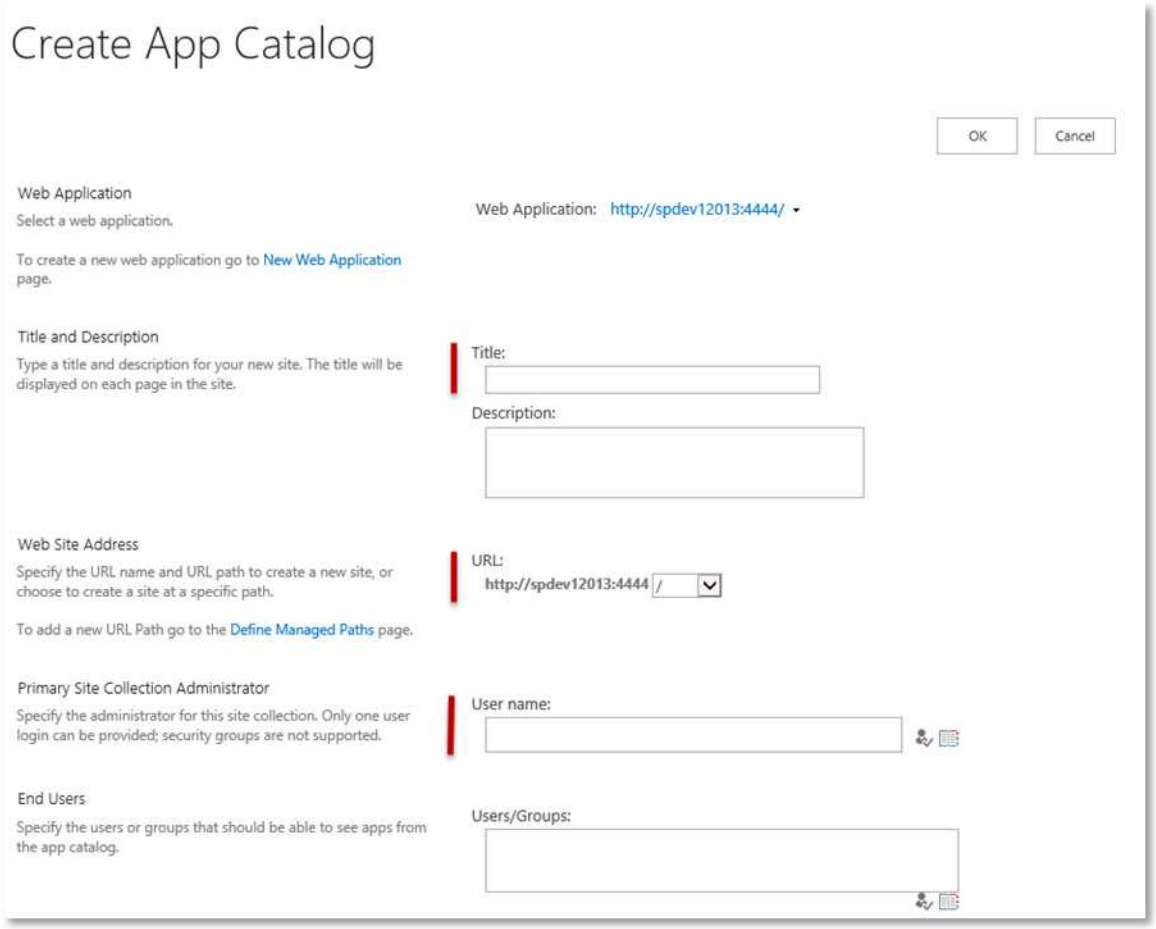
Click on the **Manage App Catalog** option



On this page, select your content web application, choose the **Create a new app catalog site** option, and click OK.

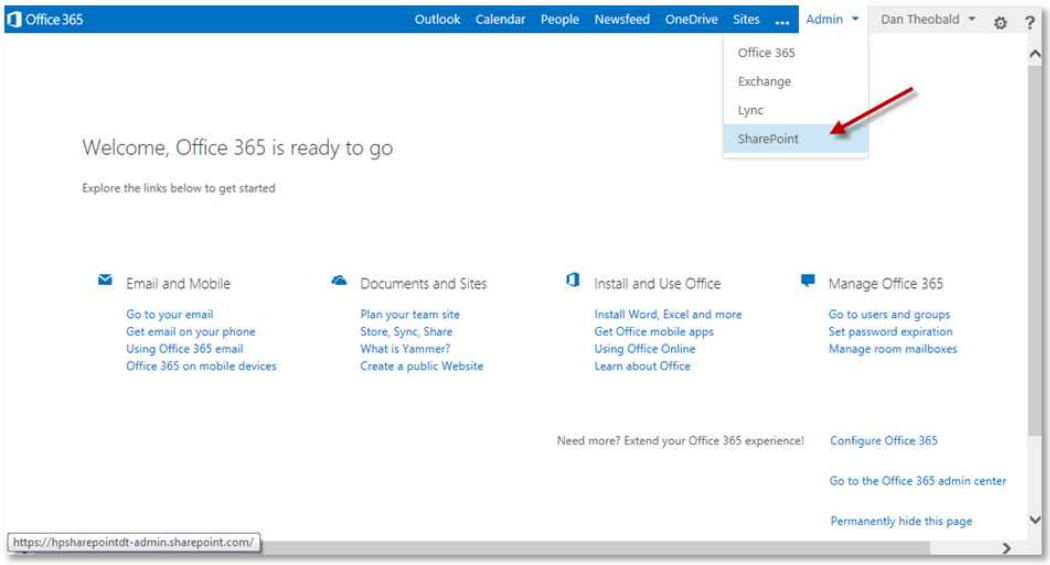


The app catalog lives in its own Site Collection. At a minimum, provide the values for **Title, URL, Site Collection Administrator** and click on the **OK** button.

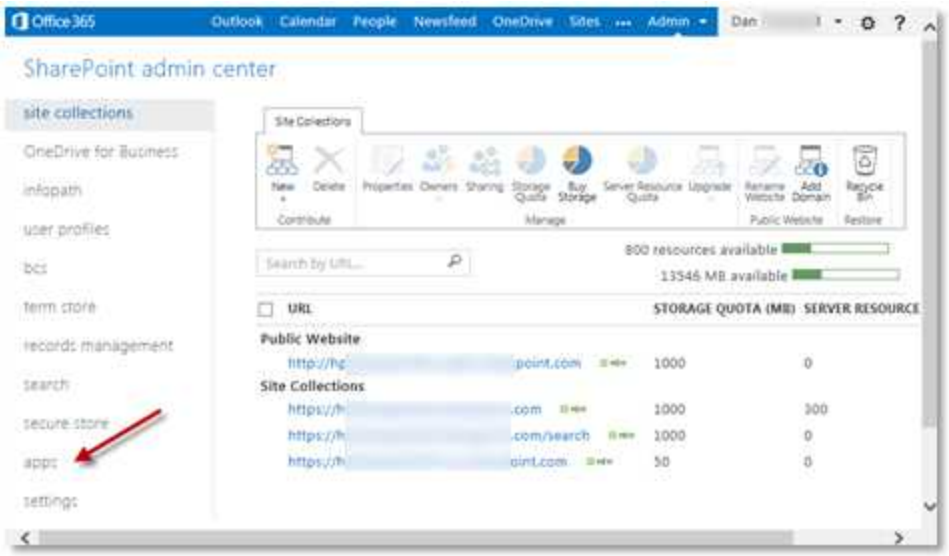


9.2.2 SharePoint Online

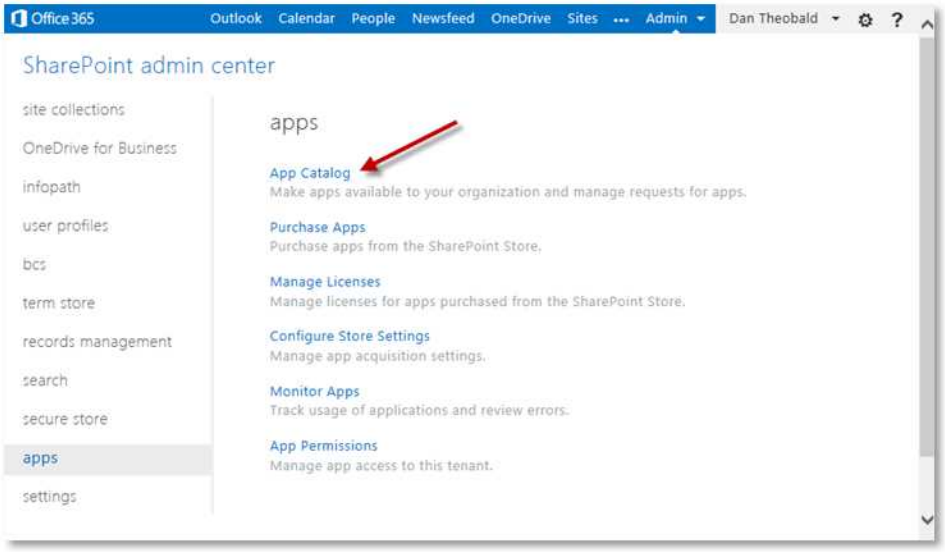
Login as a tenant administrator, go to the **Admin** menu at the top right, and click on **SharePoint:**



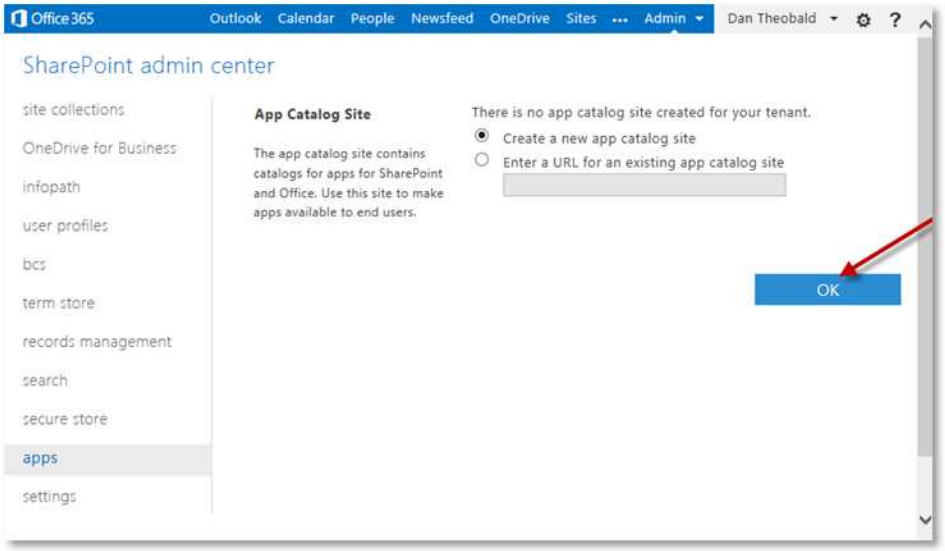
In the SharePoint admin center, you can see a list of site collections. On the left-hand menu, click on **apps**.



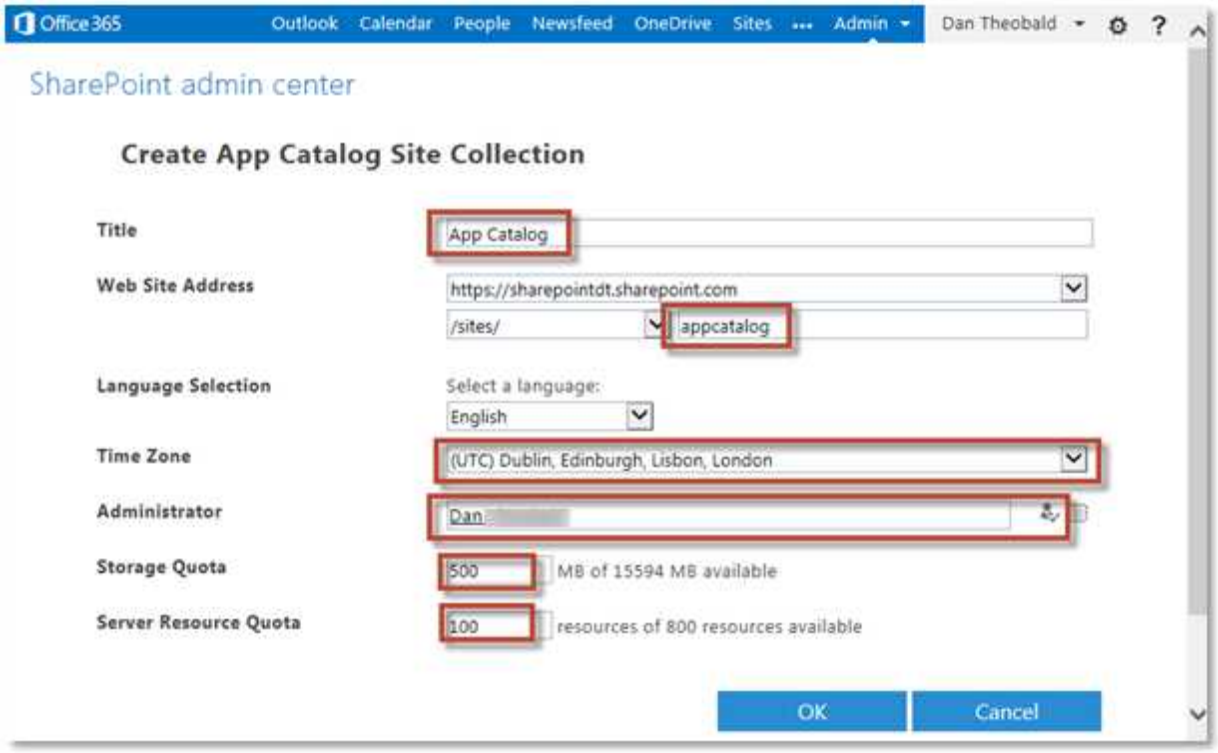
Now click on **App Catalog**



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 (See examples below).

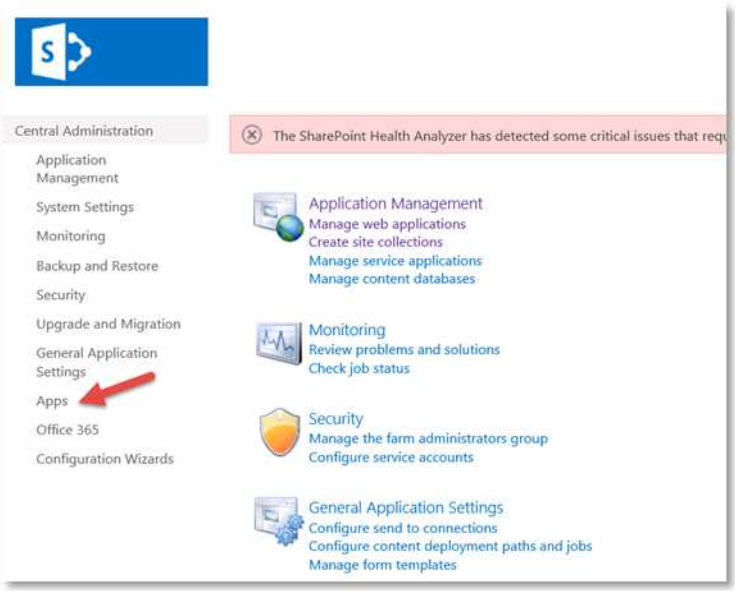


Click **OK** to provision the app catalog. This will take you back to the Admin Center.

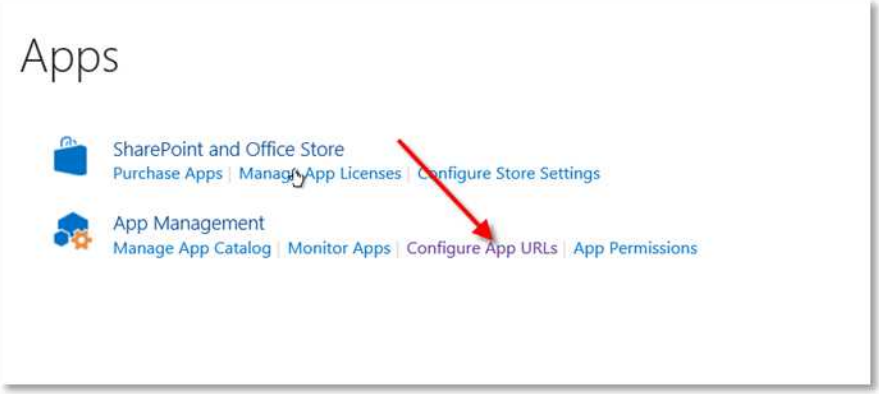
9.2.3 Configuring App URLs – On Premise only

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

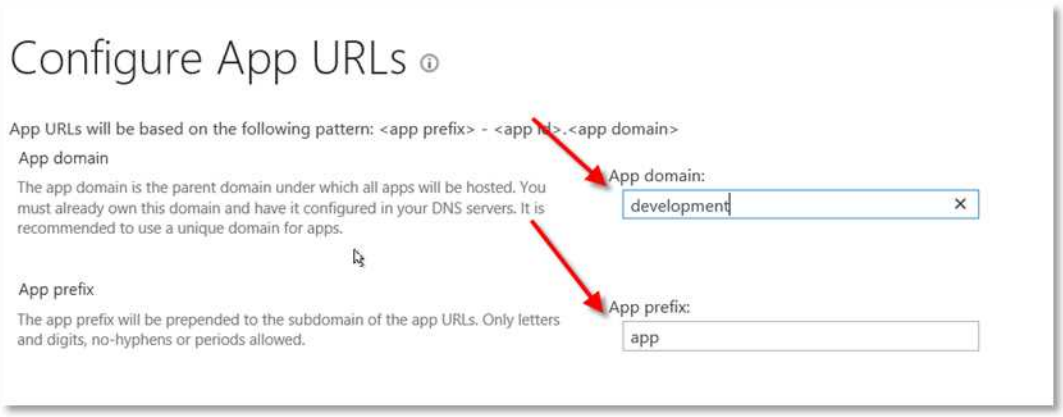
Go to SharePoint Central Administration, and click on the **Apps** link in the navigation pane



Click on the **Configure App URLs** link



Enter your domain name and enter a prefix you would like to see to indicate app URLs. For example *'app'*. Then click **OK.**



9.3 Troubleshooting app issues

This section describes some of the issues we have encountered whilst testing and developing the app. These articles are aimed at SharePoint Farm Administrators, **and include steps that can have a serious impact on the SharePoint Farm if not carried out correctly**. These are suggestions and observations only, and not stipulations on how to configure SharePoint for apps.

9.3.1 Adding the App - Error is received: 'Sorry, apps are turned off. If you know who runs the server, tell them to enable apps'

If you receive the following error when trying to add the app to a site, it may be because the Subscription Settings Service Application is not configured.

> "Sorry, apps are turned off. If you know who runs the server, tell them to enable apps."

First check in Central Administration to see if there is a provisioned Subscription Settings service

application. If not, you can use the example PowerShell script in the *Creating a Subscription Settings Service Application* appendix below, or you can choose to create one manually.

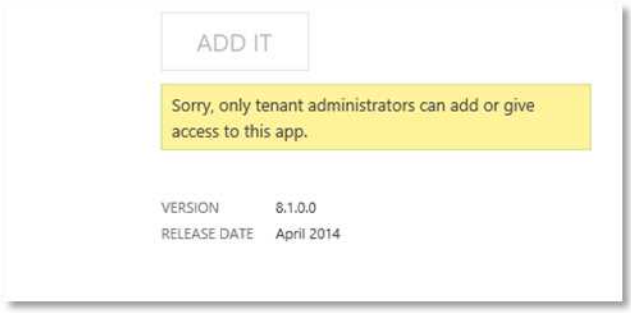
Once successfully completed, you need to configure app URLS, see the *Configuring app URLs – On Premise only* section above for details.

Once configured, perform an **iisreset** from an elevated command prompt, if still getting the same error, a server restart will be required.

9.3.2 Adding the app – Error is received: You can't add this app here. Details show 'Sorry, only tenant administrators can add or give access to this app.'

When trying to add the app to a site, you see an error stating "You can't add this app here"

And when you click on the "App details" link, you see the following message:



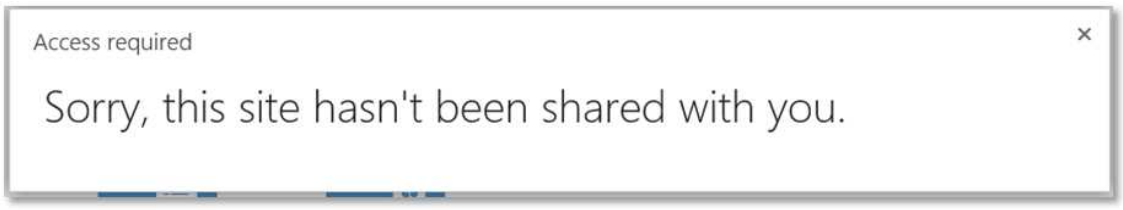
The following errors seem to occur when the **User Profile Synchronization** service has not started on the SharePoint Server.

As a farm administrator, go to **SharePoint Central Administration → Application Management → Manage services on server** and check that the service is in a 'Started' state.

If the service is 'Stopped', and will not start, it will require additional troubleshooting that is outside the scope of this document. Consult Microsoft technical documentation for help with troubleshooting this service.

9.3.3 Adding the app – Error is received: Sorry, this site hasn't been shared with you

There is a known issue with on premise installations that occurs adding an app to a site other than the first site. The following message is shown to the user:



The solution to this is to add the user attempting to add the app, to the local machine administrators group on all SharePoint machines on the SharePoint farm.

This appears to be a SharePoint issue however we are continuing to find a better solution to this issue.

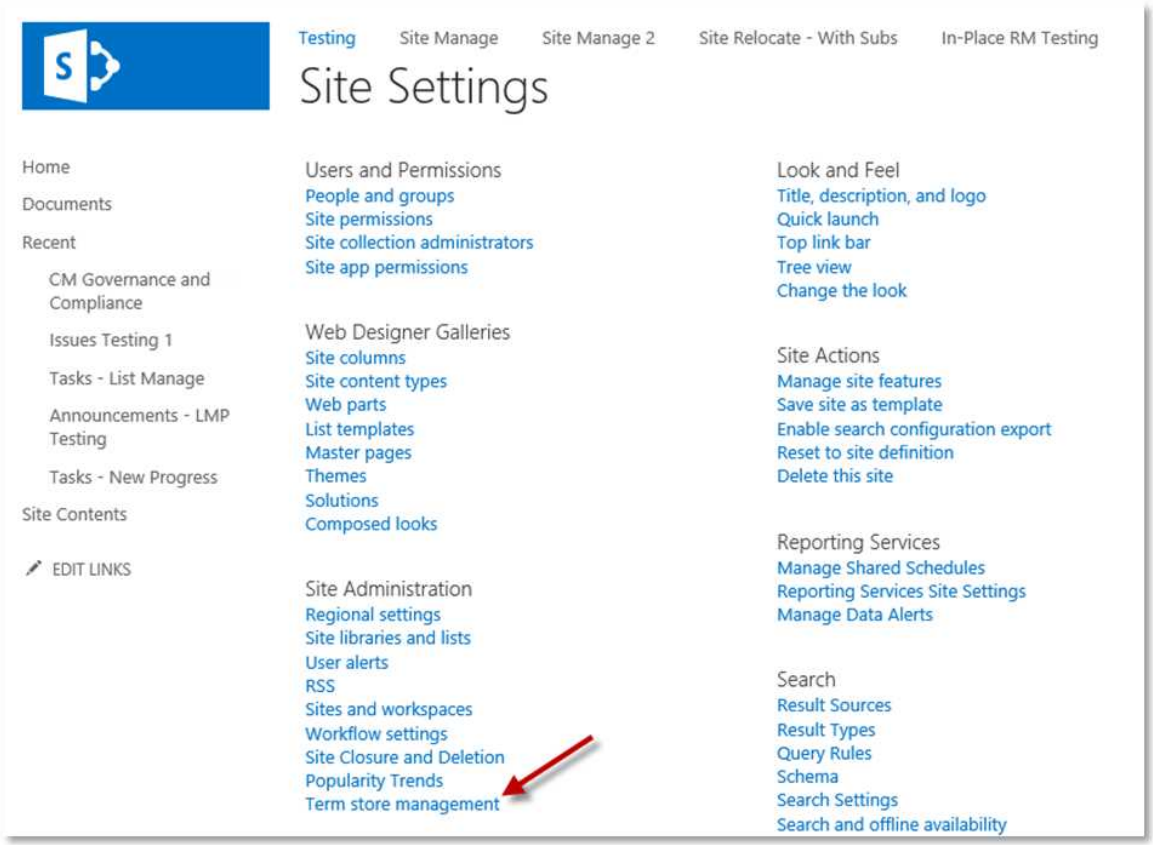
9.4 Working with the term store

9.4.1 Accessing the term store – On Premise

To access the term store:

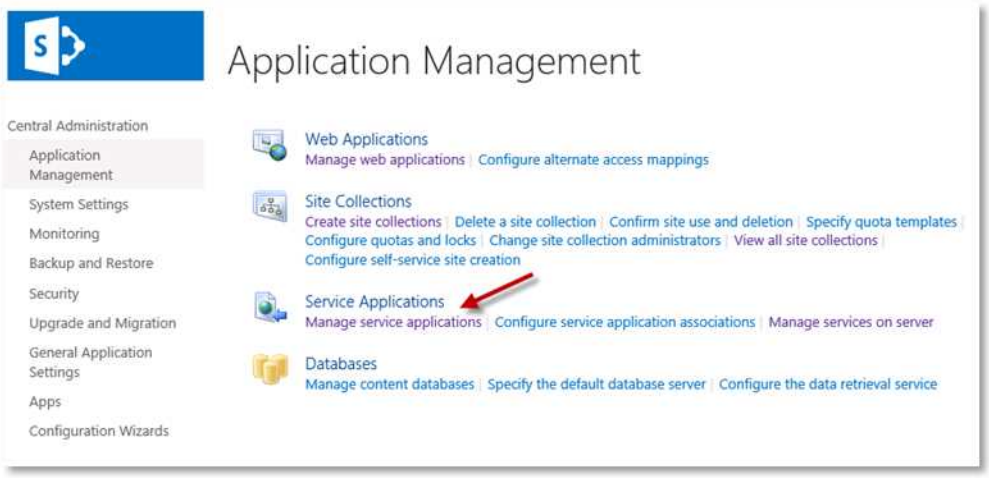
Either:

Go to **Site Settings** on any site, then under the **Site Administration** section, click on the **Term store management** link.

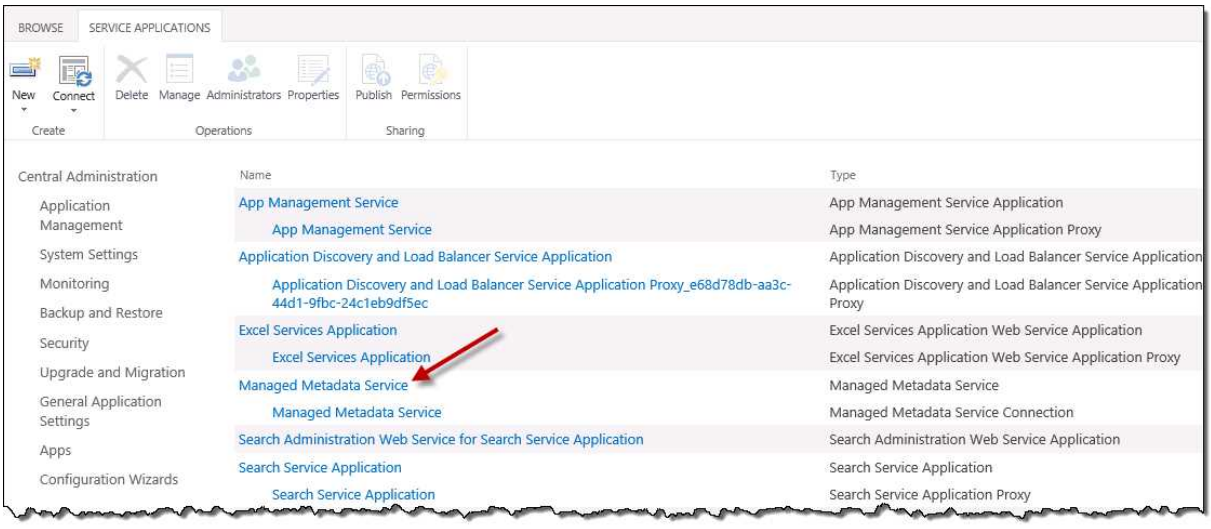


Or:

1. From SharePoint Central Administration, go to **Application Management.**
2. Under **Service Applications** click on **Manage service applications**.

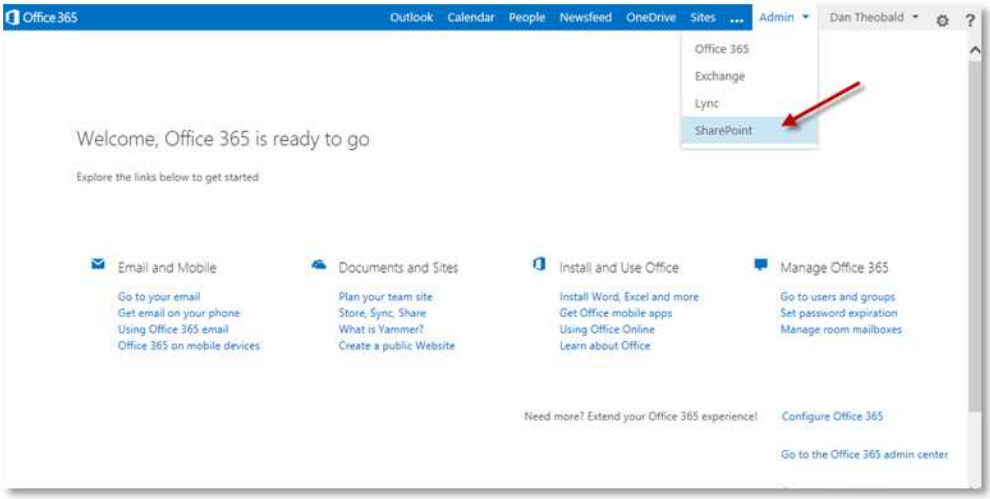


3. On the Service Applications page click on the topmost **Managed Metadata Service** link (Note, this could be named differently within your organization).

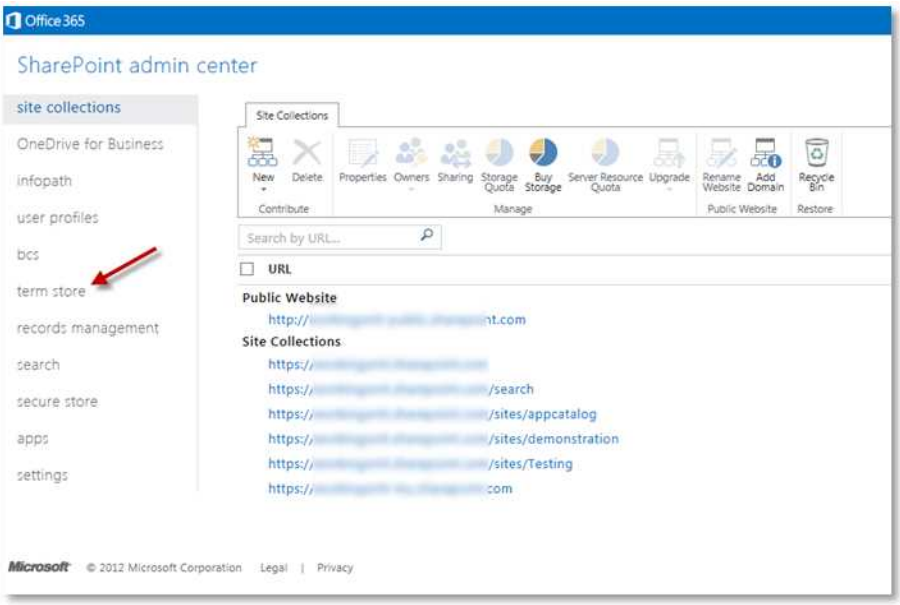


9.4.2 Accessing the term store – SharePoint Online

1. Login as a tenant administrator, go to the **Admin** menu at the top right, and click on **SharePoint**:



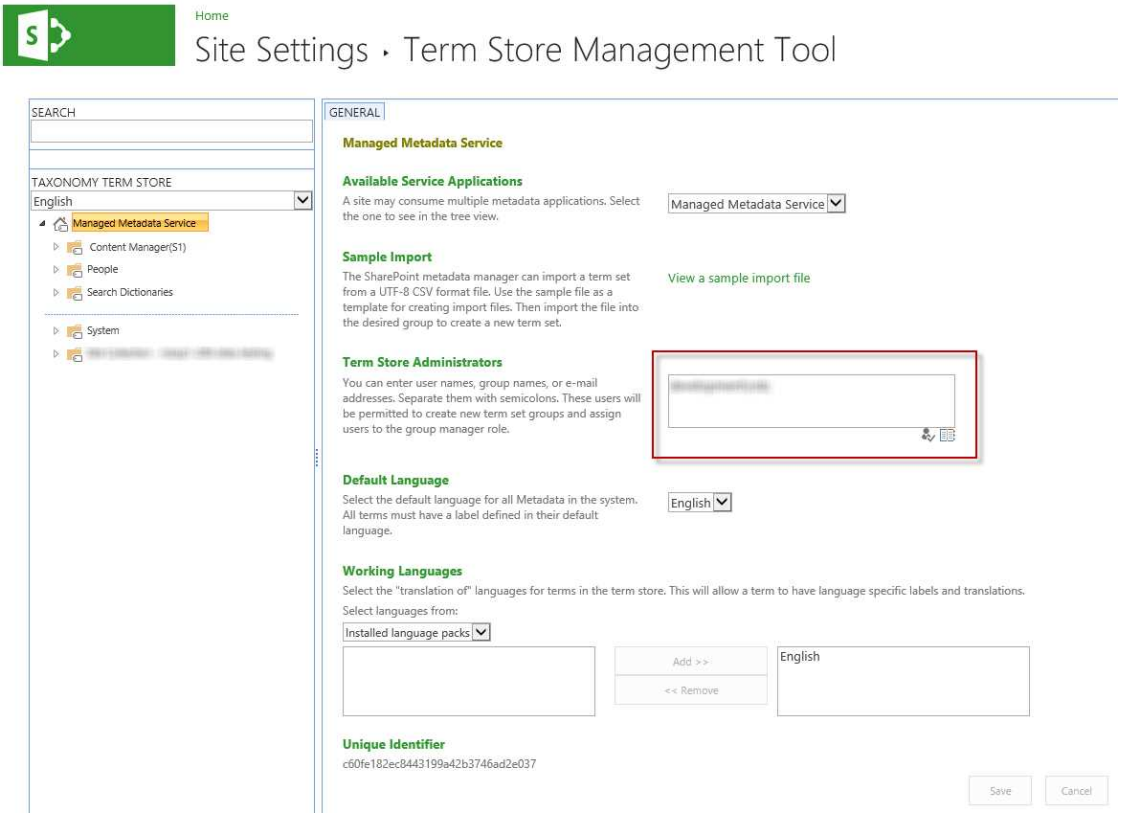
2. In the SharePoint admin center, you can see a list of site collections. On the left-hand menu, click on **term store**.



9.4.3 Adding a term store administrator

This process is the same, whether on premise, or on SharePoint Online.

