Content Manager

Software Version 25.1

Content Manager Governance and Compliance SharePoint App: User Guide

opentext™

Document Release Date: July 2023
Software Release Date: January 2025

Legal notices

Copyright 2008-2025 Open Text

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

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

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

Documentation updates

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

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

To check for updated documentation, visit https://www.microfocus.com/support-and-services/documentation/.

Support

Visit the MySupport portal to access contact information and details about the products, services, and support that OpenText offers.

This portal also provides customer self-solve capabilities. It gives you a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the MySupport portal to:

- View information about all services that Support offers
- Submit and track service requests
- Contact customer support
- Search for knowledge documents of interest
- View software vulnerability alerts
- Enter into discussions with other software customers
- Download software patches
- Manage software licenses, downloads, and support contracts

Many areas of the portal require you to sign in. If you need an account, you can create one when prompted to sign in.

Contents

1 Introduction 15
1.1 Scope 15
1.2 Target Audience 15
2 Understanding the management process 16
2.1 Four core actions for managing content 18
3 Overview of product configuration 21
3.1 Using defaults 22
3.1.1 The default site collection 22
3.1.2 Using configuration from the default site collection 23
3.2 Configuration history 24
3.2.1 Initial values 25
3.2.2 Upgrading from a version earlier than 8.3 26
4 Overview of Content Manager Governance and Compliance app 27
4.1 The app start page 27
4.2 Using with sub sites 29
4.3 Best practices 30
4.4 New Library Experience in O365 30
4.5 Bulk app deployment 31
4.5.1 Tenant-scoped app 31
4.5.2 PowerShell Deployment 31
4.6 Supports SharePoint modern experience 32
5 Configuring the default integration settings 34
5.1 Understanding page sections 34
5.1.1 Settings source 34
5.1.2 Content Manager Connection 34
5.1.3 Record Types 35
Site Record 36
List Record 36
Default Container 36
Default Item 37
5.1.4 Search options 37
5.1.5 Apply RMO Settings 37
5.1.6 Default Container Classification 38
5.1.7 Management options 39
5.1.8 Exposure Settings 39
6 Configuring specific management settings 40

6.1 Records Management Options (RMOs) 43
6.1.1 Enabling the use of RMOs 45
Enablement Prerequisites 45
Configuration Prerequisites 45
6.1.2 Site Level RMOs 45
Accessing the page 45
Page overview 45
Settings Source section for site level RMO 46
Parent Container Settings section for site level RMO 47
Folder Behavior section 50
For document sets and top level folders create a dedicated container in Content Manager 51
Create separate Content Manager containers for each sub folder 51
Automatic Container Creations Settings 52
6.1.3 List level RMOs 52
Accessing the page 53
Page overview 53
Settings Source section for list level RMO 53
Parent Container Settings section for list level RMO 54
Capturing ‘Content’ Records vs ‘Structural’ Records in Containers 54
Folder Behavior section 55
7 Configuring content 57
7.1 Determining how SharePoint Metadata is to be captured 57
7.1.1 Column mapping 57
Site column mappings vs List column mappings 58
7.1.2 The column mapping page 59
7.1.3 Unmapped columns 59
7.2 Mapping SharePoint Columns to Content Manager Fields 60
7.2.1 Accessing the column mapping page 60
The site column mapping page 60
The list column mapping page 61
7.2.2 Using defaults 61
7.2.3 Adding a mapping 61
7.2.4 Saving the mappings 63
7.2.5 Removing a mapping 64
7.2.6 Duplicate mappings 64
7.2.7 Standard mappings 64
7.2.8 Adding mapped columns to a list or library 65
7.3 Columns that use custom behavior 65
7.3.1 Record based columns 66

7.3.2 Location based columns 67
7.3.3 Classification based columns 68
7.3.4 Security and access control columns 70
7.3.5 Read only columns 70
7.3.6 URL based columns 71
8 Configuring Content Type to Record Type Mapping 72
8.1 Determining the Record Type of Managed SharePoint content 72
8.1.1 Content Types to Record Type (CT2RT) Mapping page 72
Accessing the page 72
Using defaults 72
Adding a mapping 73
Saving the mapping 74
Removing a mapping 75
9 Manage Content Using Rules 76
9.1 Overview of management rules 76
9.1.1 Management Rules 77
9.1.2 Management Instructions 78
9.1.3 Management Selectors 79
9.1.4 Examples 79
Example 1: Setting a specific title on a record 79
Example 2: Specifying a record type 80
Example 3: Using an existing container in Content Manager 81
Example 4: Setting multiple properties on a record 82
Example 5: Using properties from SharePoint to search for a container 83
Example 6: Creating a new container with automatically generated title and specified retention schedule 86
9.2 Content Manager Management Options 88
9.2.1 Creating and editing management rules 89
9.2.1.1 Creating a new management rule 89
Identification 90
Content Types 91
Management Instructions 91
Conditions 91
List specific properties 92
Template ID 92
Custom templates 92
Saving the rule 93
9.2.1.2 Editing an existing management rule 93
9.2.1.3 Deleting a management rule 93
9.2.1.4 Ordering management rules 93

9.2.1.5 Changing the management rule priority 94
9.2.1.6 Importing and exporting management rules 94
9.2.2 Creating and editing management Instructions 95
9.2.2.1 Creating a new management instruction 95
Identification 96
Instructions 96
Text based properties 97
Record based properties 99
Thesaurus based properties 99
Saving the instruction 100
9.2.2.2 Editing an existing management instruction 100
9.2.2.3 Deleting a management instruction 100
9.2.2.4 Importing and exporting management instructions 101
9.2.3 Creating and editing management selectors 101
9.2.3.1 Creating a new management selector 101
Identification 102
Content Type 103
Selection Rules 103
Creating a search based selector rule 103
Creating a condition based selector rule 104
Saving the selector 106
9.2.3.2 Editing an existing management selector 106
9.2.3.3 Deleting a management selector 107
9.2.3.4 Importing and exporting management selector 108
9.2.4 Management rules options 108
9.2.4.1 Specifying use of values from the default site collection 109
9.3 Applying management rules 109
9.3.1 Applicable rules 110
9.3.2 Constructing the collection of applicable instructions 110
9.3.3 Handling duplicate instructions 111
Critical management rules 112
Management rules with the most conditions 113
Management rule priority 113
9.3.4 Summary of management rule selection process 114
10 Manually managing content 116
10.1 Core actions 116
10.1.1 The ‘Manage’ action 117
10.1.1.1 Manage an item or document 117
How documents are managed 119
Use of the SharePoint Folder content type 119

10.1.1.2 Manage multiple items or documents 119
10.1.1.3 Manage a document set 120
10.1.1.4 Manage a folder 121
10.1.1.5 Manage a list or library 122
10.1.1.6 Manage a site 122
10.1.2 The ‘Finalize’ action 123
10.1.3 The ‘Relocate’ action 123
10.1.4 The ‘Archive’ action 123
11 Determining the management status of content 125
11.1 Management details page 125
11.1.1 Accessing the page 125
11.1.2 Management status section 126
11.1.3 Management details section 126
Unmanaged items 126
Managed items 127
11.1.4 Lifetime management policies 127
11.1.5 Relationships link 127
11.1.6 All Contacts link 128
11.2 Using column values to illustrate management status 129
12 Automating governance and compliance 131
12.1 Overview 131
12.1.1 Automate information lifecycle 131
Lifecycle decisions 133
Consequences of not making lifecycle decisions 133
Automating lifecycle decisions 133
12.1.2 Lifetime management policies (LMPs) 135
Lifecycle stages 135
Rules 136
Actions 136
The LMP gallery 136
12.1.3 Applying LMPs 136
12.1.4 How LMPs are executed 137
12.2 Defining a LMP 139
12.2.1 The LMP gallery 139
Accessing the gallery 139
Using defaults 139
12.3 Creating a LMP 140
12.3.2 Identification 140
12.3.3 Availability 141
12.3.4 Adding a lifecycle stage 141

12.3.5 Defining a rule 142
Understanding when rule maturity is calculated 143
Date based conditions 143
Text based conditions 144
Managed metadata based conditions 145
People or group base conditions 145
Item properties 145
List properties 146
Title 146
Date Created 146
Date Last Modified 146
Item Count 146
Custom templates 146
Template ID 147
Site properties 149
Title 149
Date Created 150
Date Last Modified 150
Web Template 150
12.3.6 Adding an action 152
Apply to 153
Action Type 153
12.4 Modifying a LMP 153
12.4.1 Editing an existing LMP 153
12.4.2 Implications of changing an existing LMP 154
12.4.3 Considerations if using the defaults 155
Unchecking “Use defaults” 155
Creating new LMPs 156
Modifying existing LMPs 156
12.5 Copying a LMP 156
12.6 Deleting a LMP 156
12.7 Included LMPs 157
12.8 Applying LMPs to sites 157
12.8.1 Understanding site Lifetime Management Options (LMOs) 157
Specific LMOs 157
Defaulted LMOs 160
Applying changes made to default site LMOs 161
Inherited LMOs 163
Duplicate LMPs 163
Recommendations 164

12.8.2 Setting site LMOs 165
Accessing site LMOs 165
Use defaults 165
Apply parent LMOs 166
Managing the list of LMPs 166
Saving the LMOs 168
12.9 Applying LMPs to lists 168
12.9.1 Understanding list Lifetime Management Options (LMOs) 168
12.9.2 Setting list LMOs 169
Accessing list LMOs 169
Managing the list of LMPs 169
Saving the LMOs 169
13 Preventing management of trivial content 170
13.1 Identifying content as trivial 170
13.1.1 The effect of the trivial identification 171
13.1.2 Overriding the trivial identification 172
13.1.3 Practical examples 172
Preventing folders from being managed 172
Preventing certain types of lists from being managed 172
13.2 Preventing management of system lists 172
13.3 Deleting trivial content 173
14 Securing SharePoint content with Content Manager 176
14.1 Security and access control features 176
14.1.1 Information security in SharePoint 176
Inherited permissions 177
Limited Access 178
14.1.2 Claims based authentication 178
14.1.3 Information Security in Content Manager 179
Security Levels 179
Security Caveats 180
Access Controls 181
User Permissions 182
Referenced access controls 182
14.1.4 Content Manager security applied to managed SharePoint content 182
Content Manager Security Groups 182
CM Permission Levels 183
Modifying the CM permission levels 184
Controlling access to a list item 184
Converting access controls to permissions 185
Equivalent permission levels 185

Determining permissions to apply 185
Referenced access controls 186
Creation of Content Manager Security Groups 187
Initial population of Content Manager Security Groups 187
Security levels 188
Security caveats 188
Group locations 188
User locations 188
Inclusion of Content Manager user permissions 188
Combinations of attributes 188
Maintenance of group memberships 189
Preventing malicious group modification 189
14.1.5 Capturing access controls 189
Converting Permissions to Access Controls 190
Capture of groups 191
Automatic creation of groups 191
Initial population of group locations 192
Maintenance of group locations 192
14.2 Enabling security 192
14.2.1 Enabling Options and Considerations 192
Enabling options 192
Considerations 192
Retrospective application of access controls 194
14.2.2 Content Manager Security Settings page 194
Accessing the Security Settings page 194
Settings source section 194
Use defaults 194
Inherit security settings from the parent site 194
Allow security settings to be overridden 194
Security behavior section 195
Only add existing SharePoint users 195
Limit menu options based on the user's permission in the Content Manager 195
Capture SharePoint permissions as Content Manager access controls 196
Include inherited permissions 196
Apply Content Manager access controls as SharePoint permissions 196
Apply Content Manager security as SharePoint permissions 196
Everyone group 196
Using a SharePoint group instead of an AD group 197
Considerations for the "Everyone Group" 197
Managed Item Administrators group 198

Using a SharePoint group instead of an AD group 198
Considerations 198
14.3 Setting security and access control using SharePoint 199
14.3.1 Security columns 199
Security level 199
Security caveat 199
Access control columns 199
Eligibility to be displayed 200
Filtering the locations that are displayed 200
Filtering of referenced access controls 202
Saving when locations have been filtered 202
Displaying “Everyone” access controls 203
Behavior when no entry is made 204
Restricted groups 205
Behavior when “Capture SharePoint permissions as Content Manager access controls” is checked 205
Automatic location creation 205
14.3.2 Immediate lock down of secured items 205
14.4 Determining the security of an item 206
14.4.1 Standard Content Manager columns 206
14.4.2 Security and access control specific columns 207
14.4.3 Security details page 207
Accessing the page 207
Record security 207
Item permissions 208
Pending jobs 209
14.5 Configuration Access Controls 209
14.6 Troubleshooting 210
14.6.1 Security details page 210
14.6.2 Group Membership page 211
14.6.3 Fault finding techniques 211
14.7 Implementation considerations 213
14.7.2 Site Collection Administrators 213
14.7.2 Web Application User Policies 213
14.7.3 Synchronizing with existing Content Manager locations 214
Active Directory users 214
Active Directory groups 214
SharePoint groups 214
Special AD accounts 215
15 Auditing 216

15.1 Audit sources ... 216
15.2 Item audit history ... 217
15.2.1 Enabling auditing events ... 217
15.2.2 Audit history ... 218
Management parameters ... 218
Status ... 219
15.2.3 Audit entries indicating document viewed in SharePoint ... 219
Configuring “view” audit events in SharePoint ... 219
Indicating that view events should be included in history ... 220
15.3 List audit history ... 221
15.3.1 Accessing list audit history ... 221
15.3.2 Inclusions in list audit history ... 221
15.4 Site audit history ... 221
15.4.1 Accessing site audit history ... 221
15.4.2 Inclusions in site audit history ... 222
15.5 Site collection audit history ... 222
15.5.1 Accessing site collection audit history ... 222
15.5.2 Inclusions in site collection audit history ... 222
16 One Drive for Business ... 223
17 Searching for existing Content Manager records using SharePoint search ... 224
17.1 Federated searches ... 224
17.1.1 Result sources ... 224
17.1.2 Result types ... 224
17.1.3 Query rules ... 225
17.2 Planning your search implementation ... 225
17.3 Including Content Manager in federated search results ... 225
17.3.1 Adding the app to your search site ... 225
17.3.2 Creating a result source ... 226
17.3.3 Creating a result type ... 229
Uploading the Content Manager display template ... 229
Creating the result type ... 230
17.3.4 Creating a query rule ... 231
17.3.5 Testing the federated results ... 233
17.4 Modifying the search results ... 233
17.4.1 Suppressing SharePoint items ... 233
17.4.2 The search settings page ... 233
17.4.3 Selecting the columns to include ... 234
17.4.4 Specifying what is searched by a keyword search ... 236
17.5 Changing how search results are displayed ... 236
17.5.1 Creating a custom display template ... 236

Create a copy of the Content Manager display template 237
Customizing the display template 237
Using your custom display template 237
17.6 Using SharePoint search functionality to further refine search results 237
17.6.1 Creating a more results page 237
Create the page 237
Make the page available 239
17.6.2 Viewing a records only subset of results 240
Create the page 241
Add the navigation link 241
17.7 Using SharePoint advanced search 242
17.7.1 Overview 242
Managed properties 242
Configuring the advanced search web part 243
17.7.2 Advanced search without using managed properties 247
17.7.3 Using standard mapped managed properties 247
17.7.4 Creating Content Manager managed properties 249
17.7.5 Using Content Manager managed properties in manual searches 249
17.8 Fixed searches 250
17.9 Troubleshooting 252
18 Searching for existing Content Manager records using app parts 254
18.1 Adding pre-configured app parts 255
18.2 Creating your own pre-defined search app parts 257
18.2.1 Including the search controls in custom app parts 260
18.3 Using the Content Manager Search app part 261
18.4 Including content indexes in search results 263
19 Exposing existing Content Manager records into SharePoint 265
19.1 Configuring exposure 265
19.1.1 Common configuration 266
Exposure Search Location 266
Exposure Limit 267
19.1.2 List/library specific configuration 267
Accessing the exposure settings page 267
Record Search 267
Exposure Options 269
Execution 269
Un-exposing content 269
19.2 Updating exposed records 270
19.3 Editing exposed items 270
19.4 Known limitations 271

20 Understanding the job queue ... 272
20.1 Defining a job ... 272
Job states ... 272
Job queue ... 273
20.2 Working with the job queue ... 274
Accessing the job queue ... 274
The different views ... 275
In progress jobs ... 275
Scheduled jobs ... 275
Failed jobs ... 276
Job history ... 276
Viewing the details of a job ... 277
Viewing the SharePoint location that a job applies to ... 278
20.3 Job queue settings ... 279
20.3.1 App Uninstall ... 279
20.3.2 Cleanup Thresholds ... 280
20.3.3 Job Deletions with IDs ... 280
20.4 Jobs – Reference List ... 280
20.5 Troubleshooting jobs ... 283
20.5.1 Stalled jobs ... 283
20.5.2 Jobs stay in pending state and don’t get processed ... 283
20.5.3 Deleting a job ... 283
20.5.4 Restarting a failed job ... 284
20.5.5 Management job fails ... 284
20.6 Notifications ... 285
Core Process ... 285
Exposure ... 285
Lifetime Management ... 285
System Job ... 286
Customizable Job Notifications ... 286
Use of Substitution Strings ... 287
21 Content Manager statistics ... 289
21.1 Accessing Content Manager statistics ... 289
21.2 Inclusions in Content Manager statistics overview ... 289

1 Introduction

1.1 Scope

This document is designed to provide guidance to users and information managers about the various aspects of Content Manager for SharePoint. It explains concepts and the use of particular functionality and where appropriate, provides implementation recommendations.

Consult the appropriate Content Manager or Microsoft documentation for detail on Content Manager and Microsoft SharePoint.

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

1.2 Target Audience

This document targets different audiences in different sections. The understanding of functionality and implementation recommendations are targeted towards information managers, compliance officers and IT professionals responsible for configuring the product.

Usage sections are targeted at users of SharePoint.

2 Understanding the management process

The management process is intrinsic to Content Manager for SharePoint. The way Content Manager manages content depends on number of configurations and actions. The following gives a brief overview of all the working parts.

1. **Management** is a process where SharePoint content is captured into Content Manager, and the subsequent securing, auditing, tracking, and retention of that content. Once captured, the content falls under the authority of Content Manager, any further interactions with it are intercepted and managed in a compliant manner.
2. **Configuration** of the management process is carried out at different levels within the product to determine the ***what, how, when and where***. With a complete configuration, content is captured without any required input from end-users, and is stored with all correct metadata, in the right area of the file-plan, with appropriate security and retention applied. The configuration has the following two stages:
   a. **Initial** – Considered that in most cases this will be configured as part of post-installation activities, and will rarely change
   b. **Ongoing** – These options can be configured in a default manner, but are more likely to change in different areas of a SharePoint site hierarchy, to meet differing compliance demands and requirements of individual business units and site owners

The following table gives an overview of the configuration options, and their impact on the managed content:

Configuration Stage	Configuration Element	Management Impact
Initial	Content Manager SharePoint Configuration tool	Used to define a number of things, including: • Which SharePoint site collection to use for default configuration values • Where to store all configuration data for the product • Security groups to control who can administer the job queue, and who can view SharePoint documents from Content Manager • Monitoring and notifications
	Default Integration Settings	Used to determine: • The Content Manager dataset to be used • Default Record Types to use for Content Types which have not been

Configuration Stage	Configuration Element	Management Impact
		explicitly mapped elsewhere • Default Classification, for any content not explicitly classified • Version handling for content moved out of SharePoint
	Content Types to Record Type Mapping	Used to determine which Record Type will be used in Content Manager for a given Content Type in SharePoint. For example: • ***Contract Document*** and ***Policy Document*** mapped to ***Controlled Document*** record type in Content Manager • ***Document*** mapped to ***Standard Document*** record type in Content Manager
	Column Mapping	Used to determine which columns of information from a given Content Type will get captured as part of the management process. Some default columns are mapped out-of-the-box (dates, author etc.) For example: For the ***Task*** content type, map the columns ***Title, Description, Priority, Start Date***, all other columns are considered unimportant from a compliance perspective and are not captured to the mapped record type.
Ongoing	Records Management Options	Used to determine a number of behaviors in terms of where content is stored in Content Manager options, including: • Whether or not to use a container, and if so, to use an existing container or automatically create a new one based on the SharePoint site or list • Which classification to use for the content • How to capture and represent document library folders or document sets For example, a Finance site owner may override

Configuration Stage	Configuration Element	Management Impact
		the default RMOs, to explicitly configure all finance content from a customer site to go into an already existing container within Content Manager, rather than using the default of automatically creating a new container.

- **Initiation** of the management process can be carried out in two distinct ways:
  - **Manually** through the use of ribbon menus, and links on the app page. This process is instigated by a user.
  - **Automatically** through the use of pre-configured lifetime management policies. This process is instigated automatically when configured policy rules have been met. And does not require any user intervention.

    Management actions can be instigated against individual items, multiple items, sites and lists. For details of the available actions, refer to 2.1 Four core actions for managing content section below.

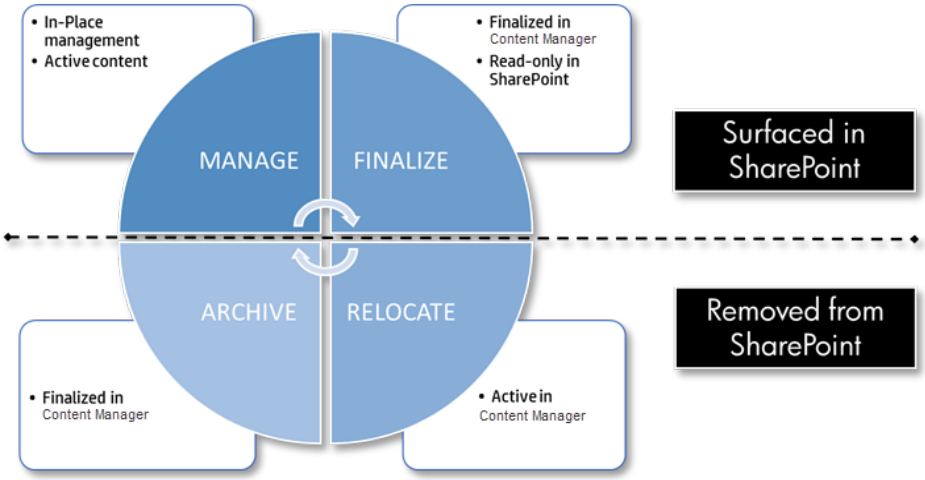
    When content is managed through either of these mechanisms, a job is raised and sent to the job queue, to be performed asynchronously. When the job processes, the content is captured according to the product configuration.
  - **Processing** of jobs in the queue is performed by the ***Content Manager SharePoint Service***, running on each Content Manager Workgroup server.

The job queue is as a centralized queue of all incoming jobs for the Content Manager Farm. Jobs are pulled from a ***Pending*** queue, with multiple jobs running in parallel on each Workgroup server. When the job is executed, SharePoint content is managed according to the defined configuration, and captured into Content Manager accordingly. In the case of manual management requests initiated by users, a notification email is sent to the individual user upon completion, informing them when content has been successfully captured and managed.

For more details, see section 20 Understanding the job queue, on page 272.

2.1 Four core actions for managing content

The Content Manager Governance and Compliance App provides four core actions for managing SharePoint content, these are available for both automatic and manual actions.