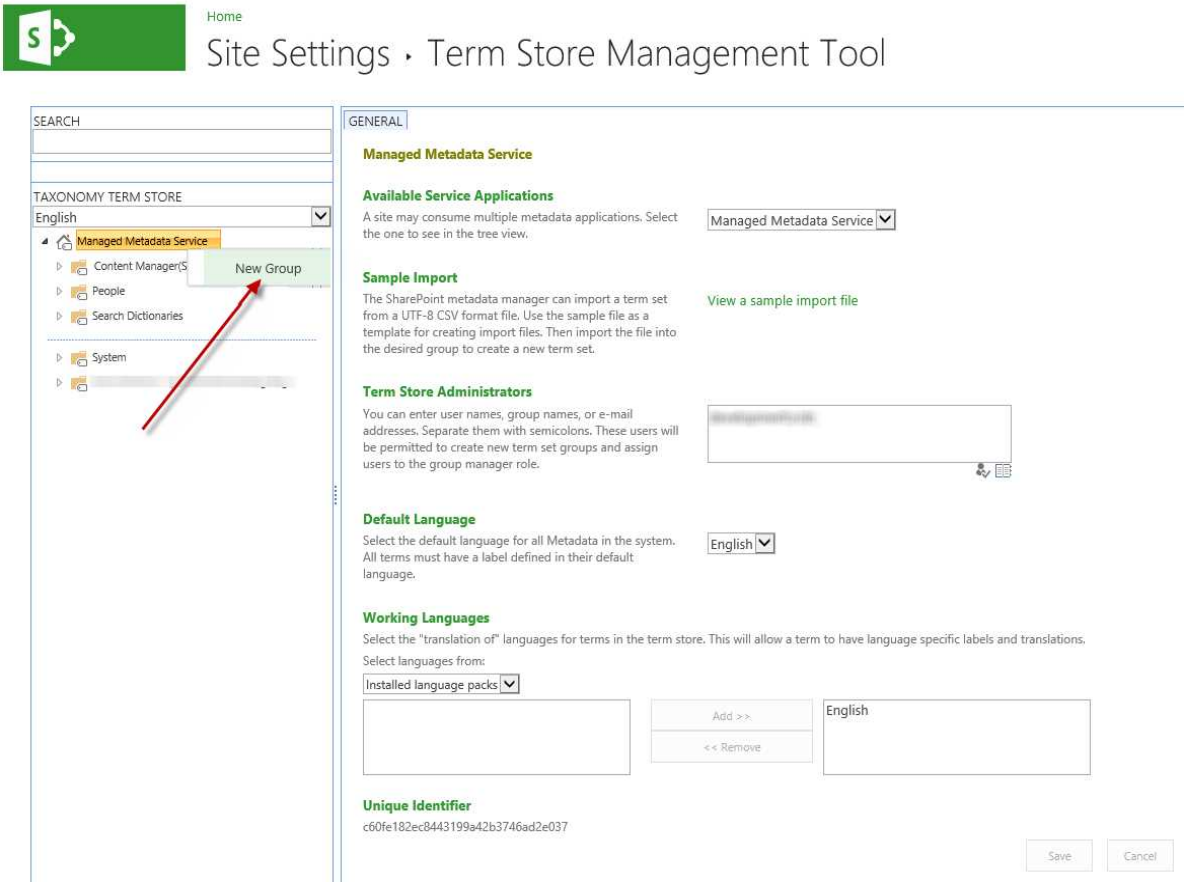
Make sure you have the root of the term store selected in the left-hand pane. Enter the appropriate account into the **Term Store Administrators** field, check the account using the tick icon, then click **Save** to apply.



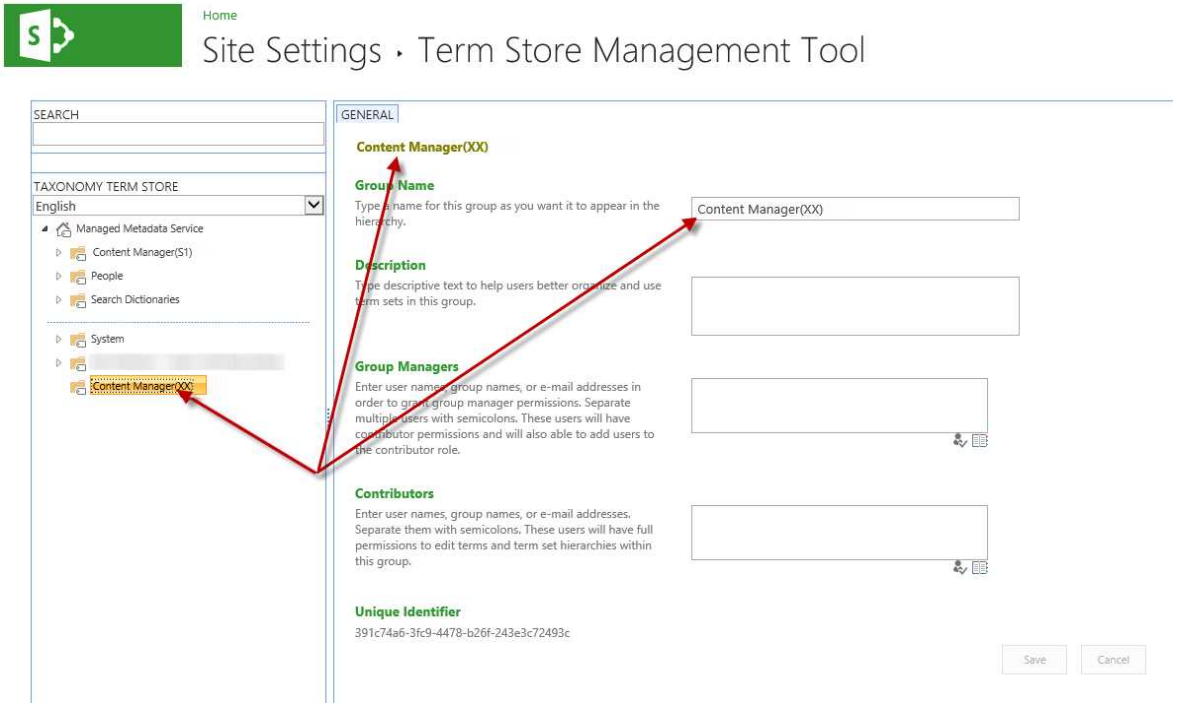
9.4.4 Creating a term store group

This process is the same for both SharePoint Online, and on premise.

In the left-hand navigation pane, click on the ‘Managed Metadata Service’ root drop-down menu and choose **New Group.**



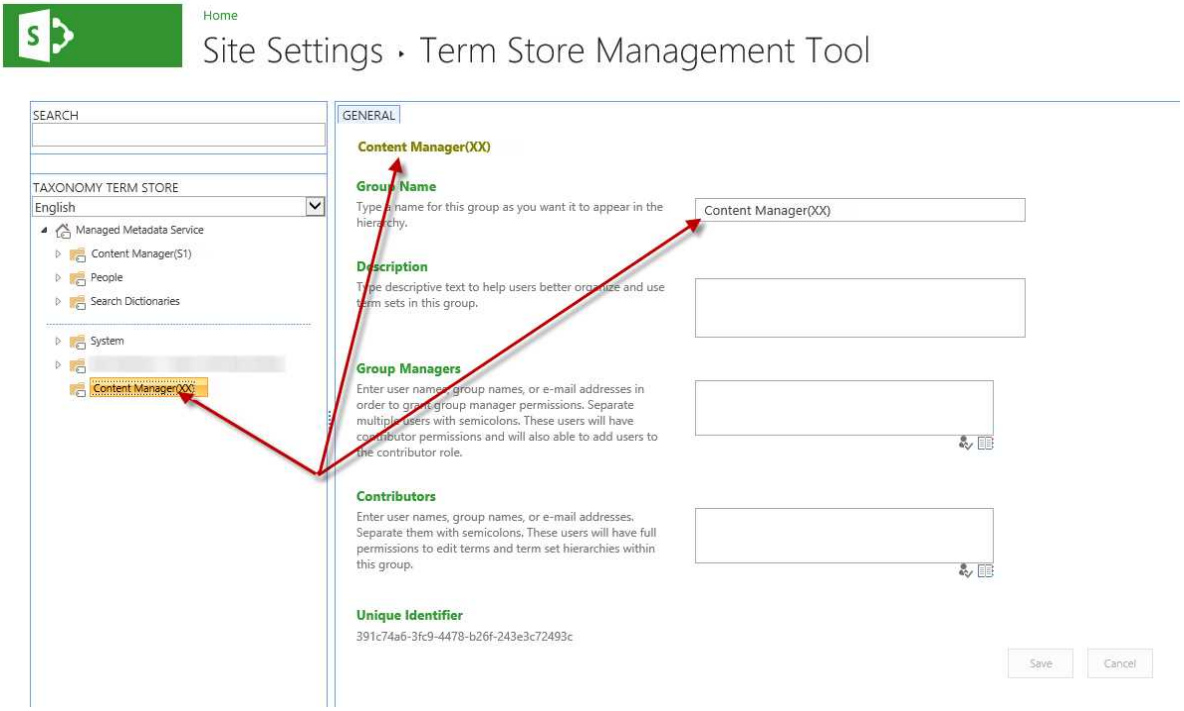
Type the group name in and press return. In the example below I have created a Content Manager group with a database ID of ‘XX’. Once the group has been created, the management page for the group is displayed.



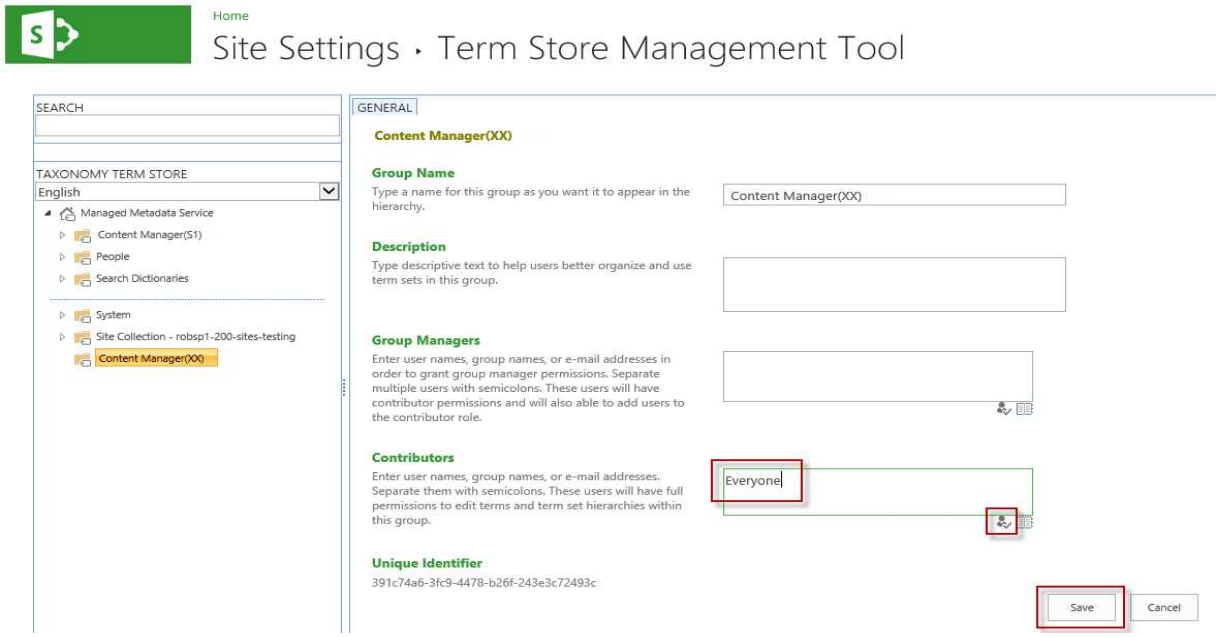
9.4.5 Granting permissions to a term store group

This process is the same for both SharePoint Online, and on premise.

In the left-hand navigation pane, select the appropriate Content Manager group, with the correct database ID. In this example I'm working with a term store group with a database ID of 'XX'.



Add ‘everyone’ to the **Contributors** section, click on the validate icon (Person with a tick), and then click **Save**.

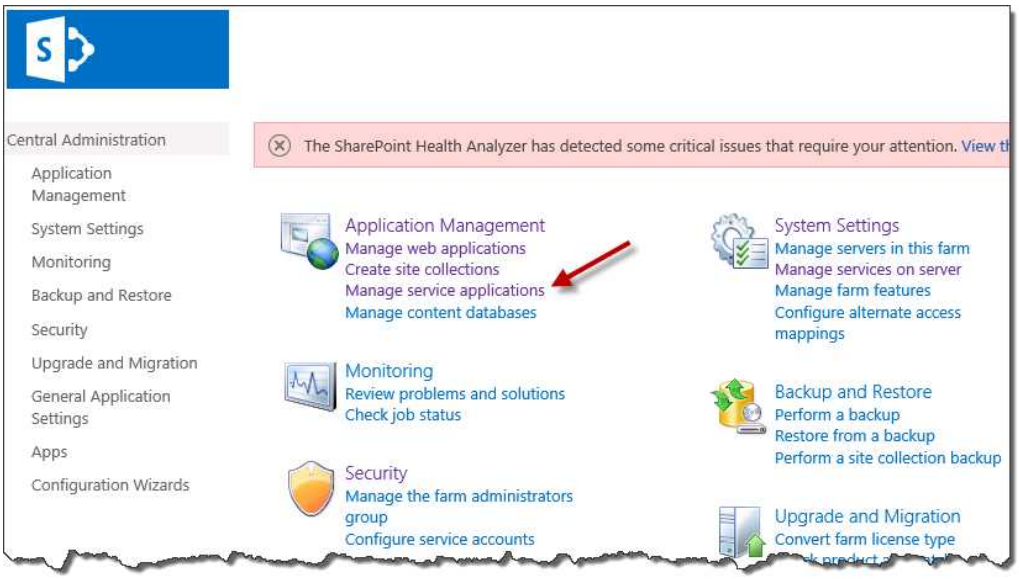


Verify that ‘Everyone’ is saved into the **Contributors** section. Sometimes, the first attempt to save the value doesn’t work, and you need to repeat it a second time.

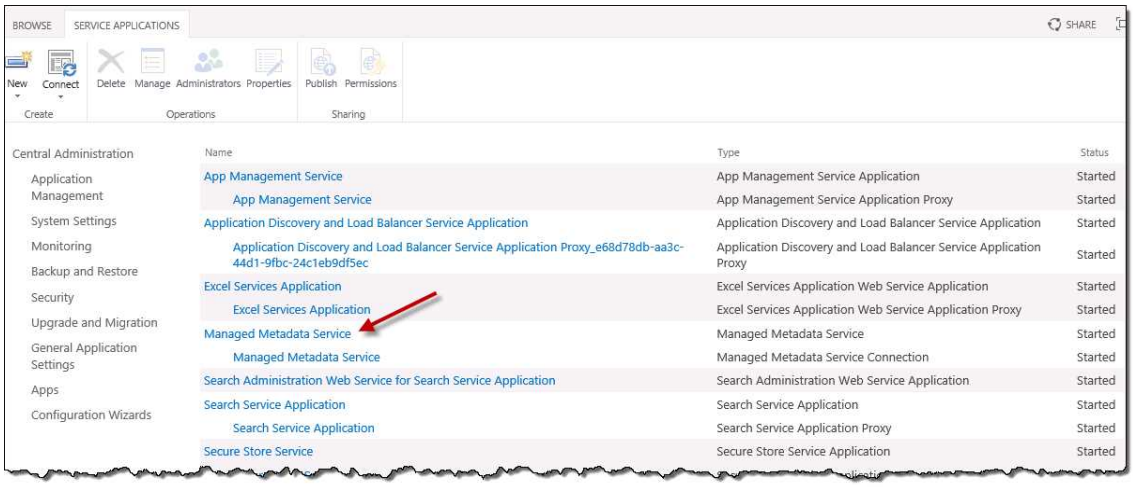
9.5 Accessing service applications

To access SharePoint Service Applications, open SharePoint Central Administration.

From the **Application Management** section, click on the **Manage service applications** link



The service application list will show all service applications on the farm, and importantly, whether or not they are **'Started'**. Click on the required service application link to manage it. Note, that if there are two links, the topmost link goes to the actual service, the bottom link is normally for configuring the associated proxy. In the example below, clicking this link will go to the **Managed Metadata Service**.



9.6 Creating a Subscription Settings Service Application

The following suggested PowerShell script will create a service called ***SettingsServiceApp***. You do not have to use this script to create the application. This is provided to fast track the creation for you. 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.

If you don't use Powershell ISE to run this script, you will need to run it line by line.

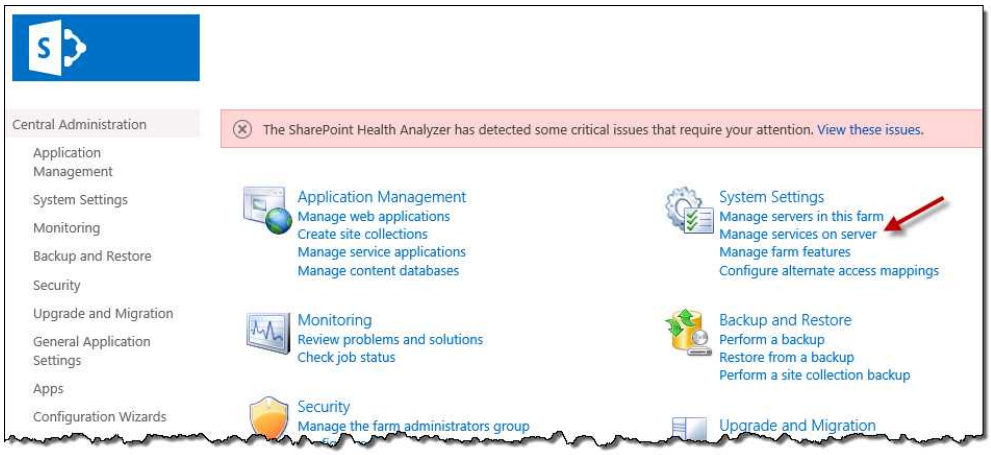
```
Remove-PSSnapin Microsoft.SharePoint.PowerShell -erroraction SilentlyContinue
Add-PSSnapin Microsoft.SharePoint.PowerShell -erroraction SilentlyContinue
$accountName = Read-Host "Enter your timer service account in "domain\username"
format"
$account = Get-SPManagedAccount $accountName
# Gets the name of the Farm administrators account and sets it to the variable
$account for later use.

$appPoolSubSvc = New-SPServiceApplicationPool -Name SettingsServiceAppPool -Account
$account
# Creates an application pool for the Subscription Settings service application.
# Uses the Farm administrators account as the security account for the application
pool.
# Stores the application pool as a variable for later use.

$appSubSvc = New-SPSubscriptionSettingsServiceApplication –ApplicationPool
$appPoolSubSvc –Name SettingsServiceApp –DatabaseName SP_2013_Subscriptions_
Service_App
# Creates the Subscription Settings service application, using the variable to
associate it with the application pool that was created earlier.
# Stores the new service application as a variable for later use.
```

```
$proxySubSvc = New-SPSubscriptionSettingsServiceApplicationProxy -
ServiceApplication $appSubSvc
# Creates a proxy for the Subscription Settings service application.
```

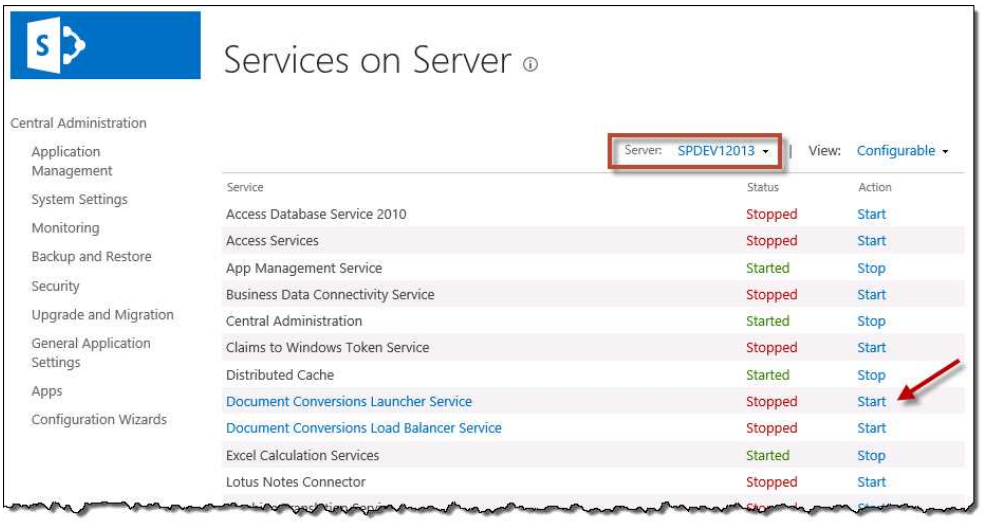
Once the script has been run on the SharePoint application server, perform an **IISreset** in an elevated **cmd** prompt. Confirm that the service application has been created. See the "*Accessing service applications*" appendix for instructions.

9.7 Starting a service

Go to SharePoint Central Administration, and from the **System Settings** section click on the **Manage services on server** link.



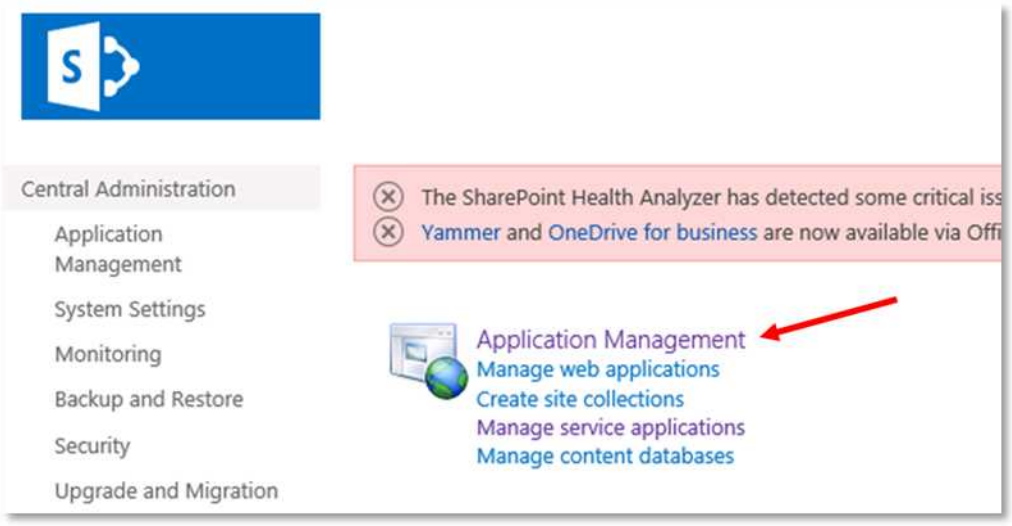
The Services on Server page, will show all services in the farm, and show which services are running on the server selected at the top of the page. Note that in multi-server farms, services may be spread across different servers. Make sure you check each server in the farm. To start a service, select the required SharePoint Server in the drop-down, locate the required service to be started and click on the **Start** link in the **Action** column. In the example below clicking **Start** will start the **Document Conversions Launcher Service** on the **SPDEV12013** server.



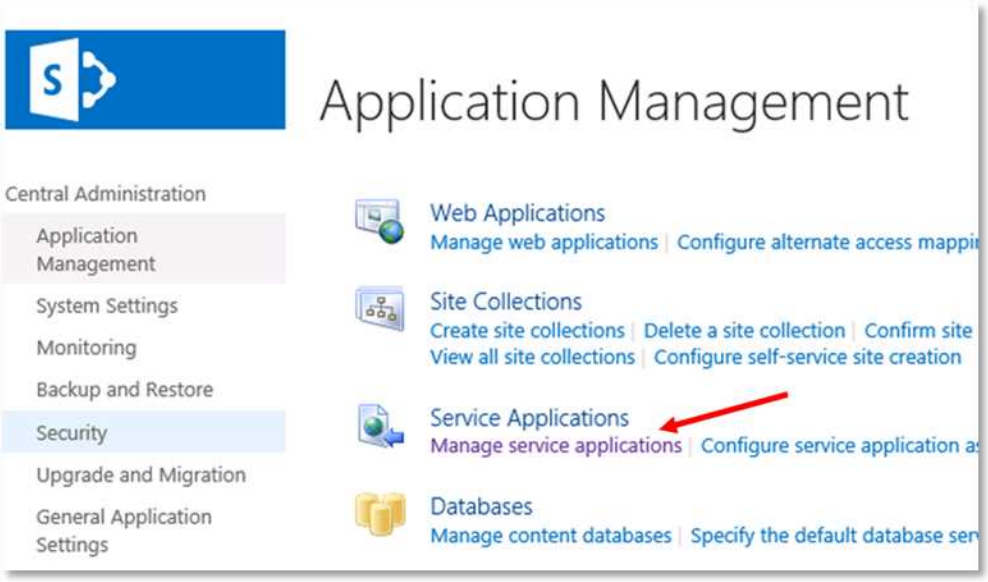
If the required service fails to start, troubleshooting the issue is outside the scope of this document. Please consult SharePoint documentation regarding how to rectify the issue.

9.8 Accessing a user profile

Using ***Central Admin***, navigate to ***Application Management***.



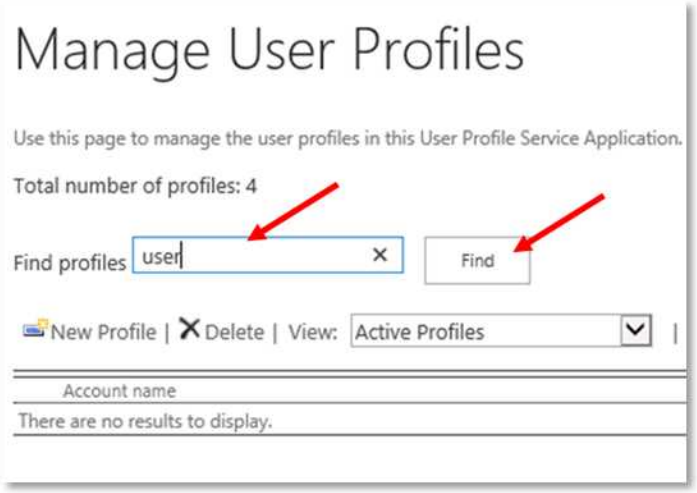
Click ***Manage Service Applications***



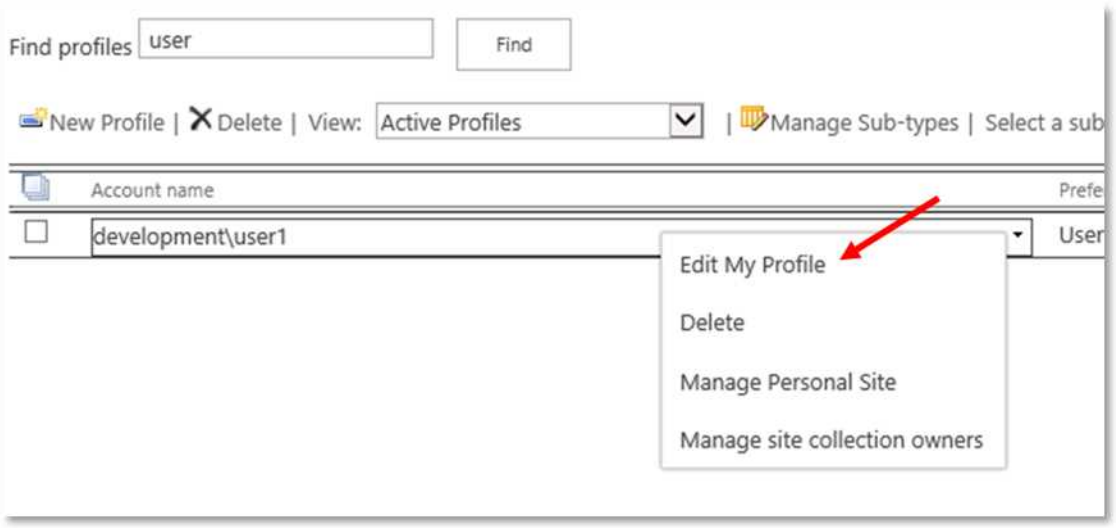
Click ***User Profile Service Application***

Choose ***Manage User Profiles***

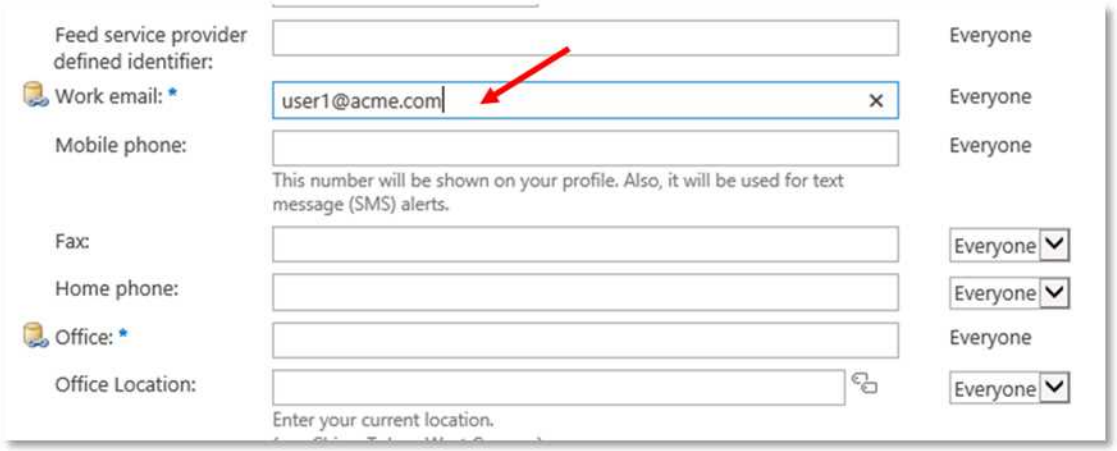
Search for the user whose profile is to be viewed



Use the ***Edit My Profile*** menu option to view the profile of the user.



Modify properties as needed. For example, to set the email address of the user, enter it in the ***Work email*** field.


Feed service provider defined identifier:
Everyone
Work email: *
user1@acme.com
Everyone
Mobile phone:
Everyone
This number will be shown on your profile. Also, it will be used for text message (SMS) alerts.
Fax:
Everyone
Home phone:
Everyone
Office: *
Everyone
Office Location:
Everyone
Enter your current location.

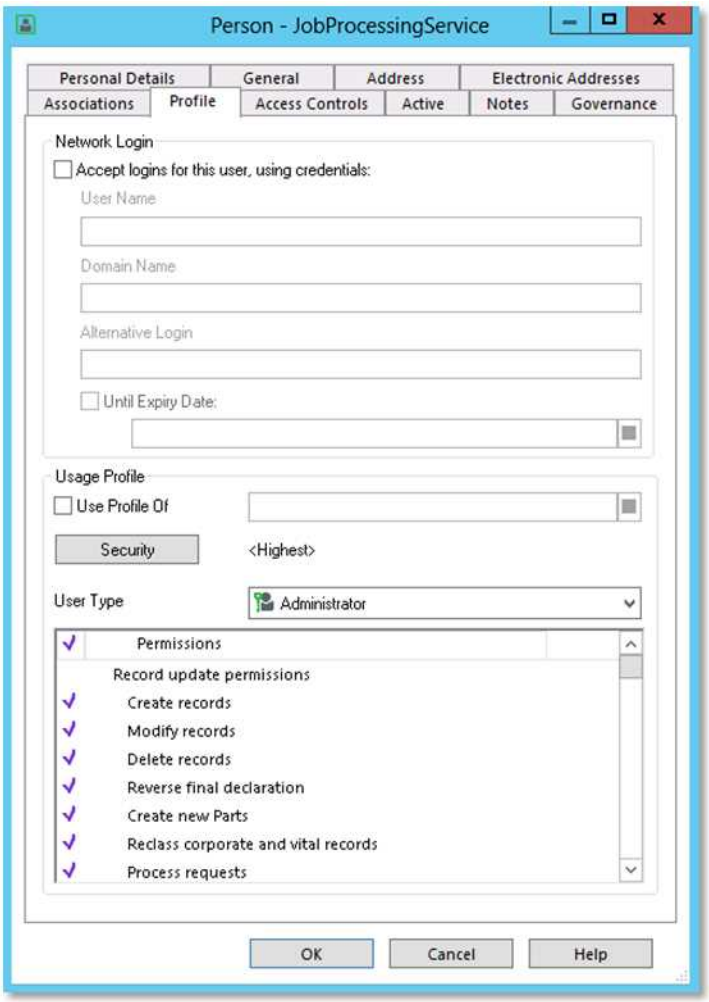
10 Appendix: Content Manager tasks

10.1 Configuring the account, permissions and granting access for a location

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

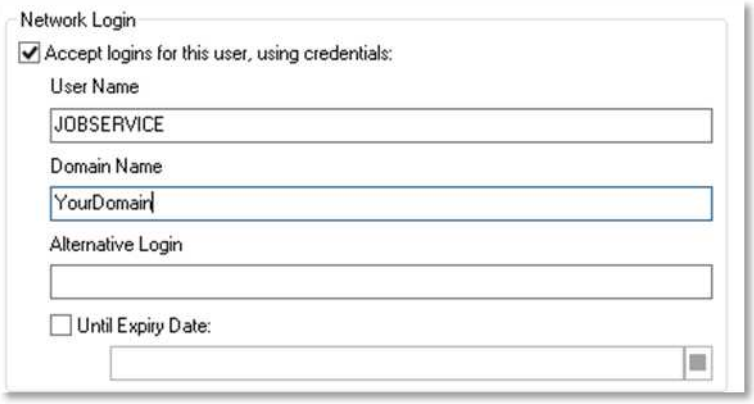
Although the following example screenshots depict configuration for the job service account; the steps are applicable for configuring the profile of any Content Manager “Person” Location.

1. Logged into the Content Manager client as an **Administrator**, locate the applicable Location using the **Internal Locations Directory** from the **Search** menu. Double-click the location name to open the properties dialog, and go to the **Profile** tab.



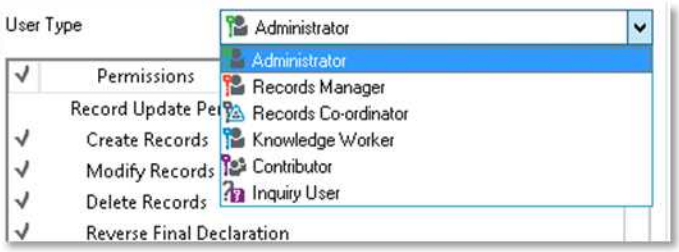
*In the **Profile** tab of the Location’s Properties:*

a. To enable a Location to accept logins, check the option to **Accept logins for this user, using login name**. Enter the domain account details (User name and Domain Name).



b. To provide a security level of <Highest> to a Location, select the **Security** button, and in the resulting dialog, select the **Highest** button. Click **OK** to return to the Properties dialog.

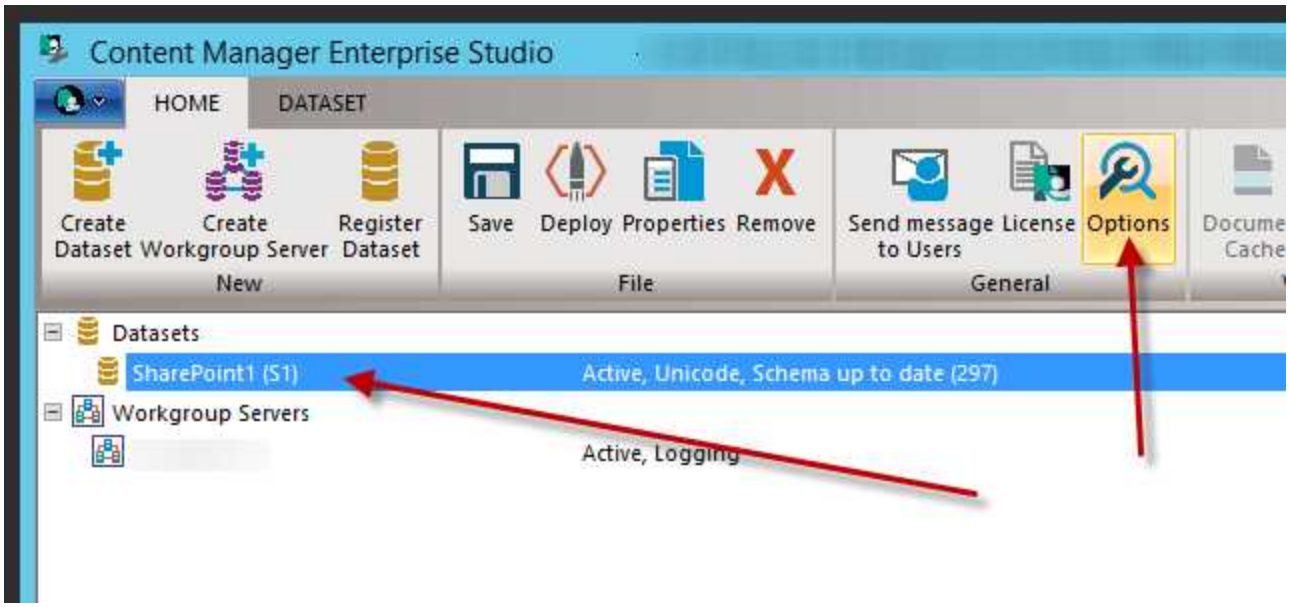
c. To set the User Type of the Location, select the applicable option from the **User Type** drop-down menu.



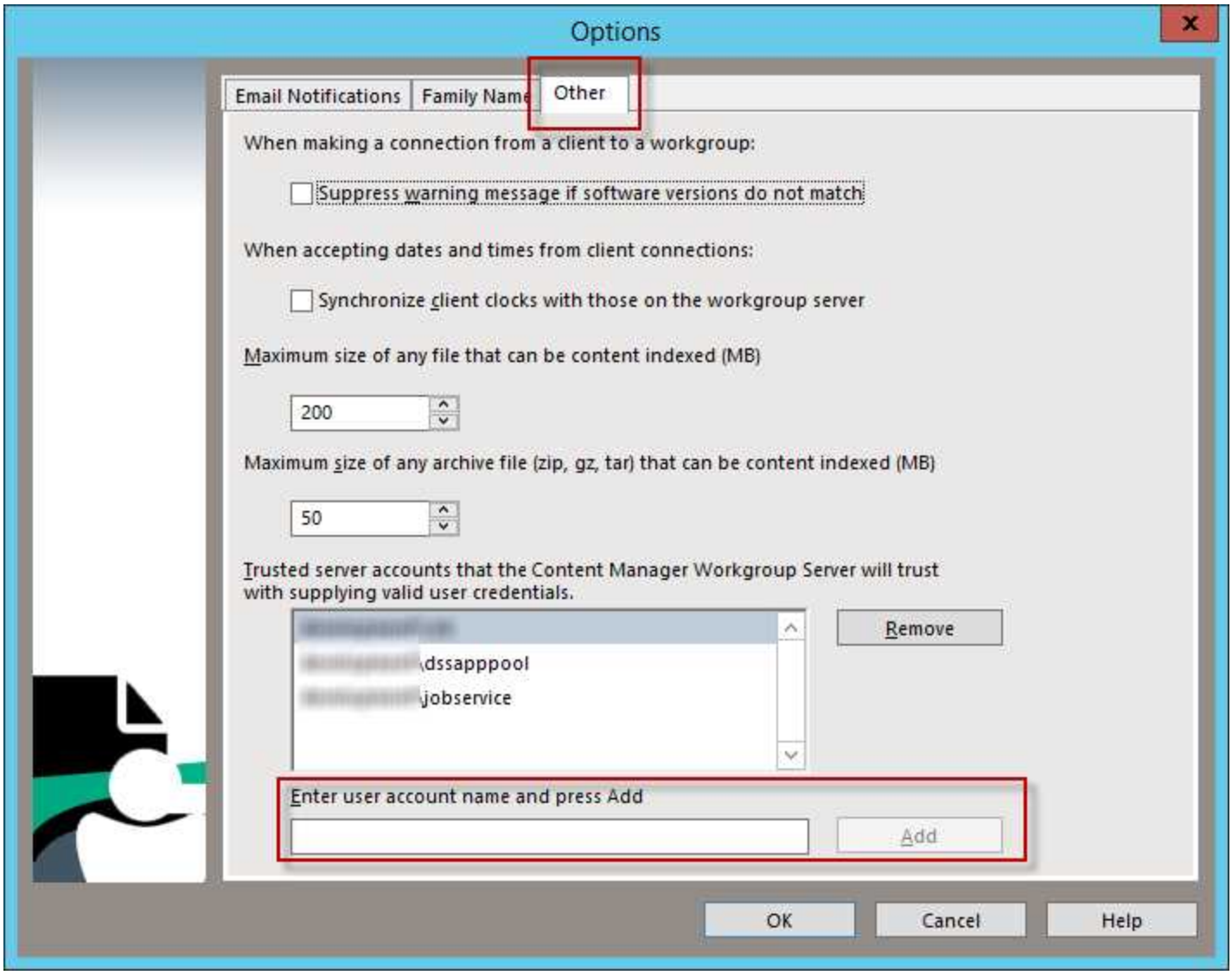
2. Click **OK** on the properties dialog to save settings.

10.1.1 Indicating an account can impersonate

1. Logged into the Content Manager Enterprise Studio as a system administrator, navigate to **General > Miscellaneous**. Right-click on the **Miscellaneous** folder and select **Properties**.



2. In the resultant **Properties** dialog, 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**.

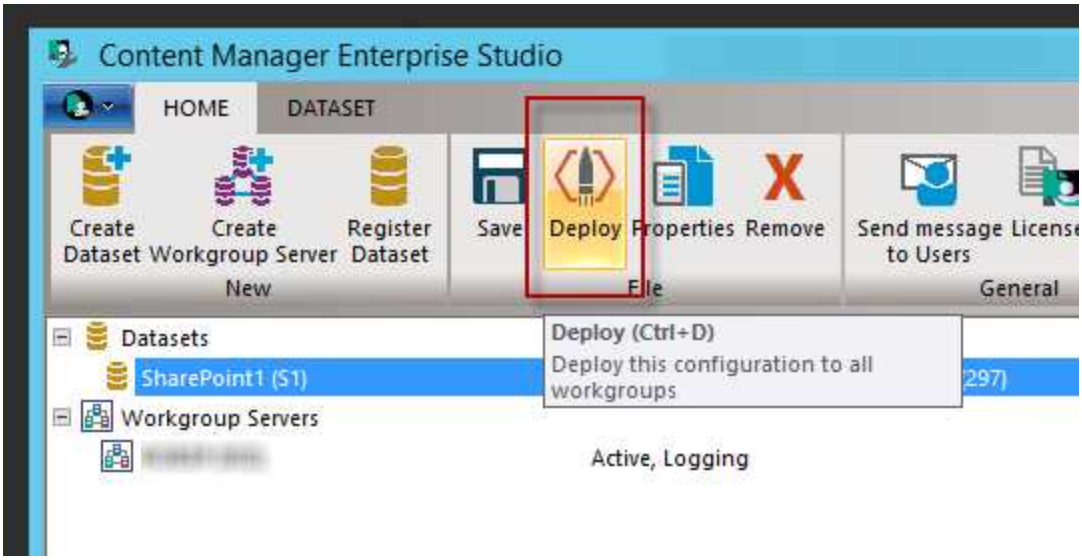


3. With the job service account added to the trusted server accounts list, click **OK** to close the dialog.
4. Save and deploy your changes in the Enterprise Studio.

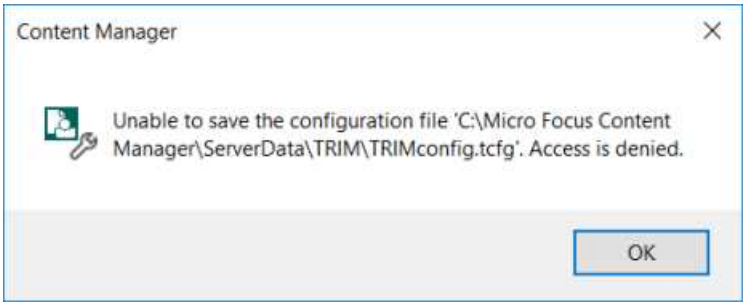
10.2 Saving and deploying Content Manager configuration settings

In the Content Manager Enterprise Studio, once you have made all the required changes:

1. Save the configuration. From the **File** ribbon, click on the **Save** icon.
2. Deploy the configuration changes. From the **File** ribbon, click on the **Deploy** icon.



If you receive an error when attempting to save configuration:



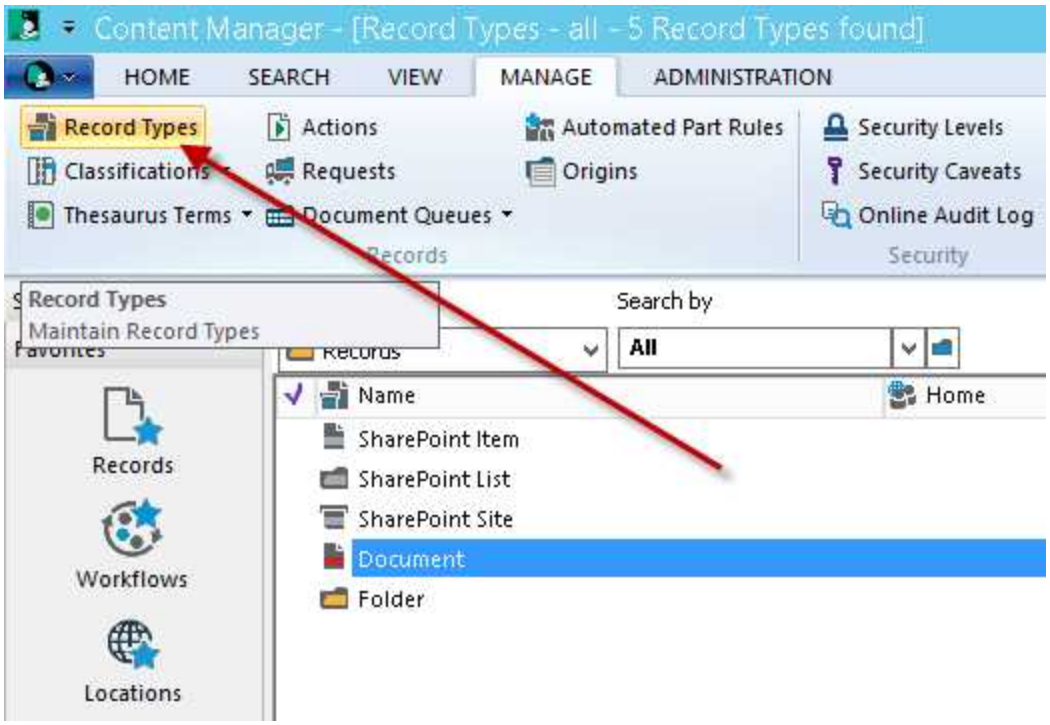
Then you need to close the Enterprise Studio, and run it again as Administrator

---

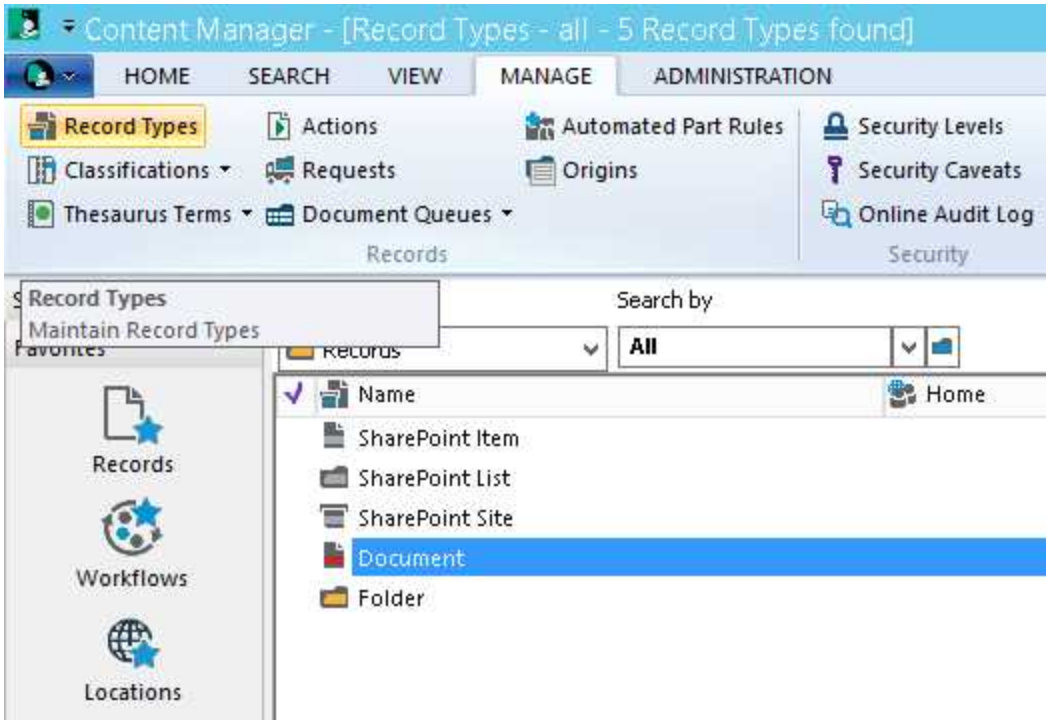
10.3 Accessing the list of record types

To access the list of **Record Types**:

1. Open Content Manager, opening the relevant dataset.
2. From the **Records** section of the **Tools** ribbon, click on **Record Types**.



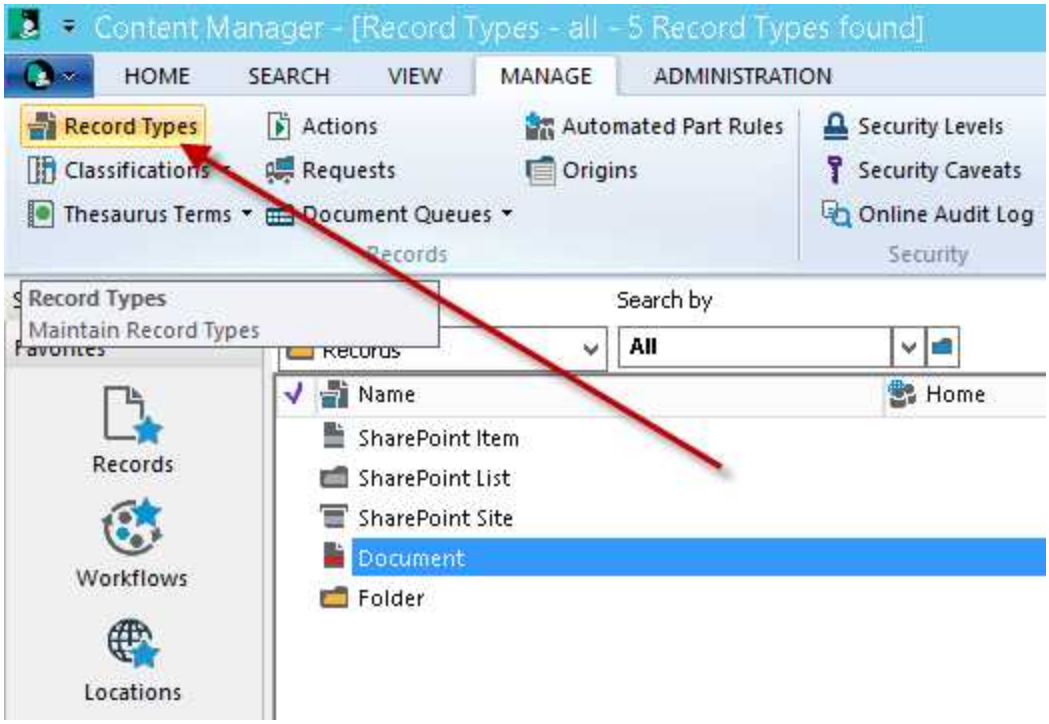
3. A list of **Record Types** in the current dataset will be displayed.



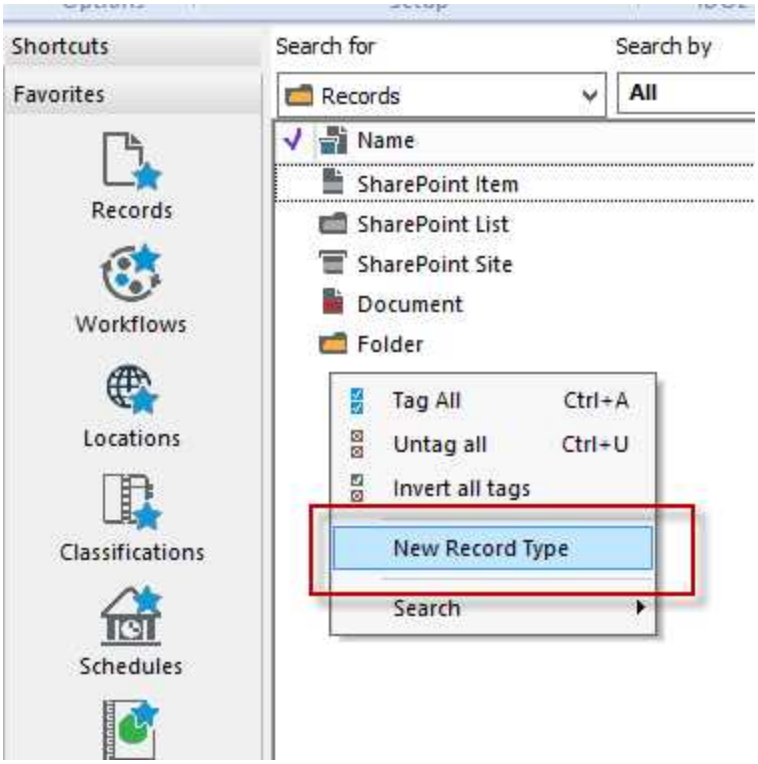
10.4 Determining the behavior of a record type

To confirm the behavior for a given **Record Type:**

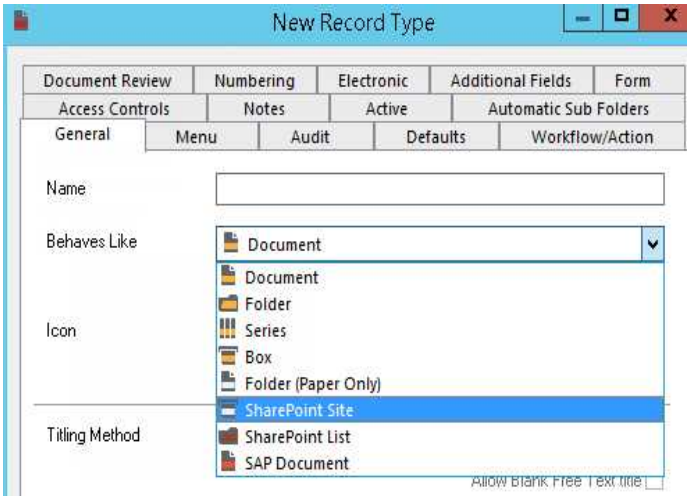
1. Open Content Manager, opening the relevant dataset.
2. From the **Records** section of the **Tools** ribbon, click on **Record Types.**



3. Double-click an existing record type in the list to open up the properties page, or right-click in white space and choose **New Record Type** to create a new one.

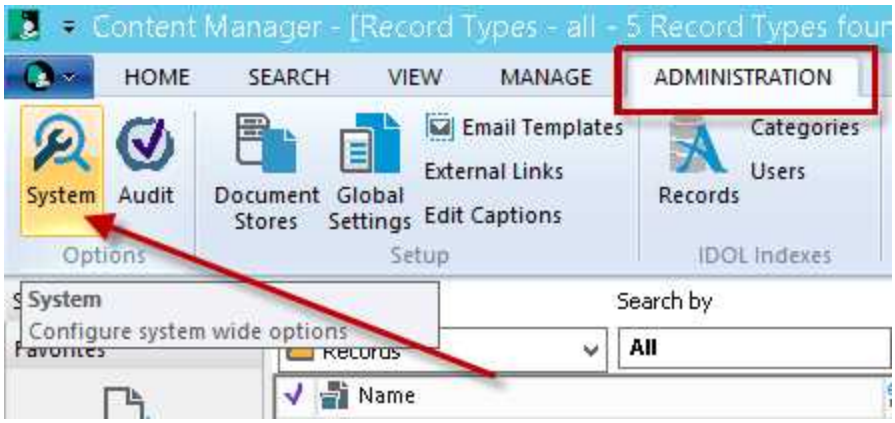


4. On the **General** tab you can see the existing Behavior in the drop-down. Change this to the desired behavior and click **OK** to save.

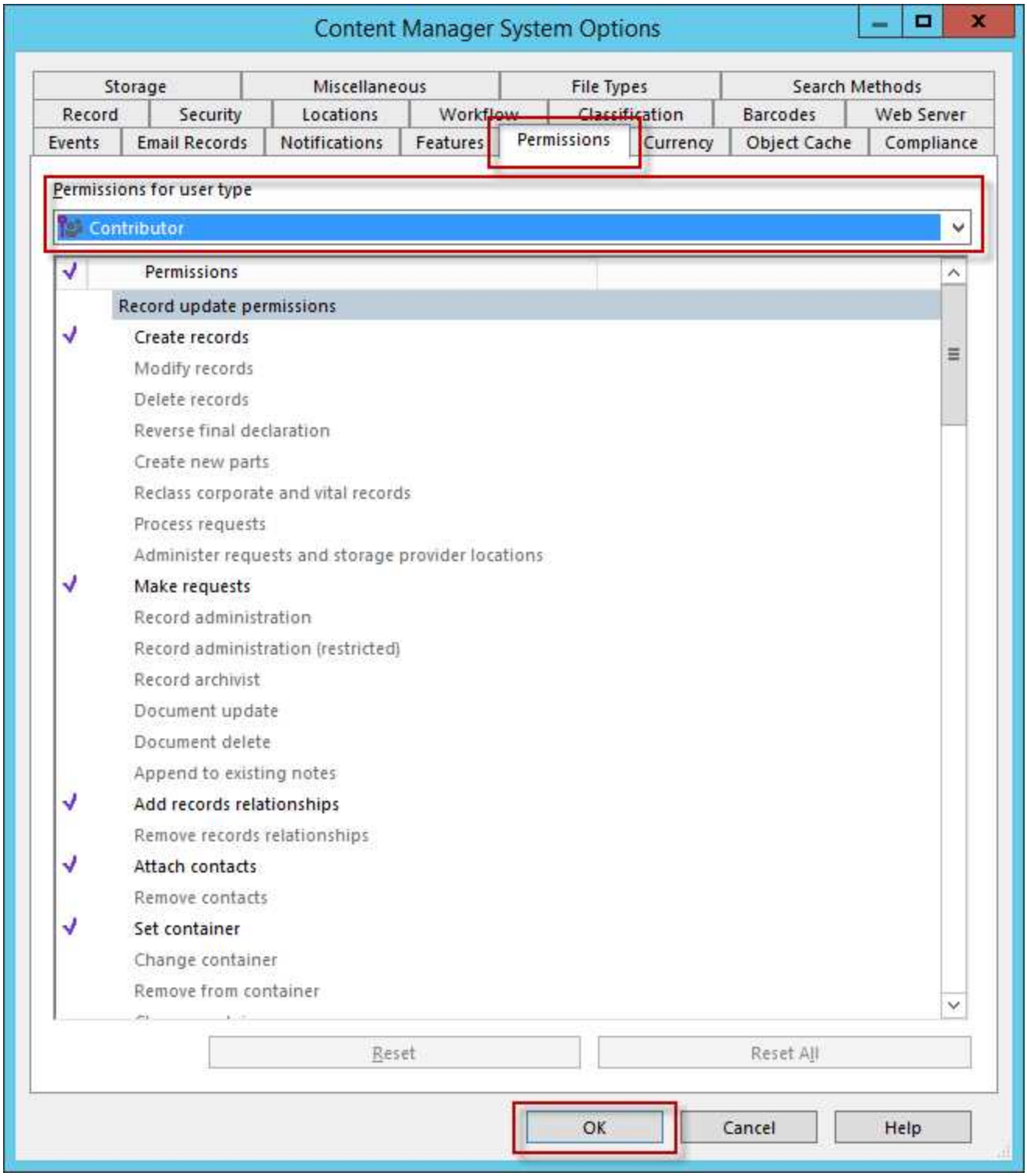


10.5 Setting the permissions granted to a user type

It is possible to modify the permissions that are granted by default to a user type in Content Manager. From the ***Administration*** tab, select the ***System*** button.



Select the Permissions tab. Select the User Type to be modified then add or remove the permissions to build the required default permission set for that type of user. Click ***OK*** to save these settings.


Content Manager System Options
Storage
Miscellaneous
File Types
Search Methods
Record
Security
Locations
Workflow
Classification
Barcodes
Web Server
Events
Email Records
Notifications
Features
Permissions
Currency
Object Cache
Compliance
Permissions for user type
Contributor
Permissions
Record update permissions
Create records
Modify records
Delete records
Reverse final declaration
Create new parts
Reclass corporate and vital records
Process requests
Administer requests and storage provider locations
Make requests
Record administration
Record administration (restricted)
Record archivist
Document update
Document delete
Append to existing notes
Add records relationships
Remove records relationships
Attach contacts
Remove contacts
Set container
Change container
Remove from container
Reset
Reset All
OK
Cancel
Help

11 Appendix: General administration tasks

11.1 Installing AppFabric

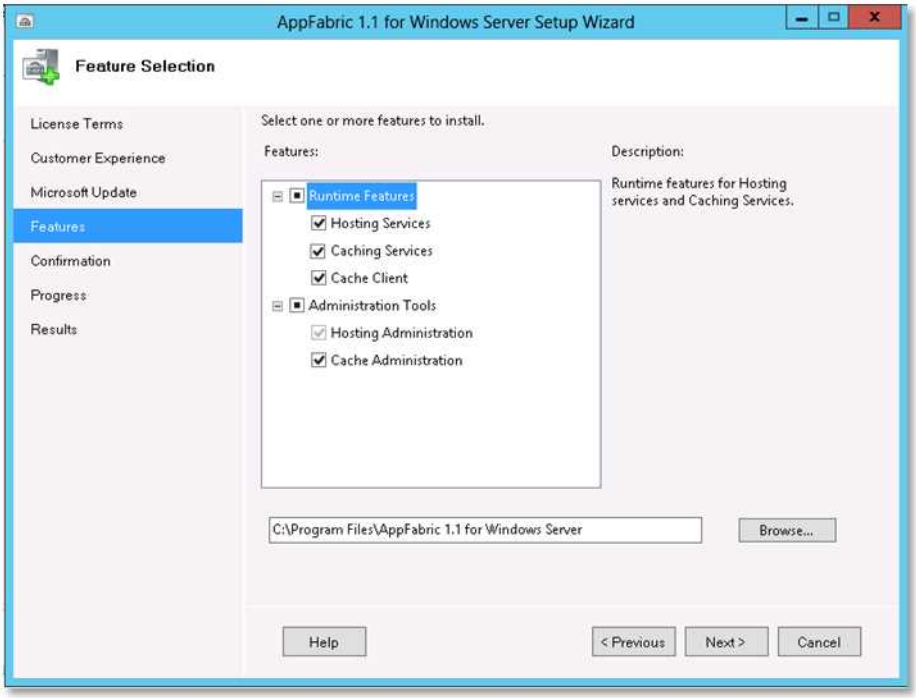
The Microsoft AppFabric framework must be installed on Content Manager Workgroup Servers, where the integration is installed (Content Manager Farm) this is used to provide configuration caching across multiple servers.

Download AppFabric 1.1 directly from Microsoft:

http://www.microsoft.com/en-au/download/details.aspx?id=27115

Note you must download and install the x64 version of AppFabric 1.1

Once downloaded, run the installer as Administrator. You can accept all the install wizard defaults, until you reach the **Features** page. On this page, select all of the options:



Complete the rest of the wizard with default settings to install AppFabric.

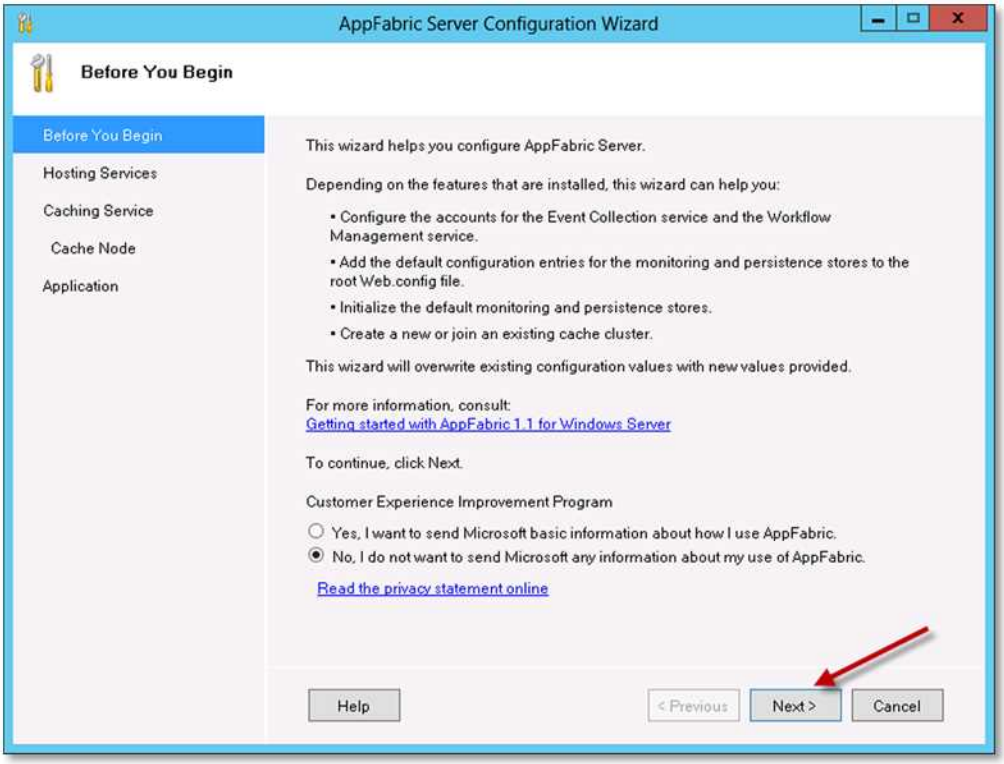
11.2 Configuring AppFabric

11.2.1 Initial Configuration

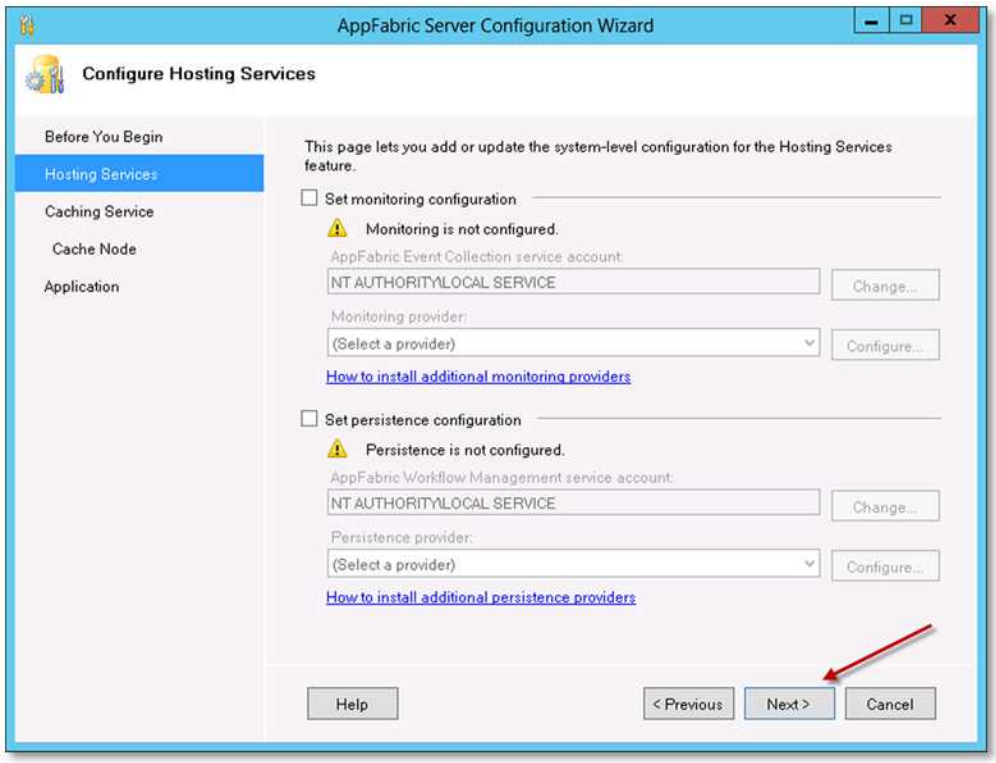
Once AppFabric 1.1 has been installed, post-installation configuration needs to be carried out.

1. The configuration wizard usually starts automatically after installation. If already started skip to Step 2. If it fails to start, you can launch it manually. From the Start menu, right-click **Configure App Fabric** and choose **Run as administrator**.