Process	Menu Name	Description
Manage	Manage with Content Manager	Managing content creates a record in Content Manager, and binds it to the associated list item in SharePoint, to ensure Content Manager's authority over the SharePoint content, while still providing full SharePoint functionality to end users. In the case of documents, a metadata-only record is created, whilst the document itself remains in SharePoint.
Finalize	Finalize with Content Manager	Finalizing with Content Manager provides a means of preserving the state of SharePoint content with Content Manager. Whilst still maintaining its presence in SharePoint, a finalized list item can no longer be modified, it becomes read-only. The record itself is finalized in Content Manager, preserving the content and preventing any further updates. In the case of documents, a metadata-only record is created, whilst the document itself remains in SharePoint.
Relocate	Relocate to Content Manager	Relocating content removes it from SharePoint, leaving only the record in Content Manager as the account of the SharePoint content. The Relocate action is therefore an excellent means of removing content from SharePoint that may no longer have any relevance in the

Process	Menu Name	Description
		operational environment, whilst still ensuring that the information itself is preserved in Content Manager. Documents are transferred to Content Manager at the time of relocation.
Archive	Archive to Content Manager	Archiving to Content Manager combines the Finalize and Relocate actions to first Finalize the record and then remove the corresponding list item from SharePoint altogether. So, much the same as the Relocate action, the Archive action is an excellent means of ensuring currency and relevance of content in the operational environment, but in addition to preserving the information, also preventing any further changes to its content via Content Manager. Documents are transferred to Content Manager at the point of archival.

IMPORTANT: Restricted file extension - SharePoint integration displays files with blocked extensions, such as .exe and .dll, in the **Management Details** page. The blocked files can only be managed or finalized and cannot be relocated or archived. Any temporary files created while relocating or archiving will be deleted.

In providing the capability to Manage ALL SharePoint content with Content Manager, the four core actions can be applied to any entity in the SharePoint hierarchy:

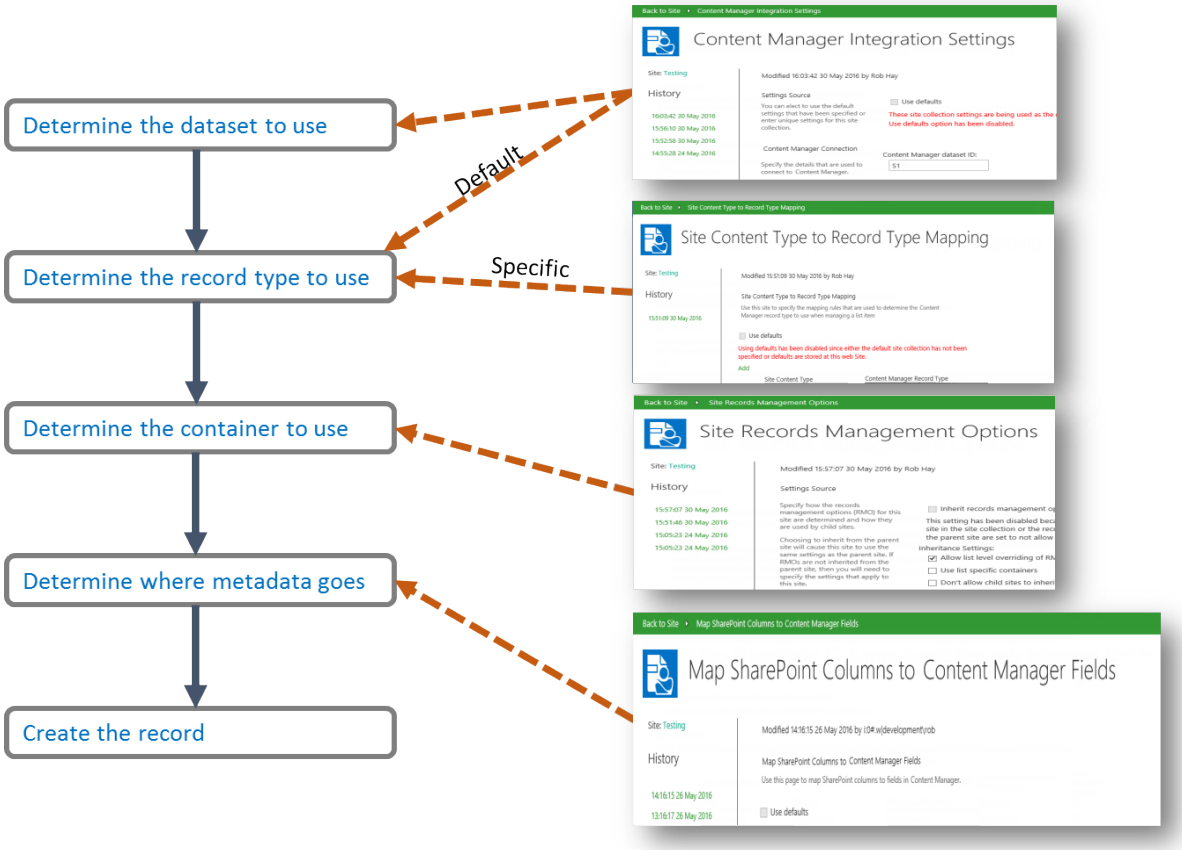
- Individual list items and documents
- Multiple items and documents
- Document Sets
- Folders
- Lists and libraries
- Sites, including all contained content

Those users who are site owners are responsible for compliance within a department. To understand the Content Manager options store and control the content, see 6 Configuring specific management settings, on page 40.

3 Overview of product configuration

This section of the document provides an overview of the various configuration values used by this product to make decisions during the management process.

Configuring how content is managed can be summarized using the following diagram:



These decisions are universal, regardless of the tool used to create the record, whether it be the Content Manager desktop client, the Content Manager Web Client or the Content Manager Governance and Compliance App.

> **NOTE:** The effect of management rules is not included in this diagram. Management rules can enforce management instructions that may determine the record type, container and field values.

The following are the steps recommended to take before you create a record:

1. **Determining the dataset to use**

   An organization will require that all managed SharePoint content for a farm resides in a single Content Manager dataset. There are however scenarios where content from different site collections must reside in different Content Manager datasets.

The Default Integration Settings page includes the ability to specify the Content Manager dataset that must be used by the site collection.

2. **Determining the record type to use**

   There are two methods that are used to determine the record type to use. The Content Type to Record Type (CT2RT) page allows specifying which Content Manager record type to use based on the content type used for the SharePoint list item. These are known as ***specific*** record type mappings.

   It is not necessary to map all content types to record types though. The Default Integration Settings page allows specifying the default record type to use if no specific mapping has been made on the ***CT2RT*** page.

   Management instructions can also be used to determine the record type. If a management instruction is applicable, this will have precedence over the values determined by the ***CT2RT*** or ***default integration settings***.

3. **Determining the container to use**

   The container used to house the created record is determined by Records Management Options (RMO). These can be set at site level or a specific list level.

   RMOs allow specifying the following container options:

   - Automatically create a container to use
   - Use of a specific container that already exists
   - Do not use a container

   Management instructions can also be used to determine the container. If a management instruction is applicable, this will have precedence over the values determined by the ***RMOs***.

4. **Determining where metadata goes**

   The Content Manager fields that are used to capture the values from SharePoint columns are determined by the Column Mapping page. This page allows specifying, for a given SharePoint column, which Content Manager field the content should be placed into.

   It is not necessary to map all columns to fields. Unmapped columns are still captured by Content Manager on the record in a field called ***SharePoint Properties***.

   Management instructions can also be used to determine the values of fields. If a management instruction is applicable, this will have precedence over the values determined by the ***column mappings***.

3.1 Using defaults

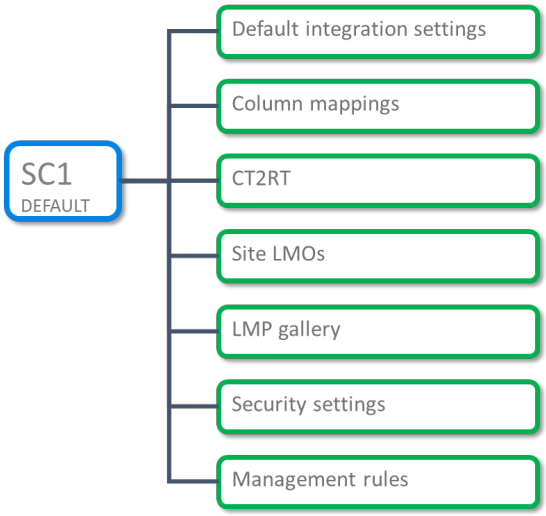
3.1.1 The default site collection

It is possible to specify configuration for every site collection. In many cases though, the configuration used by each site collection is identical, making the configuration task a repetitive one.

A site collection can be nominated as the **Default site collection** and the configuration used on this site collection is used by all other site collections.

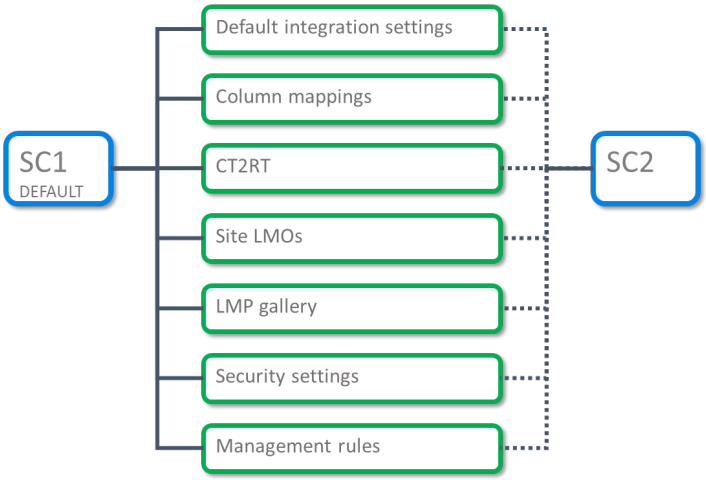
For details on setting the default site collection, see the *Content Manager Governance and Compliance SharePoint App: Installations Guide*.

In the scenario below site collection 1 (SC1) has been specified as the default site collection. SC1 has the following configuration that can be used as the defaults by other site collections:



3.1.2 Using configuration from the default site collection

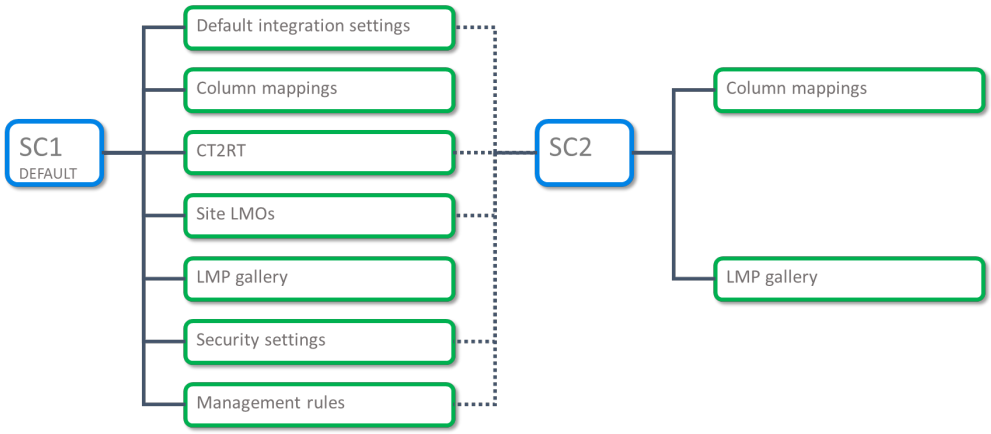
Site collection 2 (SC2) can use the configuration from SC1.



> **NOTE:** This applies to both site collections and sites. If the Content Manager Governance and Compliance app is added to a site that is not at the root of a site collection, the site will consume defaults in the same manner as the above diagram.

When the Content Manager Governance and Compliance app is added to a site or site collection, the default behavior is to use configuration from the default site collection.

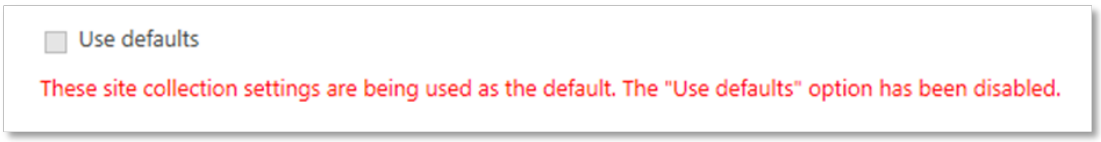
SC2 can also be configured to use some of the defaults from SC1 but specify unique settings for other configuration.



Configuration pages that support the use of default values will include a check box located near the top of the page:

Checking this option indicates that the values for the configuration managed by this page should be sourced from the default site collection. When ticked, editing of configuration for that page is prevented.

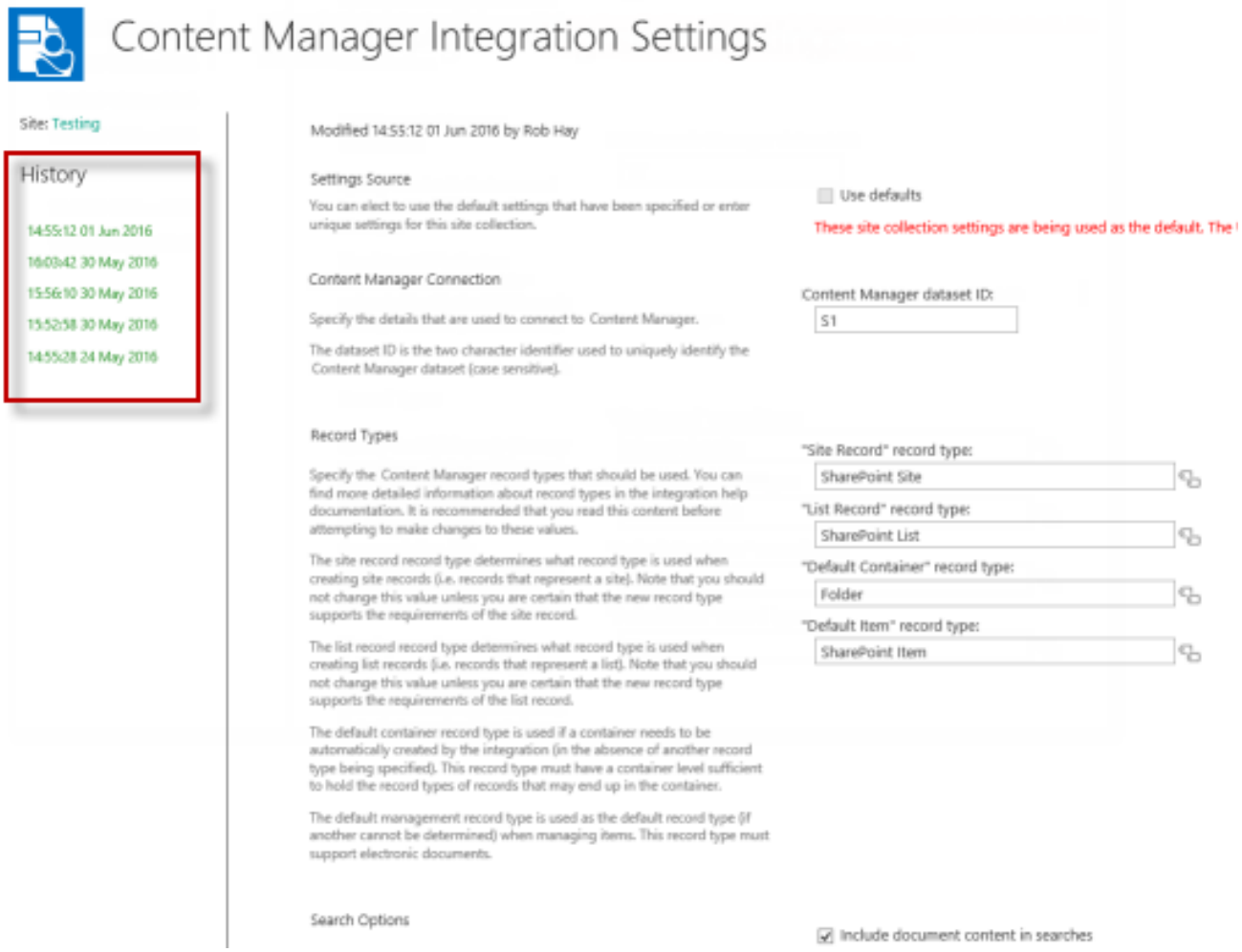
This option is unavailable for use when the configuration being edited is for the default site collection itself.



If a site has been specified as the default site collection, it cannot consume defaults from anywhere else and must have the settings specified.

3.2 Configuration history

From version 8.3 onwards, it is possible to view the history of configuration values. Configuration pages that can display history include a history panel on the left hand side of the page. The following screen shot shows the **default integration settings** page with history.



Each time configuration values are saved, a new entry will appear in the history panel showing the date and time that they were saved. The current saved value is always the top most entry in the list.

Click the history entry displays the values that were saved at this time. For any historical values (any values previous to the current ones), the configuration is shown as read only and is not editable.

You can view history for the following configurations:

- Default integration settings
- Records management options
- Content type to record type
- Column mapping
- Security settings

3.2.1 Initial values

Prior to saving configuration values for the first time, the values displayed are the default values. The history panel will show a single entry: **Initial Values**. This indicates that these are the default values but they have not been saved as yet.

Saving the configuration will cause the save date and time to be displayed for that entry.

3.2.2 Upgrading from a version earlier than 8.3

When upgrading from a version earlier than 8.3 (when configuration history was not supported), there may already be values that have been saved for configuration. These saved values will display as **Initial Values**.

If you subsequently save a change to this configuration, you will see two entries in the history. The original values that were saved prior to upgrading to 8.3 will be shown with a date and time one minute before the save just performed. The new values that were just saved will have the correct date and time.

When looking at the history of configuration for an upgraded site, it is important to understand why the history reflects this.

4 Overview of Content Manager Governance and Compliance app

Introduction to SharePoint app concepts

SharePoint introduced the concept of an ***app***. An app is used to add functionality to a SharePoint site.

For example, if you wanted to add a document library to a site, you would add a ***Document Library*** app.

There are a number of Microsoft provided apps that replace the pre-defined list templates in SharePoint 2010. The app model is essentially a set of extensions that deliver specific functionality. This same app model can be used by third-party developers to extend SharePoint.

The Content Manager Governance and Compliance app is a ***provider-hosted*** app. This means that the application itself resides on an external server, not the SharePoint servers.

The app is added to a SharePoint app corporate catalog by your SharePoint administrator. Once added and configured, it is available for use on sites throughout the organization.

Introduction to Content Manager Governance and Compliance app concepts

To add governance and compliance to a site, you add the ***Content Manager Governance and Compliance*** app.

You can add the app to a site collection or site. Adding the app enables the following:

- Item and list ribbon menu options for manually managing content.
- List menu options for configuring Records Management Options and Lifetime Management Options.
- An app start page with links to various configuration pages, and manual actions for managing sites.

Note that if you wish to manually manage content on a site, you must add the app to that site. However, lifetime management policies can be defined at site collection level, and can be used to manage sub-sites, even those without the app. See Site Columns, on page 129 for information.

Any of these columns can be added to lists to display the value of that record property.

Note, if you are upgrading to Content Manager from a previous version, the label for site columns will remain **Content Manager Columns**.

4.1 The app start page

The **app start page** is the page that provides access to most of the configuration options for the app.

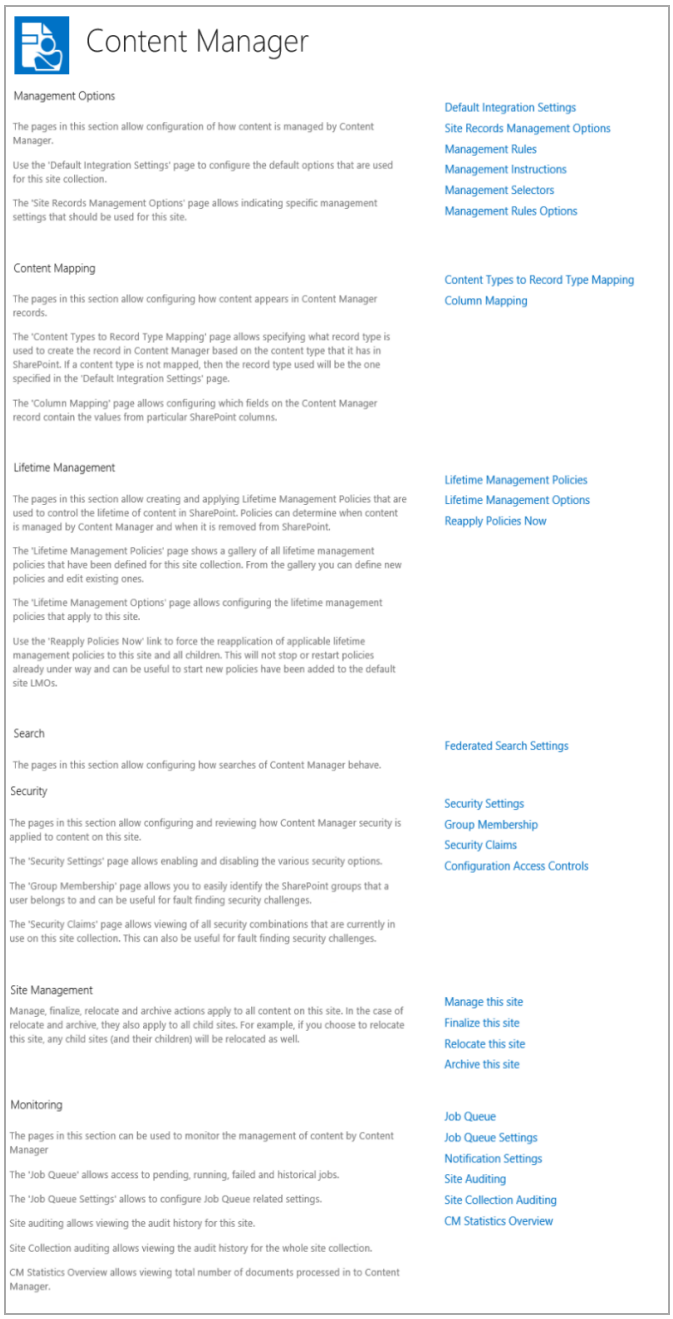
Accessing the page

> **NOTE:** You must have **manage site** permission to access the app start page.

1. Navigate to the required SharePoint site.
2. From the site quick-launch pane, click on **Site Contents**.
3. Locate and click on the **Content Manager Governance and Compliance** app icon, to open the app start page.

Page overview

The app start page includes a number of sections grouping together related configuration options.



Each of the sections of the app start page are covered in detail in this guide.

Click **Back to Site** link at top-left will navigate back to the originating SharePoint site.

4.2 Using with sub sites

The SharePoint app model is very much aimed at apps working within the scope of a particular site.

However, the **Content Manager Governance and Compliance** app is very flexible in terms of where you decide to add it. As previously discussed in Introduction to Content Manager Governance

and Compliance app concepts, on page 27, adding the app enables access to the app start page, and adds ribbon menus for manual management and configuration.

However, it is not necessary to add the app to every site within a site collection, particularly when using lifetime management policies to automate compliance and management actions.

An app does not need to be added to the site collection root site, nor is there any requirement for a parent site to have the app installed either.