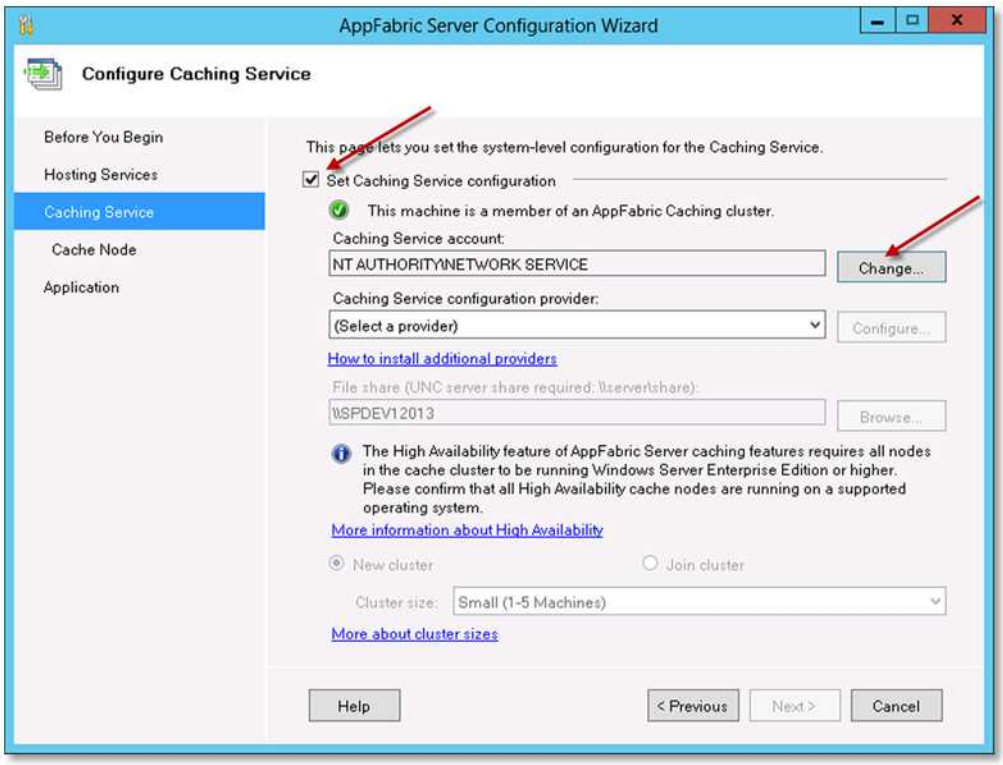
2. On the initial page, accept the wizard defaults and click **Next**



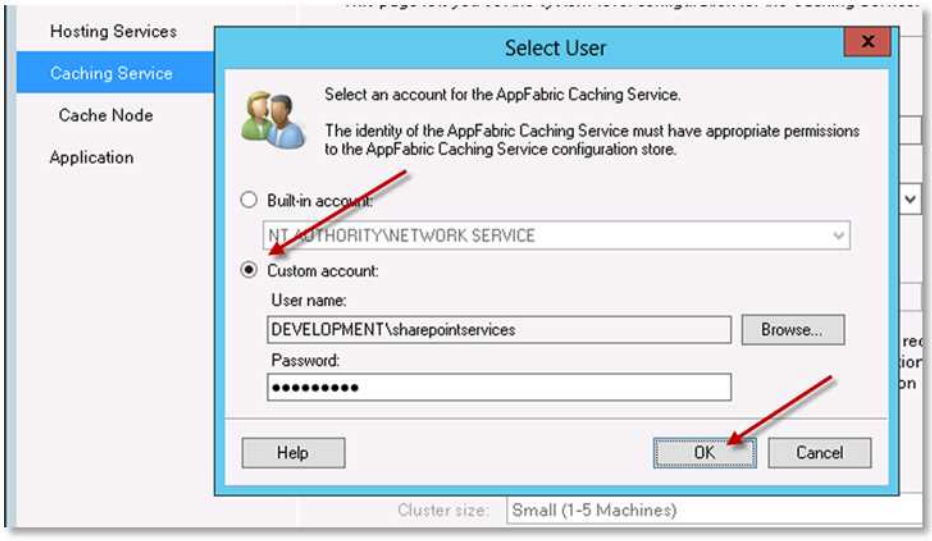
3. On the Hosting Services page, accept the defaults and click **Next**



4. On the Caching Services page, select the **Set Caching Service configuration** checkbox and click the **Change** button

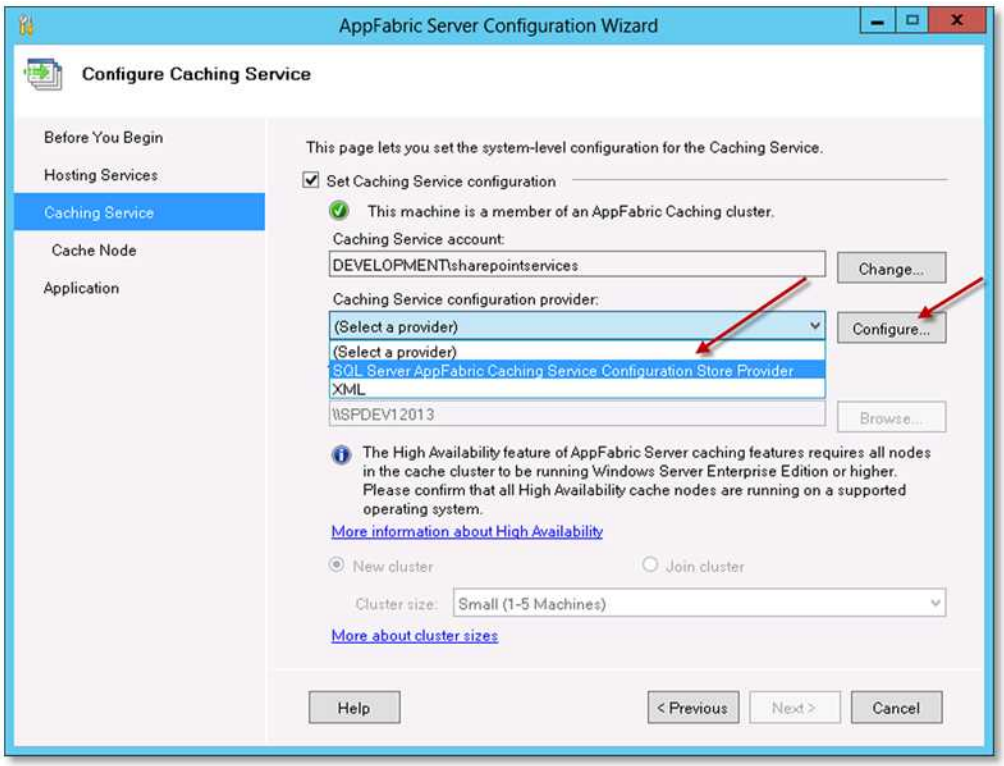


5. On the select user dialog, choose the **Custom account** option. Nominate a domain account for the AppFabric Caching Service, enter the relevant password and click **OK**



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

the **Configure** button

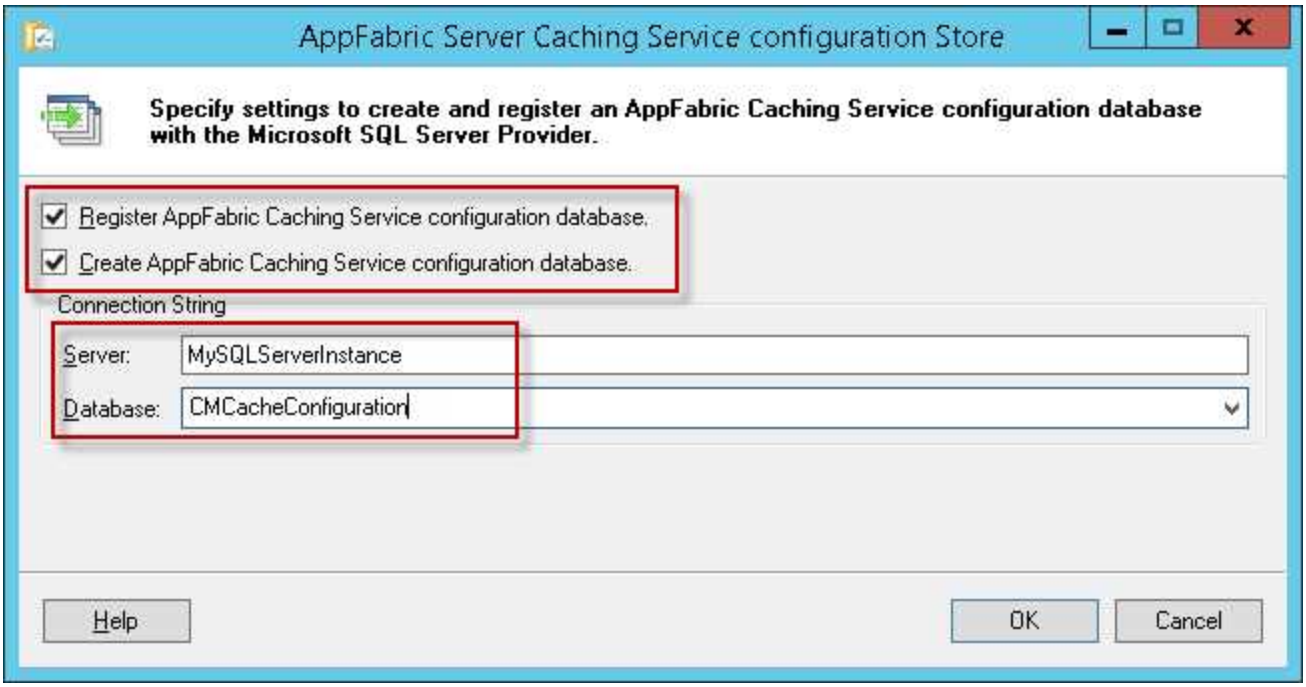


7. On the **AppFabric Server Caching Service Configuration Store** dialog, select checkboxes for both:

   - Register AppFabric Caching Service configuration database
   - Create AppFabric Caching Service configuration database

   Fill in your SQL Server name and provide a name for the caching configuration store database. The example given is **'CMCacheConfiguration',** but you can use any name you deem appropriate. This will create a new database in SQL Server.

   Click **OK**



8. Click **Yes** on the following prompt

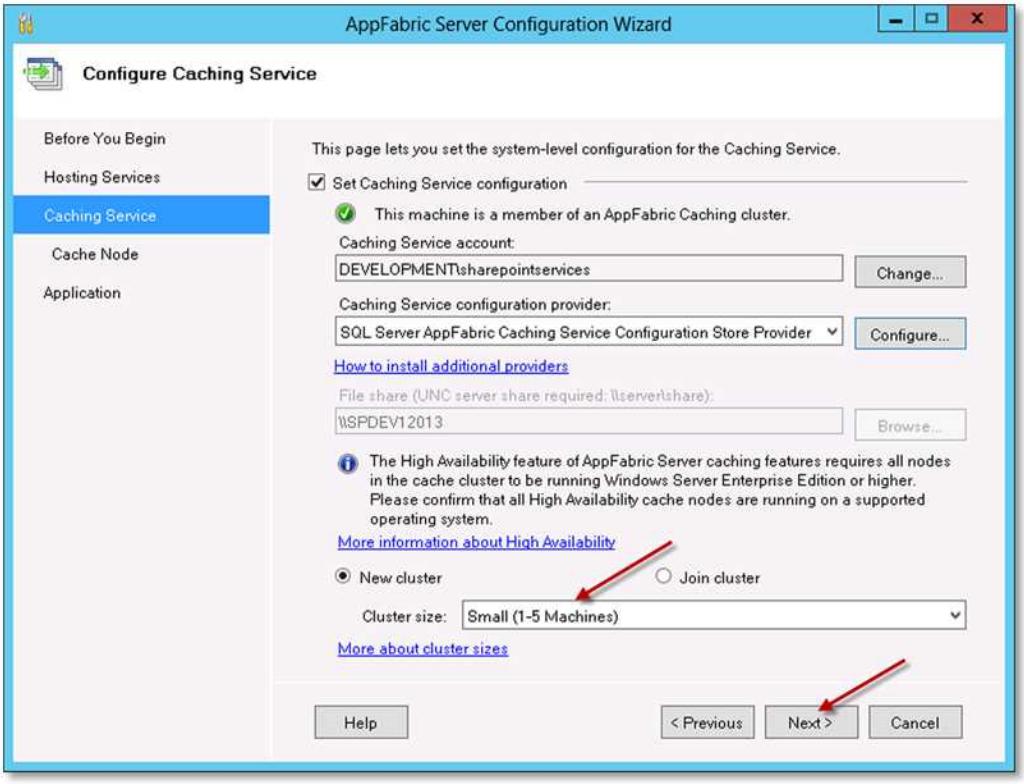
9. Click **OK** on the confirmation dialog

10. 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.

Note the example below shows the wizard defaults

Click the **Next** button

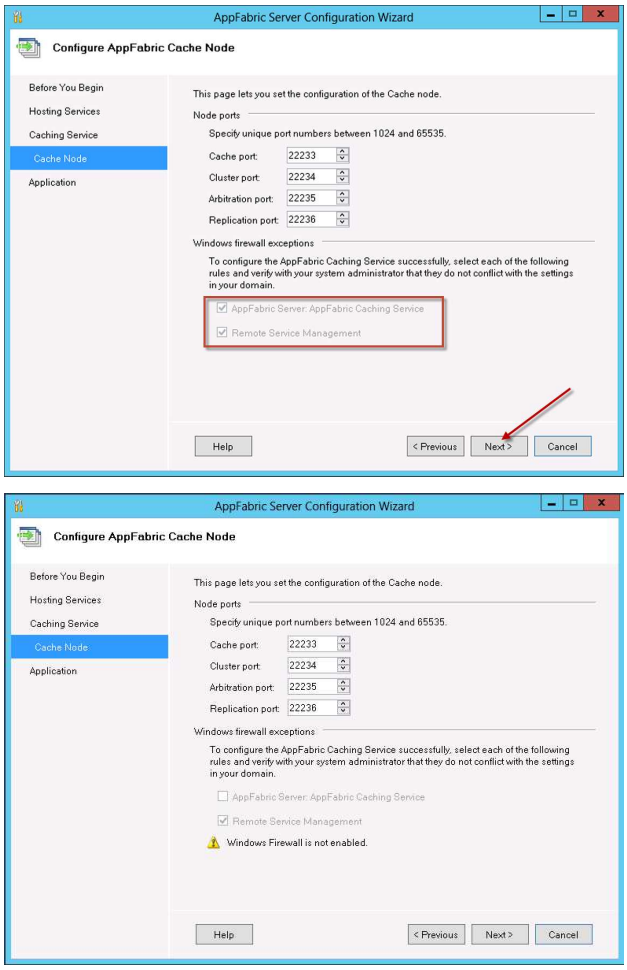


11. On the **Configure AppFabric Cache Node** page, if you have **Windows Firewall** enabled, select both checkboxes:

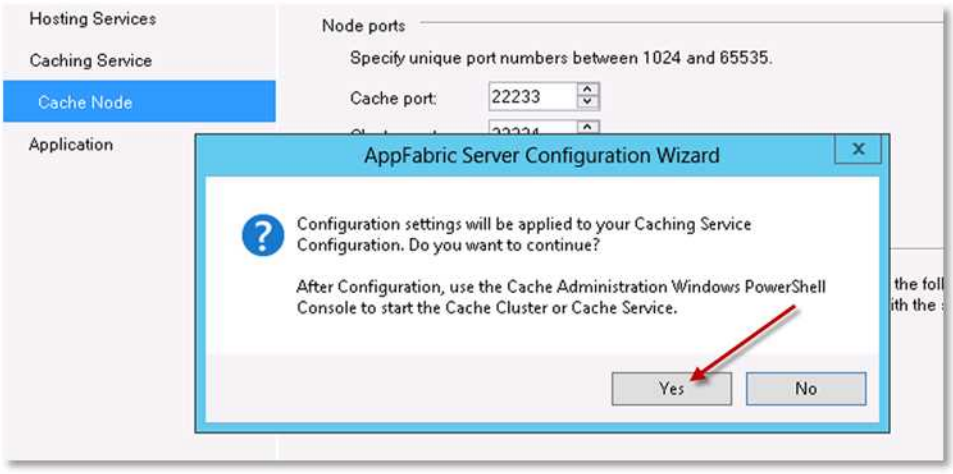
    - AppFabric Server AppFabric Caching Service
    - Remote Service Management

    For other firewalls, you need to configure them manually to allow these ports, to enable communication between the SharePoint farm and Content Manager Servers. Note that if the **Windows Firewall** is not enabled, you will see a warning message. *See both variants below*.

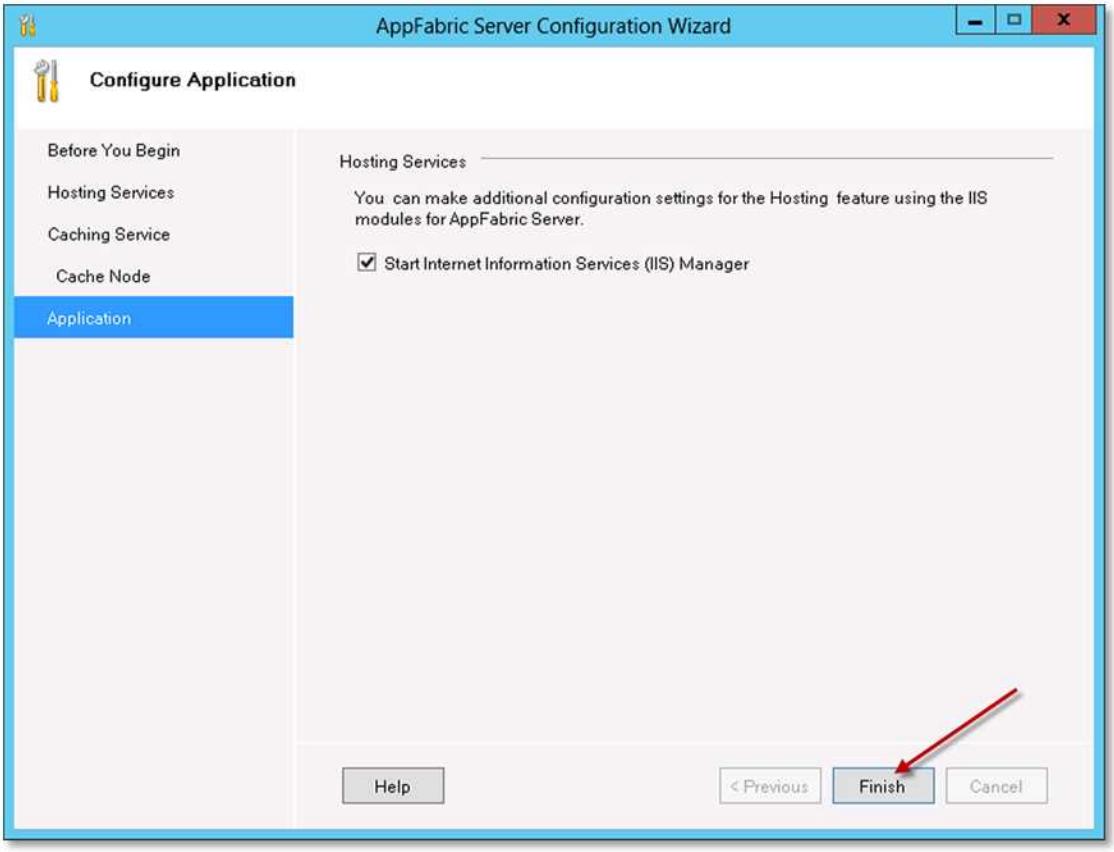
    Click on the **Next** button



12. Click **Yes** on the configuration settings prompt



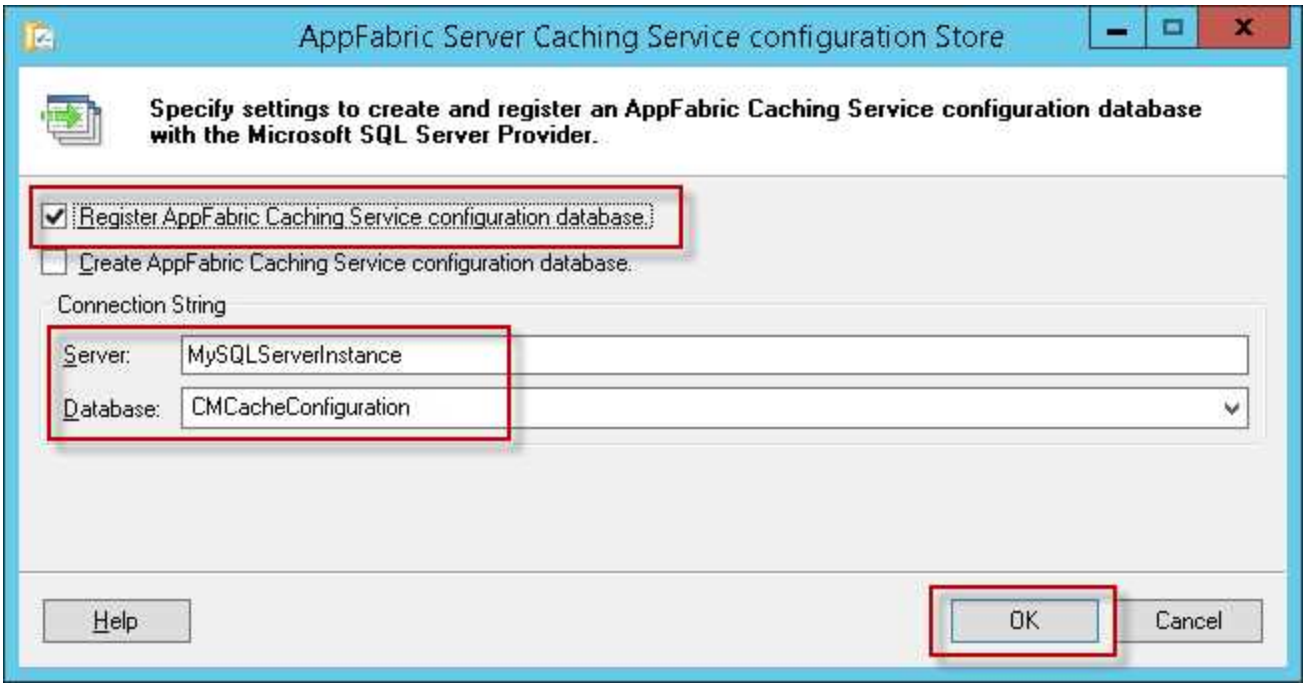
13. A progress bar is displayed while the configuration settings are applied. Once this has completed, on the Application page, click **Finish**



11.2.2 Joining a server to an existing cache cluster

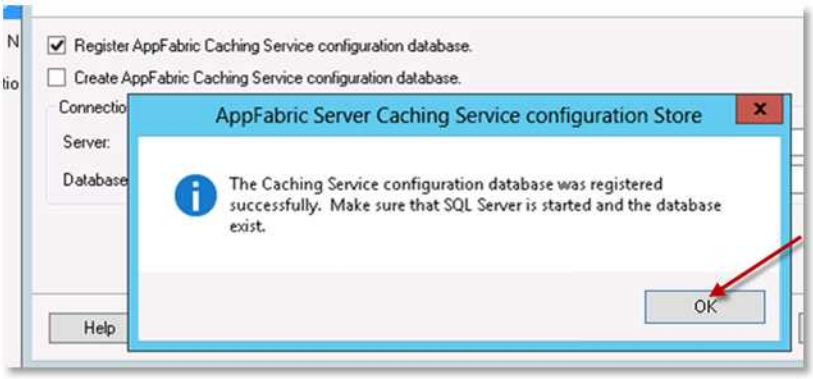
Follow steps 1-6 from the 11.2.1 Initial Configuration, on page 189 section above. From step 7, follow the process below:

7. On the **AppFabric Server Caching Service Configuration Store** dialog:
    i. select the checkbox for **Register AppFabric Caching Service configuration database**
    ii. Leave the **Create AppFabric Caching Service configuration database** option unselected. Fill in your SQL Server name and select the database you created during initial configuration.
    iii. Click **OK**

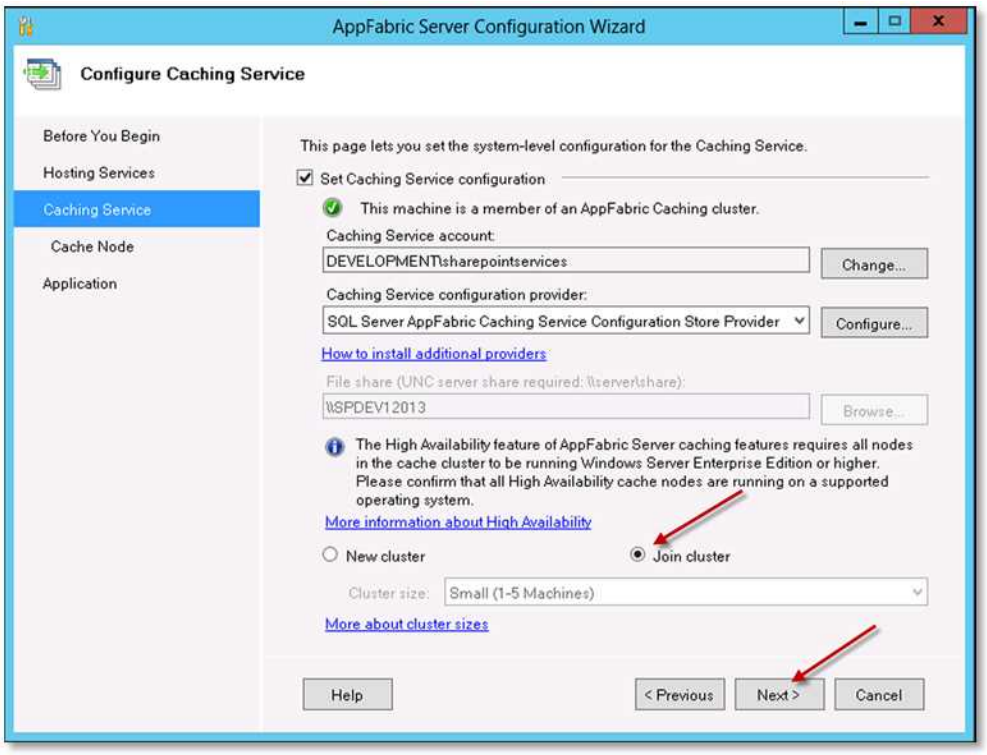


8. Click **Yes** on the following prompt

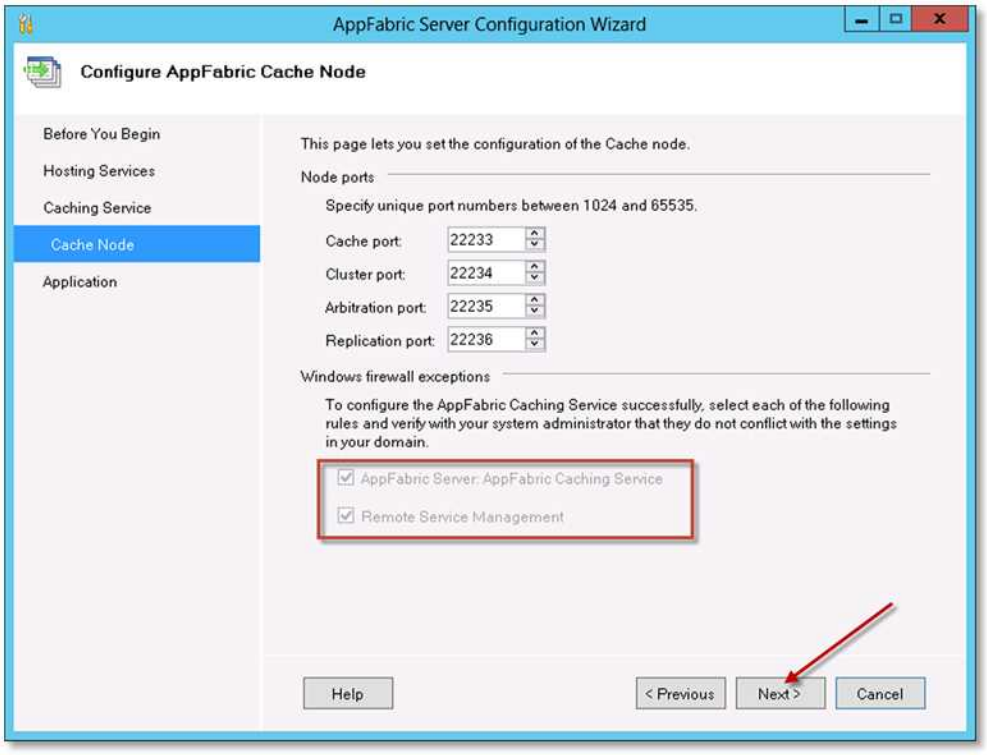
9. Click **OK** on the confirmation dialog



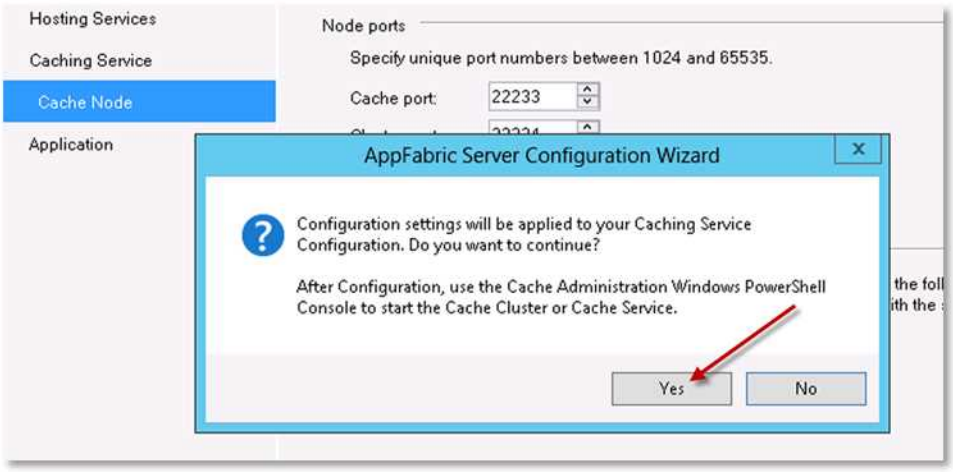
10. Select the option **Join cluster** and Click **Next**



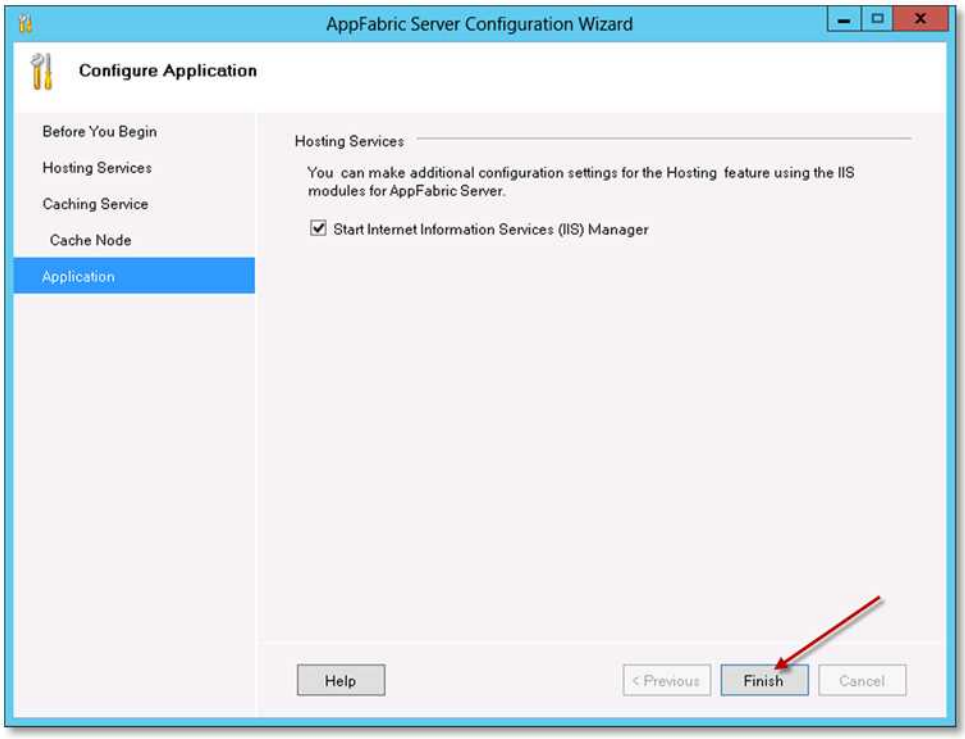
11. On the Cache Node page, click **Next**



12. Click **Yes** on the configuration settings prompt



13. A progress bar is displayed while the configuration settings are applied. Once this has completed, on the Application page, click **Finish**



11.3 Troubleshooting AppFabric

11.3.1 Installation issues – AppFabric install fails with errors

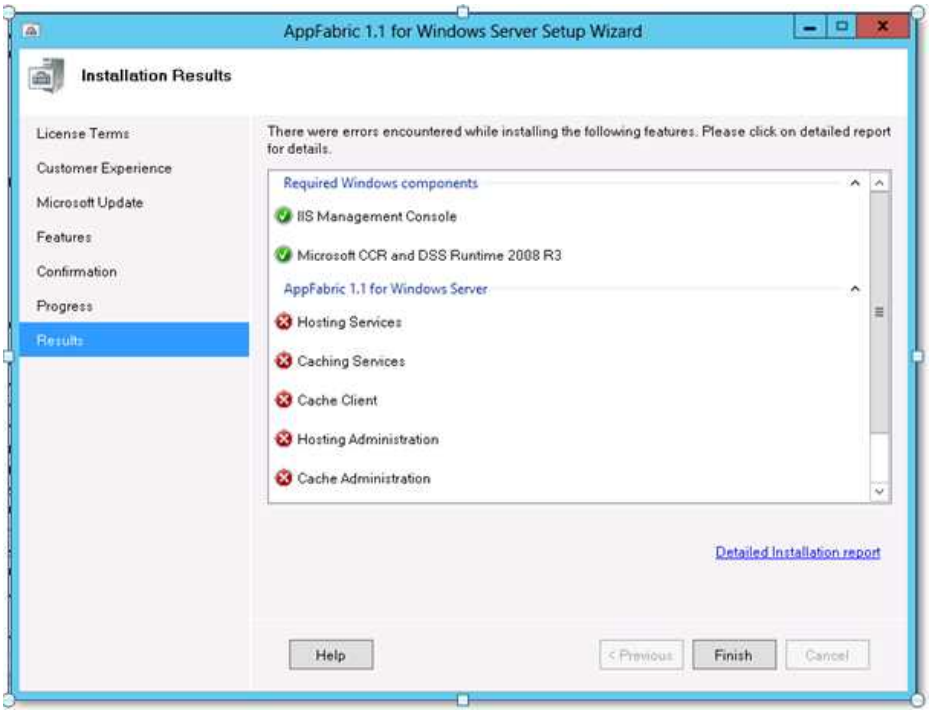
AppFabric can initially be a tricky beast to install and configure. There are a number of resources available on the internet to assist with resolving AppFabric issues such as:

http://jefferytay.wordpress.com/2013/12/11/installing-appfabric-on-windows-server-2012/

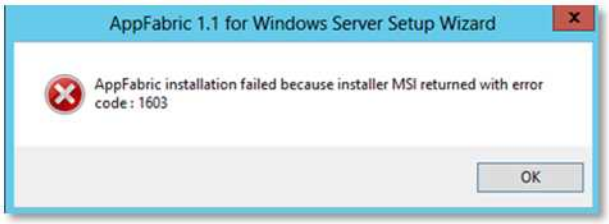
This section aims to provide solutions to the more common issues found with AppFabric.

First ensure you have the pre-requisites installed as defined in the *2.4.3 Server roles and features, on page 31* section.