Add the app to a site where you require one or more of the following:

- Manual management of content using ribbon menus
- Changes to where content gets stored in Content Manager
- Changes to applied lifetime management policies
- Quick access to the app start page and the links contained on it

4.3 Best practices

The following are the best practices for using the app:

- It's recommended to add the app at the top-level of each site collection. This allows you to define some default behaviors for that site collection, which will be applied to all sites within that site collection (Unless overridden by specified configuration) for example:
  - A default classification for any content that doesn't get specifically classified.
  - Folder behaviors for document libraries containing folder hierarchy.
  - Default lifetime management policies that will be applied to all sites in the site collection.
- Add the app to any departmental sites, allowing you to configure default records management options for the department.
- Add the app to specific sites where you know users will be manually declaring content as records (**Manage**).
- Add the app where you want to override the default lifetime management policies, and apply some specific policies to suit different process, and compliance requirements.

4.4 New Library Experience in O365

Currently there is a problem with the way the new list experience mode renders the Ribbon items for the Content Manager SharePoint Governance and Compliance App. Some are repeated and do not correctly launch the associated dialog.

In addition if certain SharePoint site columns created by the Configuration Tool are added to a list with either the 'Default experience set by my administrator' or 'New experience' option selected, there will be an error when trying to browse the list.

The workaround is to make sure the list is set to use the 'Classic experience' option.

For further information about the new list experience settings please refer to: https://support.office.com/en-us/article/Switch-the-default-for-lists-or-document-libraries-from-new-or-classic-66dac24b-4177-4775-bf50-3d267318caa9.

4.5 Bulk app deployment

4.5.1 Tenant-scoped app

SharePoint provides a mechanism for automating app deployment to site collections and sites. This is called a tenant-scoped app.

However, there is a significant limitation in using this approach, custom ribbon actions cannot be deployed. This means that the app will get deployed, and the app start page will be accessible for configuration and site management.

However, note that the following features will not be available if this method of activation is used:

- Item and list ribbon menu actions
- Search app parts

Consider using this in those cases where access to configuration options and site management is sufficient, to automatically add the app without user intervention, and prevent it from unauthorized removal.

App deployment can be automated against several criteria:

- Deployment to named site collections
- Deployment to all sites under a particular managed path
- Deployment to all sites created from a certain site template

For more details on adding an app to the tenant-scope, please see the following Microsoft MSDN article:
http://msdn.microsoft.com/en-us/library/office/fp179896(v=office.15).aspx#Tenant

4.5.2 PowerShell Deployment

Bulk app deployment and management can be carried out using PowerShell scripts.

PowerShell is beyond the scope of this document, and should be used by those responsible for administering SharePoint infrastructure. It should be used with caution, as the impacts of bulk actions can be significant. Refer to *Content Manager Governance and Compliance SharePoint App: Installations Guide* for more details.

4.6 Supports SharePoint modern experience

Overview

The Content Manager Governance and Compliance for SharePoint app supports SharePoint Site User experience for Documents and Custom Lists in your site collection. A new template (**CMModernUIGovernanceComplianceTemplate.app**) is available in the install directory to support SharePoint Site User experience.

> The **Multiple Items and Documents** functionality in the SharePoint hierarchy is not supported in Modern User experience. See Multiple items and documents functionality.

Impact on integration

If you are integrating Content Manager with SharePoint for the first time, during app configuration using the Wizard or Tool, you have the option to choose the SharePoint Site User experience (**Classic** or **Modern**). Based on your selection, respective template will be used to create the app.

If you want your existing integration to work with SharePoint Site User experience then, in the App configuration settings, modify the SharePoint Site User experience option to **Modern** using the Configuration Tool, configure the app and then publish it. Complete rest of the necessary steps by adding the app to your site collection.

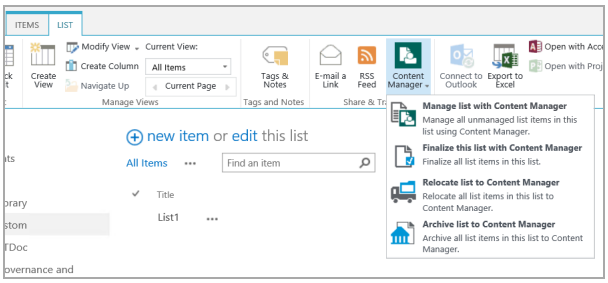
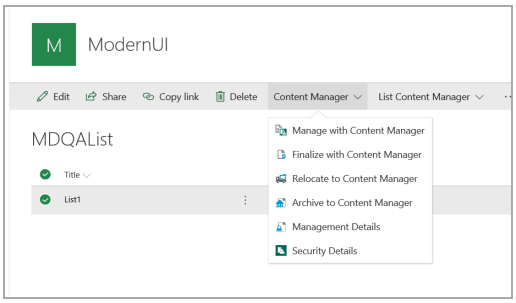
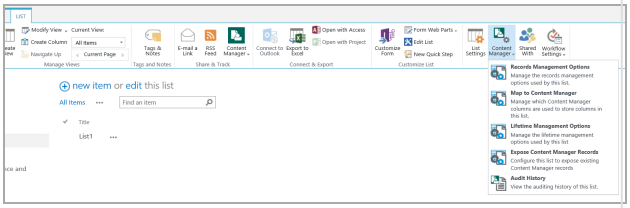
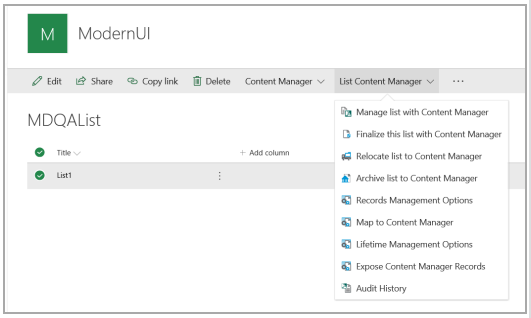
For detailed steps, see *Content Manager Governance and Compliance SharePoint App: Installations Guide*.

Content Manager integration options

To know whether you are using the right template for the experience you chose, check the app title once you have added it to your site collection. For classic experience, the app title will be **Content Manager Governance and Compliance app**. For SharePoint Site User experience, the app title will be **Content Manager Modern UI Governance and Compliance app**.

With the SharePoint Site User experience, Content Manager options will be available on the horizontal navigation bar of your site pages for Documents and Custom Lists. Except for the title of the app, the menu options and its functions are same as the classic experience.

Quick look at the experience with Content Manager integration

Classic look	Modern look
	
	

5 Configuring the default integration settings

The default integration settings includes the following:

- Content manager dataset
- record types for management
- behavior of search
- default classification for automatically created containers
- global management options

The above settings apply to the site collection as a whole.

5.1 Understanding page sections

The default integration settings page comprises several sections that group together related controls.

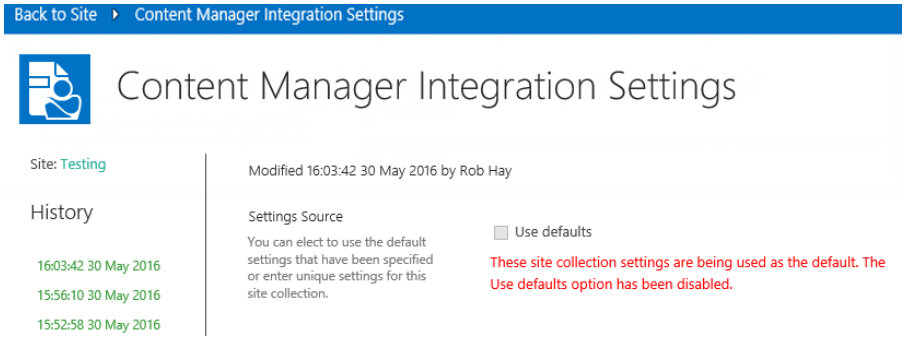
5.1.1 Settings source

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.

If the default site collection settings are used, 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.

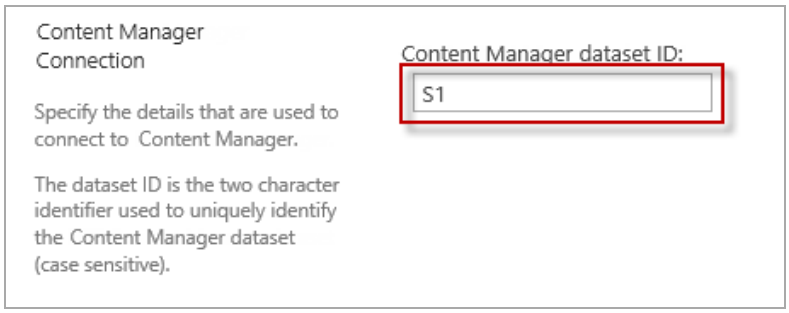
If this site collection is the nominated default site collection, then the **Use defaults** check box is disabled.



5.1.2 Content Manager Connection

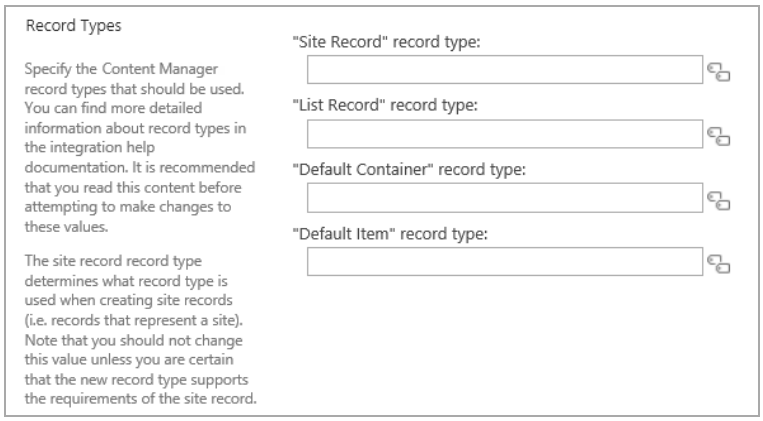
The Content Manager Connection section of the page allows specifying the ID of the Content Manager dataset to be used.

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



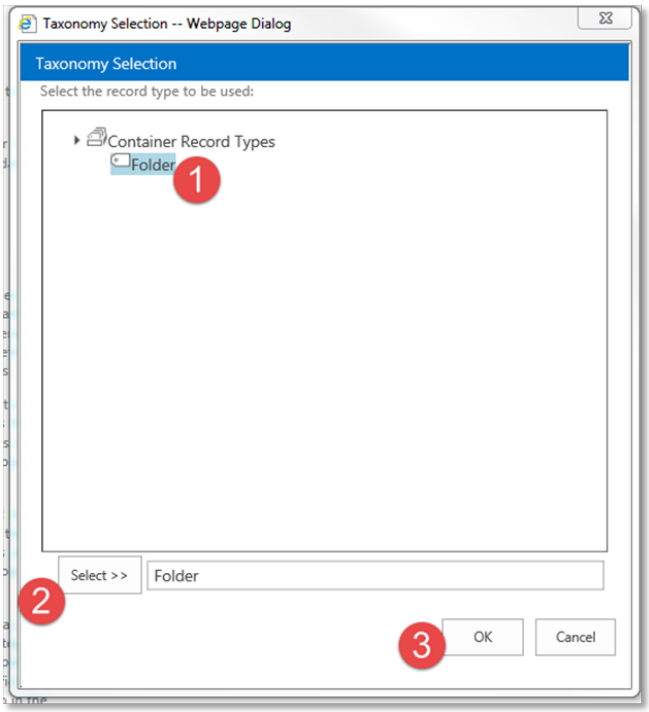
5.1.3 Record Types

The record types section of this page allows specifying the Content Manager record types that should be used by default during management if they cannot be determined through other configuration (such as the content type to record type mapping).



To select a value, click the icon next to the control.

This will open a dialog allowing you to select a Content Manager record type. To choose the record type either double click the required record type or select the record type then click the **Select** button. Click **OK** to finish selecting the value.



NOTE: Make sure to enter a value for all the four record types. For more details, see *Content Manager Governance and Compliance SharePoint App: Installations Guide*.

NOTE: 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. See the *Content Manager Governance and Compliance SharePoint App: Installations Guide* for details of synchronizing Content Manager record types.

Site Record

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

The record type specified here determines the record type that will be used to create records to represent a SharePoint site in Content Manager.

List Record

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

The record type specified here determines the record type that will be used to create records to represent a SharePoint list in Content Manager.

Default Container

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.

If a record type cannot be determined using the CT2RT mapping, the record type specified here will be used to when containers are automatically created in Content Manager.

Default Item

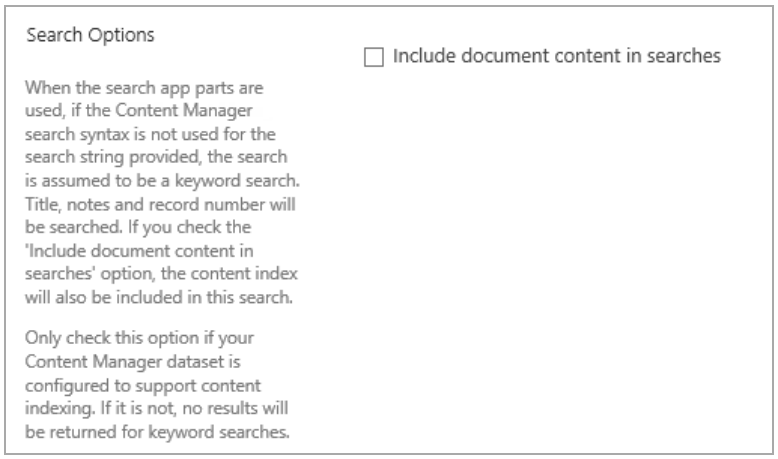
The **Default Item** record type will allow you to select any record type that has a behavior of **Document** and is marked as suitable for being a list item record.

If a record type cannot be determined using the CT2RT mapping, the record type specified here will be used to when a records is created in Content Manager to represent a list item.

> **NOTE:** Ensure that the Default Item record type has a container level in Content Manager that is lower than the Default Container record type.

5.1.4 Search options

The ***Search options*** section of the DISP allows configuring global settings that are used by the search web parts.



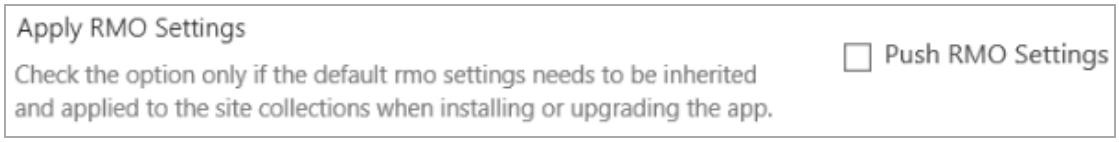
This section includes a single option. Checking the **Include document content in searches** check box indicates that when searches are performed by search web parts, that document content indexing will be included in the search.

For more detail, see search section.

> **NOTE:** You should only check this option if your Content Manager dataset has a current document content index. If it doesn't, no search results will be returned.

5.1.5 Apply RMO Settings

The **Apply RMO Settings** section allows to inherit RMO settings to site collections during installation or upgrading the app.



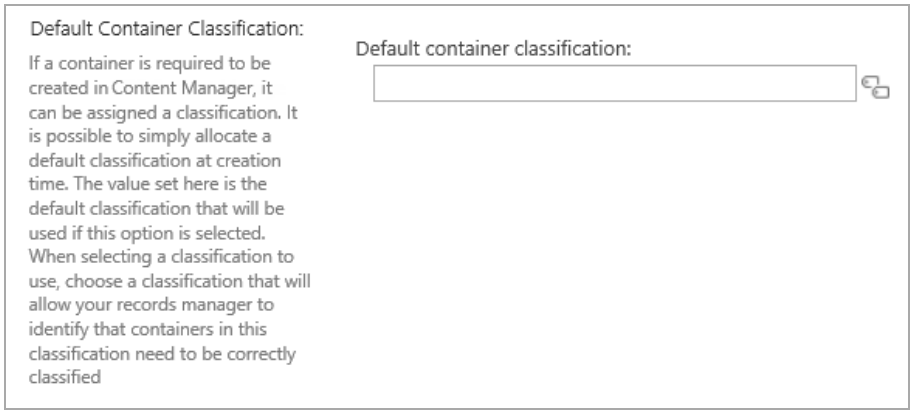
Check the **Push RMO Settings** checkbox to inherit the RMO settings to all your site collections.

For more information, see section 6.1 Records Management Options (RMOs).

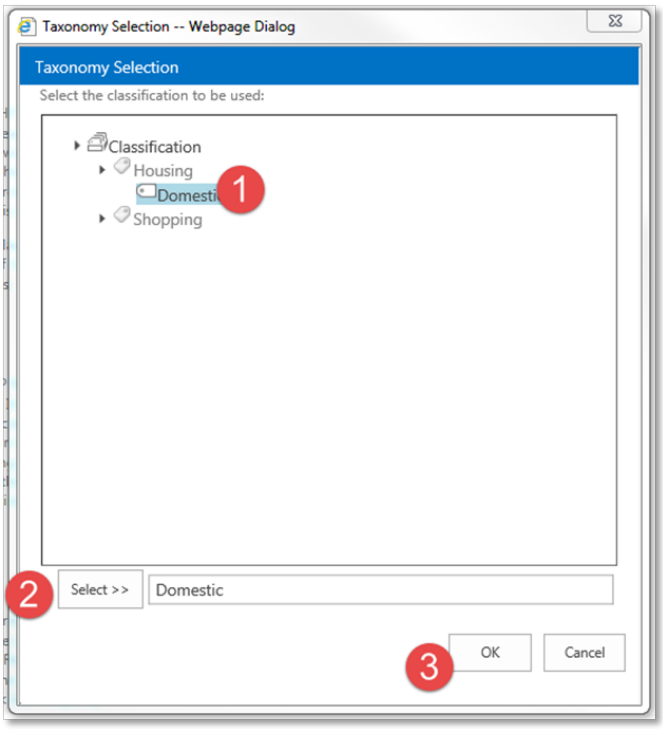
5.1.6 Default Container Classification

The **default container classification** section allows specifying what classification will be applied to automatically created containers if the classification cannot be determined by another method.

To choose a classification, click the button to the right of the control.



This will open a dialog allowing you to select a Content Manager classification. To choose the classification either double click the required classification or select the classification then click the **Select** button. Click **OK** to finish selecting the value.



NOTE: Only classifications 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 a

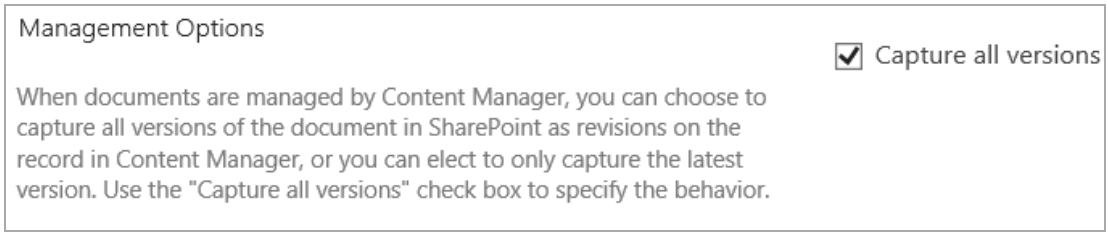
> classification or the selection dialog will not show any values. See the *Content Manager Governance and Compliance SharePoint App: Installations Guide* for details of synchronizing Content Manager classifications.

To clear the selected classification, click the button to open the dialog, then click **OK** without selecting a classification.

5.1.7 Management options

The **Management options** section of the page allows configuring global options that are used by management.

The **Capture all versions** check box is used to determine whether all versions of a document are captured by Content Manager or just the latest version. For more details, see the How documents are managed section.



5.1.8 Exposure Settings

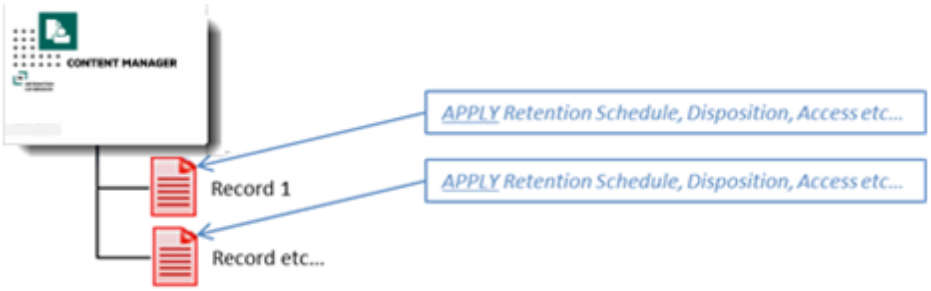
For details, see the Common configuration section.

6 Configuring specific management settings

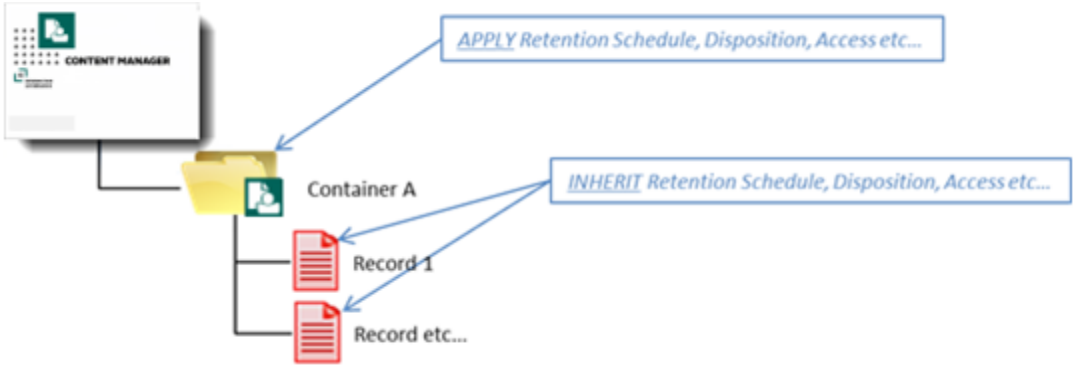
How information is created and consumed in SharePoint, in order to align with business process and general usability, may not necessarily be compatible with that organization's standards and authorities for its retention and disposal.

From a records management perspective, best practices dictate that information should be either:

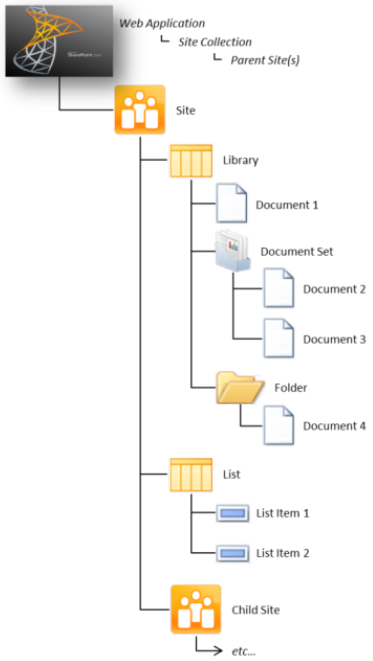
- Classified directly so as to identify the retention and disposal of the individual item:



- Or placed on a file, i.e. within a single container so as to inherit the appropriate retention schedule, along with information of similar subject matter and function, from the container itself.



Whilst structuring records in this manner facilitates the processes of securing, retaining and disposing content in accordance with governing standards, it does not provide the flexibility that information workers typically need to access and create content in line with their day-to-day activities. As a result, records management is often perceived by users as a hindrance rather than of benefit.

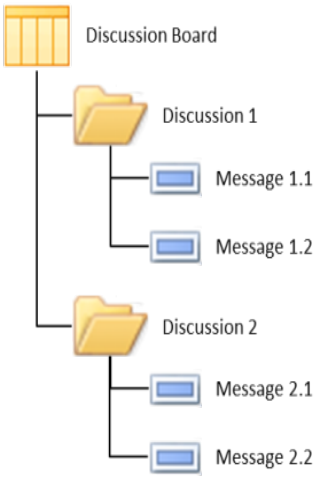


SharePoint information on the other hand often has deep hierarchical structures of various combinations of sites, sub-sites, lists and folders.

While facilitating collaboration and daily operations, in terms of information governance, such structures can easily become unruly; making information difficult to locate, access and manage, through unpredictable arrangements and ad-hoc access controls.

Further, with the host of different information formats available in SharePoint, such as documents, workspaces, web sites and pages, discussion boards, blogs, calendars and so on; what actually constitutes a discrete body of “information” is not necessarily an individual item residing at the ‘end’ of the hierarchical structure.

Consider for example a Discussion Board:



A SharePoint Discussion Board is a List that supports the Discussion content type, which is essentially a Folder with ***Subject*** and ***Body*** columns attached to register the discussion topic. To raise a discussion involves creating one of these items and populating the columns accordingly.

To contribute to this discussion, users ***reply*** to the discussion topic, those replies being generated as items of the Message content type within the Discussion folder.

So while the ***Message*** is the most granular object in the hierarchy, it in itself does not necessarily constitute a discrete body of information.

As an isolated entity, the ***Discussion*** itself doesn't represent a record of what has transpired either. In effect, it actually only represents the first revision/version of the entire discussion.

It's only in acknowledging the Discussion as the sum of its parts (i.e. the Discussion folder and all reply Messages in order) that the full account of the discussion is evident and hence a record. And so where inconsistent or inadequate management of these parts may result in the premature destruction or deletion of any one of them it effectively invalidates the integrity of all of them as a complete record.

The same could apply to a Blog site, whereby ***posts*** and ***comments*** that are retained in entirely separate lists are considered revisions/versions of the same record.

And so the actual ***information*** within SharePoint therefore not only resides within unbound tiers of folders, lists and sites within a site collection, but in certain scenarios also equates to the sum of those structures, rather than just an individual entity.

So the challenge becomes how to bring governance and compliance to SharePoint information that is:

- Contained within unbound, flexible structures;
- Of a range of different information formats, even when relating to the same subject matter and function (and hence warranting the same retention);
- Potentially an incomplete piece of information in its own right unless retained in the context of the SharePoint site, list and/or folder hierarchy within which it resides.

The Content Manager Governance and Compliance App overcomes this significant challenge by providing the capability to manage content in Content Manager in accordance with an entirely separate paradigm to that with which it is "used" in SharePoint.

Through use of the functionality outlined in this chapter, information can still be intuitively grouped in one location (Site/List/Folder) in SharePoint to accommodate the end user's operating needs, while also being logically structured in Content Manager across possibly a number of containers or classifications for governance or retention purposes at the very same time.

In short, this approach provides in-place management of SharePoint content, by applying a structured file plan, without SharePoint content having to be moved or processes changed to support this.

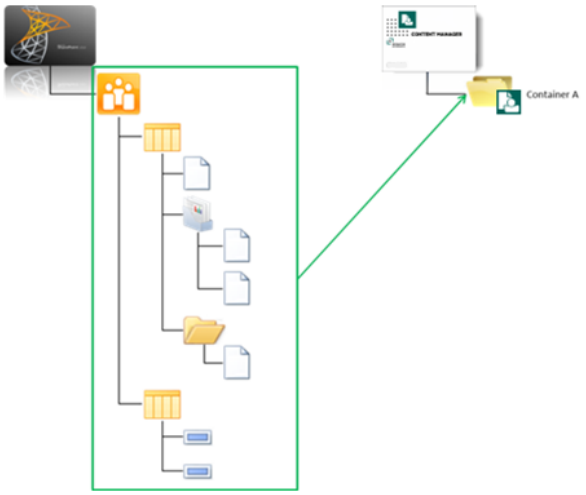
Conversely, this approach also supports centralised management, control and retention of SharePoint information residing in geographically separate content silos (web applications, site collections, sites, lists or folders), without impeding on the existing SharePoint processes and architecture.

Or if so required, entire sites, lists and folders can be managed holistically, ensuring the integrity of the entire record is preserved regardless of the format in which it may have been generated.

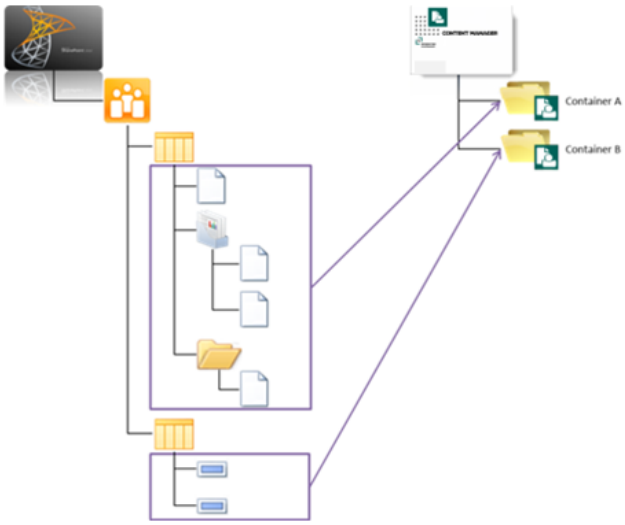
6.1 Records Management Options (RMOs)

The Content Manager Governance and Compliance App achieves all of this through the **Records Management Options** (RMOs) feature. RMOs allows specifying where content from SharePoint is to be managed by Content Manager and are configurable:

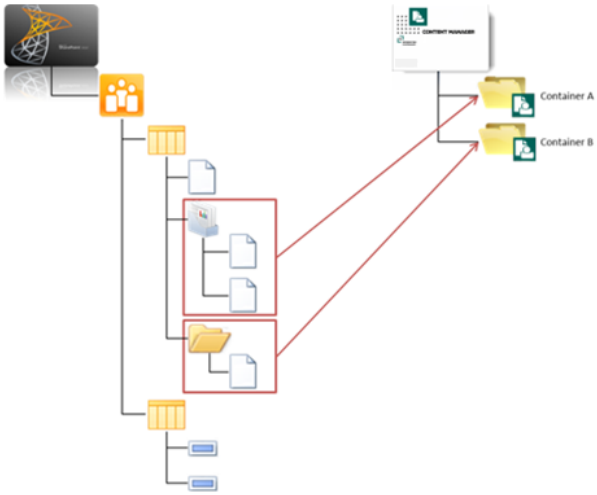
1. On a per-site basis:



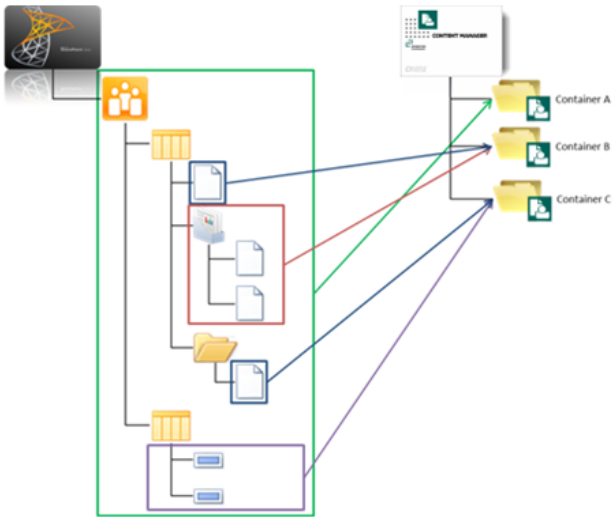
2. On a per-list basis:



3. On a per-folder (or document set) basis:



4. Or any combination thereof:



> **TIP:** While these examples all assume that SharePoint content is to be captured in a Container in Content Manager, as mentioned above, RMOs can also be used to specify a classification to be directly applied to content in these same granular tiers.

As further detailed in this section, RMOs also include capabilities to simplify and minimize the effort required to configure them. This includes:

- Automation of container creation when required
- Inheritance of RMOs from parent sites to child sites and lists

These capabilities allow those responsible for governing the information of an organization to specify how information is to be managed once, without the need for involvement every time a new site or list is added.

RMOs are at the core of resolving the information governance paradox, and allow users to continue to use SharePoint as it should be used (i.e. to organize their information in a manner that facilitates its

operational use) while also allowing records managers and compliance officers to ensure compliance and information integrity.

6.1.1 Enabling the use of RMOs

> **NOTE:** The Site Parent Container or List Containers should not be deleted from Content Manager manually as this breaks the container relationship between the records. Also it will corrupt the integration database.

Enablement Prerequisites

RMOs are made available for configuration at both site and list level, once the ***Content Manager Governance and Compliance App*** has been added to a given site. If the app has not been added, the app start page and menus, and consequently Records Management Options, will not be accessible for that site.

Configuration Prerequisites

The actual configuration of RMOs is considered a function of SharePoint **Site** or **List Administration**, depending on the level at which they are being configured.

In addition, the user performing the configuration must also have a valid Location established in Content Manager that accepts logons. It is not necessary to have a Location type above **Inquiry User** to be able to configure and save RMOs, however this will likely be an impractical level of access in subsequently using that RMO-enabled site.

6.1.2 Site Level RMOs

Site level RMOs govern the structure in which SharePoint content is managed in Content Manager for that entire site, i.e. all items within lists within that site, as well as all child sites within that site which inherit RMO settings (as is the default).

Even in scenarios where it may be desirable for all sites within a site collection to employ the same RMOs configuration, consideration should still be given to what that configuration is to be at the root site of the site collection, so that they are correctly inherited throughout the hierarchy.

The configuration of site level RMOs is made on the site's **Site Records Management Options** page.

Accessing the page

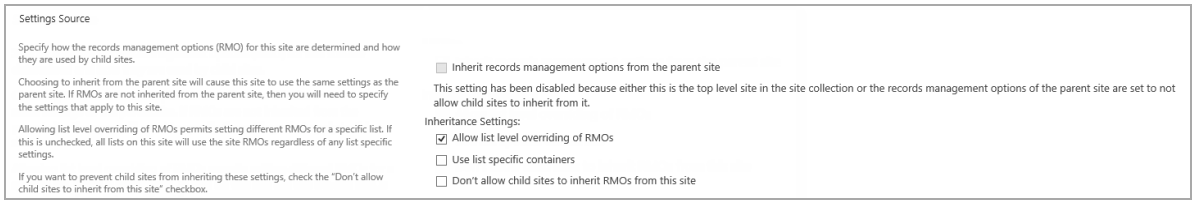
From the app start page click the **Site Records Management Options** link.

> **NOTE:** You must have **manage site** permission to access this page.

Page overview

The **Site Records Management Options** page is comprised of three main sections: the **Settings Source** section, **Parent Container Settings** section and the **Folder Behavior** section.

Settings Source section for site level RMO



The **Settings Source** section determines how the RMO settings for this specific site operate in terms of inheritance to and from other sites and lists within the site collection.

If the site level RMOs are being inherited, a link to the parent site's RMOs is provided at the top of the section.

The controls available for configuration in this section are as follows:

1. **Inherit records management options from the parent site**

   If selected, this option ensures that the RMOs of the parent site are also applied to the content of this site. As such, the site from which the settings are being inherited is indicated in the text immediately above the control, which provides a hyperlink to that parent site's RMO page. All other controls on the page are also disabled as no further configuration is required.

   > **NOTE:** This option is selected by default, except if accessing the site RMOs page of the root site of the site collection or of a site whose parent site does not allow inheritance of RMOs. In these cases this option is unselected and the control disabled by default as inheriting RMO settings is not possible.

2. **Allow list level overriding of RMOs**

   Selecting this option enables the ability to configure specific RMOs on each list and library within the site. This alone does not necessarily mean that each list and library within the site must have unique RMO settings configured though – list RMOs will continue to inherit from the parent site until specifically configured otherwise.

   > **NOTE:** This option is checked by default.

3. **Use list specific containers**

   Checking this option indicates that a container is required for each list in the site. When this option is checked, the list RMOs for each list on the site have the ***Parent Container Settings*** section defaulted to ***Automatically create a container***. Lists will still by default inherit the ***Automatic container creation settings*** as specified on the site RMOs, however these are able to be overwritten at list level if necessary.

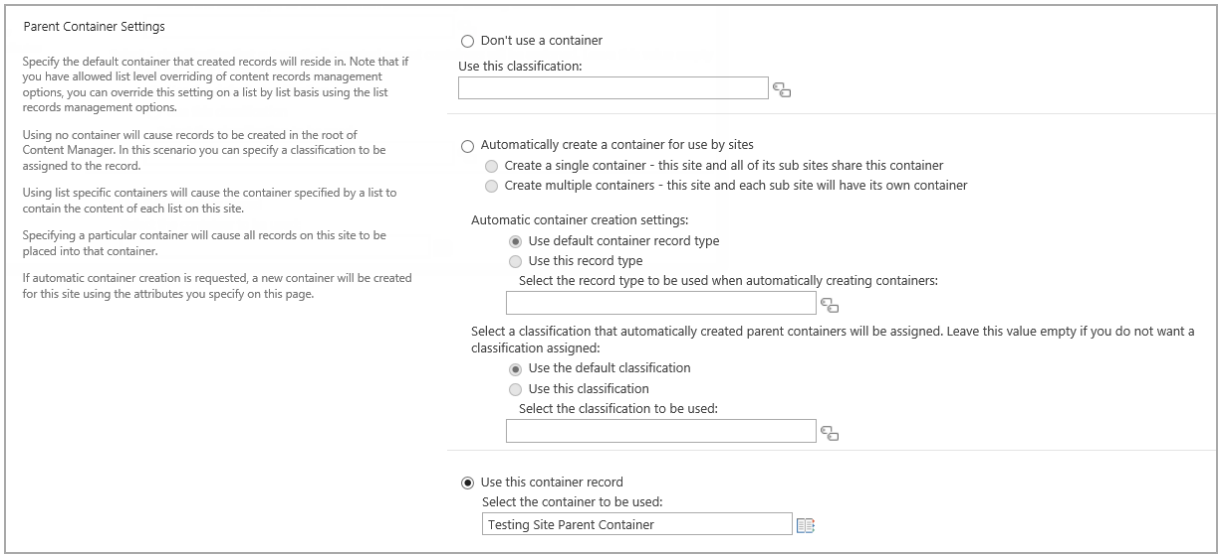
   > **NOTE:** As this option is obviously dependent on whether unique RMOs can actually be configured for lists within the site, if the **Allow list level overriding of RMOs** option is not selected in the **Settings Source** section, this control will be disabled.

4. **Don't allow child sites to inherit RMOs from this site**

If this option is selected, then although the RMOs specified on the page can still be inherited by lists on the site, no child sites are able to inherit RMOs from this site.

> **NOTE:** This option is not selected by default.

Parent Container Settings section for site level RMO



This section is where the specific options for how SharePoint content is managed are configured. The controls provided allow for specifying the capture method of SharePoint content in Content Manager, i.e. capture either direct to classification or within a “container”.

> **TIP:** In the context of the Content Manager Governance and Compliance App, a **Container** is an Content Manager record with a behavior of **Folder**, which is used in Content Manager to group records, thereby allowing for (amongst a number of other functions) bulk sentencing through inheritance by individual records of any retention and disposal settings applied at the parent Container level.
>
> An Content Manager record with a behavior of **Folder** is referred to as a **Container** in the context of this integration so as to differentiate the object from the SharePoint **Folder** content type.

In capturing the content by either ‘method’; further configuration options then allow for specifying *how* that information is then to be registered, including which record type is to be used; and which Content Manager Classification (if any) is to be applied, either directly or via the container itself.

To achieve all of this, the controls provided in this section are structured so as to only provide relevant configuration options based on the capture method that has been chosen. They are:

Choose the Default Parent Container to Use

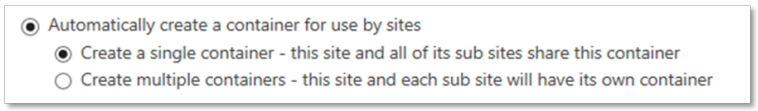
These controls allow for specifying an existing container or classification to be used:

1. **Don't use a container**

   If this option is chosen, then managed SharePoint content will reside in the root of Content Manager, i.e. it will not be grouped with any other Content Manager content.

   In selecting this option, the ***Use this Classification*** control (below the option buttons) becomes enabled, allowing for a specific Content Manager Classification to be applied to content individually upon management, in lieu of it being contained. It is not however mandatory to specify a Classification when not using a container.

2. **Automatically create a container for use by sites**

   a. **Create a single container – this site and all of its sub sites share this container**

      This option will generate a new container in Content Manager upon the first instance of management of content within a site. The container will then be used to contain all subsequently managed content in that site, including any content managed within its sub sites.

      > **TIP:** Selecting this option enables the **Automatic Container Creation Settings** on the page, as detailed below.

   b. **Create multiple containers – this site and each sub site will have its own container**

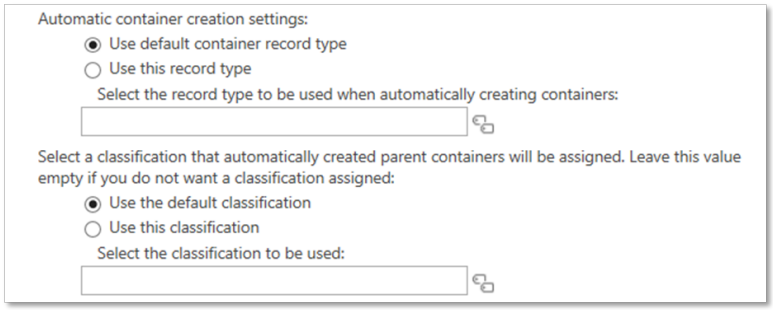
      Upon the first instance of management of content within a site, this option will generate a new container in Content Manager in which to capture that content. However for sub sites that inherit RMOs from this site, individual containers will be created for each of those sub sites, on the occasion of first management of content within them.

      > **TIP:** Selecting this option enables the **Automatic Container Creation Settings** on the page, as detailed below.

      > **NOTE:** For sites that do not inherit RMOs, this option is selected by default.

3. **Automatic container creation settings**

   These controls are only applicable when automatically creating the site parent container (based on settings made previously):



a. **Use default container record type**

With this option selected, the default container record type, as specified in 5.1.3 Record Types, on page 35 section, will be used to create the site parent container.

b. **Use this record type**

Selecting this option allows for specifying the record type to be used in creating the site parent container by then using the ***Select the record type to be used when automatically creating containers*** control.

> **NOTE:** If this option is selected, a record type must be specified.

c. **Use default classification**

With this option selected, the default classification, as specified in 5.1.6 Default Container Classification, on page 38 section, will be applied to the site parent container upon creation.

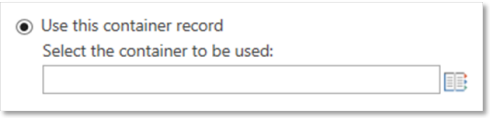
d. **Use this classification**

Selecting this option allows for specifying the classification to be applied to the site parent container upon creation by then using the ***Select the classification to be used*** control.

> **NOTE:** If this option is selected, it isn't mandatory to then select a classification. Omitting a classification will simply result in no classification being applied to the site parent container.

4. **Use this container record**

Selecting this option allows for specifying an existing Content Manager container to be used as the site parent container, and enables the **Select the container to be used** control to select which existing Content Manager container shall be used.

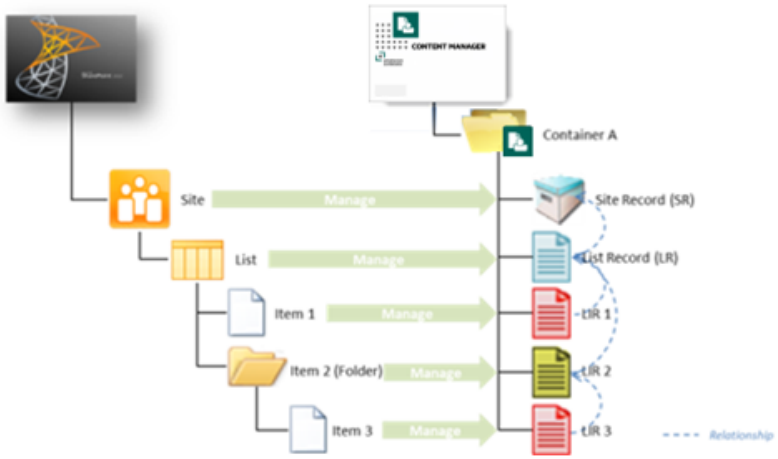


> **NOTE:** If the **Use this container record** option is selected, a container must be specified.

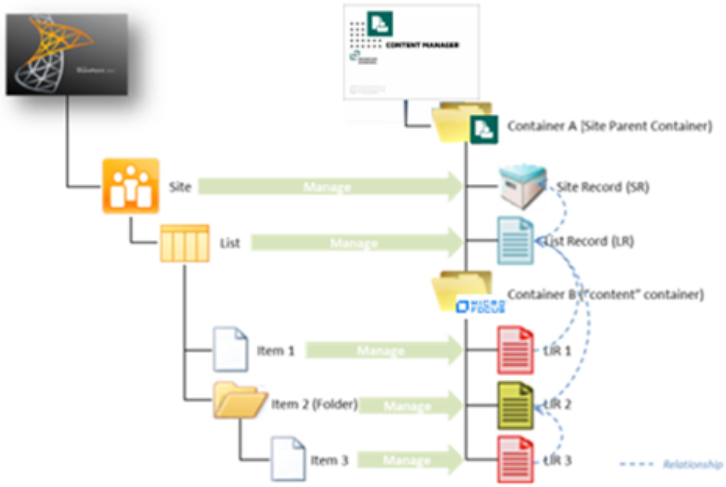
Folder Behavior section

The default behavior for the application of RMOs that utilise an Content Manager container is to either:

- Create a parent container at site level (Site Parent Container) to house all the individual records, together with structural information (Site and List Records):



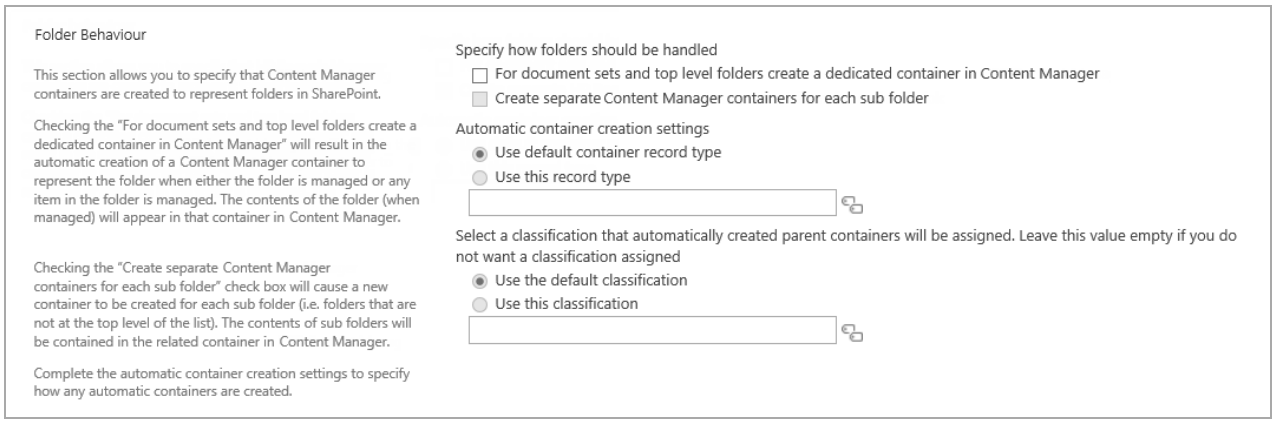
- Or create the parent container of the content on a per-list basis, to isolate content records from structural ones:



In both scenarios, relationships are used on the Content Manager records to preserve hierarchical context of the information as it resides in SharePoint, whilst establishing a flattened structure in Content Manager so as to facilitate retention and management of the records themselves.