If you see the following errors when installing, try the following troubleshooting steps before retrying the installation:



Click Finish, you may see the following error message, or you see the same message when viewing the install log:



Check all of the steps in the following table before retrying the installation:

AppFabric Installation Troubleshooting Steps
Check the PSModulePath environment variable: 1. Go to My Computer, right-click Properties

2. On the System' page, click Advanced System Settings on the left-side pane.
3. If you receive a UAC prompt, click on Yes to launch the System Properties dialog box
4. From the Advanced tab, click Environment Variables
5. Within the System Variables section in the lower half, select PSModulePath and click on Edit (or double-click PSModulePath)
6. Check that it includes the v1.0 entry (SQL entry will only be there if SQL Server is installed locally), and remove any extraneous quotation marks “

   ```
   C:\Windows\system32\WindowsPowerShell\v1.0\Modules\;C:\Program Files (x86)
   \Microsoft SQL Server\110\Tools\PowerShell\Modules
   ```

7. If this fails, delete the PSModulePath variable completely and then retry the installation

Check that the windows service **Remote Registry** is running, and set to **Automatic**

Enable **Windows Update**, and ensure that **Critical** updates are up to date

Prior to installing AppFabric, the groups **AS_Observers** and **AS_Administrators** must not exist. To check if they exist for you and to get rid of them you just go into Administrative Tools → Computer Management→ Local Users and Groups → Groups and if **AS_Observers** or **AS_Administrators** exists, delete it as shown here msdn.microsoft.com/en-us/library/ff637696(v=azure.10).aspx

11.3.2 Post-Installation - ‘Failed to access app fabric cache’ errors in the integration log

Follow the steps below to fix any errors related to AppFabric configuration, while publishing settings via the Content Manager SharePoint Configuration tool or when the **AppFabric Caching Service** (Windows Service) is not running

Example log Message:

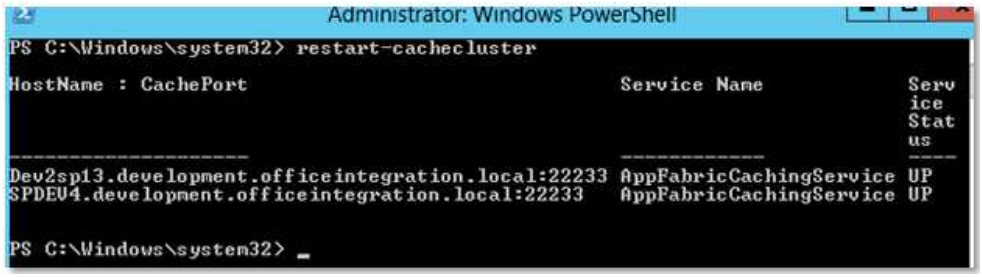
```
Failed to access app fabric cache. Details
are:ErrorCode<ERRCA0017>:SubStatus<ES0006>:There is a temporary failure. Please
retry later. (One or more specified cache servers are unavailable, which could be
caused by busy network or servers. For on-premises cache clusters, also verify the
following conditions. Ensure that security permission has been granted for this
client account, and check that the AppFabric Caching Service is allowed through the
firewall on all cache hosts. Also the MaxBufferSize on the server must be greater
than or equal to the serialized object size sent from the client.)
```

AppFabric Post-Installation Troubleshooting Steps

Run the **Caching Administration** PowerShell, right-click and **Run as Administrator**.

From the PowerShell window, execute the following command to restart the cache cluster.

restart-cachecluster

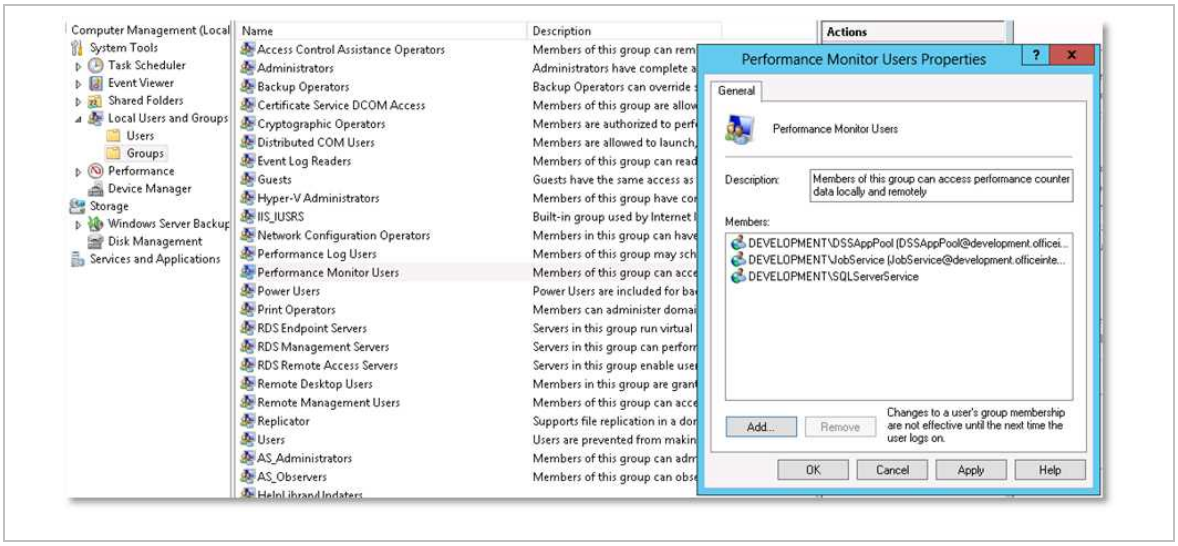


Ensure the **Service Status** is **UP**. If it is in stuck in the **STARTING** state, restart the server.

Check to make sure that the following domain service accounts are in the local security group **Performance Monitor Users:**

- Job Service Account
- Application Pool Account
- SQL Server Service Account

To do this go to Administrative Tools → Computer Management→ Local Users and Groups → Groups and double-click the **Performance Monitor Users** group to show the members



11.4 Creating an Azure cache

The Azure cache capability is very much in flux at the moment, this section is up-to-date as of the publication date, but bear in mind that the cache creation process may change in the future.

> *Note – The managed cache PowerShell commands were added late May 2014, so if you already have Azure PowerShell installed and configured, make sure you update to the latest version.*

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

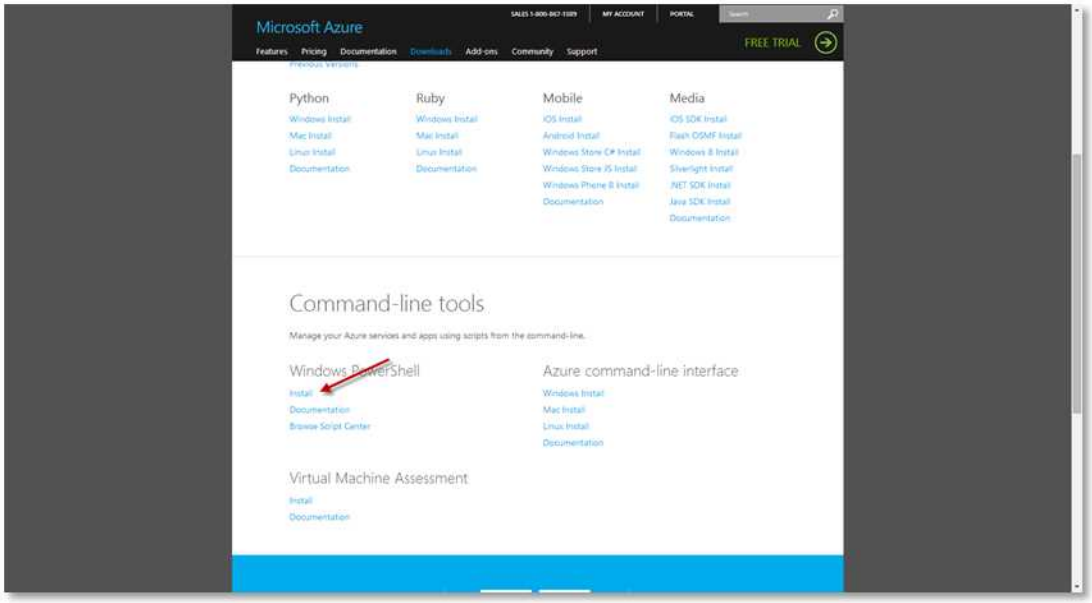
- Managed
- Redis

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

11.4.1 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.

To install **Windows Azure PowerShell** go to http://azure.microsoft.com/en-us/downloads/ and under the **Windows PowerShell** section, click on **Install**.



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 follwing commands *(Note you should change the location to match your Azure VMs region):*

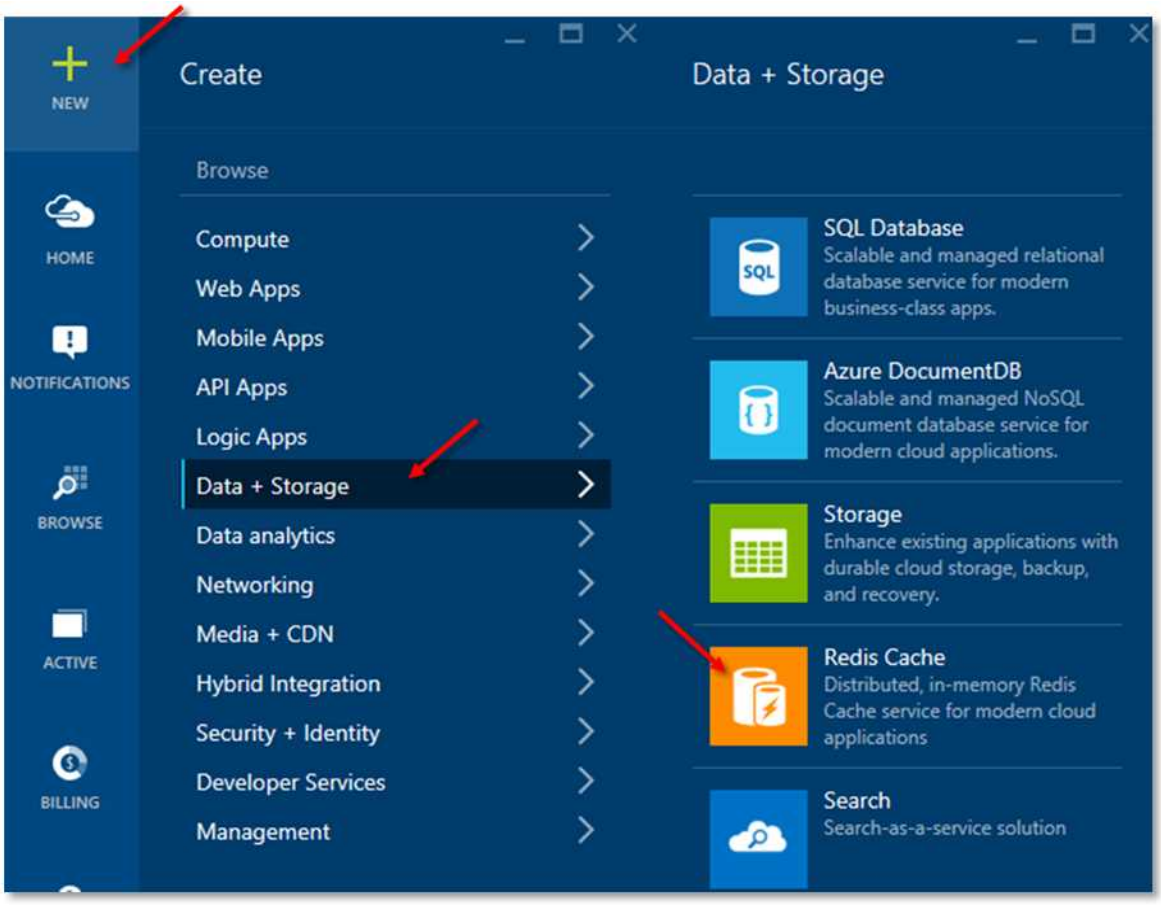
```
New-AzureManagedCache -Name hprm -Location "East Asia" -Sku Basic -Memory
128MB
Get-AzureManagedCache
```

3. This creates a cachenamed ‘hprm’, 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.

11.4.2 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 (https://portal.azure.com)

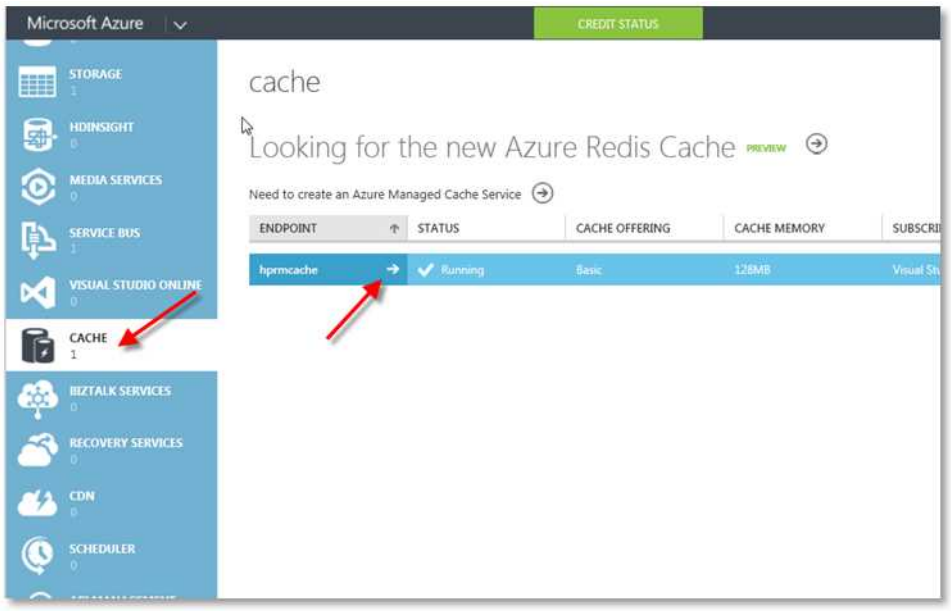
Click ***New***, then ***Data + Storage*** then ***Redis Cache***.



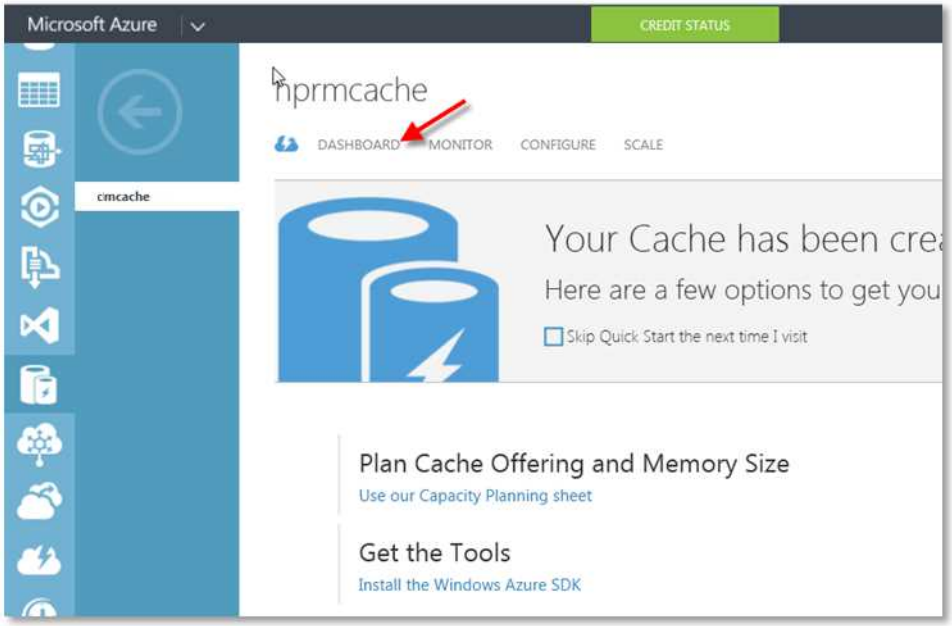
Complete the requested details to create the cache.

11.5 Obtaining the Azure cache endpoint

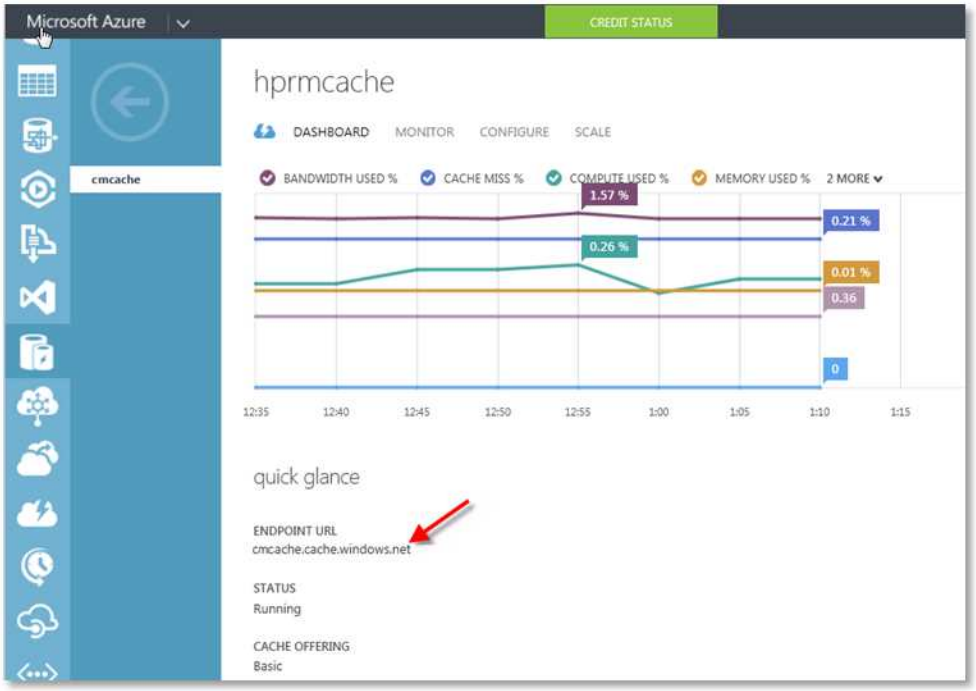
1. Log in to your Windows Azure management portal, select **Cache** in the left-hand navigation pane, and then click on the arrow next to your cache endpoint.



2. Click on the **DASHBOARD** menu



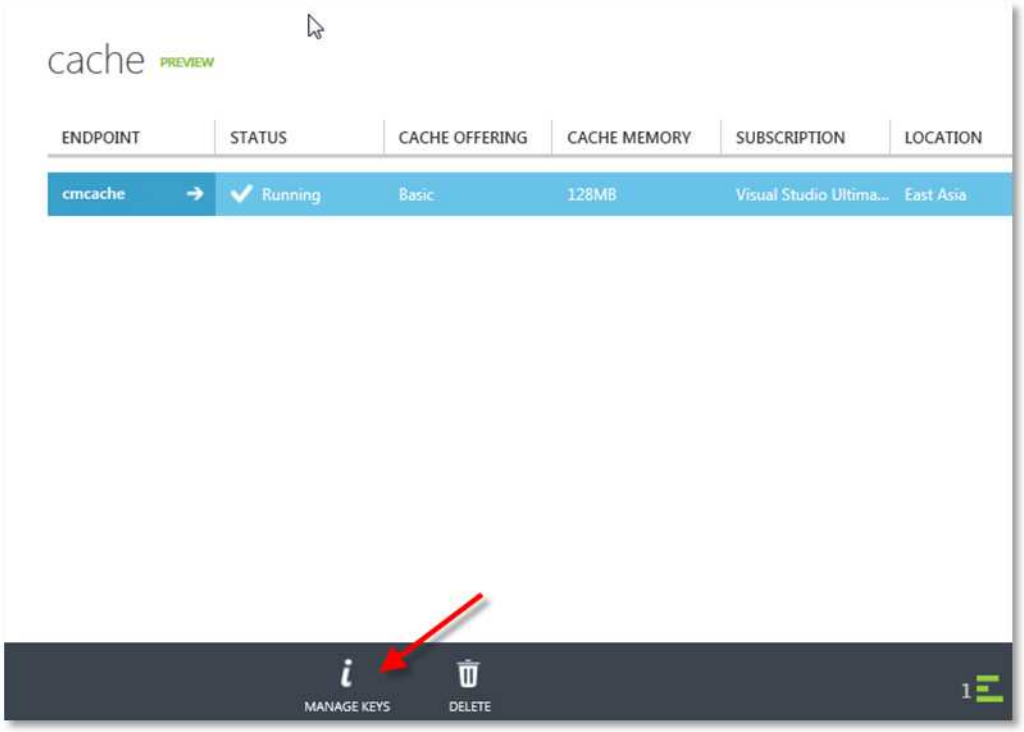
3. Select and copy the value of the **ENDPOINT URL**



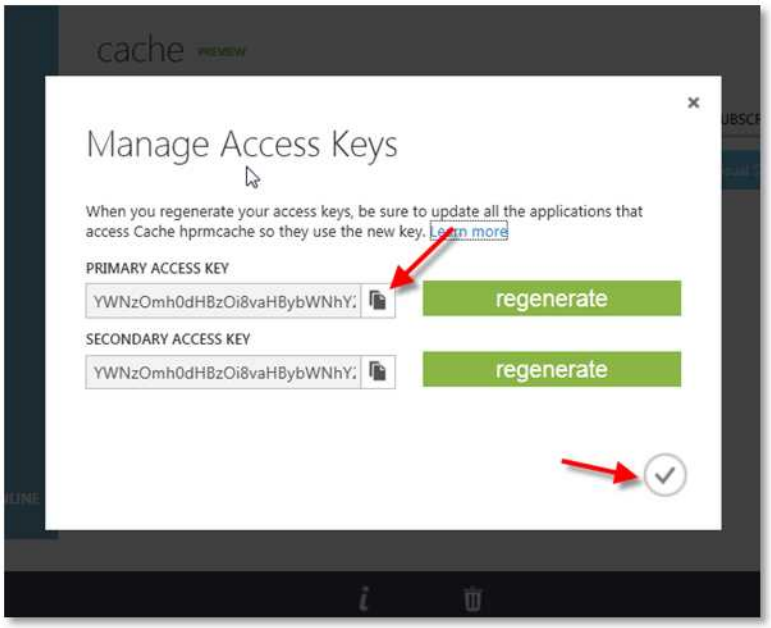
11.6 Obtaining the Azure access keys

11.6.1 Managed cache

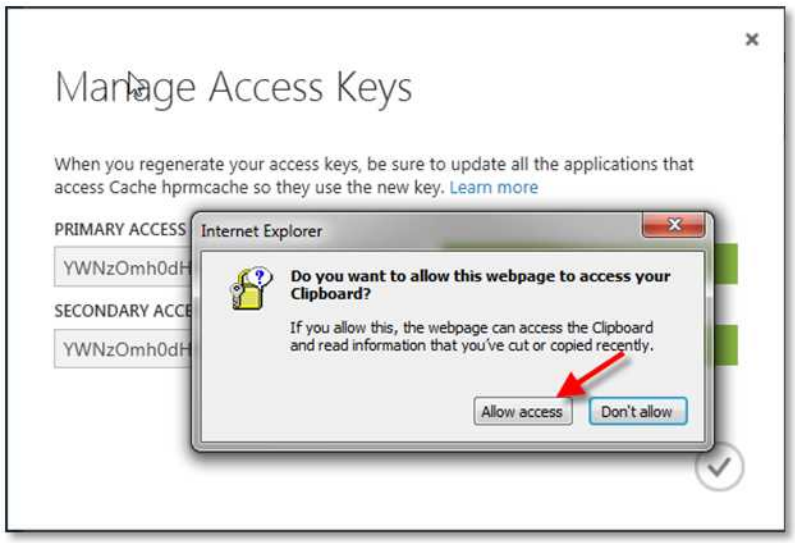
1. Select the cache you just created and click on the **MANAGE KEYS** option in the bottom toolbar.



2. On the Manage Access Keys dialog, Click on the Copy to Clipboard button next to the PRIMARY ACCESS KEY

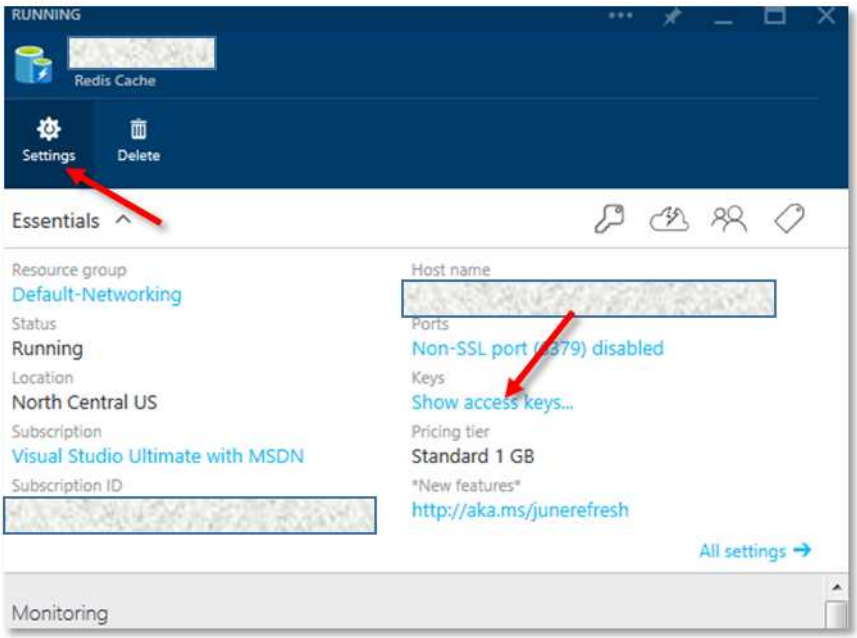


3. On the clipboard prompt, click on **Allow access**.



11.6.2 Redis cache

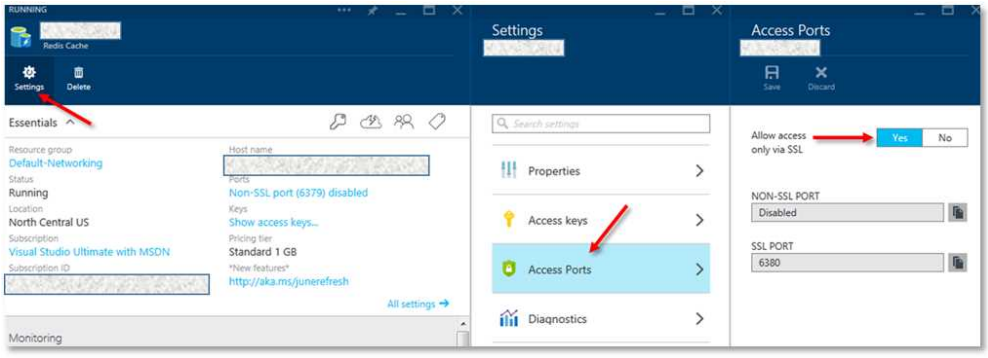
Using the ***Azure portal***, navigate to the ***settings*** for the Redis cache in use. Click the ***Show access keys*** link to reveal the keys in use.



11.7 Determining if the Azure cache is configured to use SSL

11.7.1 Redis cache

Using the ***Azure portal***, navigate to the ***settings*** for the Redis cache in use. Under the ***Access Ports*** section the value of ***Allow access only via SSL*** will indicate if the cache is configured to only use SSL.



11.8 Enabling HTTPS for a site

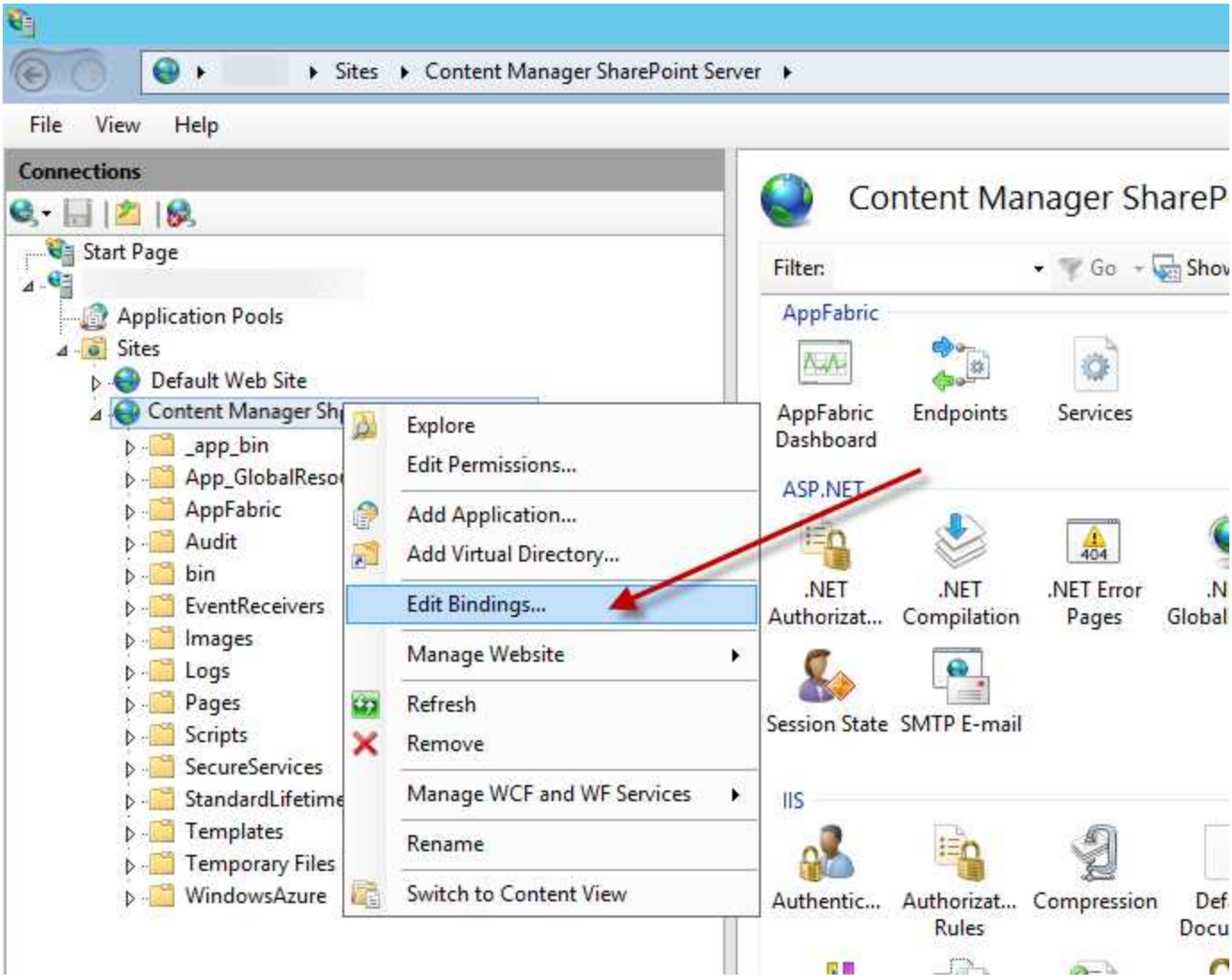
To enable HTTPS for the **Content Manager SharePoint Server** website, you will first need to have obtained an SSL certificate, or use an existing SSL certificate for your internal domain. There are a number of options to obtain a certificate, the process of obtaining the certificate is beyond the scope of this document, and there are lots of publicly available articles from Microsoft detailing the process:

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

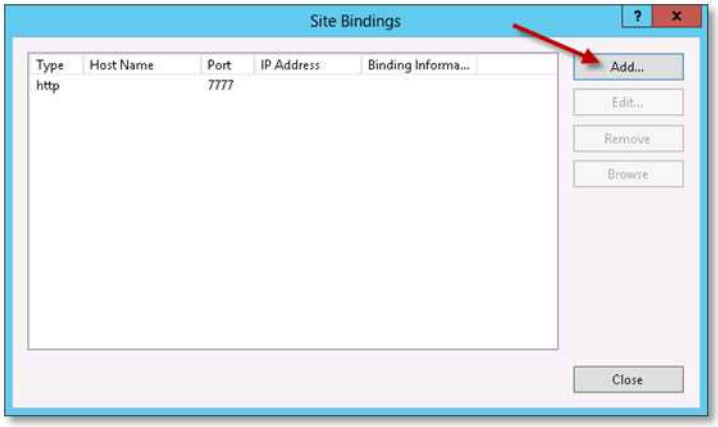
Self-signed Certificate	Created within IIS, can be used in some scenarios (SharePoint High-Trust) for testing/development	Not suitable

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

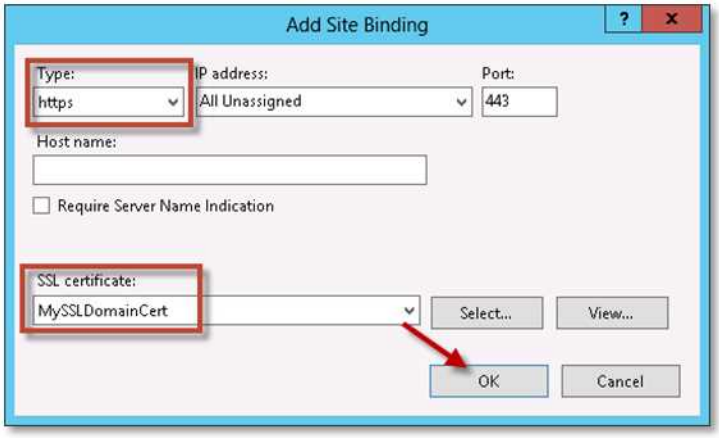
1. Open **IIS Manager**, and navigate to the **Content Manager SharePoint Server** website.
2. Right click on the site name in the **Connections** pane, and choose **Edit Bindings.**



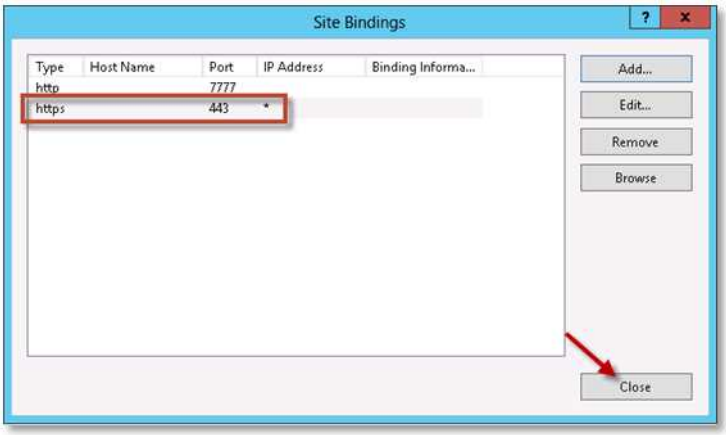
3. On the **Site Bindings** dialog, click **Add**.



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. Note the **https** entry has been added. **Close** the **Site Bindings** dialog.