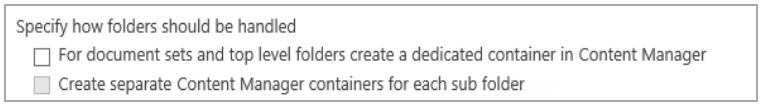
Depending on the size and hierarchical depth of list sub-structure however, these models may be insufficiently granular to sentence list content appropriately (assuming this is being achieved via container inheritance in Content Manager).

The **Folder Behavior** section of the RMO page allows for generating Content Manager containers as representation of folders within a list, thus enabling separate classification of groups of content within the same list.

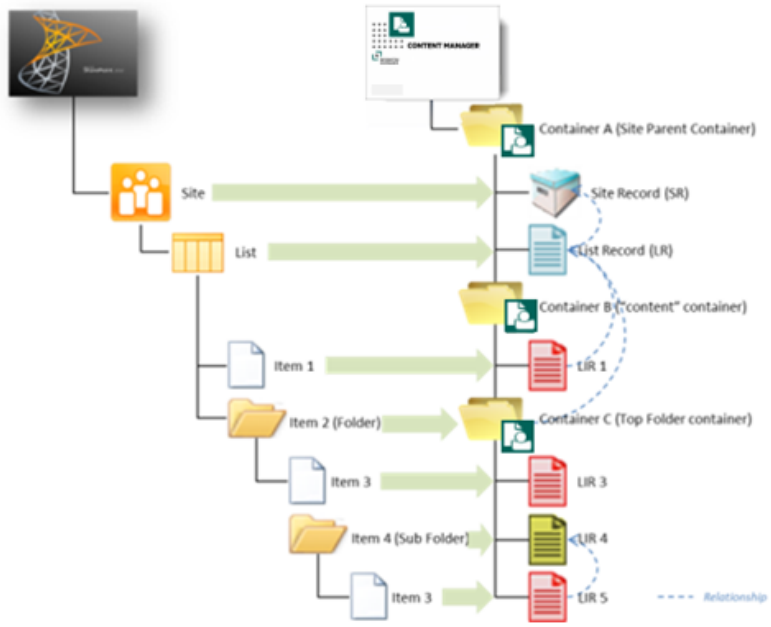


The following controls are available for specifying how folders should be handled in the site:

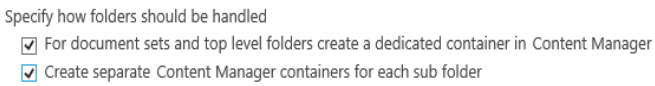
For document sets and top level folders create a dedicated container in Content Manager



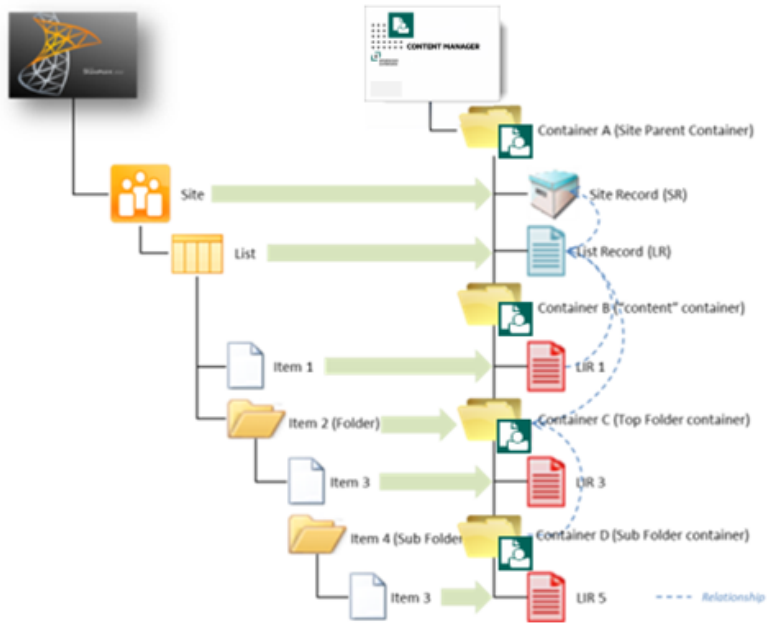
As the title suggests, selecting this checkbox ensures that upon management with Content Manager, folders and document sets that reside at the root of the list are created as containers in Content Manager, allowing for them to carry unique classifications and other attributes, thus facilitating their independent management and retention. However, any sub-folders will still be flattened in Content Manager, and represented as related records.



Create separate Content Manager containers for each sub folder



Selecting this option also generates unique Content Manager containers for each sub-folder in the list.



> **NOTE:** The sub-structure of the list will not be replicated in Content Manager. Containers are instead generated as sibling records in Content Manager and utilise relationships to preserve the hierarchical context with which they reside in SharePoint.

Automatic Container Creations Settings

These controls are only applicable when creating containers in Content Manager to represent folders in the list. They allow for specifying to either use the default ***Container*** record type (as specified on the Default Integration Settings page), or a different one as specified in the ***Use this record type*** control; and similarly for determining a classification to be applied to the container (if any).

6.1.3 List level RMOs

List level RMOs facilitate the application of a more granular approach to records management of SharePoint content than site RMOs by allowing each individual list and library within a site to have unique settings.

The ability to apply list level RMOs is dependent on the **Inheritance Settings** that have been made in the Settings Source section for site level RMO, on page 46 section of the parent site's RMOs. If enabled, any specific settings made on the list level RMOs only apply to the specific list for which they were configured.

List level RMO settings are configured on the list's ***Records Management Options*** page.

Accessing the page

> **NOTE:** You must have **manage list** permission to access this page.

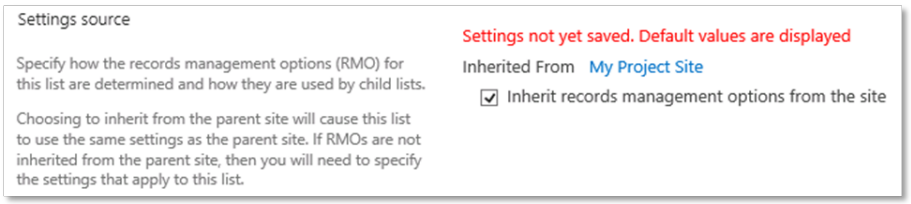
To open the list **Records Management Options** page:

1. Navigate to the required SharePoint list.
2. Expand the list/library ribbon menu, and under the **Settings** section, click on the **Content Manager** drop-down.
3. From the drop-down menu, choose **Records Management Options**.

Page overview

Similar in appearance to the Site RMOs page. The List Records Management Options page is also comprised of the three main sections: the **Settings Source** section, the **Parent Container Settings** section and the **Folder Behavior** section.

Settings Source section for list level RMO



The **Settings Source** section of the List Records Management Options page only allows for determining whether RMOs are to be inherited from the parent site. No subsequent **Inheritance Settings** are required as list level RMOs cannot themselves be inherited.

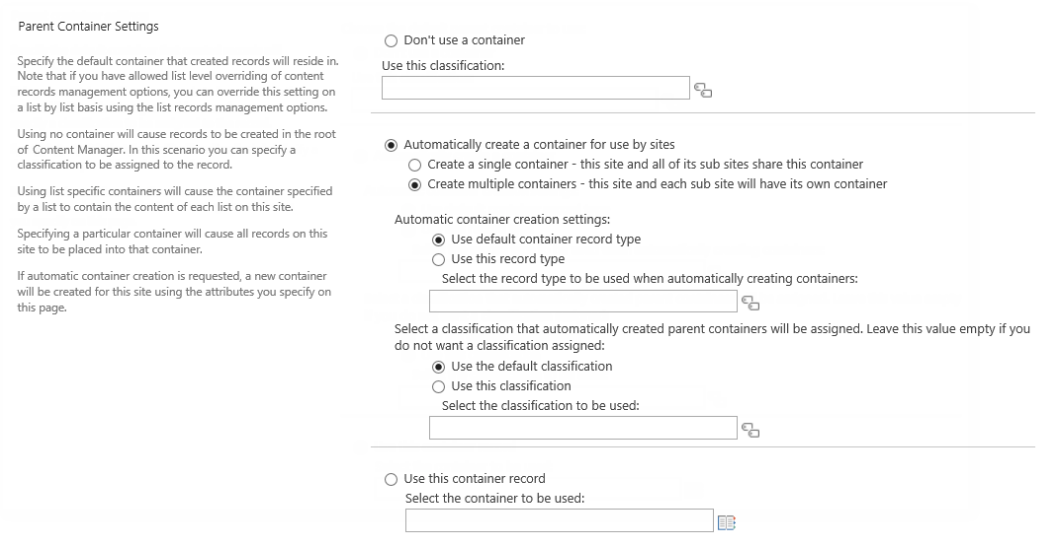
If list level RMOs are being inherited, a link to the parent site's RMOs is provided at the top of the section.

If the parent site does not ***Allow list level overriding of RMOs***; then the list level RMO option to **In*herit records management options from the site*** is selected by default and unable to be changed. If however the parent site does allow override, then while inheritance remains on by default, it can be manually turned off and unique settings applied.

Further, if ***Use list specific containers*** is checked on the site level RMOs, then the ***Parent Container Settings*** value of the List RMOs is defaulted to ***Automatically create a container***.

> **TIP:** The Automatic Container Creation Settings remain inherited from the site RMOs in this scenario but can also be overwritten.

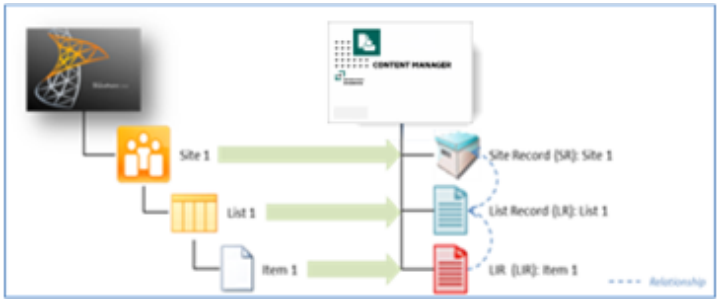
Parent Container Settings section for list level RMO



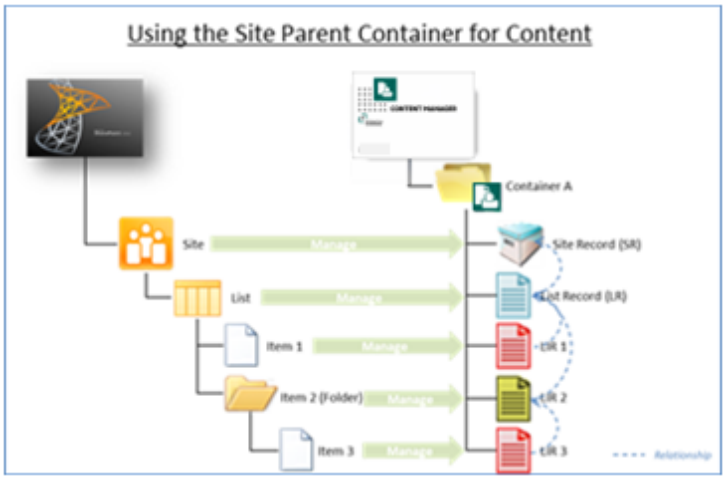
The list **Parent Container Settings** are more or less identical in behavior to the Parent Container Settings section for site level RMO with regard to determining the capture method and container/classification settings for SharePoint content, however there are a few obvious discrepancies:

- The ***Use list specific containers*** control is omitted as these settings are already being made at list level;
- The ***Automatically create a single container – this site and all of its sub sites share this container*** option is modified to ***Automatically create a container*** as there are no sub sites; and
- The ***Automatically create multiple containers – this site and each sub site will have its own container*** *option is removed for the same reason as above.*

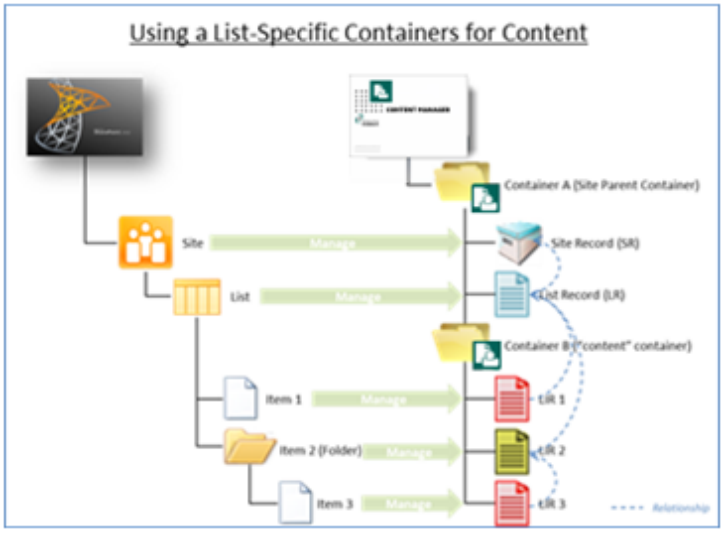
Capturing 'Content' Records vs 'Structural' Records in Containers



When SharePoint content is managed with Content Manager, a List Item Record (LIR) is created in representation of the now Managed List Item (MLI). In addition, Site and List Records (SRs/LRs) are also created (if not already present as the result of a previous ***manage*** action) as a means of recording the SharePoint hierarchy in which the content resides, with relationships established accordingly between each of these content and structural records to preserve that SharePoint operational context.



When specifying RMOs to capture these records within Content Manager containers, if using the site's parent container to capture all content within that site (i.e. not using list-specific containers), the content record (the LIR) and structural records (the LR and SR) will be co-located in that container.



If however containers are specified for the capture of list-specific content, then as expected all 'content' records will be captured in the list-specific container. The List Record (LR) of that list will however still be created in the site's parent container.

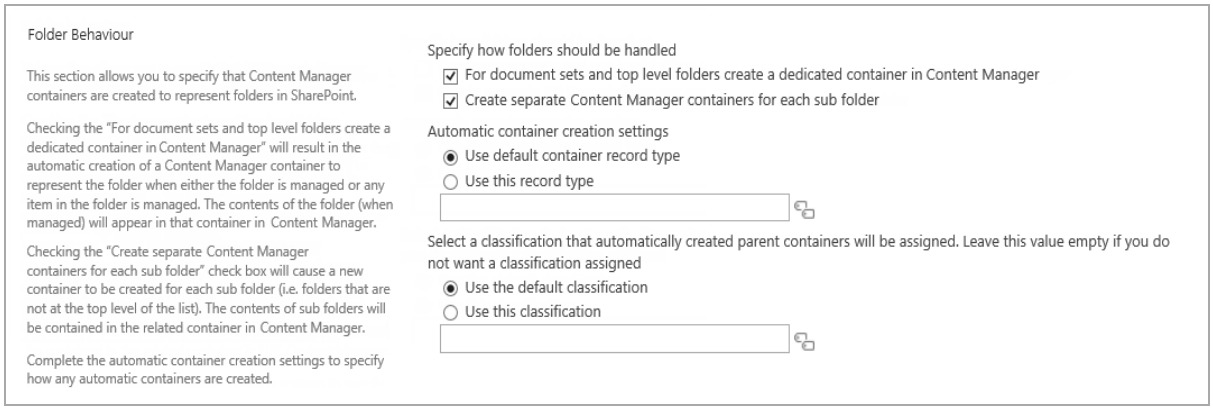
This behavior achieves segregation of the 'structural' records of the site from the actual 'content' records that reside within a list for records management purposes whilst still retaining the context of the information as it resides in SharePoint through use of relationships that are able to transcend the Content Manager container structure.

> **TIP:** Introducing **Folder Behavior** into this equation achieves even more granular capture of 'content' records whilst still capturing all site and list records in the site parent container.

Folder Behavior section

The ***Folder Behavior*** options provided at list level are identical in function to the Folder Behavior section, on page 50 options. Default values may be present based on inheritance, however may be

overridden if the site RMOs are configured to ***Allow list level overriding of RMOs***.



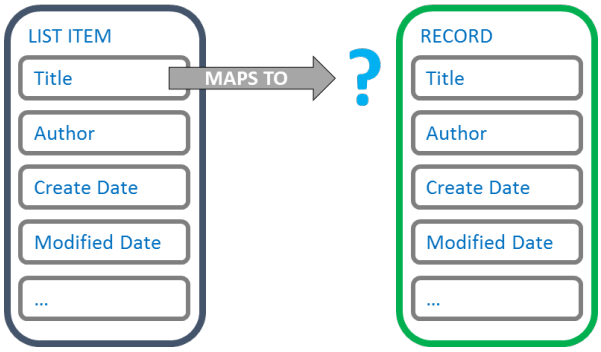
7 Configuring content

7.1 Determining how SharePoint Metadata is to be captured

When a list item is managed with Content Manager, a record is created to represent the list item. Records have fields that are used to hold the metadata associated with a record. A record may have over 100 fields.

List items also contain metadata. Metadata in SharePoint is retained in columns.

The metadata stored in the columns of a list item, often equates to the value that should be placed into a particular field on the record.

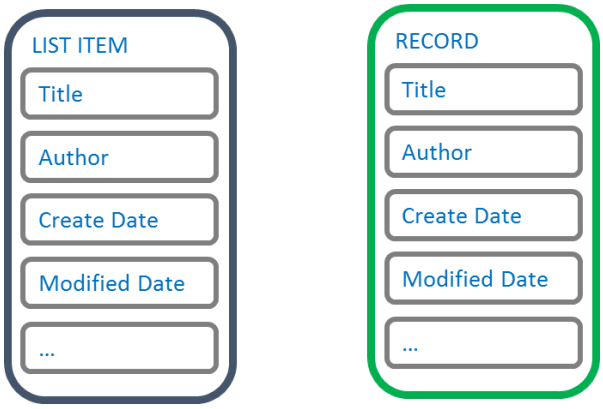


This chapter describes how to configure where column metadata is placed on a record.

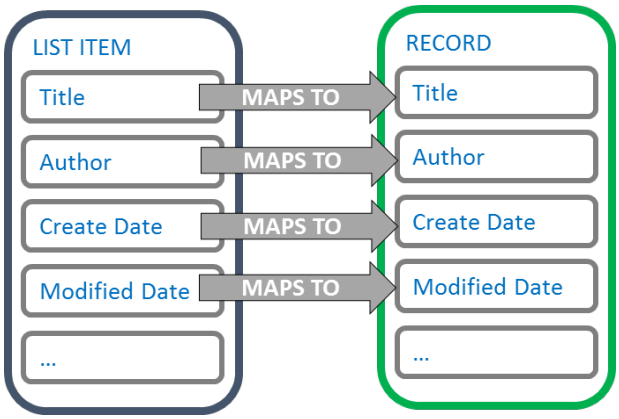
7.1.1 Column mapping

Column mapping is the configuration that is used to determine which record field that list item column values should be placed into.

If we look at the following example, it may appear quite obvious where column metadata should reside:



As there is a one to one relationship between the list item columns, and the record fields, it could be deduced that the following mapping is applicable:

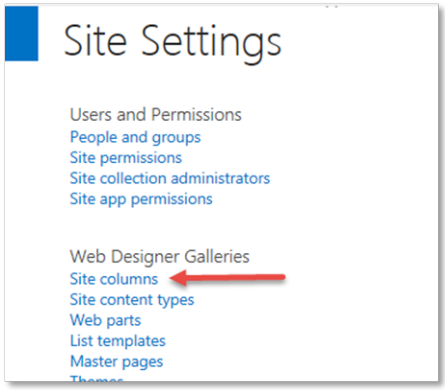


Column mappings are not always this obvious though. Column mapping is therefore something that is configurable.

Site column mappings vs List column mappings

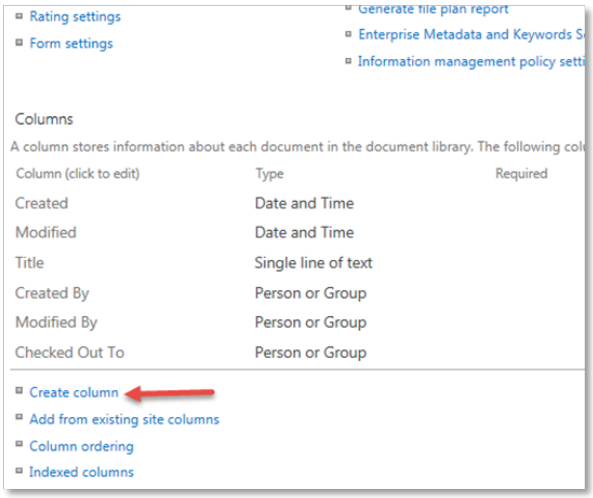
SharePoint supports two types of columns:

1. **Site columns**: these are columns that are defined at site level and can be shared/used in multiple content types and added to multiple lists. Typically, you access site columns from site settings for the site or site collection.



2. **List columns**: these are columns that are associated with one, and only one list. These are the columns that you create through the list or library settings for a list or library, or the **Create**

Column ribbon button for a list or library.



Mappings of site columns, apply wherever that site column is used.

Mappings of list columns only apply to the single list that the column is used on.

7.1.2 The column mapping page

The **column mapping** page is used to manage column mappings. Depending on where you access this page, it allows you to create mappings for site columns, or list columns.

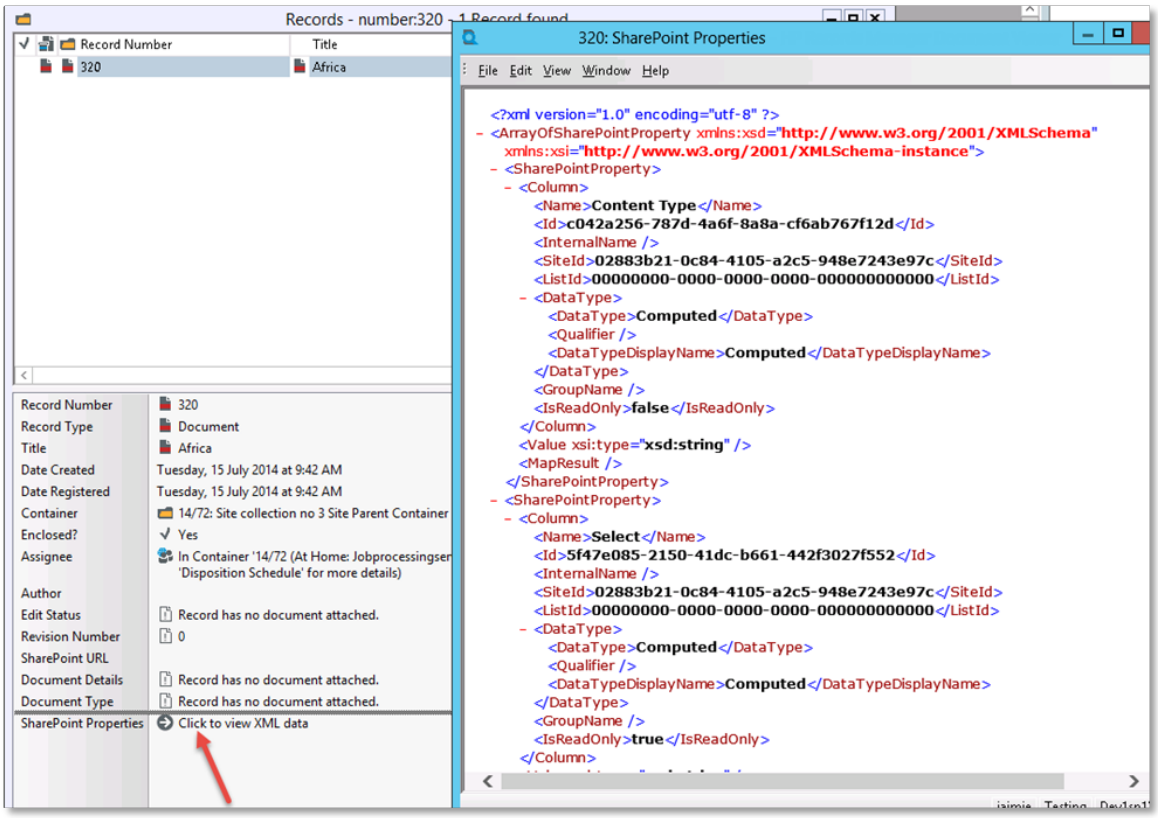
7.1.3 Unmapped columns

It is not necessary to map all columns to Content Manager fields. You should only map the columns that the values are specifically required to appear in a particular Content Manager field.

Columns that are not mapped, are referred to as **unmapped columns**. Unmapped columns still have the column data captured by the record in Content Manager. The first time that a record type is used to create a record for managing a SharePoint list item, the record type is modified to have an additional field added to it. This field is called **SharePoint Properties**.

The SharePoint properties field can be viewed in Content Manager in the same way as any other field. See the Content Manager documentation for details regarding how to view the content of a field.

After adding the SharePoint properties field to the view pane, the value can be viewed by clicking on it. The content is an XML representation of the unmapped properties.

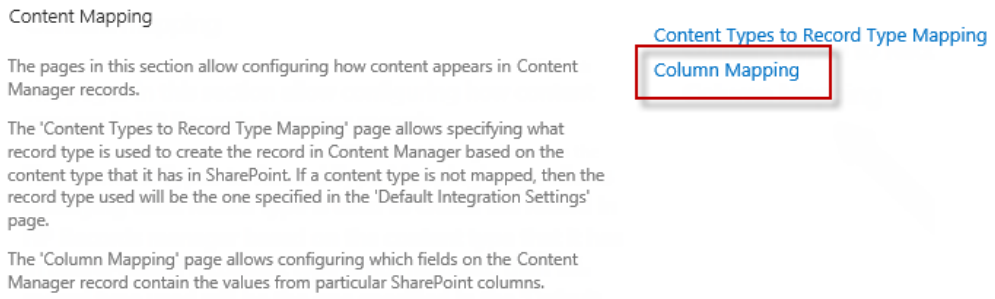


7.2 Mapping SharePoint Columns to Content Manager Fields

7.2.1 Accessing the column mapping page

The site column mapping page

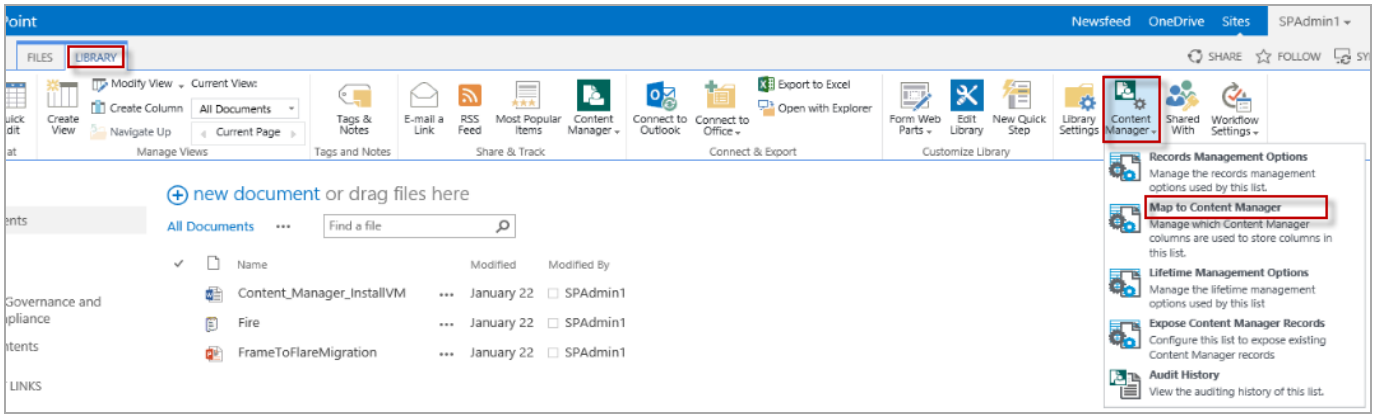
The site column mapping page is accessed via the app start page . The **Content mapping** section includes a link to the **Column Mapping** page.



> **NOTE:** You must have **manage site** permissions to access this page.

The list column mapping page

To access the column mapping page for mapping of list columns, go to **Library ribbon > Settings tab > Content Manager** and select **Map to Content Manager** drop down.



NOTE: You must have **manage list** permissions to access this page.

7.2.2 Using defaults

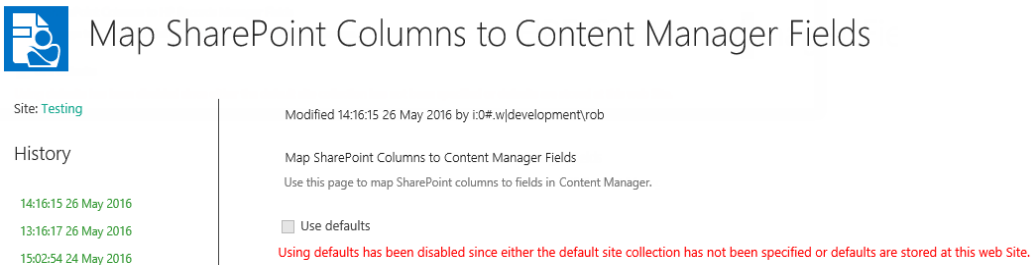
NOTE: This section applies to the site column mapping page only.

Following the page description is the **Use defaults** check box.

Checking this option indicates that this site should use the column mapping that is specified for the default site collection.

If this option is checked, it is not possible to modify the column mapping. The values specified in the column mapping of the default site collection will be displayed as read only on the page.

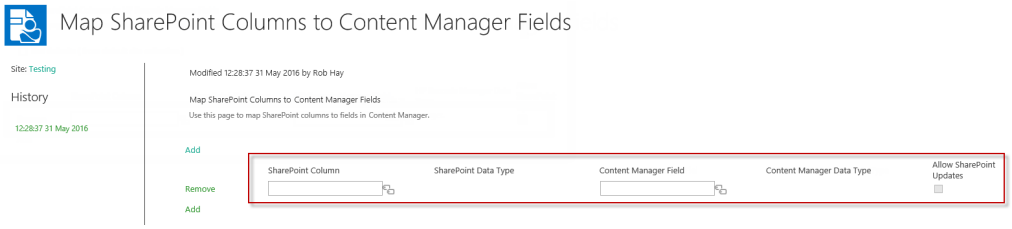
If the column mapping being modified is that of the default site collection, this check box will be disabled.



7.2.3 Adding a mapping

Adding a mapping involves selecting the column to map, then choosing the Content Manager field to map it to. Click **Add** link.

A new blank mapping row is added to the page:



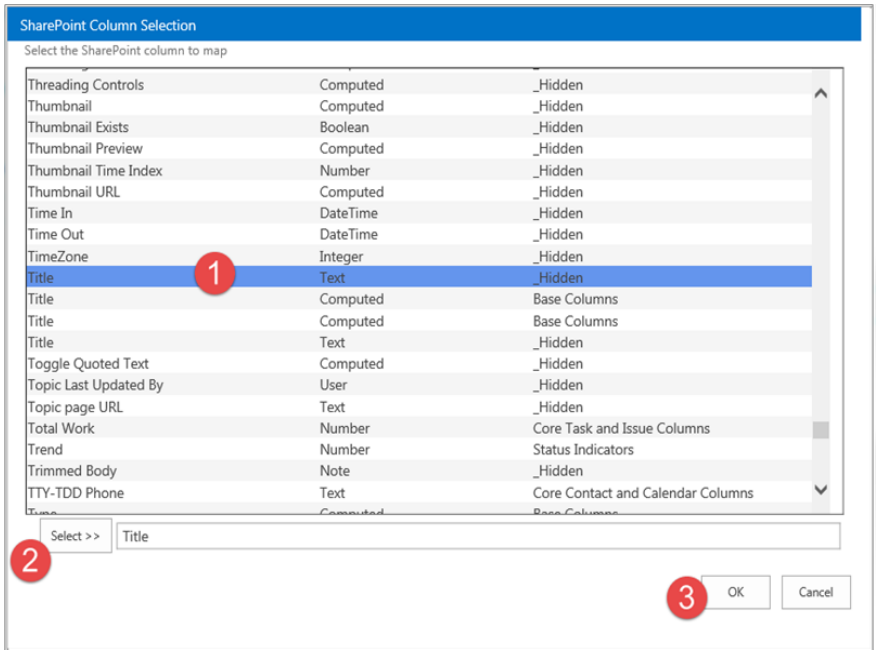
Click the selection icon next to the blank SharePoint column entry.

The **SharePoint Column Selection** dialog is displayed. This dialog will contain the list of columns that are valid to be mapped. In the case of site column mapping, the list will contain all site columns for this site.

> **NOTE:** If this site is a child site, you will not see site columns that are defined on parent sites.

If list column mapping is being performed, only those columns that are specific to this list (and are not site columns) will be available for selection.

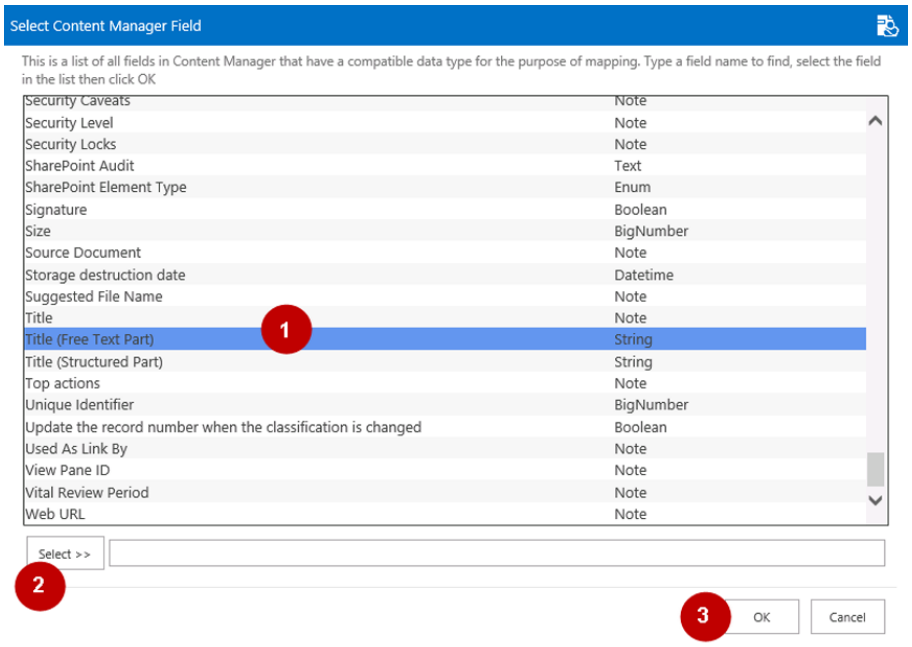
To choose a column, select it from the list, click **Select** then click **OK**.



Once the SharePoint column has been selected, click the button next to the **Content Manager Field** to choose the field that the column is mapped to.

This will open the **Select Content Manager** Field dialog. The columns that are displayed in this dialog are dependent on the data type of the column that was selected. Only Content Manager fields with suitable data types for the content in the selected column are displayed. This means that not all Content Manager fields are displayed in this list.

To choose a field, select it from the list, click **Select** then click **OK**.



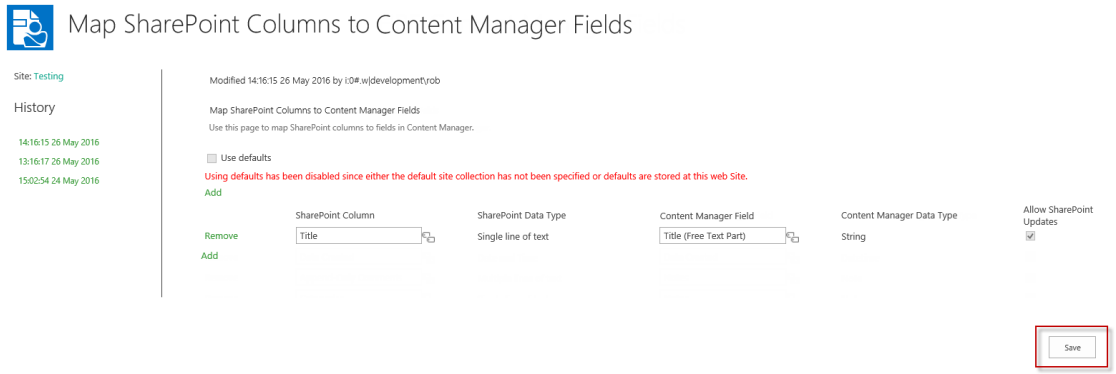
Once selected, the new mapping has been entered, ready to be saved.

The **Allow SharePoint Updates** column contains a read only value that indicates whether updates made in SharePoint will be allowed. The value of this checkbox is automatically populated when you add the details of the mapping and cannot be changed.

There are fields in Content Manager that are not user modifiable. For example, it is not permitted to modify the record number of a record, however, it may be required to display the record number column in SharePoint. If you map any column to the Record number field in Content Manager, any changes made to that column in SharePoint will be prevented.

7.2.4 Saving the mappings

Once mappings have been entered, click **OK** to save them.

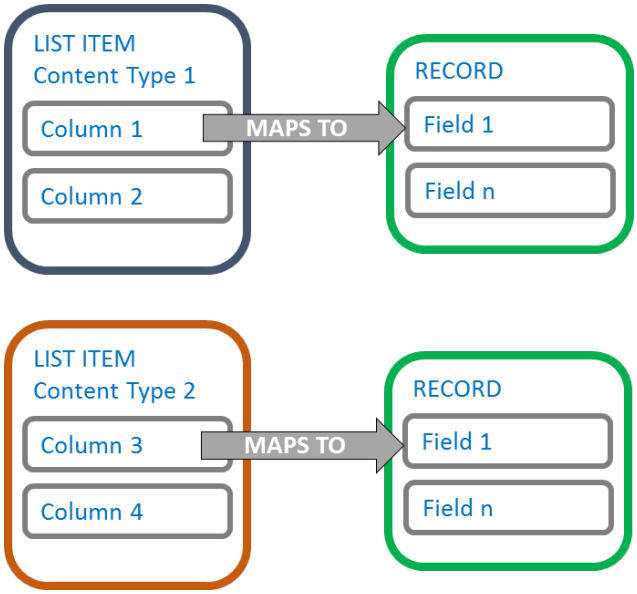


7.2.5 Removing a mapping

Next to each mapping is a **Remove** link. Click this link to remove the mapping from the column mapping.

7.2.6 Duplicate mappings

It is possible to map multiple columns to the same Content Manager field. This is a valid scenario. For example, you may require that a different column be used to provide the value of a Content Manager field depending on what content type is used.



In this example, both ***Column 1*** and ***Column 3*** would be mapped to ***Field 1***

If another content type (content type 3) was to include both ***Column 1*** and ***Column 3***, whichever column appeared first in the content type would be used. Therefore, if content type 3 had columns in this order:

1. Column 3
2. Column 2
3. Column 1

Column 3 would be used to provide the value for field 1. Column 1 would be considered an unmapped column.

7.2.7 Standard mappings

There are some obvious mappings that can be made between columns and Content Manager fields. The default site collection will initially include these mappings as standard.

SharePoint Column	SharePoint Data Type	Content Manager Field	Content Manager Data Type	Allow SharePoint Updates
Title	Single line of text	Title (Free Text Part)	String	☑
Date Created	Date and Time	Date Created	Datetime	☑
Append-Only Comments	Multiple lines of text	Notes	Note	☑
Categories	Single line of text	Notes	Note	☑
Date Modified	Date and Time	Date Modified	Datetime	☐
Date Picture Taken	Date and Time	Date Created	Datetime	☑
Revision	Single line of text	Revision Number	Number	☐
Subject	Single line of text	Title (Free Text Part)	String	☑
Name	File	Title (Free Text Part)	String	☑
Version	Single line of text	Revision Number	Number	☐
Date Completed	Date and Time	Date Closed	Datetime	☑
Attached Labels	Single line of text	Attached Labels	Note	☐
Last Updated By	Single line of text	Last Updated By	Location	☐
Unique Identifier	Single line of text	Unique Identifier	BigNumber	☐

Remove or modify these mappings if they do not suit your requirements.

7.2.8 Adding mapped columns to a list or library

If you add a mapped site column to a list or library, the value of the corresponding Content Manager field will be displayed in this column for each managed item.

For example, consider a document library with 10 managed documents in it and users have asked for a way of readily identifying the record number of the record used to manage these documents. This can be achieved by:

1. Creating a site or list column to display the record number
2. Mapping that column to the ***Record number*** Content Manager field
3. Adding the column to the document library

A job is added to the job queue to populate the column values with the Content Manager values. As this job executes, the record numbers will begin to appear in the column. When the job completes, all managed documents will have the record number displayed in the column.

Any subsequently managed documents will have this record number column automatically populated as part of the management process.

7.3 Columns that use custom behavior

There are data types used by Content Manager fields that do not equate well to the standard data types used by SharePoint. Columns created by the column creation tool modify the behavior of some SharePoint data types to provide an experience more consistent with the type of data being displayed.

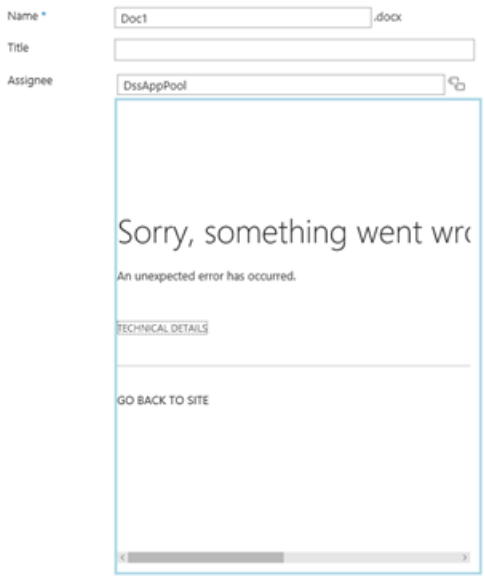
This section describes these custom columns and the behavior.

These columns can only be used if the site has the app added to that actual site. Even if the app is added to the site collection, any child sites will need to also have the app added. If not added, the browser may show the following error when opening a SharePoint list view that includes these columns:

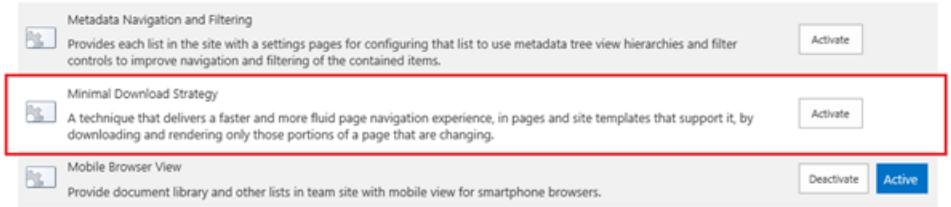
```
Line: 1

Error: Sys.ScriptLoadFailedException: The script 'http://sharepoint/subsite/_
catalogs/masterpage/hprmfieldbehaviour.js?ctag=0$$15.0.4569.1000' failed to load
```

The following only affects an on-premise installation of SharePoint 2013 and later versions, it does not apply to SharePoint Online.

If the following error is seen while trying to select a new value for one of the Integration columns:

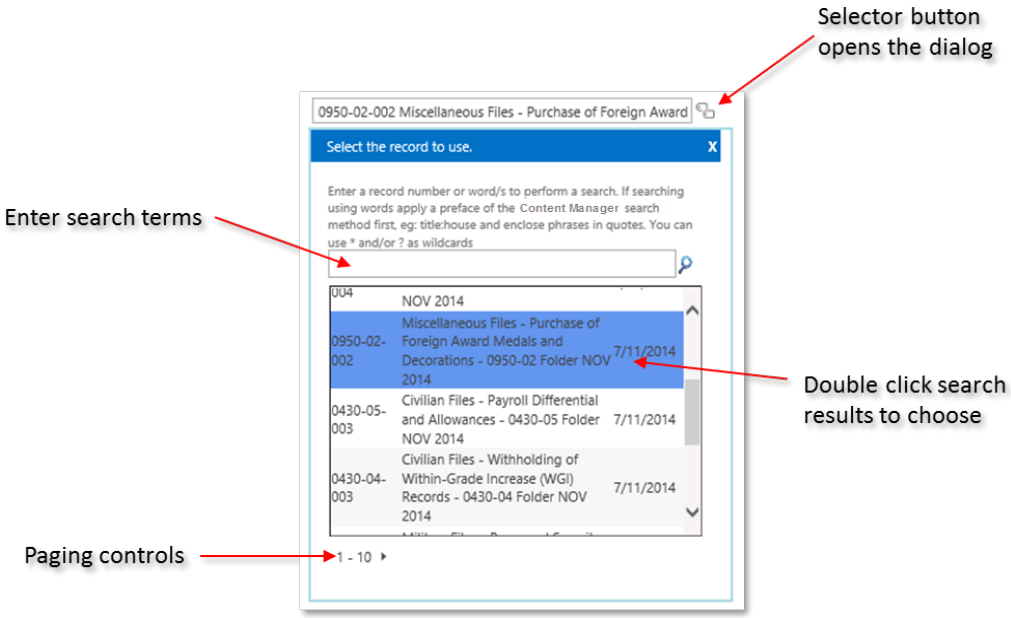


Then either refresh the browser page or de-activate the **Minimal Download Strategy feature** from **Site Settings > Site Actions > Manage Site features** page.



7.3.1 Record based columns

Columns that are designed to allow the selection of a record or container provide a select button to the right of the control that displays a search and selection dialog that can be used for finding and choosing the relevant record.



By default, if the column allows selection of any record, then the records initially shown are all records in Content Manager with the latest registered records shown first. If the column allows selection of a container, then the values in the dialog are filtered to only show containers that have a behavior of ***folder*** in Content Manager.