6. To test, open a browser and navigate to https://<yourURL>/pages/dialogloader.html where yourURL is your load balanced URL, or the name of the Content Manager server, or configured

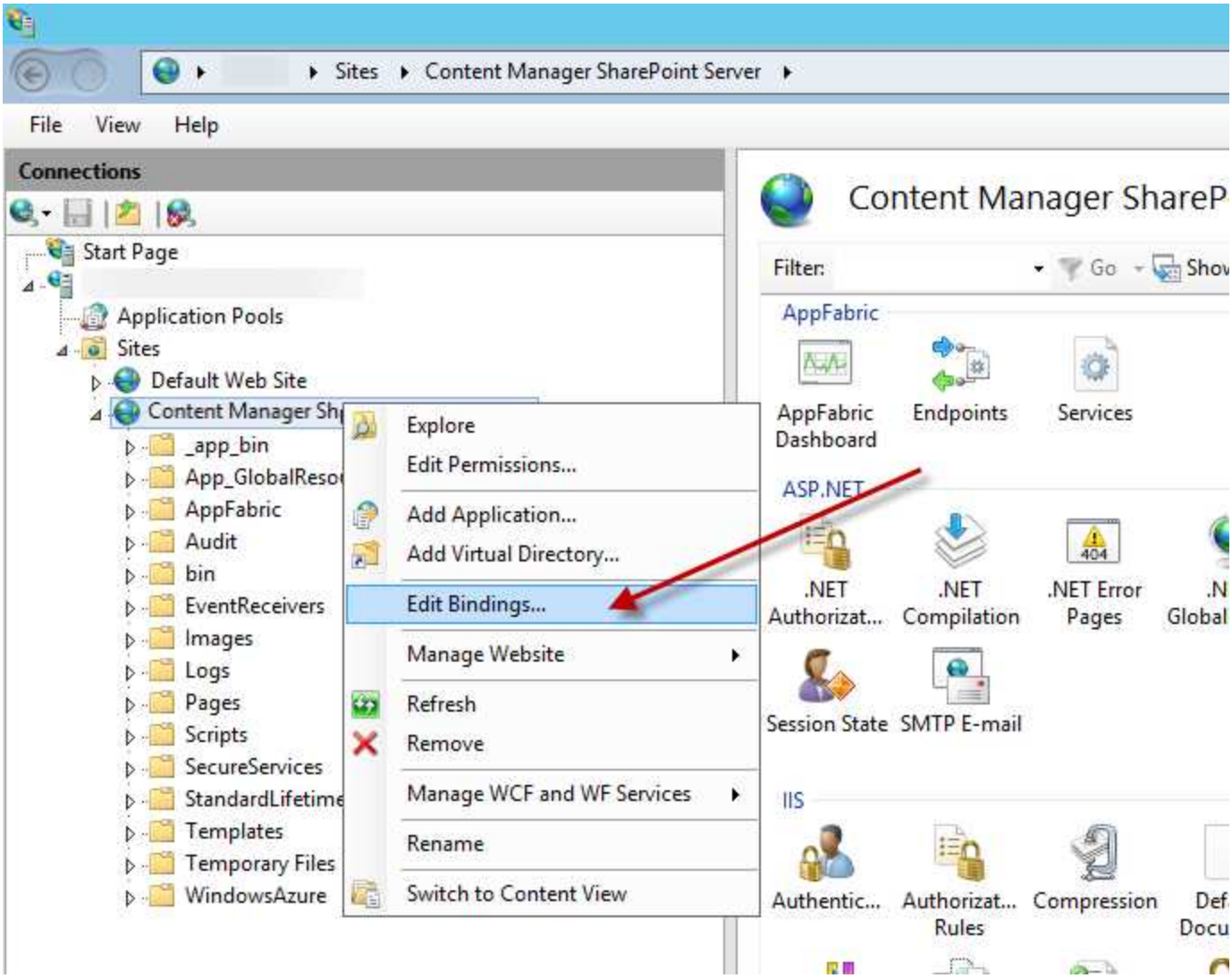
host header. You should see the 'Working on it' page, without any certificate errors.

The integration website is now configured to use HTTPS.

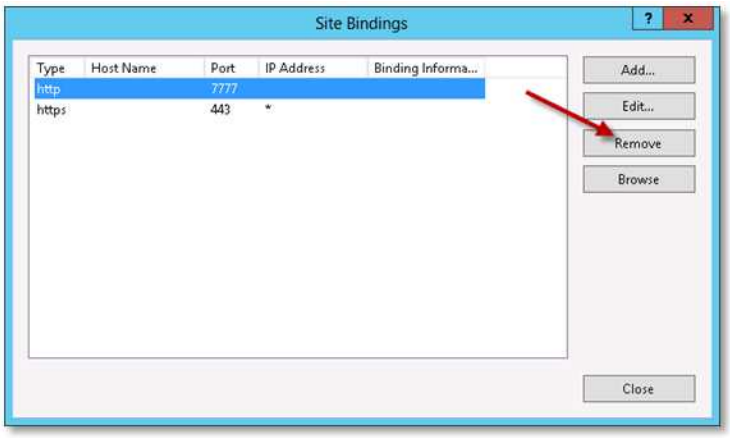
11.9 Disabling HTTP for a site

To remove the HTTP binding (This can sometimes cause problems with an SSL secured integration website) follow these steps:

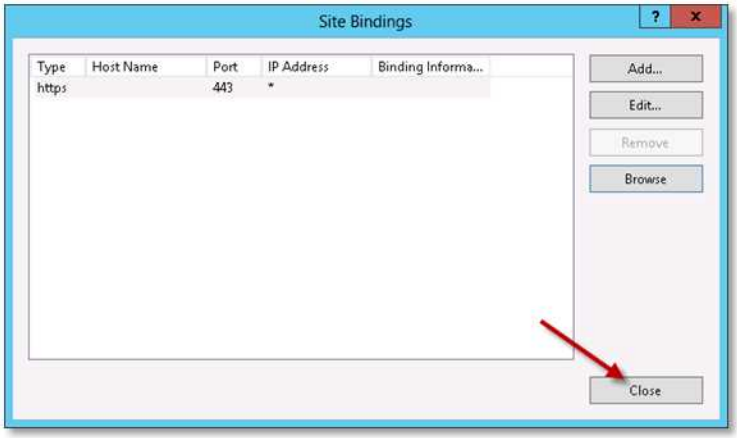
1. Open **IIS Manager**, and navigate to the **Content Manager SharePoint Server** website.
2. Right click on the site name in the **Connections** pane, and choose **Edit Bindings.**



3. On the **Site Bindings** dialog, highlight the **http** entry and click **Remove**.



4. Click **Yes** on the confirmation prompt.
5. Confirm the **http** entry has been removed and click **Close** on the **Site Bindings** dialog.



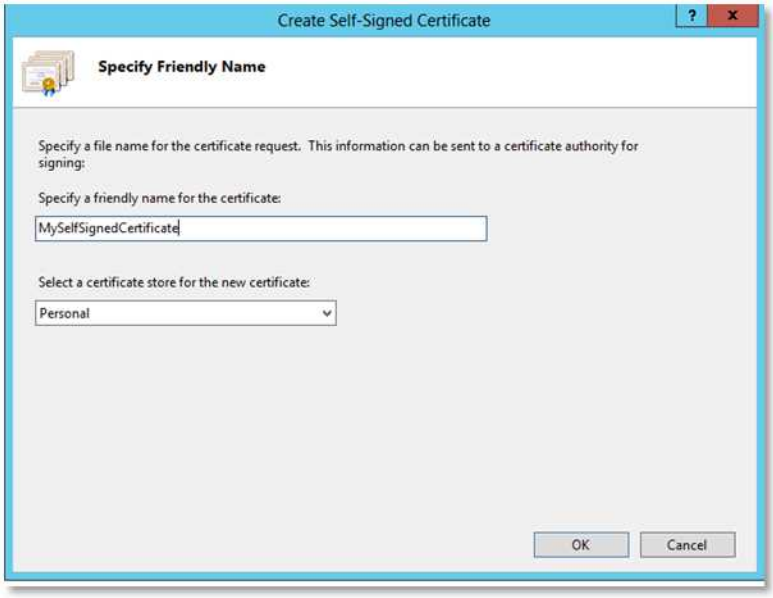
11.10 Creating a self-signed certificate

This section details the steps to create a self-signed certificate. It is assumed that you have already identified the folder that the certificate should be exported to, that the location has been created and the relevant permissions assigned to it.

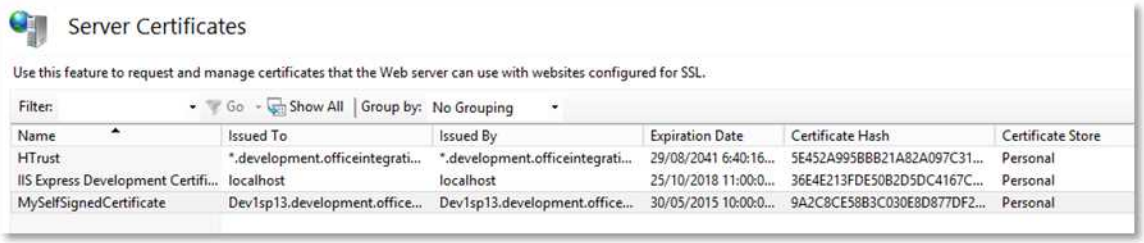
- Open IIS Manager
- In IIS Manager, select the server node in the tree view on the left.
- In the pane on the right (with “Features View” selected at the bottom) double click the “Server Certificates” icon

- Select the **Create Self-Signed Certificate** link from the set of links on the right side

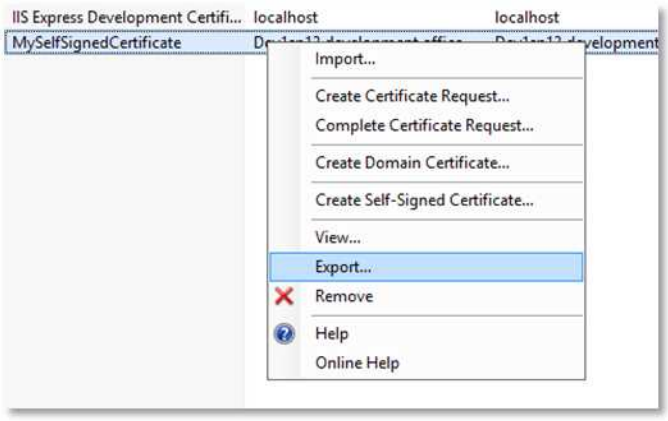
- Give the certificate a suitable name and choose “Personal” as the certificate store.



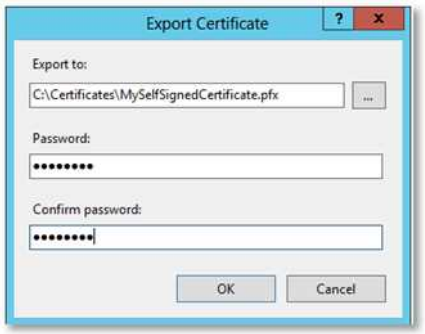
- You should now see the certificate in the list of server certificates



- Right-click the certificate in the list, and then select **Export**.

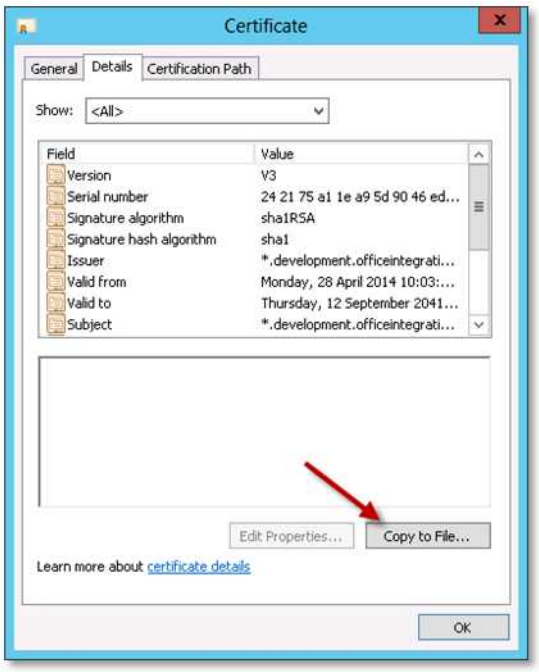


- Enter the full path to the file (choosing ".pfx" as the extension) as well as a password for the certificate. Then click OK



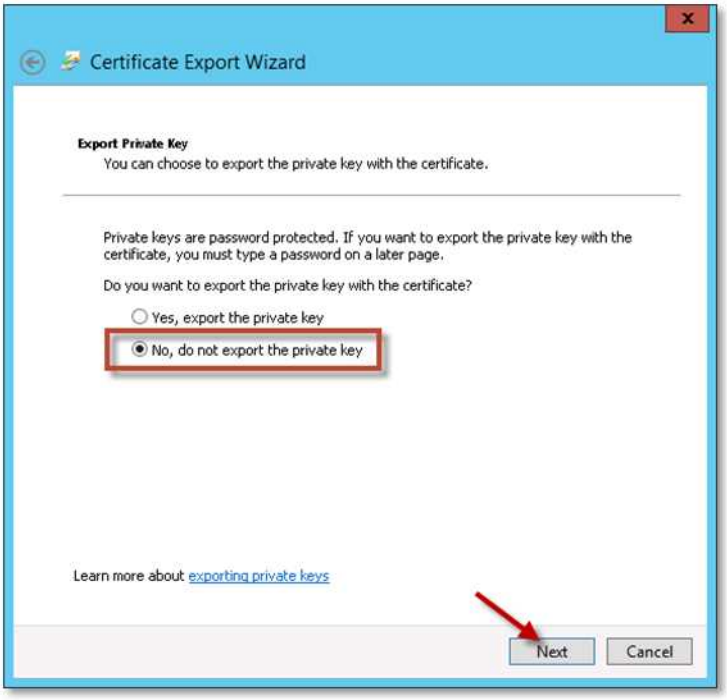
The following steps allow the creation of a corresponding ".cer" file for the certificate

- In IIS Manager, select the server node in the tree view on the left.
- In the pane on the right (with "Features View" selected at the bottom) double click the "Server Certificates" icon.
- Locate the required certificate in the list, double-click it to show the certificate details, and go to the details tab.
- Choose "Copy to File" to launch the Certificate Export Wizard.

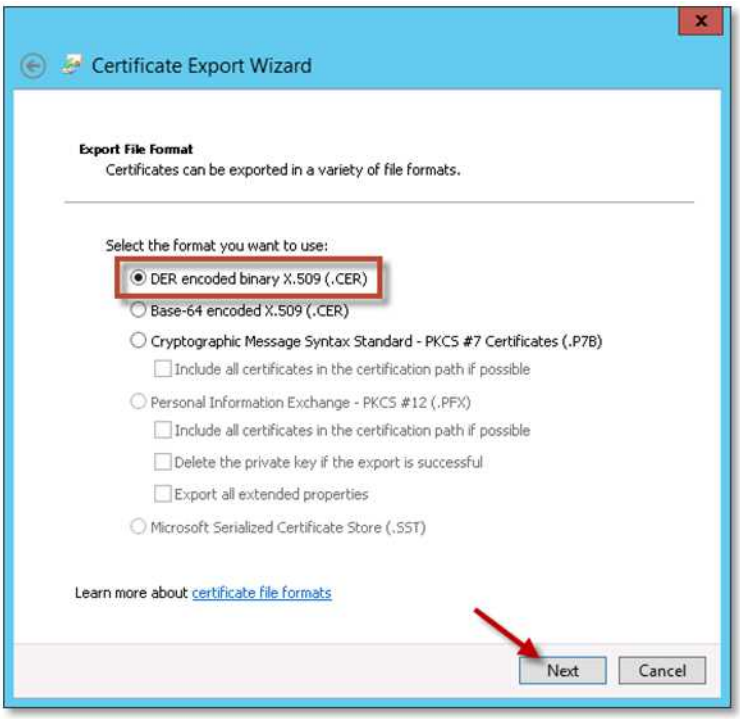


- Once the Certificate Export Wizard opens, click **Next**

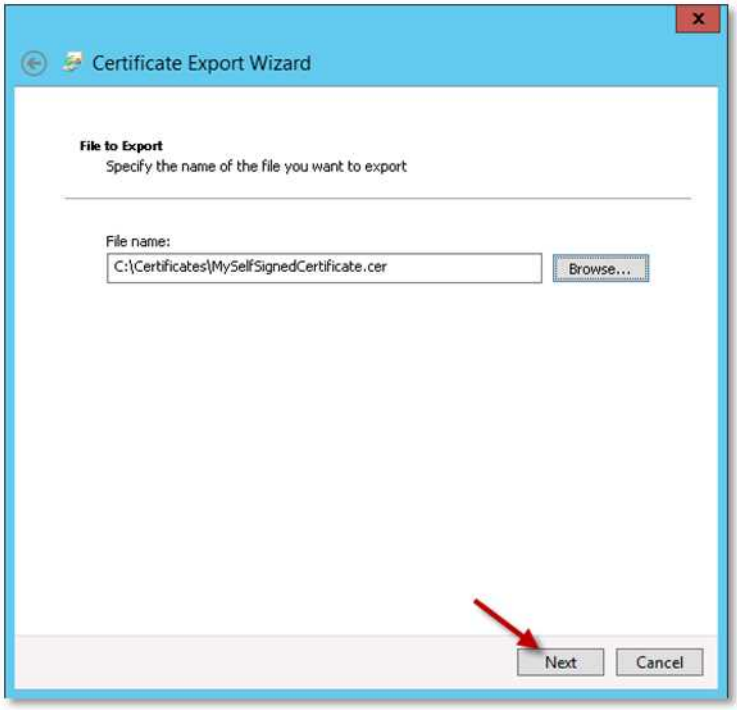
- Select “No, do not export the private key” and click **Next**



- Select to export as “DER encode binary X.509”, and click **Next**



- Specify the full file path to export the “.cer” file too, and click **Next**

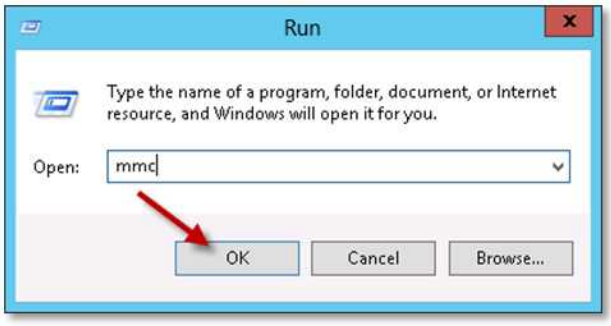


- Click **Finish** on the final page of the wizard

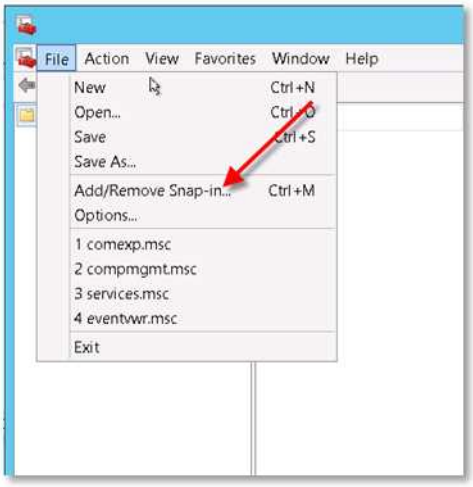
11.11 Using the Certificate MMC snap in

To open the **MMC** (Microsoft Management Console).

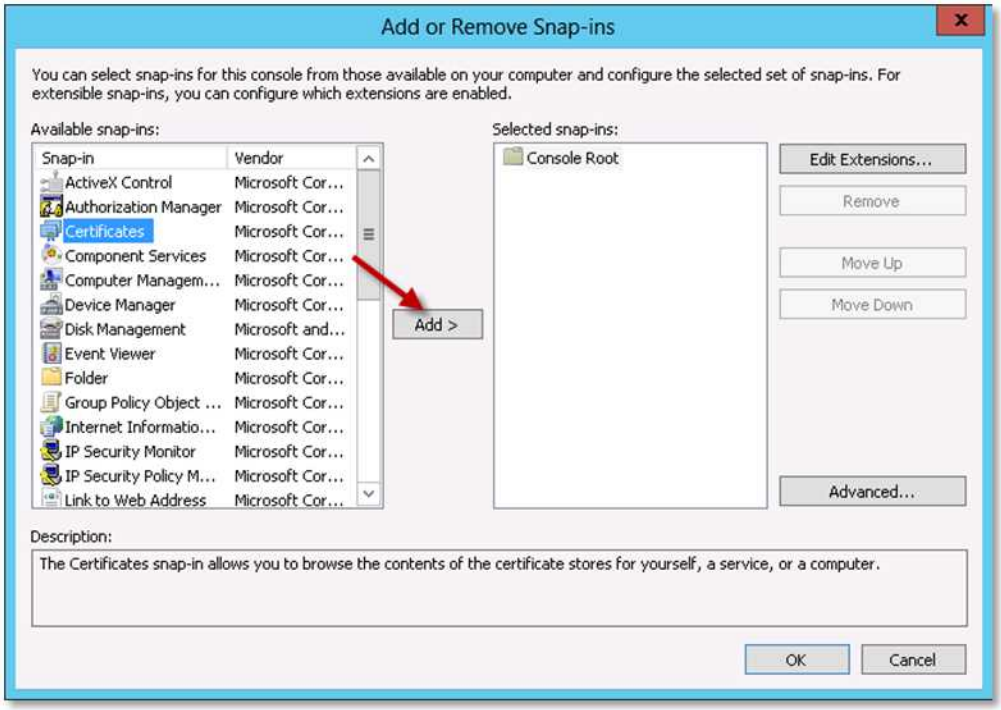
1. Open the Run window (Hit Start, type ‘run’, and launch).
2. In the **Run** dialog, type in ‘mmc’ and click **OK**.



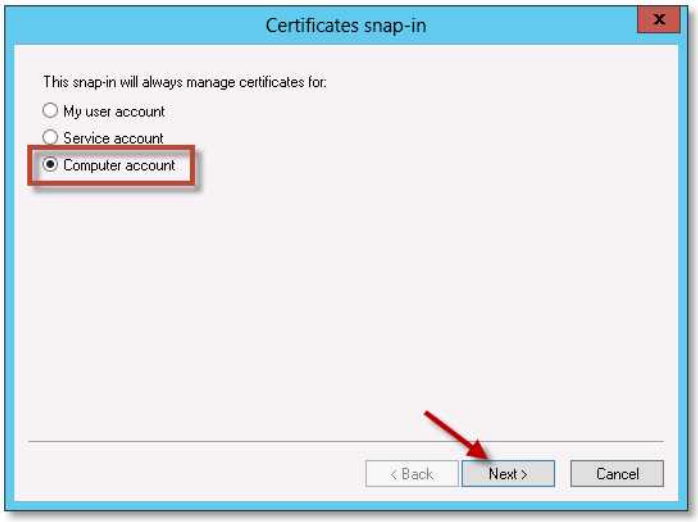
3. When the console opens, go to the **File** menu and select **Add/Remove Snap-ins**.



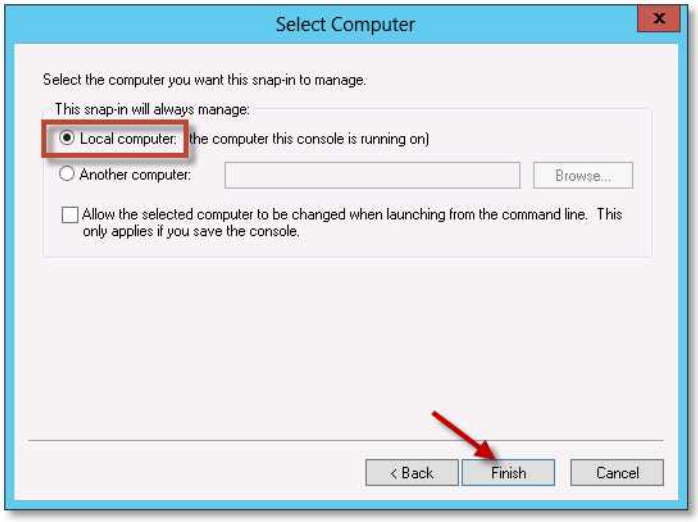
4. Select **Certificates** and click **Add**.



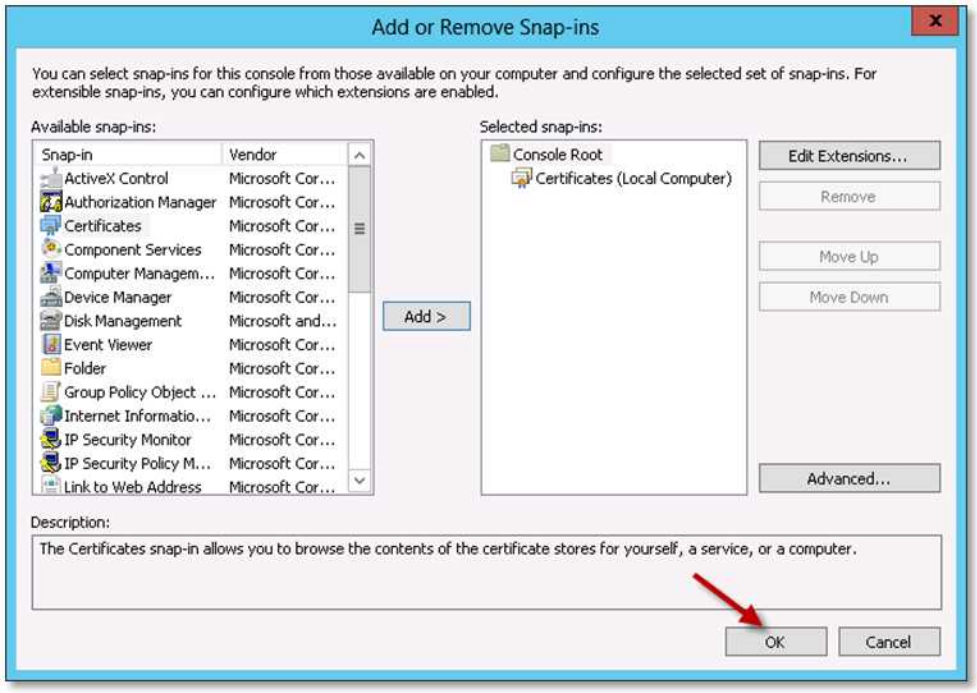
5. On the Certificates snap-in dialog, select **Computer account** and click **Next**.



6. Select **Local computer: (the computer this console is running on)**, and click **Finish**.



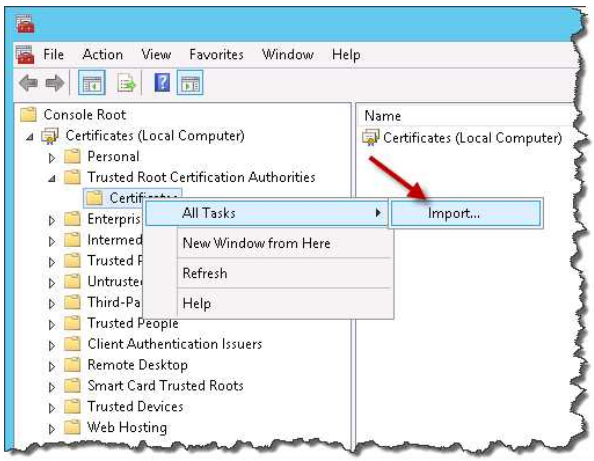
7. Click **OK** on the **Add or Remove Snap-ins** dialog.



11.12 Adding a certificate in the Trusted Root Certification Authorities store for a machine

Open the machine **MMC** with the certificate snap in. See the *Using the certificate MMC snap-in* appendix for instructions regarding how to do this.

- Expand the **Certificates** node in the left-hand pane.
- Expand the **Trusted Root Certification Authorities** node. Right-click on the **Certificates** sub-node, and select **All Tasks ->Import**.



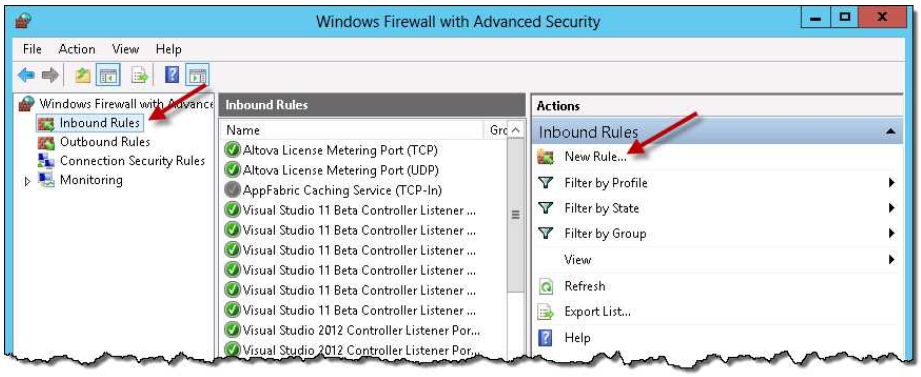
- Choose the ".cer" file to be imported.
- Ensure **Place all certificates in the following store** is selected and the certificate store is **Trusted Root Certification Authorities**.
- Click **Next**.

More details can be found in this article: http://technet.microsoft.com/en-us/library/cc754841.aspx

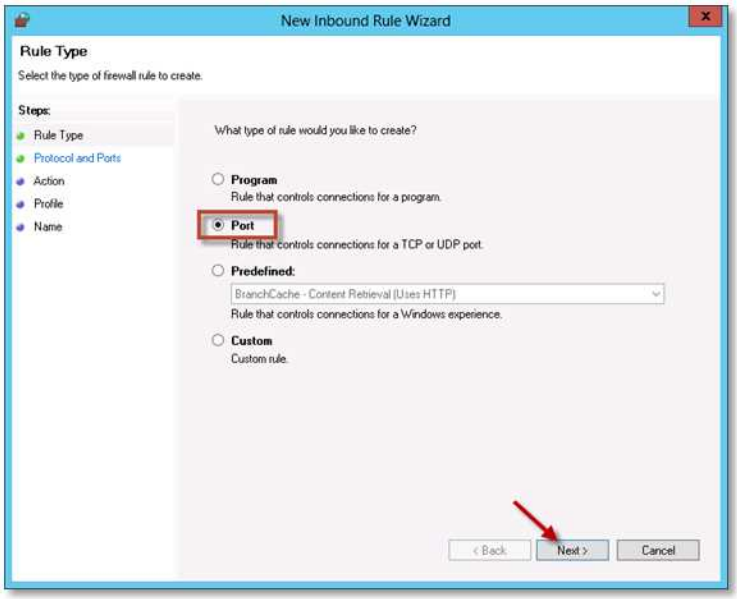
11.13 Opening a port

To open a port in the Windows Server 2012 Firewall:

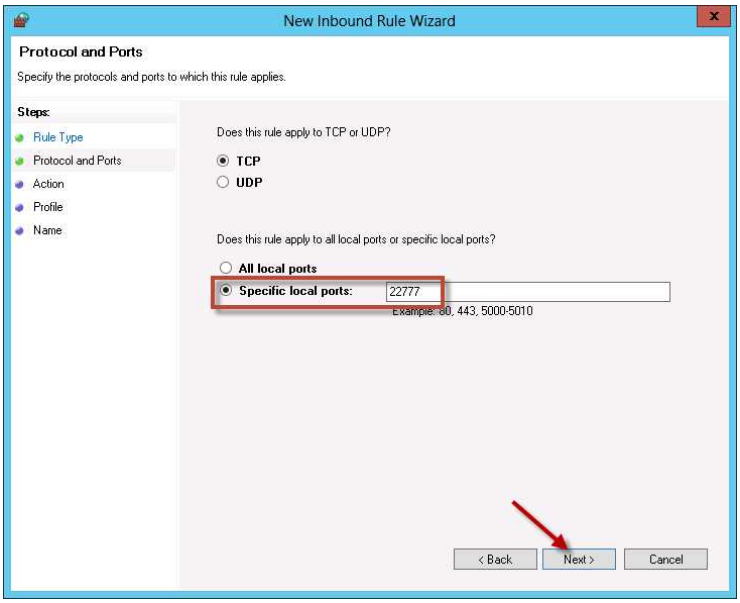
1. Go to the Windows **Start** menu, and type 'firewall'
2. Launch the **Windows Firewall** application.
3. In the left-hand navigation pane, click **Inbound Rules**. In the **Actions** pane, click on **New Rule**.



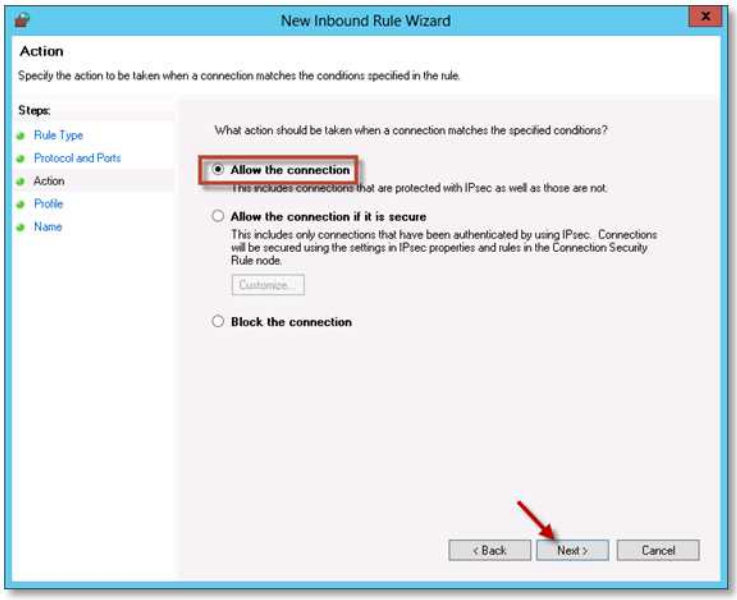
4. In the **New Inbound Rule Wizard**, choose **Port** and click **Next**.



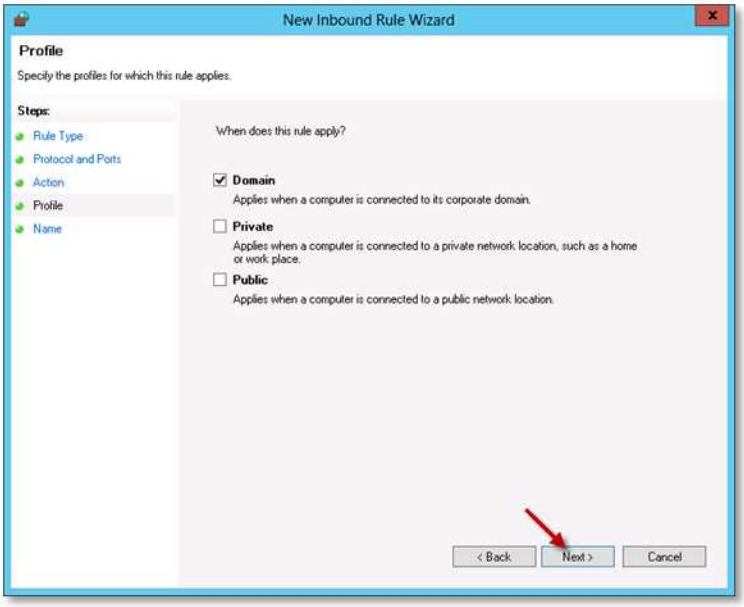
5. Make sure **TCP** is selected, and enter the specific port for the integration website. In this example, **port 22777** is being opened. Click **Next**.