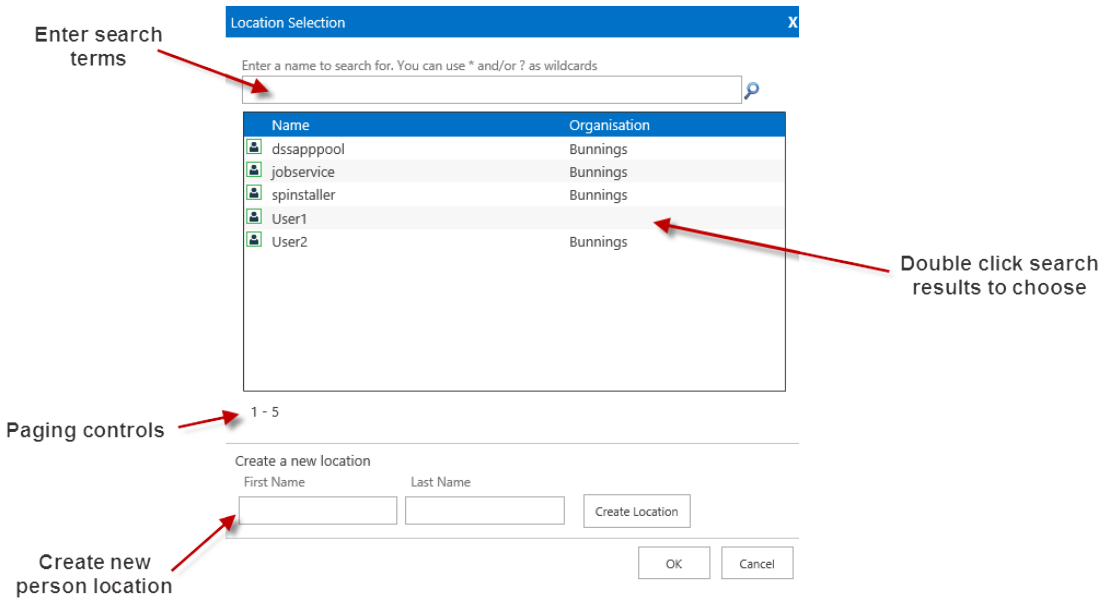
Examples of columns that use this behavior are:

- Container
- Alternative container

> **NOTE:** Only records that a user has permission to access are included as available for selection.

7.3.2 Location based columns

Columns that are designed to allow the selection of a location provide a select button to the right of the control that displays a search and selection dialog that can be used for finding and choosing the relevant location.



By default, the locations initially shown are all locations in Content Manager ordered alphabetically.

Examples of columns that use this behavior are:

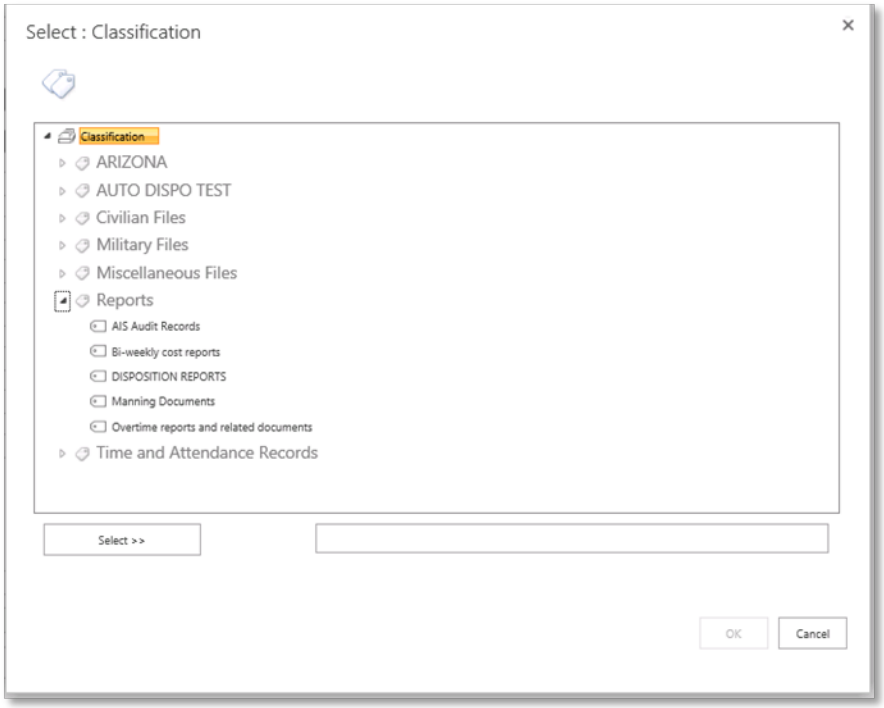
- Author
- Assignee
- Addressee
- Other contact
- Representative

> **NOTE:** Only location that a user has permission to access are included as available for selection.

7.3.3 Classification based columns

Two classification based columns are included in the standard columns.

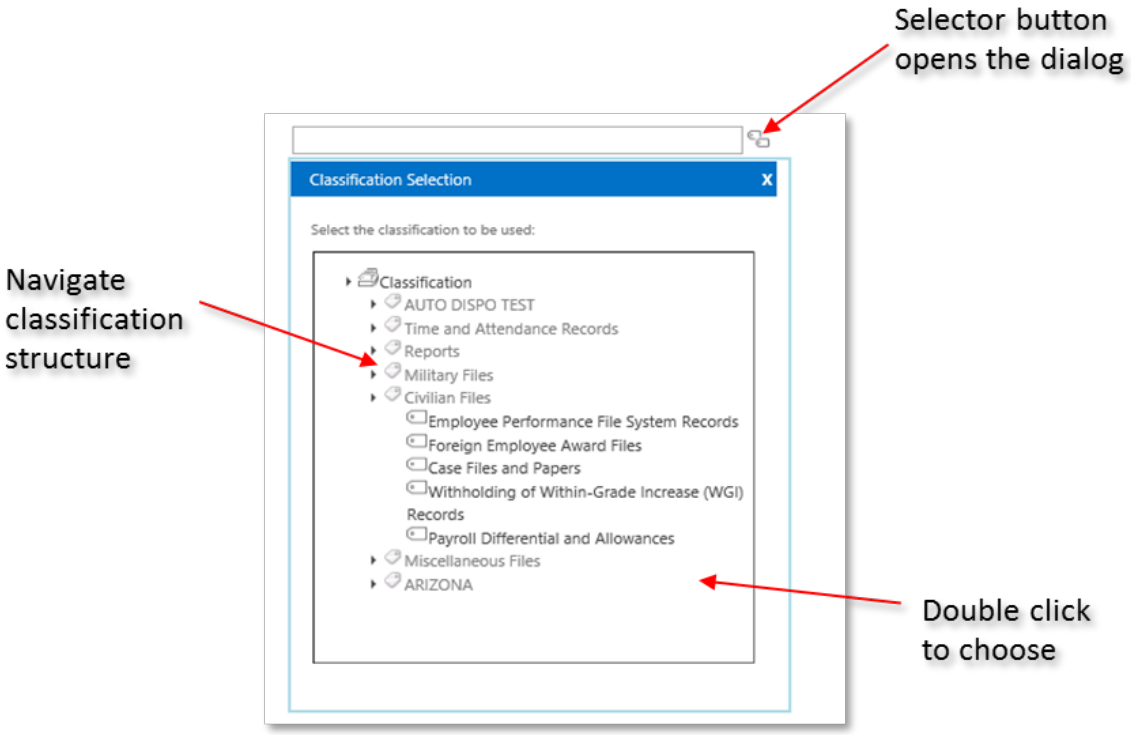
The first column, **Classifications (all)** is based on the Classification termset that is created by the termset creation tool. This column allows the user to select the classification from the termset.



This column will always show all classifications to the user regardless of their permissions in Content Manager. It may be possible for them to select a classification they are not entitled to use which will cause a failure during management.

This column is useable through the Microsoft Office suite of products also.

The second classification column, **Classifications**, provides a select button to the right of the control that displays a search and selection dialog that can be used for choosing the relevant classification.



This control, unlike the termset based one, only shows the user classifications they are permitted to use in Content Manager. It cannot be used in the Microsoft Office suite of products.

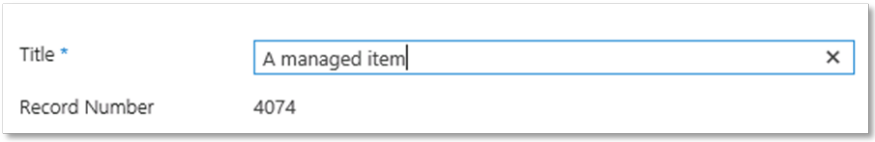
7.3.4 Security and access control columns

The Setting security and access control using SharePoint section of this document describes four columns that are created by the column creation tool for the purposes of viewing and modifying security and access control attributes.

7.3.5 Read only columns

Some Content Manager metadata is not editable and is designed to be displayed in a read only format. Read only columns will be displayed in a read only format on all forms included the **new** and **edit** forms for a list item.

For example, the **Record Number** column is shown as read only as this value is not editable.

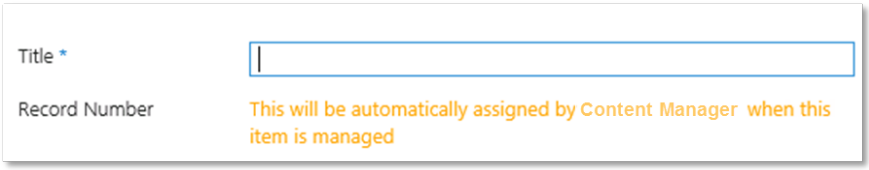


Examples of columns that use the read only behavior are:

- Record number
- Disposition schedule
- Document size

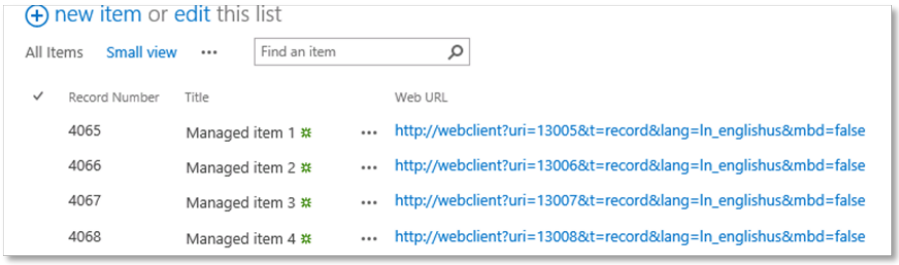
- Document status
- Mime type

Record number is a special case of read only column. Until the item is managed, the value of the record number column will display as follows:



7.3.6 URL based columns

Columns that contain URLs are displayed as read only hyperlinks. For example, the **Web URL** column will display a URL to the web client showing the record.



8 Configuring Content Type to Record Type Mapping

8.1 Determining the Record Type of Managed SharePoint content

To create a record in Content Manager requires selecting a record type to use. The record type is used to determine a number of key attributes of a record including (but not limited to):

- The metadata supported by the record
- Default values for metadata
- Which metadata is mandatory
- The record numbering pattern
- Default access controls

A record type can be thought of as a ***blueprint*** for a record. It is in many ways equivalent to the concept of a content type in SharePoint. As such, the determination of the record type to use is based on the content type of the items being managed at the time.

The ability is provided to indicate which record type to use based on the content type of the item. This is known as the ***Content Type to Record Type*** mapping (CT2RT). This mapping is administered using the **Content Types to Record Type Mapping** page.

8.1.1 Content Types to Record Type (CT2RT) Mapping page

Accessing the page

From the app start page, click the **Content Types to Record Type Mapping** link in the **Content mapping** section.

> **NOTE:** You must have **manage site** permission to access this page.

This will take you to the CT2RT page.

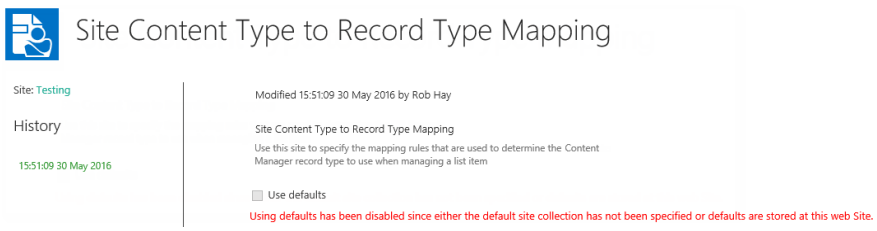
Using defaults

Following the page description is the **Use defaults** check box.

Checking this option indicates that this site should use the CT2RT mapping that is specified for the default site collection.

If this option is checked, it is not possible to modify the CT2RT mapping. The values specified in the CT2RT mapping of the default site collection will be displayed as read only on the page.

If the CT2RT being modified is that of the default site collection, this check box will be disabled.



Adding a mapping

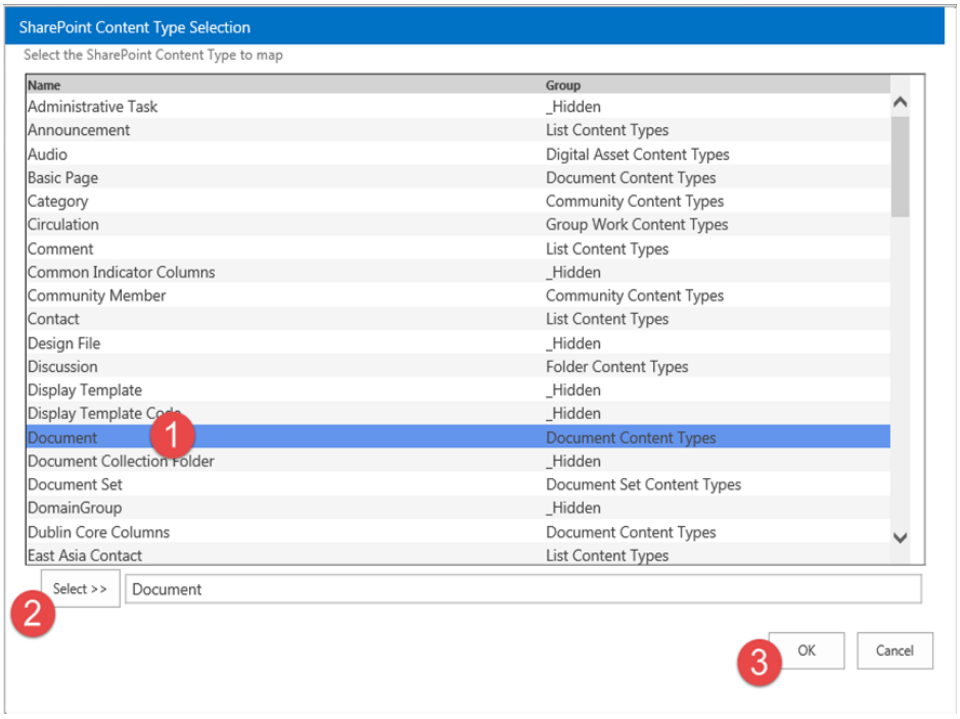
Adding a mapping involves choosing a content type then specifying the record type to use. To add a mapping, click the **Add** link.

A blank mapping is created.

Choose the content type for mapping. Click the icon next to the **Site Content Type** control.

The **SharePoint Content Type Selection** dialog is displayed with the list of all content types that belong to this site. This means that if you are currently on a site that is not at the top level of the site collection, you will not see any content types that have been created at site collection level.

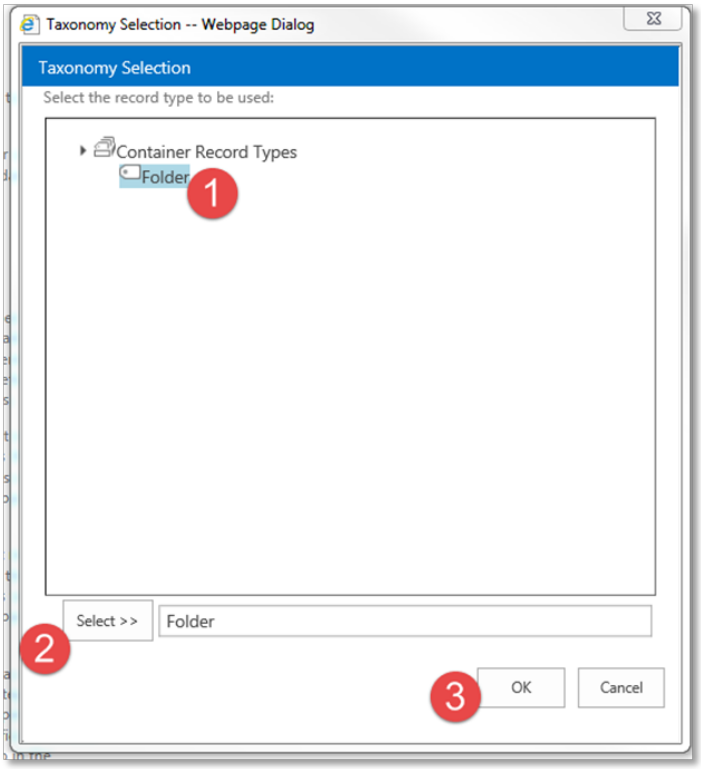
To select a content type, select the content type from the list, click **Select** and then click **OK**.



Once the content type has been selected, the Content Manager Record Type must be selected to complete the mapping. Click the icon next to the **Content Manager Record Type** control.

The **Taxonomy Selection** dialog is displayed with the list of suitable record types for mapping. If the selected content type inherits from the **Document** content type, then only record types that are marked as suitable for SharePoint documents.

To choose the record type either double click the required record type or select the record type then click **Select**.



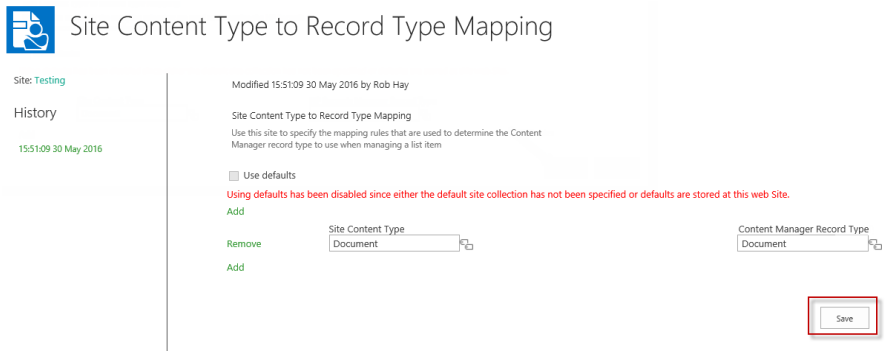
For details regarding record type requirements, see the **Prepare record types** section in the *Content Manager Governance and Compliance SharePoint App: Installations Guide*.

> **NOTE:** Only record types that existed prior to creating term sets or a term set maintenance job running will be available for selection. See the installation guide for details of synchronizing Content Manager record types.

Once the mapping is completed, it is possible to add additional mappings by repeating this process.

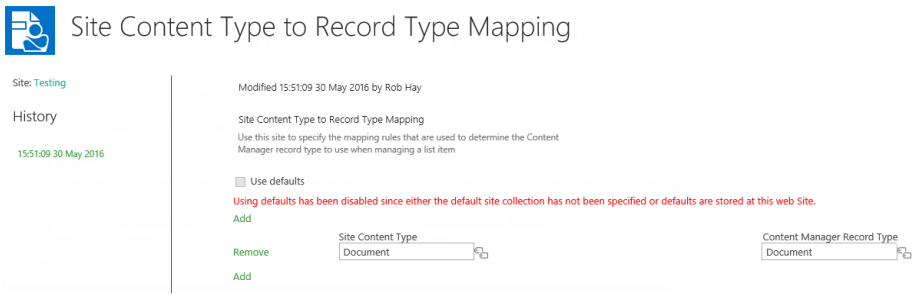
Saving the mapping

Once all mappings have been entered, to save the mapping, click **OK**.



Removing a mapping

If a mapping is no longer required, it can be removed using the Remove link next to the desired mapping.



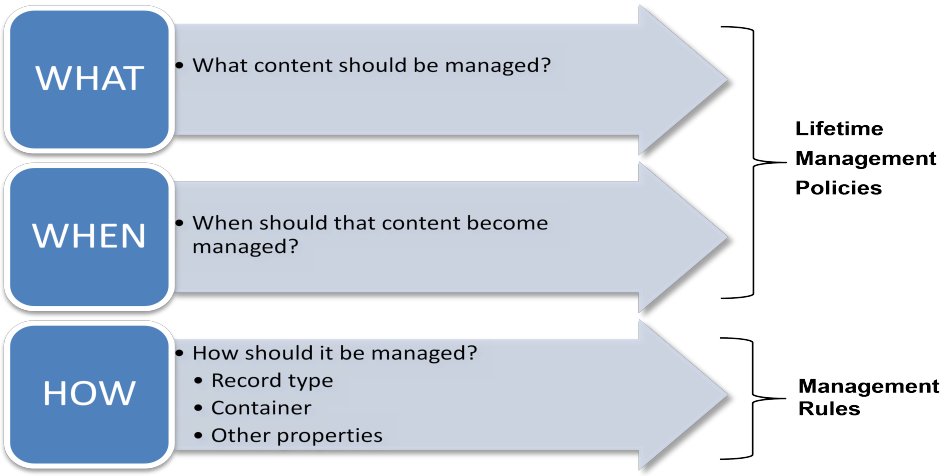
9 Manage Content Using Rules

There are often scenarios where you want to explicitly specify how a record is created in Content Manager. These requirements are specific to your organization and often vary significantly depending on the type of content that is being managed.

Management Rules, ***Management Instructions*** and ***Management Selectors*** allow you to implement very specific criteria that describe how a record is captured, regardless of where it resides in SharePoint. This provides a much more granular way of managing content in SharePoint, and are complementary to the existing RMOs.

All three are defined in site collection galleries, from the app-start page, and once configured can be re-used. Configuring on the defined default Site Collection means rules can be defined once and applied across many site collections.

Combining management rules with lifetime management policies gives you complete control over your SharePoint content:



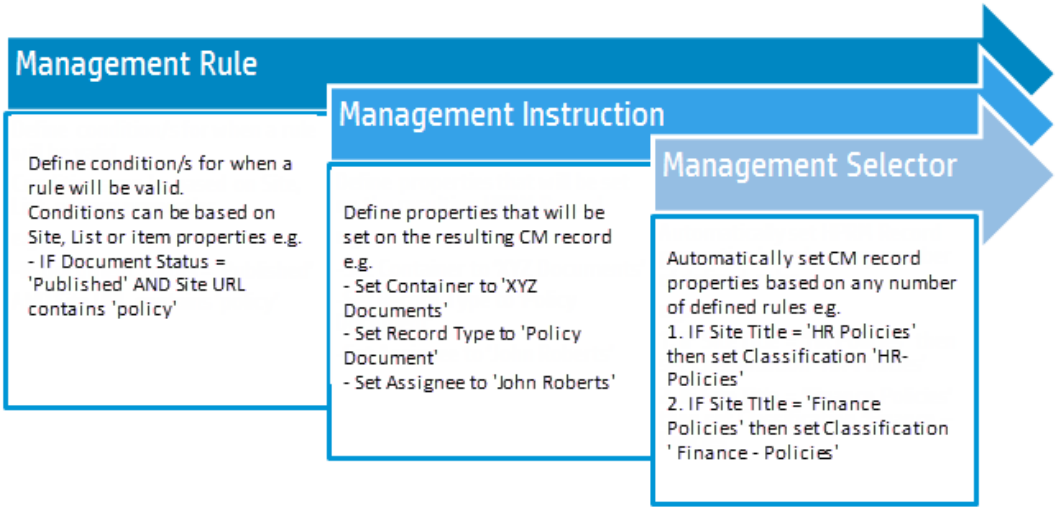
We have deliberately kept the' What' and 'When' separate from the 'How'. This gives maximum flexibility, without having to define 1000's of rules to cover every eventuality.