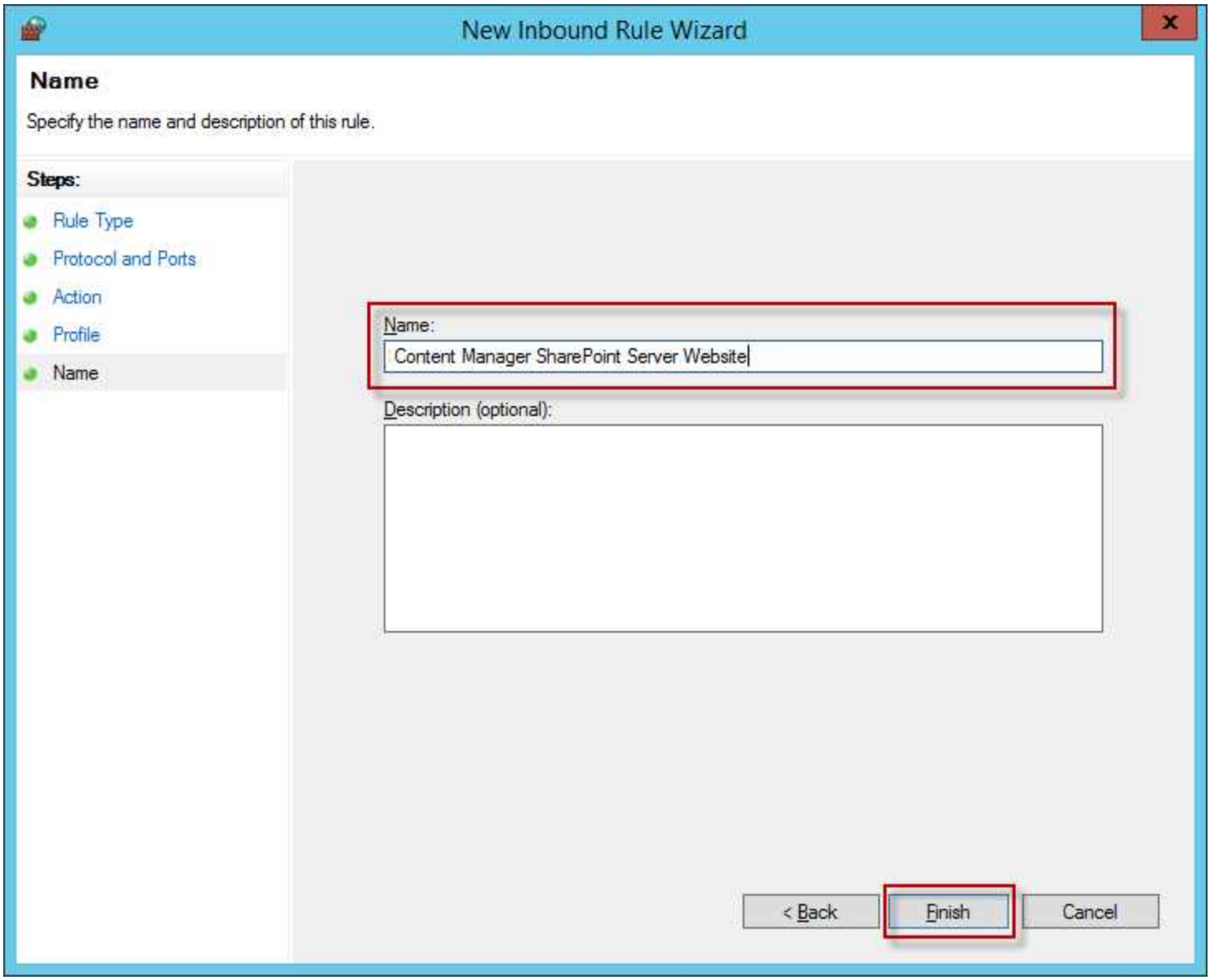
6. Accept the default option **Allow the connection** and click **Next**.



7. Choose which profile to apply the rule to (You may just want to apply to the **Domain** profile). Click **Next**.



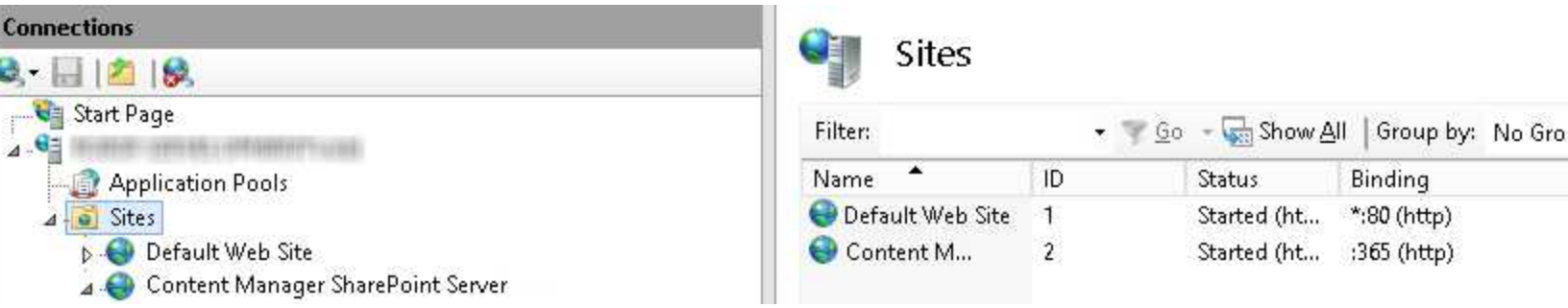
8. Give the rule a name e.g. ‘Content Manager SharePoint Server website’ and description. Click **Finish**.



11.14 Determining ports in use by IIS

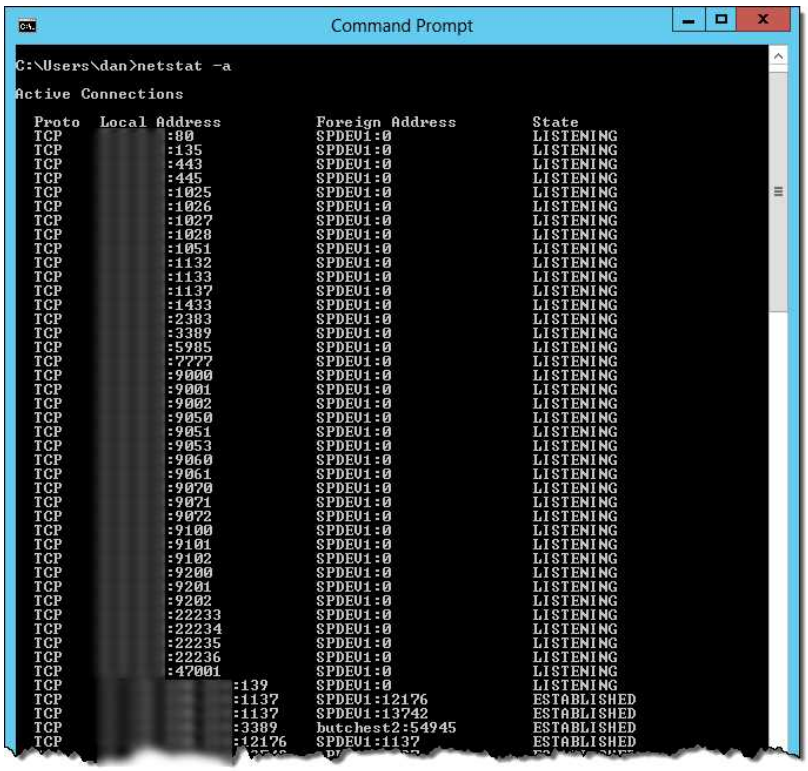
To determine which ports are already in use by existing IIS websites:

1. Open IIS Manager, and in the left-hand **Connections** pane, select the **Sites** node.
2. The list of websites, and their associated port bindings will be displayed in the main window.



Alternatively, to display a list of all ports in use (Not just IIS websites):

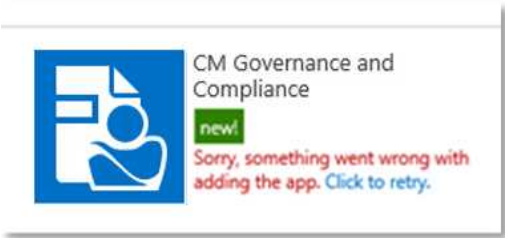
1. Open a **cmd** prompt.
2. Type `netstat -a`
3. A list of active ports will be displayed.



12 Appendix: Troubleshooting

12.1 Issues adding the app to a site

When adding the app to a site, you may see the following:



This can occasionally occur when this is the first instance of the app being added to the SharePoint farm. Usually a second attempt (using the “Click to retry” link) will resolve this issue.

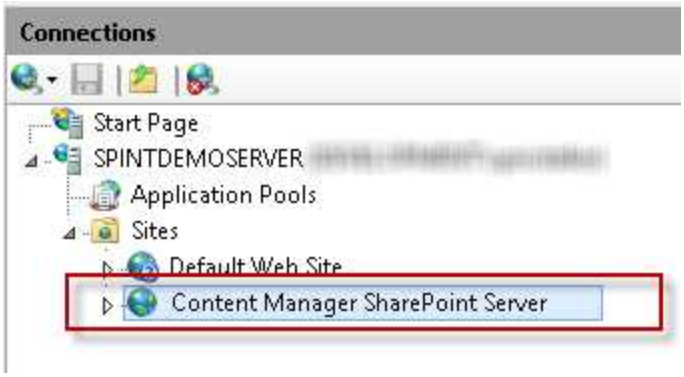
However, in rare cases, it has been found that an authentication setting for the server has been installed incorrectly. In this scenario, looking at the details of the app will provide further information regarding the installation error.

The error displayed may be similar to the following:

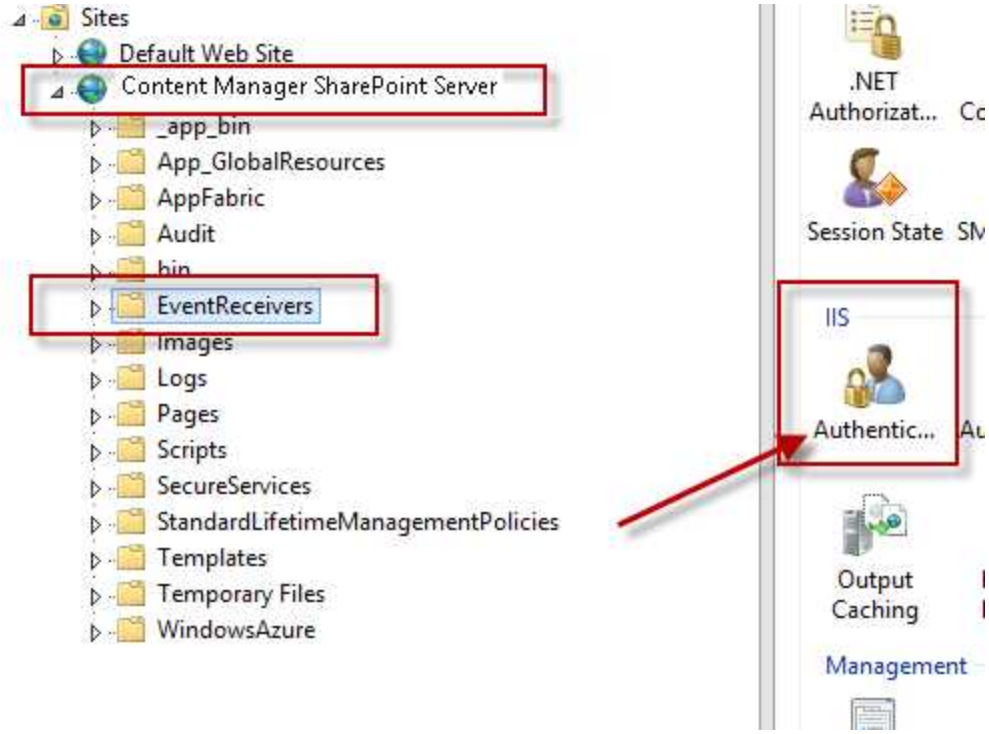
```
The remote event receiver callout failed.

Details: The HTTP request is unauthorized with client authentication scheme
'Anonymous'. The authentication header received from the server was ''
```

If a second attempt to install still doesn't succeed, and/or you are receiving a similar error to above, follow these steps.

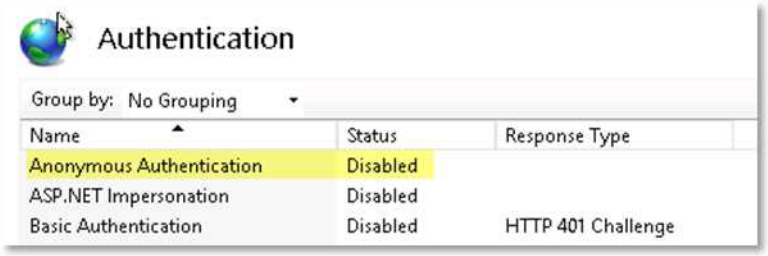
1. Open **IIS Manager** and expand the site: **Content Manager SharePoint Server**



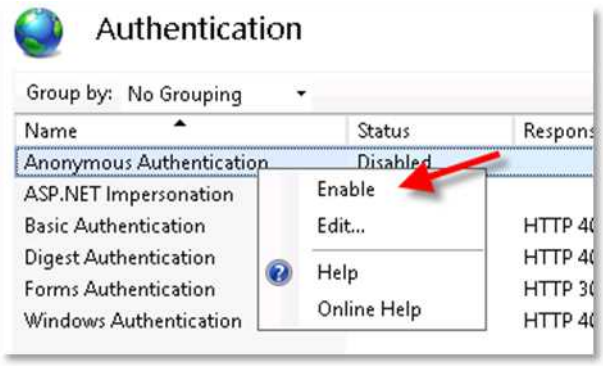
2. Select “EventReceivers”, in the right-hand pane, using the “Features view”, locate and double-click the “Authentication” icon



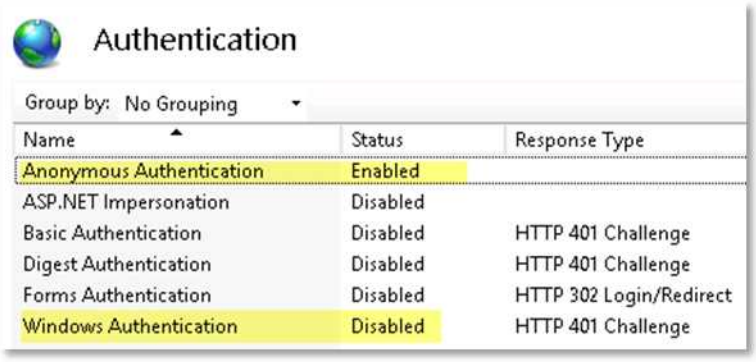
3. If “Anonymous Authentication” is “Disabled”, then it must be enabled.



4. Right click on “Anonymous Authentication” and select “Enable”



5. The authentication should now be set as follows



6. Confirm that you can browse to the URL *https://YourUrl/EventReceivers/AppEventReceiver.svc*

You should now be able to add the app to the site.

12.2 Viewing the log file

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. By default, this will be:

```
C:\Program Files\Micro Focus\Content Manager\Content Manager SharePoint Integration\Logs
```

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.

12.3 Turning on additional information

When exceptions occur, in some cases, there is additional information that can be provided to the user. This is turned off by default as it may contain information that could be used by malicious users. It is possible to turn this on if required.

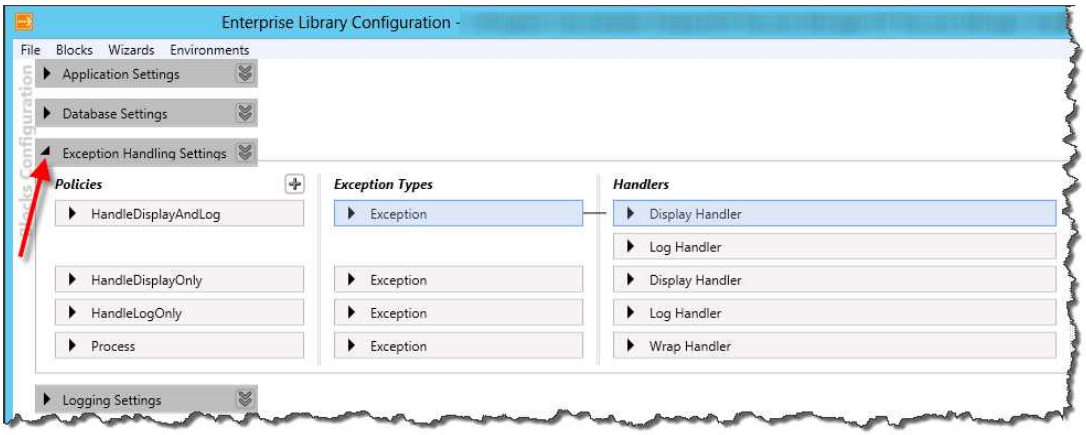
1. Navigate to the installation directory and locate the “bin” subdirectory. Double click the file named:

   ```
   EntLibConfig.exe
   ```

2. This opens the **Microsoft Enterprise Library** Configuration Console.
3. From the “File” menu choose “Open” then navigate to the installation directory and find the file named:

   ```
   EnterpriseLibrary.config
   ```

4. Select and open that file.
5. Expand the “Exception Handling Settings” section:



6. For the “HandleDisplayAndLog” handler, expand the “Display Handler” and locate the attribute “ShowAdditionalInformation”. Set this value to “true”

7. Repeat these steps for the “HandleDisplayOnly” block

8. Once complete, choose “File” then “Save”.

You must complete these steps on all servers in the Content Manager farm.

12.4 Turning on success logging

During fault finding, you may be asked to turn on success logging. This enables verbose logging that will allow the support team to better diagnose where issues may be occurring.

Success logging has a performance impact. Do not enable it unless absolutely necessary and disable it once fault finding is complete.

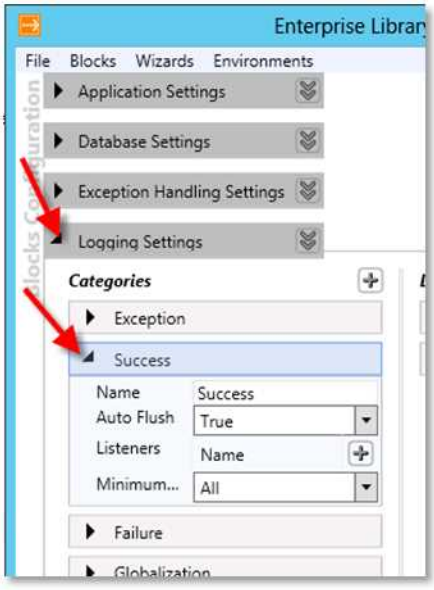
1. Navigate to the installation directory and locate the “bin” subdirectory. Double click the file named:

   ```
   EntLibConfig.exe
   ```

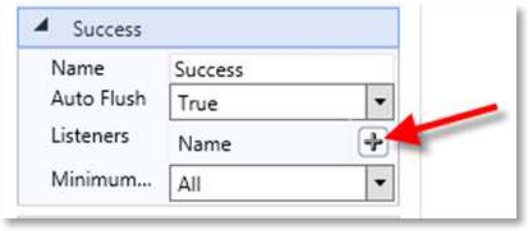
2. This opens the Microsoft Enterprise Library Configuration Console.
3. From the “File” menu choose “Open” then navigate to the installation directory and find the file named:

   ```
   EnterpriseLibrary.config
   ```

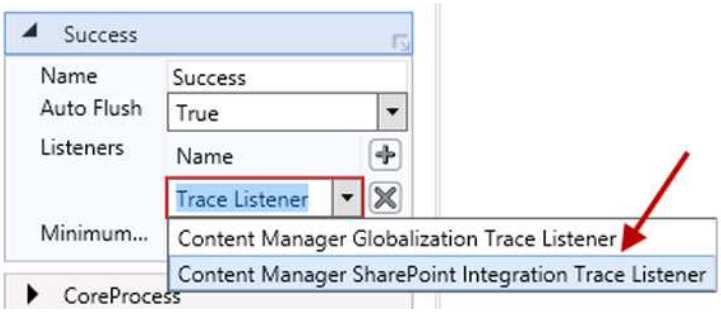
4. Select and open that file.
5. Expand the “Logging Settings” section followed by the “Success” block:



6. Click the “+” button next to the “Listeners” row:



7. From the drop down that is added, choose the “Content Manager SharePoint Integration Trace Listener”.



8. Once complete, choose “File” then “Save”.

You must complete these steps on all servers in the Content Manager farm.

12.5 Other logging categories

In 9.1 the following categories were introduced to reduce the amount of verbose logging.

- CoreProcess
- Search
- Security
- ManagementRules
- App
- RemoteEvents
- LifetimeManagement
- Jobs

Turning on the "Search" category will only log messages related to search. This is to make the fault finding process a lot easier. Refer to section 12.4 for turning on verbose logging.

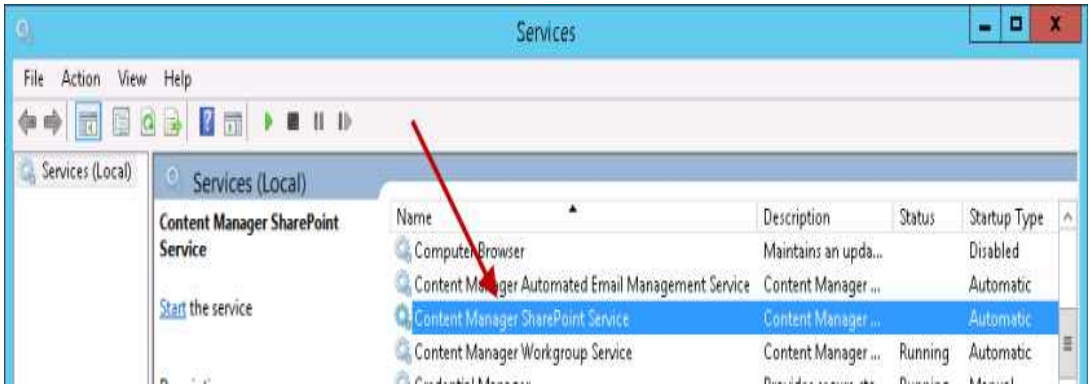
These logging has a performance impact. Do not enable it unless absolutely necessary and disable it once the fault finding is complete.

12.6 Job process fails to start

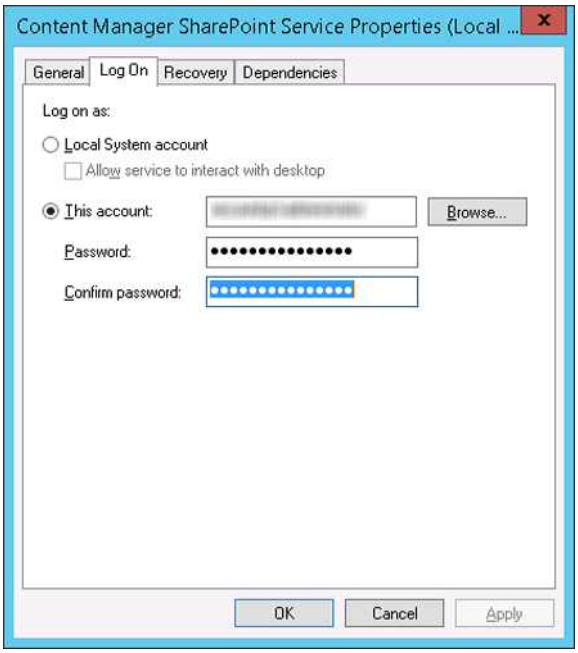
If the Content Manager SharePoint Service fails to start, any jobs added to the queue will stay in a pending state, and will not get processed. This is typically because the account details (username and password) were entered incorrectly during installation.

To rectify this:

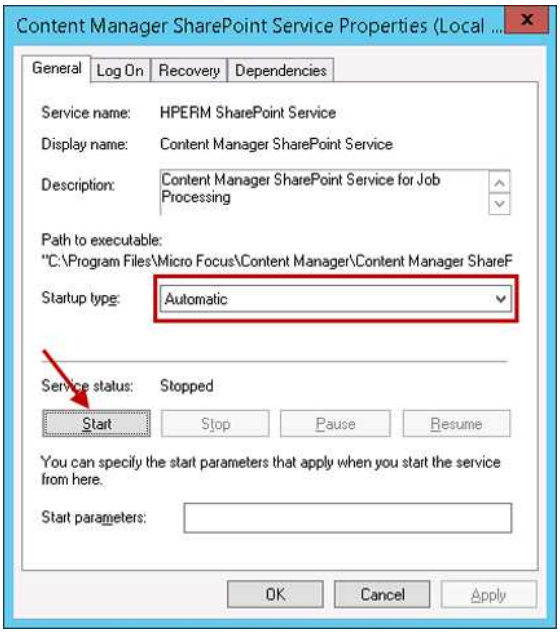
1. Go to Windows Services on the Content Manager Workgroup Server, where you installed the SharePoint integration MSI
2. Locate the Content Manager SharePoint Service in the list



3. Double-click the service name to open up the properties dialog, and go to the **Log on** tab
4. Browse for the appropriate domain service account, to ensure you are using a valid account in the directory



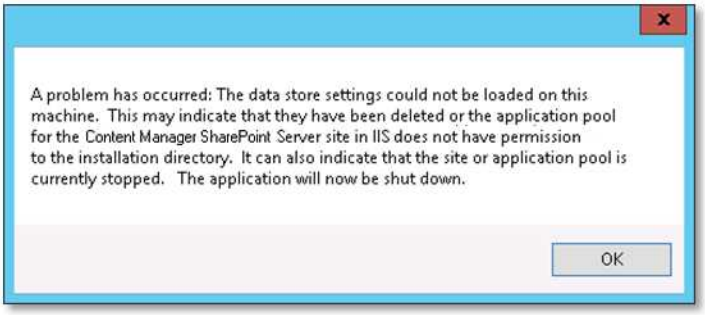
5. Re-enter the password, and confirm it, then click **Apply**
6. Go back to the **General** tab, make sure the **Startup** type is **Automatic**, and click on **Start**



7. If the account details are valid, the service should start, click **OK** to close the dialog

12.7 Cannot open the configuration tool due to error

When launching the integration configuration tool to change existing settings, you see the following error:



Firstly, make sure that you are launching the configuration tool using 'Run as Administrator'. If this doesn't resolve the problem, then continue with fault finding.

The error message does describe some potential causes, and these should be checked, but the most likely issue is that the configuration database is not accessible for some reason. Check to make sure that the SQL Server where the configuration database is hosted is available, and that the configuration database is still listed as an active DB in SQL Server Management Studio.

If for some reason, the database is no longer available, restore from backup and retry the configuration tool.

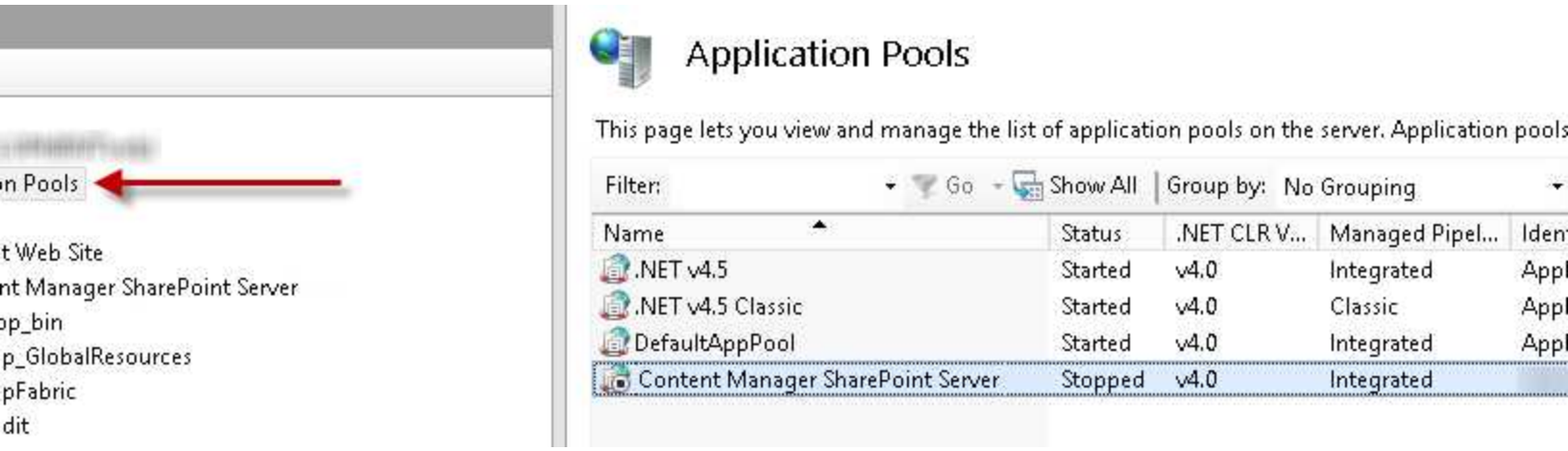
In the worst case scenario, if the database is irretrievable, you will need to delete the connection string stored for the existing database, before creating a new one. To do this follow the steps in *4.2.2 Creating a new app configuration database, on page 72* to establish a new configuration database.

12.8 App pages display – 'HTTP Error 503. The service is unavailable

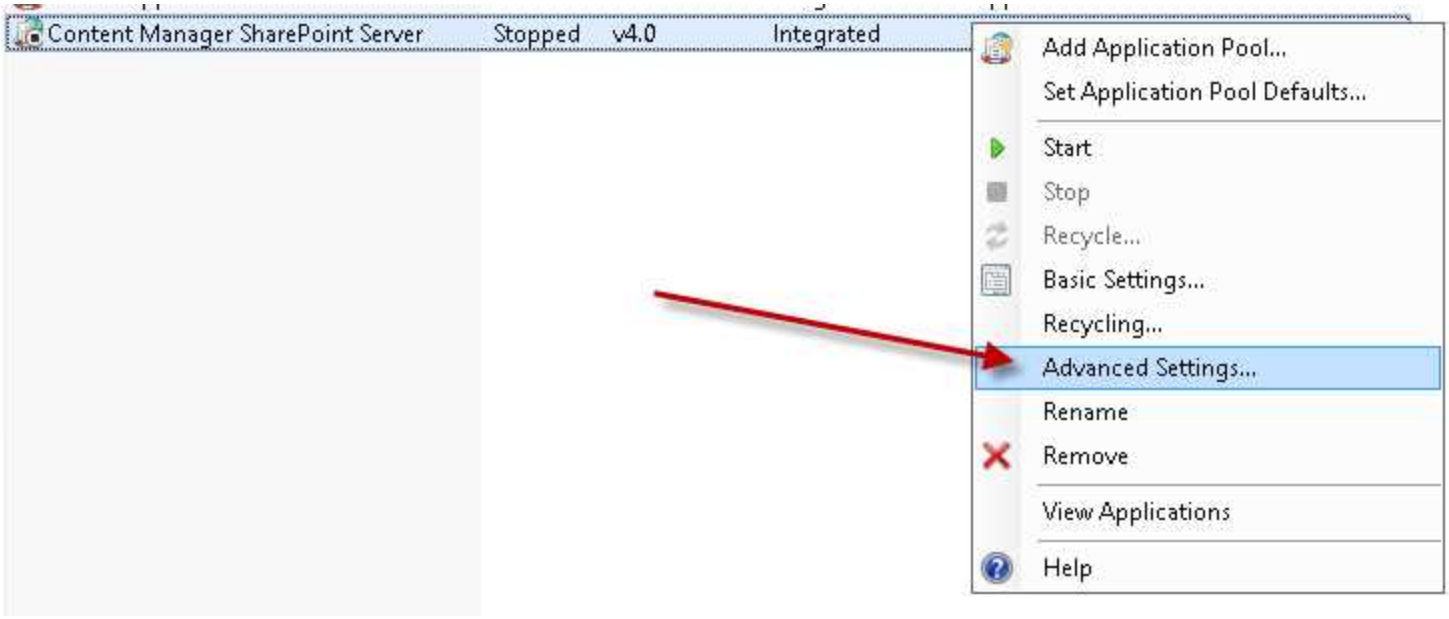
If when navigating to Content Manager Governance and Compliance app pages, you see the following page:

This means that the application pool for the **Content Manager SharePoint Server** website has failed to start, most likely due to incorrect account credentials. To rectify this:

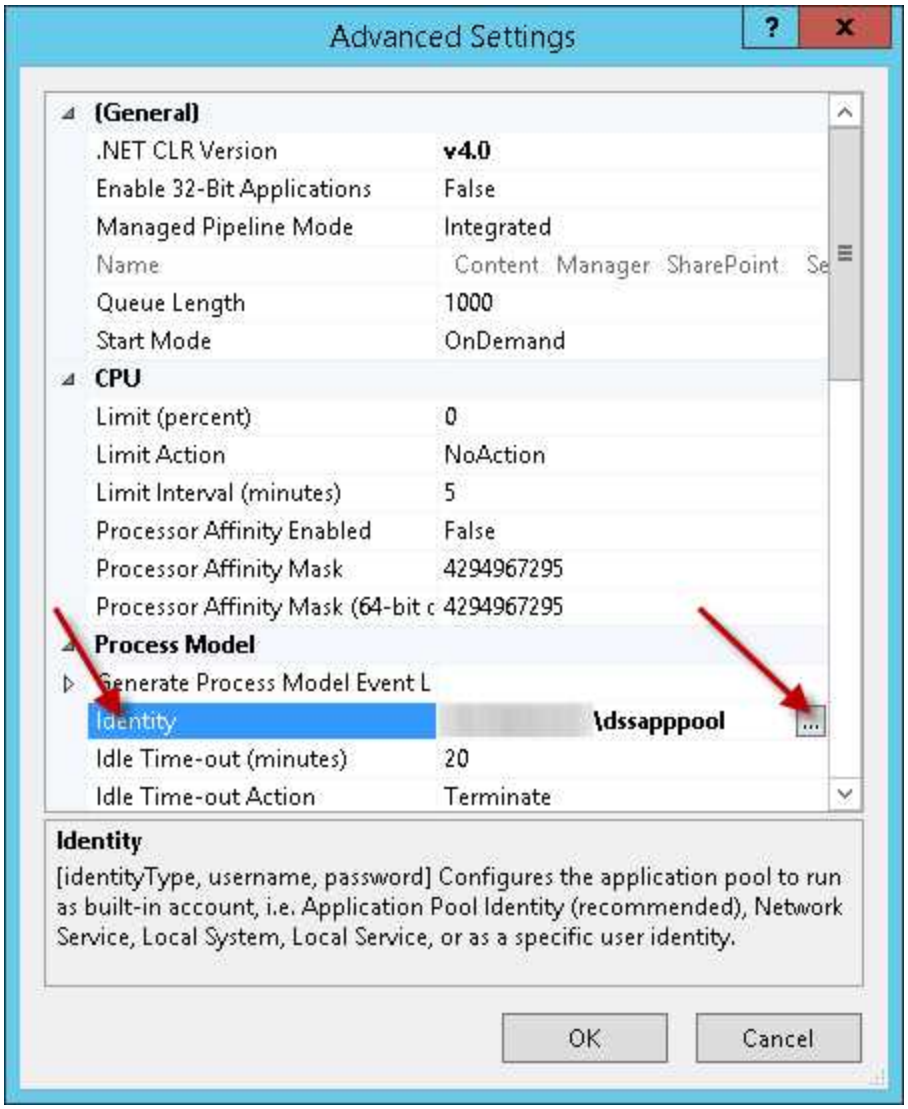
1. Open **IIS Manager**, and in the **Connections** pane, click on **Application Pools**. The main window will display a list of all application pools



2. Locate the **Content Manager SharePoint Server** application pool in the list
3. Right-click on the entry and choose **Advanced Settings**

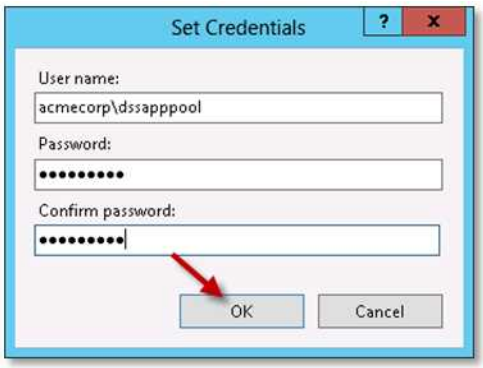


4. In the **Advanced Settings** dialog, locate the **Identity** row, select it, and then click on the **Browse** button that appears alongside the account name

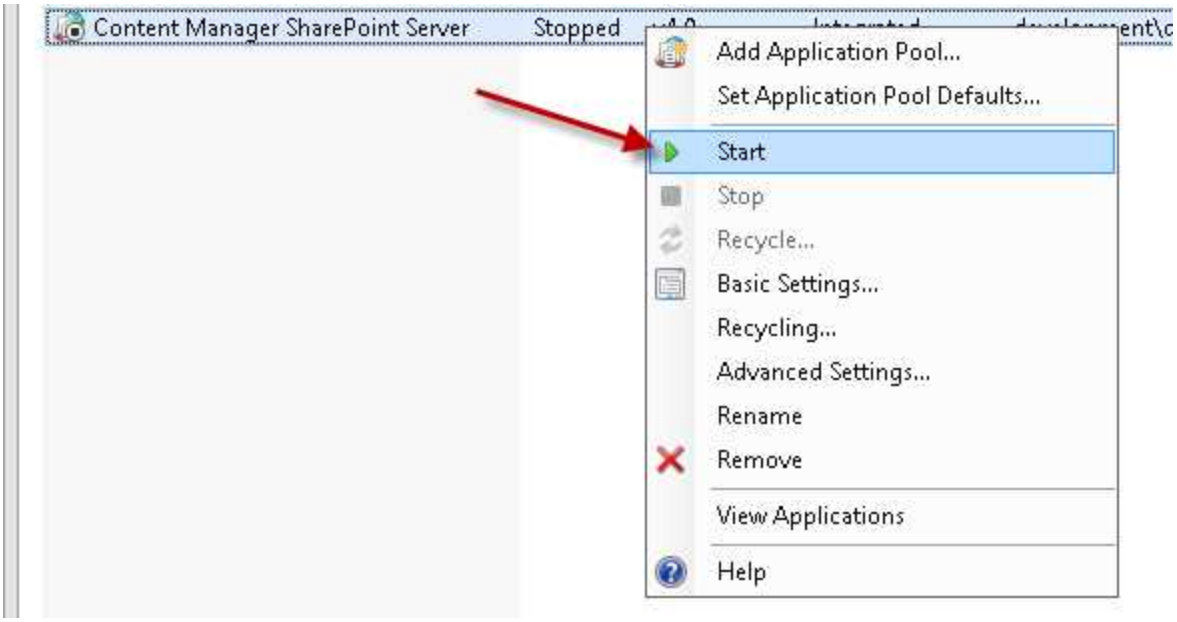


5. In the **Application Pool Identity** dialog, click on **Set**

6. In the **Set Credentials** dialog, re-enter the correct account credentials, with username in the format domain\username. Click **OK**



7. Click **OK** to close the **Application Pool Identity** dialog, and then **OK** to close the **Advanced Settings dialog**
8. the **Content Manager SharePoint Server** application pool in the list, and choose **Start**



9. If the account credentials are now valid, the status of the application pool will change to **Started**

12.9 Configuration tool takes a long time to load

If the configuration tool takes a long while to start up, this is an indication that caching is incorrectly configured, or not working. To resolve this:

For on premise environments

Refer to the *Configuring AppFabric* and *Troubleshooting AppFabric* appendices. Ensure AppFabric is correctly installed and that the cache cluster is running before restarting the configuration tool.

For Windows Azure environments

If using Windows Azure, it is likely that the caching options have not been set in the tool. See section *4.3 Set caching options, on page 76* for more details.

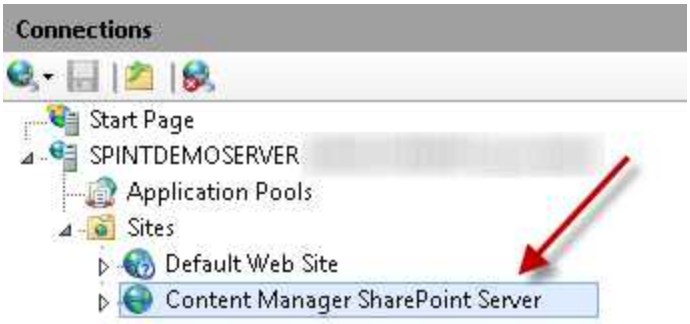
12.10 Failed to create client context error on pages

If when visiting Content Manager Governance and Compliance app pages, you see a **Sorry, something went wrong** error:

> Message: Failed to create client context for site, http://spi10-spwfem2/sites/Content Manager. This means that the current user does not have the permission on this site or the app configuration settings are invalid.
>
> IntegrationException - Error Number:C1904, Additional Information:, Message:Failed to create client

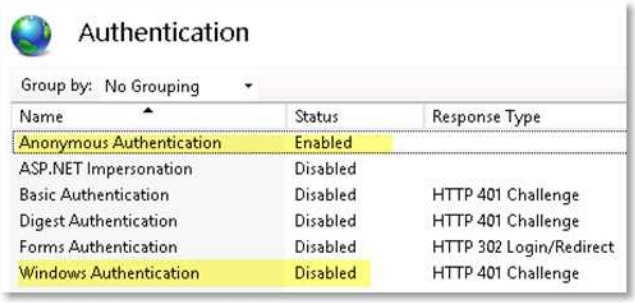
This is because, in some scenarios, during installation, the Content Manager SharePoint Server inadvertently uses anonymous access in IIS. To resolve the issue:

1. Open IIS Manager and select the site: **Content Manager SharePoint Server**

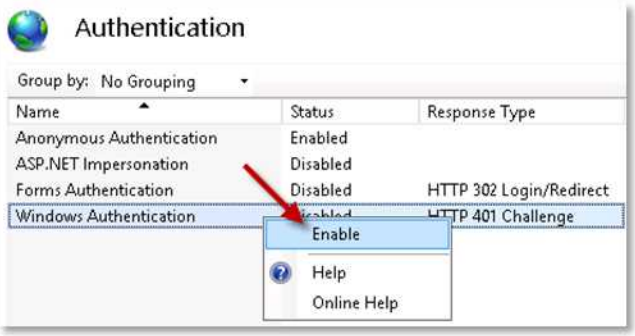


2. In the right-hand pane using the "Features view" locate and double click the **Authentication** icon

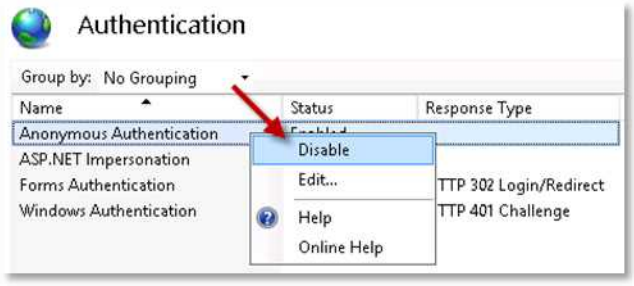
3. Authentication will initially show **Anonymous Authentication** as **Enabled** and **Windows Authentication** as **Disabled**



4. Right-click on **Windows Authentication** and choose **Enable**



5. Right-click on **Anonymous Authentication** and choose **Disable**



6. Test the app pages again, they should load without any errors

13 Appendix: Example PowerShell Scripts

These example scripts are provided to help with troubleshooting, and in some cases to aid in bulk actions.

> Micro Focus takes no responsibility for the use of these scripts. They are intended to be used by administrators with sufficient PowerShell knowledge, in order to customize and tweak these scripts in accordance with local systems and policies. If you are unsure, test the script in a non-production environment. If you are still unsure, DO NOT USE them.

13.1 SharePoint

13.1.1 List all SharePoint Trusted Security Token Issuers

```
Get-SPTrustedSecurityTokenIssuer | select Name,RegisteredIssuerName | fl
```

13.1.2 App Management

Remove Content Manager app from all sites and site collections in a web application

```
## Remove-App.ps1
## Remove (uninstall) all app instances for a product id on an particular web
application
##
## Usage:
##
##  ## Remove an App by uninstalling all the instances of an App
##  Remove-App -productId <ProductId> -webAppUrl <webAppUrl>
##

param(
    [Parameter(Mandatory=$true)] [String] $webAppUrl
    )

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

# Set excluded paths as comma-delimited strings, replace these examples
[array]$excludedPaths = "http://spdev12013/sites/inplacerm/not",
                        "http://spdev12013/sites/my/nothing"

# Set Content Manager App ProductID
$productId = "C493061F-E2BB-4516-8537-45C4FB005D83";

function RemoveInstances($productId = $null, $webAppUrl = $null)
{
    $outAppName = "";
    $sites  = Get-SPSite -WebApplication $webAppUrl
```

```
    $outWebs = @()
    foreach($site in $sites){
        if($site.AdministrationSiteType -ne "None"){
            continue;
        }
        $webs = Get-SPWeb -site $site
        foreach($web in $webs) {
            $appinstances = Get-SPAppInstance -Web $web
            foreach($instance in $appinstances) {
                # Check if there are sites where the property should not be changed

                if ($excludedPaths -notcontains $_.Url) {
                   if($productId -eq $instance.App.ProductId) {
                     if ($outAppName -eq "") {
                         $outAppName = $instance.Title;
                         }
                         $outWebs += $web;
                         Write-Host "Uninstalling from" $web.Url;
                         Uninstall-SPAppInstance -Identity $instance -
confirm:$false
                     }
                }
            }
        }
    }
    return ($outAppName,$outWebs)
}

$confirm = Read-Host "This will uninstall all instances of the App and is
irreversible. Proceed? (y/n)"
if($confirm -ne "y"){
    Exit
}

$global:appName = $null;
$global:webs = $null;

[Microsoft.SharePoint.SPSecurity]::RunWithElevatedPrivileges(
{
    $returnvalue = RemoveInstances -productId $productId -webAppUrl $webAppUrl;
    $global:appName = $returnvalue[0];
    $global:webs = $returnvalue[1];
}
);

$count = $global:webs.Count;
if($count -gt 0){
    Write-Host "All the instances of the following App have been uninstalled:";
    Write-Host "App Name:" $global:appName;
    Write-Host "Product Id: $productId";
    Write-Host "Number of instances: $count";
    Write-Host "";
    Write-Host "Urls:";
```

```
    foreach($web in $global:webs) {
        Write-Host $web.Url;
    }
}
else {
    Write-Host "No instances of the App with Product Id $productId found.";
}
return;
```

13.1.3 Removal of the SharePoint 2010 Integration Solution

Please do not retract and remove the SharePoint 2010 Integration solution. Instead please read this blog article for latest information on the correct steps and tools to use to perform the removal and clean-up of the SharePoint 2010 Integration solution: http://www.imsharepoint.net/blog/2017/6/21/how-to-upgrade-from-sharepoint-2010-integration-solution-to-sharepoint-2013-integration-app

13.2 Windows Azure

13.2.1 Create an Windows Azure Managed Cache

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

14 Appendix: Custom Claims Implementation

The information contained within this appendix is worded using Engineering terms and concepts, please be aware that this appendix is intended for an audience which requires a software development background.

In order to leverage the new custom claims feature within the application, you will need to ensure that you have set up the claim rules on your AD server. For more information on how to set up your AD, see Chapter 4.7 Additional configuration to support ADFS.

As a starting point, the application comes with a sample custom claim to allow you to see how the features work using custom claims from an LDAP setup. In your installation directory, you can see two new files:

- SampleClaimDescriptionMapping.xml
- ClaimDescriptionProviders.xml

Located on the MSI is a C# project which will allow you to write a custom claims implementation of your own.

The ClaimDescriptionProviders file is provided to allow administrators the ability to define their own endpoints to use as custom claim providers.

Below is the XML content of that file, showing that **for each**custom provider an associated tag must be placed within the "Providers" element ensuring that the following attributed are also supplied:

Assembly	The fully qualified name of the dynamic link library (.dll) file which provides the functionality for the custom claim.
Class	The fully qualified name-space which is used as the entry point to the aforementioned assembly.

```
<?xml version="1.0" encoding="utf-8" ?>
<Providers>
 <Provider Assembly="HPE.Integration.SharePoint.Claims.Provider"
Class="HPE.Integration.SharePoint.Claims.Provider.SampleProvider"></Provider>
</Providers>
```

In order to leverage the custom claims functionality, you also need to provide a mapping which defines what your custom claim is using as the authentication component.

```
<?xml version="1.0" encoding="utf-8" ?>
<ClaimDescriptions>
 <!-- This sample provider assumes you have created a custom ADFS claim
description and mapped that to the department user property -->
 <ClaimDescription Name="Department" ActiveDirectoryAttribute="Department" />
 </ClaimDescriptions>
```

The SampleClaimDescriptionMapping file clearly shows how to create such an entry. As in the previous file, each custom claim requires its own "ClaimDescription" XML tag with the following attributes present:

Name	A plain text attribute which will be used on the user interface.
ActiveDirectoryAttribute	The name of the variable which will be used as the claim.

> **NOTE:** This is an example only. You will need to ensure that the custom code you use to

15 Appendix - 8.3 Upgrading the Records Manager Farm database

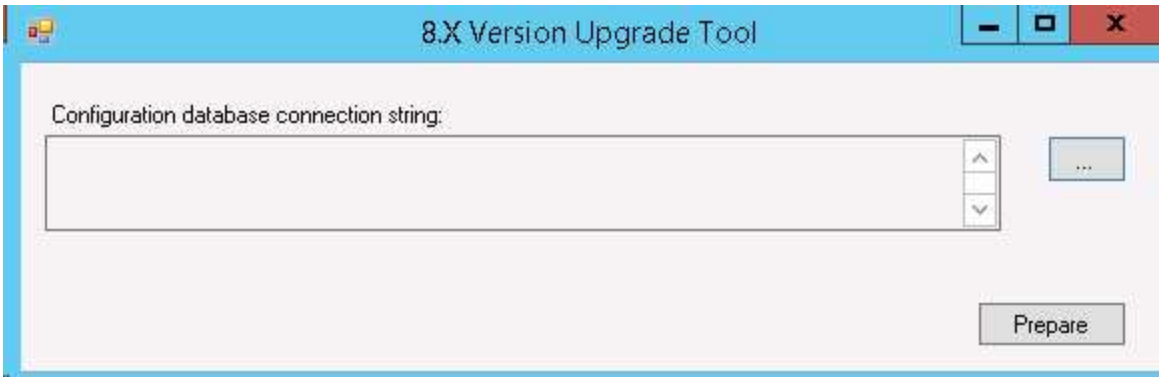
When upgrading from 8.3 the Records Manager Farm database needs to be upgraded using the HPE.Integration.SharePoint.8xVersionUpgradeTool.exe tool

To perform this upgrade follow the below steps:

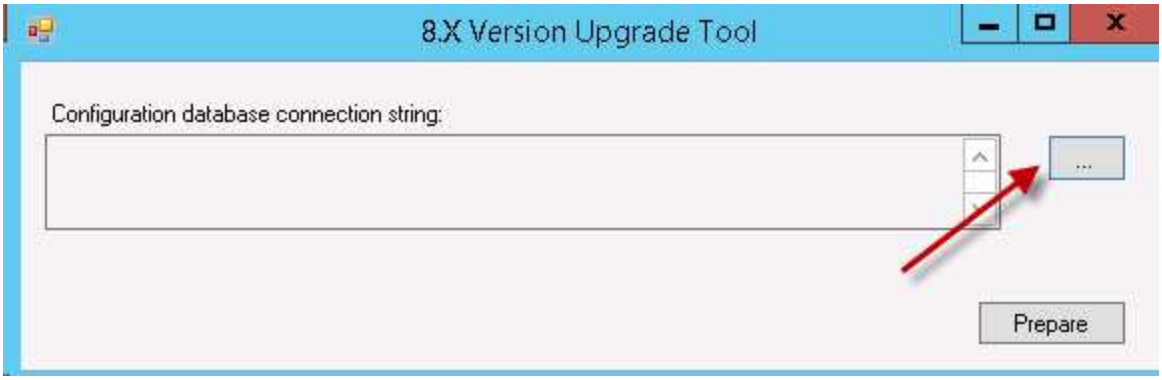
1. Upgrade the SharePoint Integration using the CM_SharePointIntegration_x64.msi

2. Navigate to the installation directory > Bin > and run the tool as Administrator:

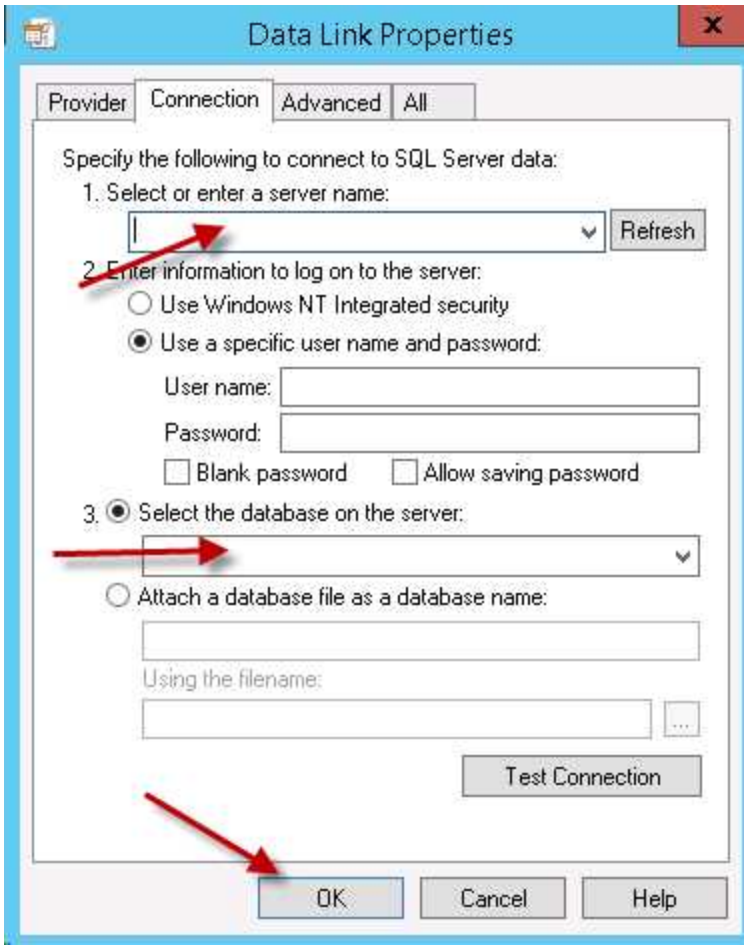
HPE.Integration.SharePoint.8xVersionUpgradeTool.exe



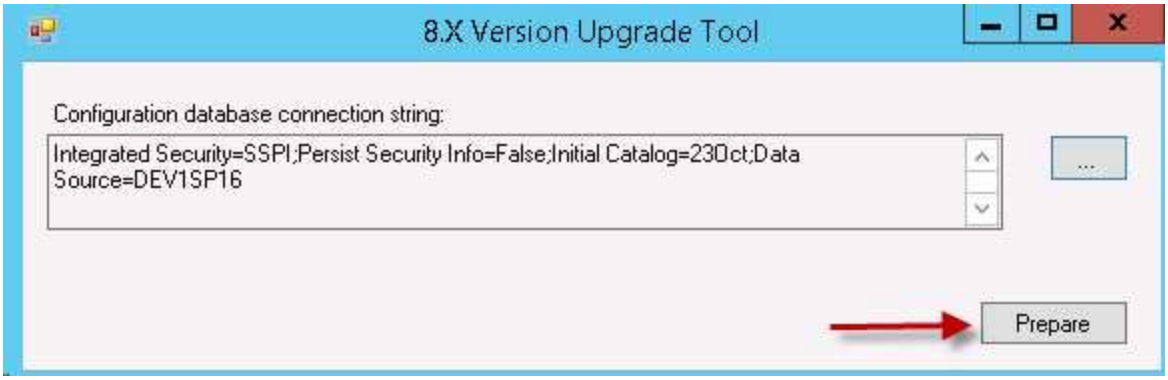
3. Click the quickselect:



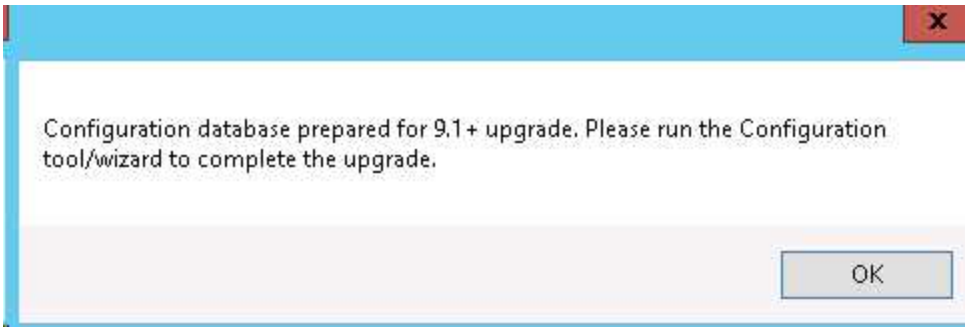
4. Populate the database:



5. Select Prepare:



6. Once the Version upgrade tool completes the below message will display:



After the Version upgrade tool has completed the Configuration Tool need to be configured. To do this:

1. Populate the 'Content Manager Farm database connection string'.

2. Before publishing the configuration navigate to Tenants > tenant > configure > Permissions Tab and populate the Primary Configuration Administrator.

3. Continue with 5.5 Upgrading the SharePoint App

16 Appendix - Additional configuration for a multi domain (SharePoint and Content Manager in 2 separate domains) ADFS setup

This chapter describes the additional configuration steps that need to be performed to get the Content Manager Governance and Compliance app running in an ADFS environment when the SharePoint instance and Content Manager server are located on two separate domains. These steps are applicable if and only if your SharePoint instance is located on premise. For SharePoint online please refer to the document "Configuring Content Manager integration for SharePoint Online using Azure AD authentication". The assumption is made that you have enabled ADFS for your SharePoint web application and for the Content Manager Governance and Compliance app IIS site. If not refer to 4.7 Additional configuration to support ADFS

The following configuration need to performed, before you publish the settings using the configuration tool.

1. Token Provider

The Content Manager Governance and Compliance app comes with a token provider. This provider is available in the assembly HP.Integration.SharePoint.Token.Provider which can be found under the installation directory along with the other integration assemblies. The Content Manager Governance

and Compliance app will load this provider, in an ADFS environment when a token is required (during configuration propagation and while relocating older versions of a document).

1.1 Configuring Token Provider

This token provider reads the values for the ADFS from the STSDetails.xml under the installation directory. The contents of this file are:

```
<STSDetails>
  <EndPoint></EndPoint>
  <UserName></UserName>
  <Password></Password>
  <RelyingPartySharePoint></RelyingPartySharePoint>
  <RelyingPartyUrlSharePoint></RelyingPartyUrlSharePoint>
  <RelyingPartyGovernanceApp></RelyingPartyGovernanceApp>
  <RelyingPartyUrlGovernanceApp></RelyingPartyUrlGovernanceApp>
</STSDetails>
```

EndPoint - The full URL of the usernamemixed or windowsmixed federation endpoint. Note that the endpoint is not enabled by default, once the endpoint is enabled, you need to restart the **Active Directory Federation Services** windows service. If the global authentication policies in ADFS is set to use forms, as well as windows authentication you can use the windowsmixed endpoint. Use the usernamemixed endpoint if forms authentication alone is setup. If you are using windowsmixed endpoint, there is no need to specify the username and password.

Yes	Yes	/adfs/services/trust/13/usernamemixed	WS-Trust 1.3	Password
No	No	/adfs/services/trust/13/issuedtokenasymmetricbasic256	WS-Trust 1.3	SAML Token (Asym...
Yes	Yes	/adfs/services/trust/13/windowsmixed	WS-Trust 1.3	Windows
No	No	/adfs/services/trust/13/windowstransport	WS-Trust 1.3	Windows

For example if your ADFS root URL is https://spadfsdc.sharepointadfs.local, then the full URL for username mixed federation endpoint is

https://spadfsdc.sharepointadfs.local/adfs/services/trust/13/usernamemixed

UserName - UPN of the job processing account. Required only when forms authentication alone is setup in ADFS.

Password- Job processing account password. Required only when forms authentication alone is setup in ADFS.

RelyingPartySharePoint – The urn identifier of the SharePoint relying party trust in ADFS

RelyingPartyUrlSharePoint – The URL identifier of the SharePoint relying party trust in ADFS (the one that ends in "_trust")

RelyingPartyGovernanceApp – The urn identifier of the Governance app relying party trust in ADFS

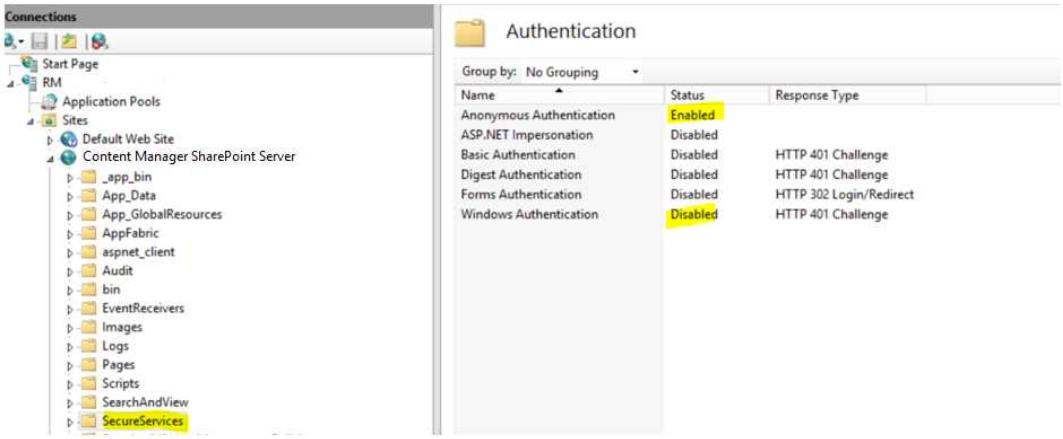
RelyingPartyUrlGovernanceApp – The URL identifier of the Governance app relying party trust in ADFS

2. Configuration propagation

Publishing the configuration settings requires the ADFS details from the STSDetails.xml. The ADFS details need to be specified in the STSDetails.xml file and the following changes need to be made in the web.config file before the settings can be published. Set the value of clientCredentialType to “None” in the webHttpBinding.

```
<webHttpBinding>
        <binding name="wbBind" maxBufferSize="2147483647"
        maxReceivedMessageSize="2147483647">
        <security mode="Transport">
                <transport clientCredentialType="None"/>
        </security>
        </binding>
 </webHttpBinding>
```

Change the authentication settings of the SecureServices folder from Windows Authentication to Anonymous:



3. Relocating older versions of a SharePoint document

The relocation process needs the SharePoint relying party information from the STSDetails.xml. If the ADFS values for the environment is not specified in this file only the latest version of a SharePoint document will be relocated.

4. Extending the Token Provider

If the global authentication policy settings in the ADFS is set that only forms authentication is enabled the username mixed endpoint neesd to be specified in STSDetails.xml.

In the case to attain the token from ADFS the token provider that comes along with the integration will require the username and password for the job processing account be available in the configuration file.

The password needs to be unencrypted. If the organizational policy doesn't allow this then it is possible to create a token provider and register it. The Content Manager Governance and Compliance app will load the provider while propagating the configuration changes and while relocating older versions of a SharePoint document.

The sample provider can be used as reference. Please contact Content Manager Support for the source code for the sample provider.

4.1 ITokenProvider Interface

To create a custom token provider implement the ITokenProvider interface, which is available in the HP.Integration.SharePoint.Common assembly.

```
namespace HP.Integration.SharePoint.Common
    {
        /// <summary>
        /// Token Provider interface
        /// </summary>
        public interface ITokenProvider
        {
            /// <summary>
            /// Gets the cookie for the specified url
            /// </summary>
            /// <param name="url">the url</param>
            /// <param name="relyingParty">the relying party</param>
            /// <returns>the cookie for the specified url</returns>
            Cookie GetCookie(string url, RelyingParty relyingParty);
        }
    }
```

4.2 Registering your own custom token provider

Once the custom provider assembly has been copied to the bin subdirectory under the installation directory:

a. open the TokenProvider.xml file which is available under the install directory.

```
<TokenProvider>
  <AssemblyName>HP.Integration.SharePoint.Token.Provider, Version=1.0.0.0,
Culture=neutral, PublicKeyToken=c0e8a57fc919aedb</AssemblyName>
  <ClassName>HP.Integration.SharePoint.Token.Provider.SampleProvider</ClassName>
</TokenProvider>
```

b. Replace the “AssemblyName” and “ClassName” in this file with the custom assembly name and class name. Note that the class name should include the

namespace.

5. IIS Configuration

The following IIS configuration is required for Federated Search using the Content Manager Manager results source and for viewing managed SharePoint documents using Content Manager.

1. Create a new directory “SearchAndView” under you SharePoint Integration installation directory

2. Copy the bin directory from the installation directory to this “SearchAndView” directory

3. Copy the following files to the “SearchAndView” directory

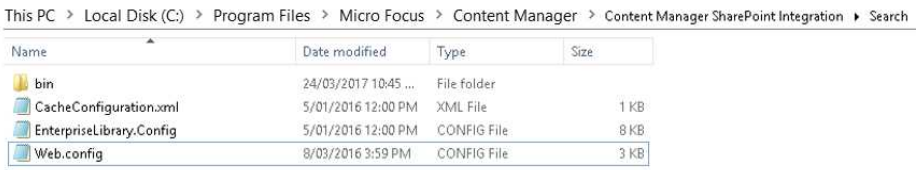
    a. CacheConfiguration.xml

    b. EnterpriseLibrary.Config

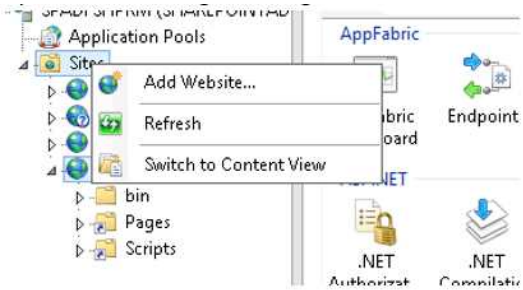
    4. Create a new web.config file and copy the following contents to it

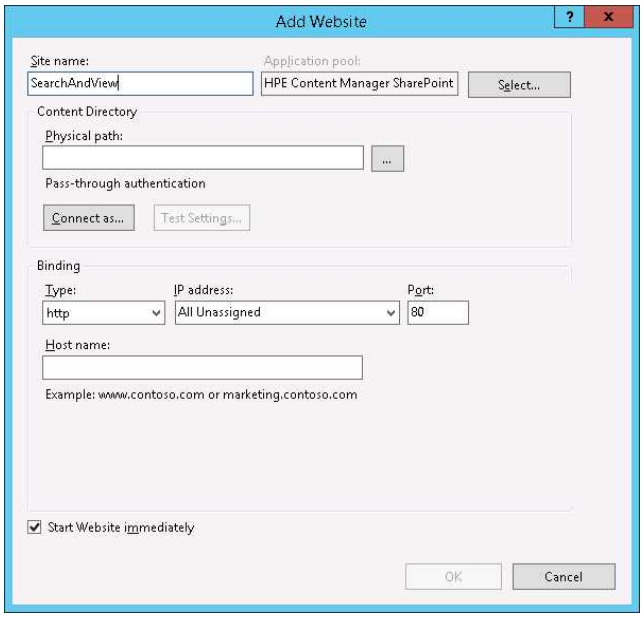
```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <configSections>
  </configSections>

  <system.web>
    <customErrors mode="Off" />
    <compilation debug="false" targetFramework="4.5" />
    <httpRuntime requestValidationMode="4.5" executionTimeout="2400" />
    <pages controlRenderingCompatibilityVersion="3.5" clientIDMode="AutoID"
/>
    <identity impersonate="false" />
  </system.web>
  <system.web.extensions>
    <scripting>
      <webServices>
        <jsonSerialization maxJsonLength="2147483647" />
      </webServices>
    </scripting>
  </system.web.extensions>
  <system.serviceModel>
  </system.serviceModel>
  <system.webServer>
    <validation validateIntegratedModeConfiguration="false" />

    <!--
        To browse web app root directory during debugging, set the value
below to true.
        Set to false before deployment to avoid disclosing web app folder
information.
      -->
    <directoryBrowse enabled="false" />
  </system.webServer>
  <runtime>
    <legacyCorruptedStateExceptionsPolicy enabled="true" />
  </runtime>


</configuration>
```

Once these steps have been performed the “ViewAndSearch” directory will look like this:



6. Create a new IIS Site





a. Type in “SearchAndView” for the Site name.

b. Select the Content Manager SharePoint Server as the application pool.

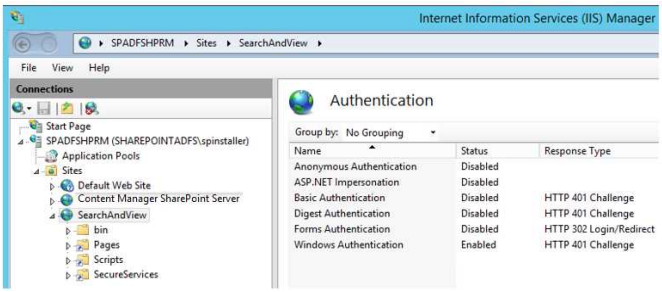
c. Make sure the firewall is allowing access to the port used by the SearchAndView website. If access is not allowed SharePoint search will timeout and will not

display any results.

d. Set the physical path to the “SearchAndView” directory that was created above and click OK

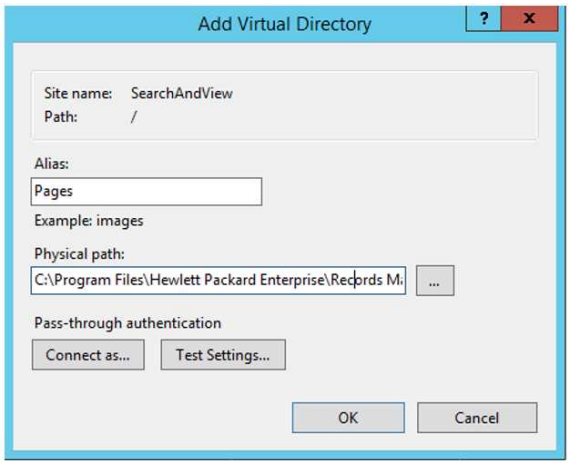
7. Setup the authentication

Enable Windows Authentication for the Search site:

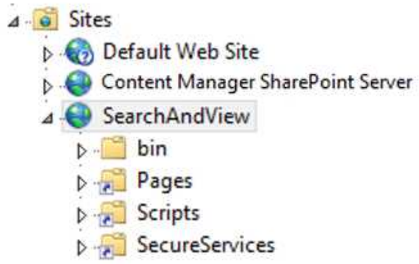


8. Create virtual directories

Right click on the ViewAndSearch site in IIS > Manage and select the option “Add Virtual Directory”



Choose “Pages” for Alias and set the physical path to the “Pages” sub directory under the install directory. Similarly create another virtual directory for “Scripts” and one for “SecureServices”. Once the virtual directories have been created the ViewAndSearch IIS site will look like this:



9. To view managed documents in Content Manager

a. Browse to the installation directory and edit the DocumentViewDetails.xml.

b. Set the value of the LoadBalancedUrl to the URL of new SearchAndViewSite and save it.

c. Restart the jobprocessing service.

10. Federated Search

a. Browse to the SharePoint site collection and edit the Result Source. Refer to Chapter 17 Searching for existing Content Manager records using

SharePoint search in the ***SharePoint Integration User Guide.pdf***

b. Modify the Source URL of the Content Manager Result Source in SharePoint such that it now points to the SearchAndView IIS site. Note that you need to

change the root segment of the URL.