9.1 Overview of management rules

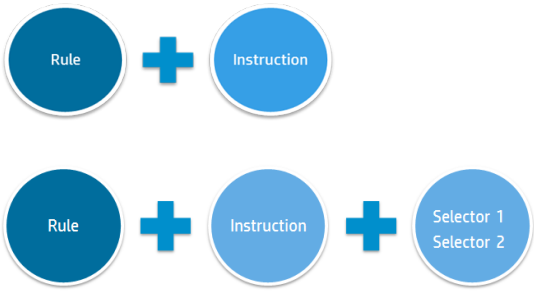
The overview section talked about three things that make up management rules as a whole:

- Management Rules (MR)
- Management Instructions (MI)
- Management Selectors (MS)

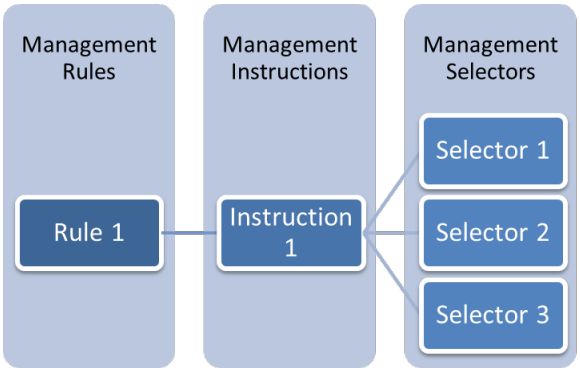
These three management components are interlinked.



A rule must include an instruction, and instructions can optionally use selectors. So valid rule sets include:



The best way to think about the three components working together is as a hierarchy. A rule has a linked instruction, and instructions can have one to many selectors linked to them. So, a complete ***Management Rule*** set might look like this:

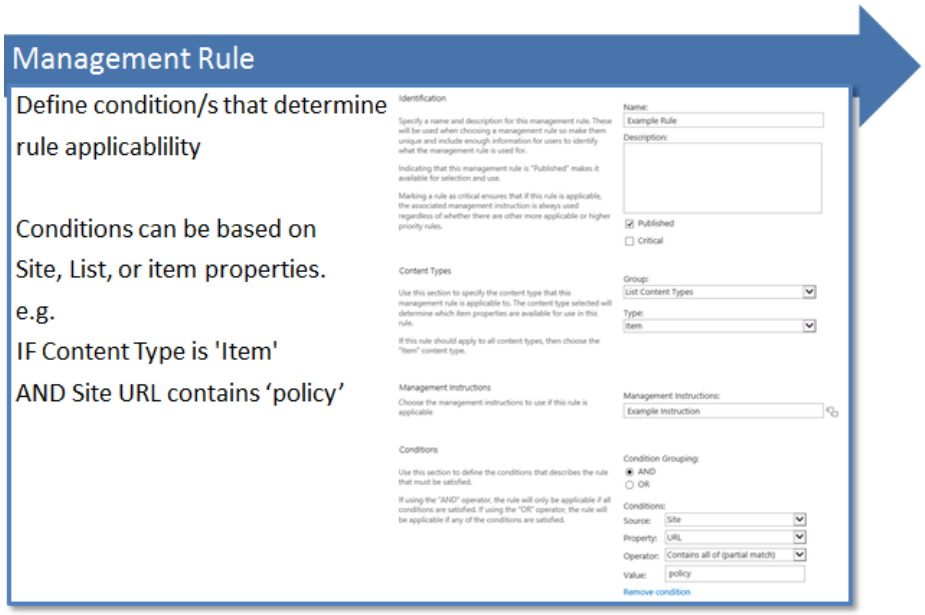


Instructions can be used by multiple rules and selectors can be reused by many instructions.

9.1.1 Management Rules

A management rule defines a set of conditions that must be met. When these conditions are satisfied, the rule is said to be ***applicable***. When a rule is applicable, the instruction associated with

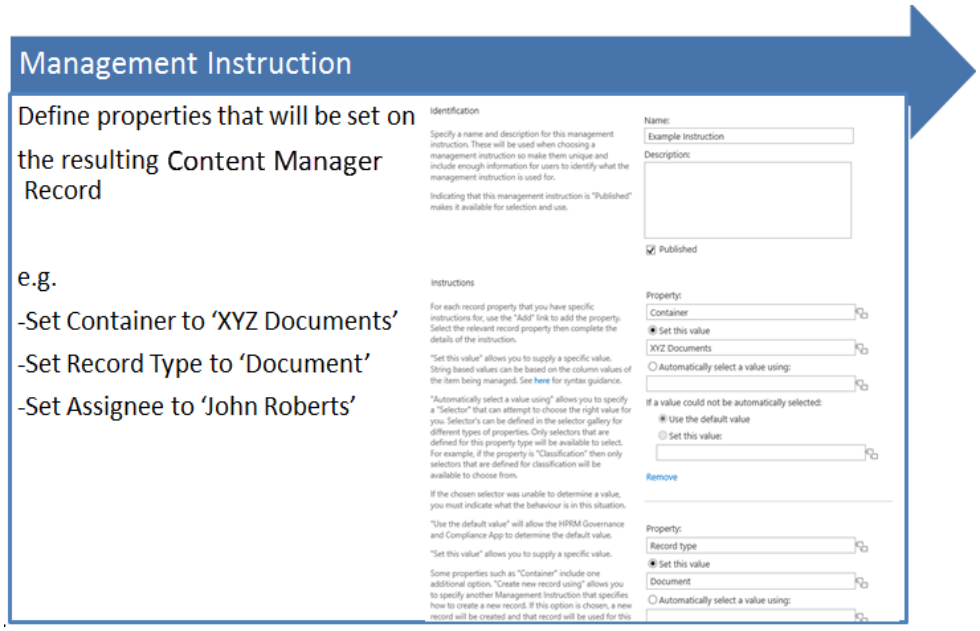
the rule is used.



See following examples for different use cases and the associated rules used to address them.

9.1.2 Management Instructions

A management instruction is used to set specific properties on the record created in Content Manager. Properties can optionally use a selector to provide automatic, rules-based selection of records. Multiple management rules can re-use the same instruction.

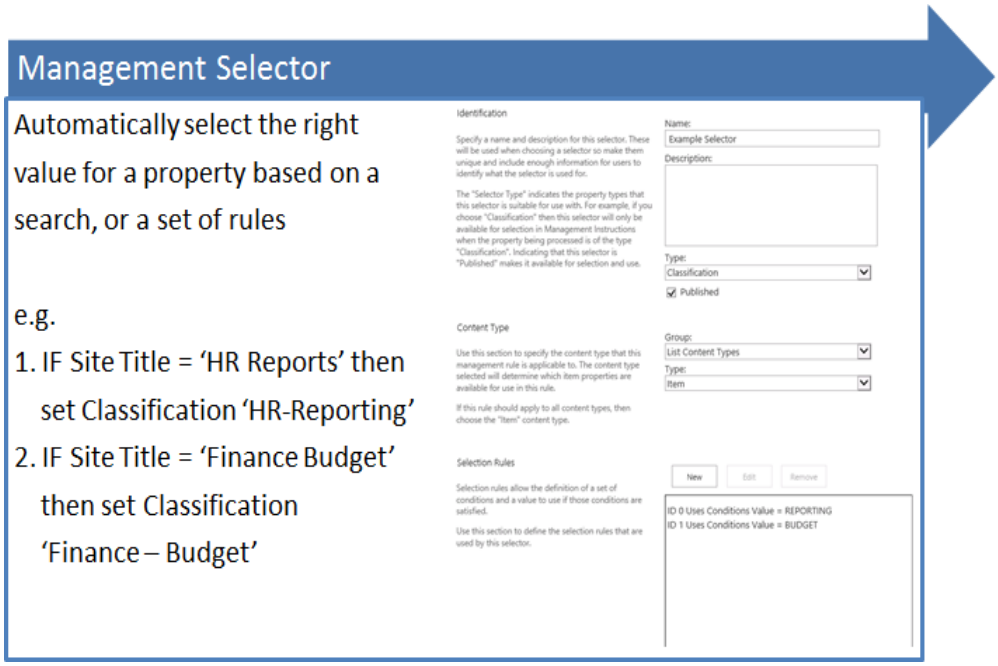


Instructions can also be used for the automatic creation of containers.

See the Examples section for a number of different use cases, and the associated rules used to address them.

9.1.3 Management Selectors

Management selectors allow the definition of criteria that are used to select the right object. For example, a selector could be created to select the correct container to use based on a combination of the site, list and item properties.



See the Examples section for a number of different use cases, and the associated rules used to address them.

9.1.4 Examples

These examples are designed to give you an idea of what can be achieved using management rules. There are number of ways you can address specific requirements. Each example will include a business requirement, a plan to address it using management rules, and then details of each rule, instruction and selector used to address the requirement.

Example 1: Setting a specific title on a record

This first example uses a simple rule and instruction to set one property on the record in Content Manager.

Situation

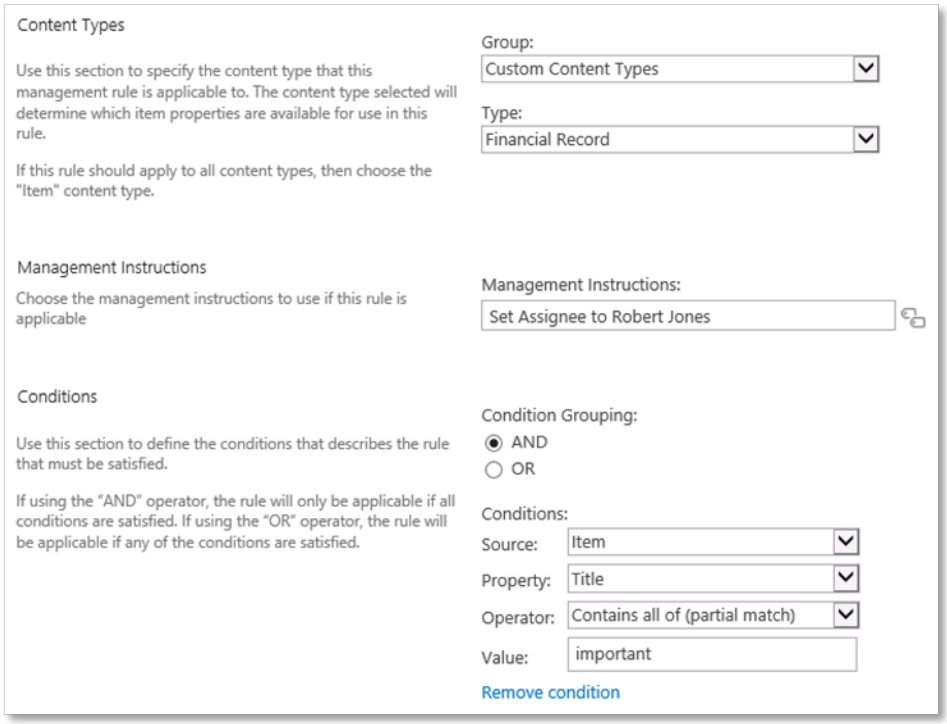
A document library contains a number of financial records. Financial records are identified in the library as they use the ***Financial Record*** content type.

This organization has a process of marking documents as important by including the word important in the title of the document. A financial document that is marked as important must always be reviewed by ***Robert Jones*** when they are captured as a record in Content Manager.

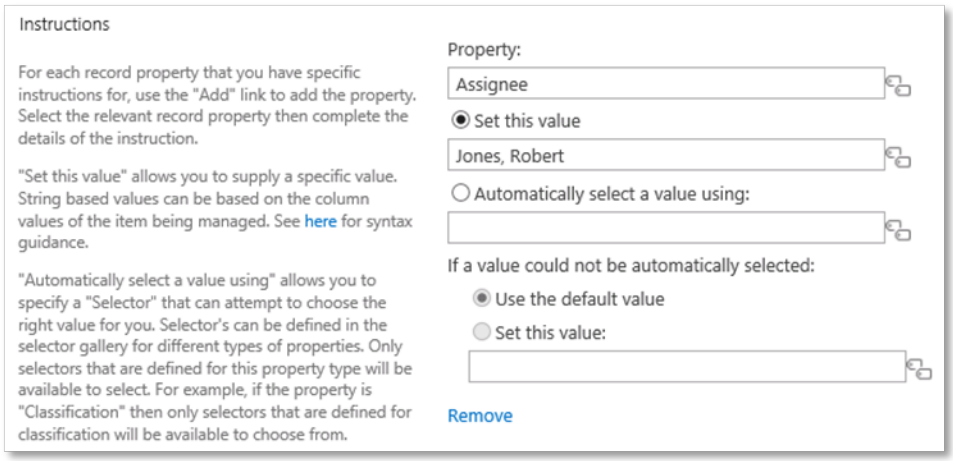
Implementation

A management rule is created to identify these important documents using the criteria:

- The content type of the item is “Financial Record”
- The title of the item includes the word “Important”



A management instruction is created to set the assignee of the record to “Robert Jones”. This instruction is set to be used by the management rule.



Example 2: Specifying a record type

Situation

A document library contains a number of financial records. Financial records are identified in the library as they use the ***Financial Record*** content type.

This organization requires that financial records are created in Content Manager using the “Finance” record type.

Implementation

A management rule is created to identify these financial records using the criteria:

- The content type of the item is “Financial Record”

A management instruction is created for use with this rule with the following instruction:

- Set the record type to “Finance”

> **NOTE:** Both the rules, this rule and the previous rule, can be applicable. If a document with a content type of Financial Record and a title that includes “important” in the title is managed, both rules will be considered applicable and the record will use the “Finance” record type and be assigned to Robert Jones.

See the Applying management rules section for how applicable rules are determined and applied.

Example 3: Using an existing container in Content Manager

This example uses a rule and instruction to place items in an existing Content Manager container when certain conditions are met.

Situation

A team is working on a project for a property inspection at ***123 Hindley St***. A document library on the project site stores a number of different types of project documents, all relating to the same project.

The document library includes a column called ***Document Type*** which allows users to select from a dropdown the type of document this is. The selectable values are:

- Project
- Financial
- Contract Management
- Correspondence

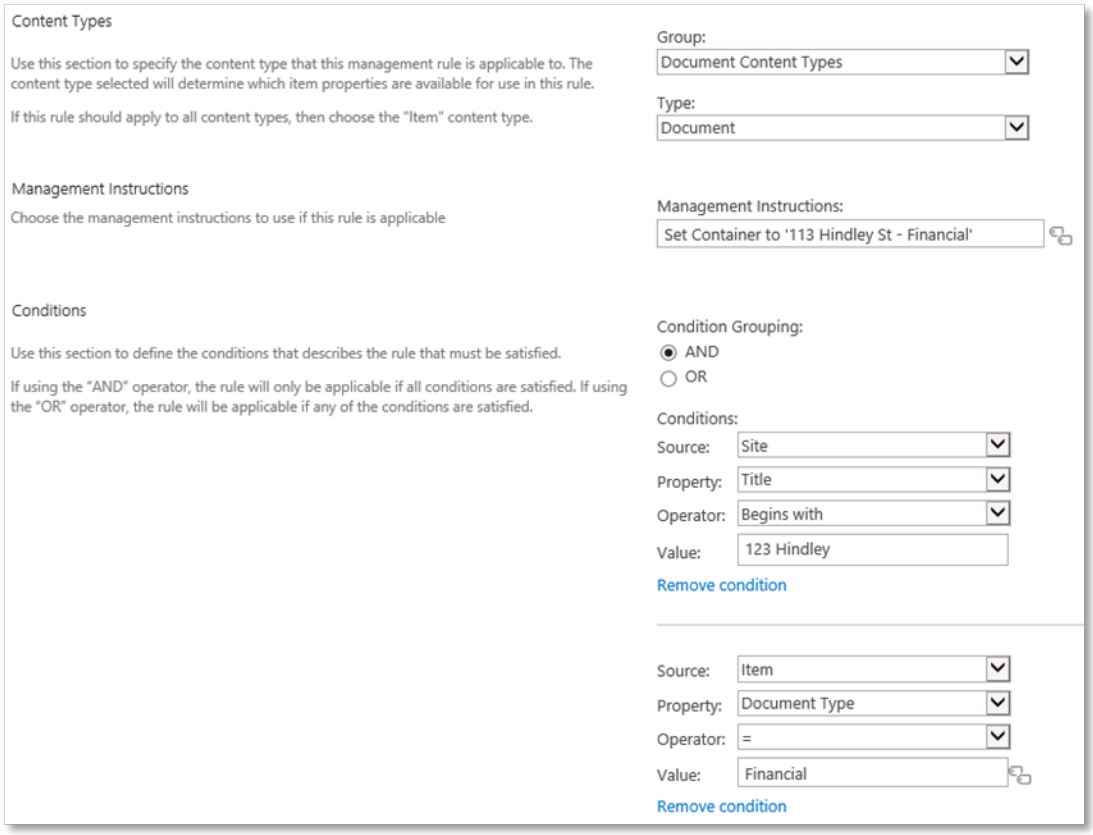
Most records for this project are stored in a project specific container in Content Manager but records marked as having a document type of “Finance” must be stored in a separate container in Content Manager called “Property Inspection Financial Records”.

This behavior should only apply to documents stored on this project site.

Implementation

A management rule is created to identify these financial records using the criteria:

- The content type of the item is “Document”
- The title of the site is “123 Hindley St”
- The document type property of the item being managed is “Finance”



A management instruction is created for use with this rule with the following instruction:

- Set the container to “Property Inspection Financial Records”

This is a very simple example of selecting the right container. See Example 5.

Example 4: Setting multiple properties on a record

Situation

Documents are created by staff in a document library. The document library supports multiple content types. Documents that use the “Finance” content type when managed must:

- Use the “Financial” record type for the record
- Be placed into the “Financial Records” container in Content Manager
- Be assigned to the location “Financial Controller”

Implementation

A management rule is created to identify these items using the criteria:

- The content type of the item is “Finance”

A management instruction is created for use with this rule with the following instruction:

- Set the record type to “Financial”
- Set the container to “Financial Records”

- Set the assignee to “Financial Controller”

Example 5: Using properties from SharePoint to search for a container

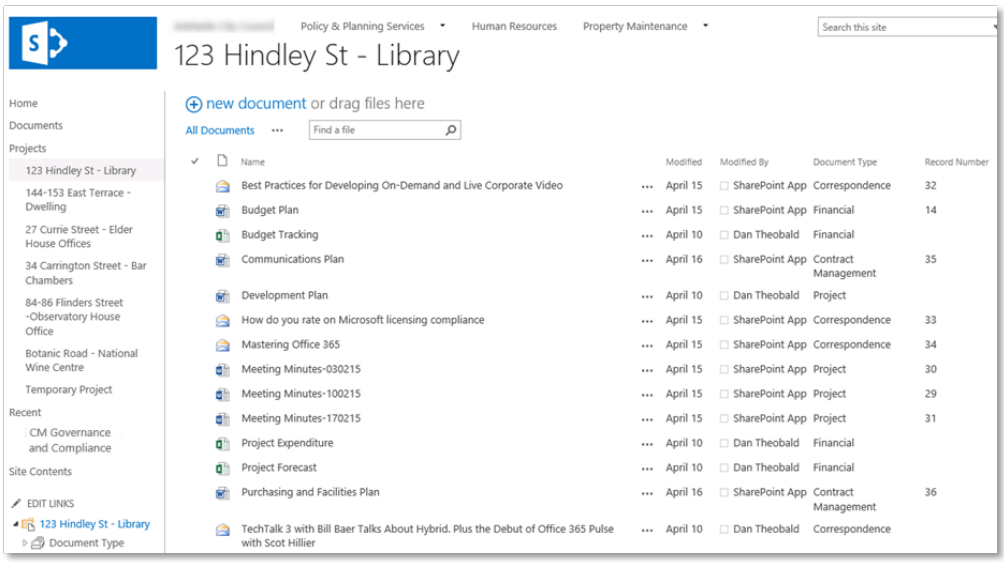
This example uses a rule, instruction and selector to place items in the appropriate Content Manager container when certain conditions are met. In particular this example shows how to use properties from SharePoint to search for content in Content Manager, using replacement syntax.

Situation

A team is working on a number of projects for property inspections at various addresses. For each project, a document library is created on the relevant project site. There are many project sites. The document library is used to store a number of different types of project documents but, all relating to the same project.

The document library includes a column called “Document Type” which allows users to select from a dropdown the type of document this is. The selectable values are:

- Project
- Financial
- Contract Management
- Correspondence



Different types of documents must be stored in different containers in Content Manager. These containers have already been created by the record manager and have a title that consists of the project name, the site name, and the type of document. They are in the format:

```
List Title – Site Title – Document Type
```

For example:

```
123 Hindley St – Strategic Planning - Financial
```

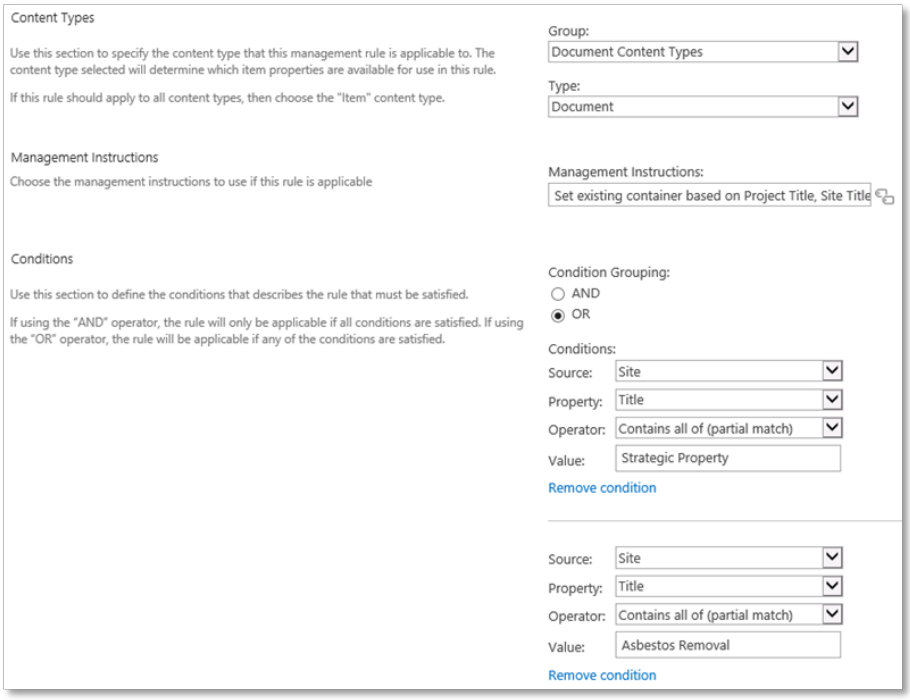
At this time, although they have many project sites, the organization only wants this behavior to apply to documents stored on the following project sites:

- Strategic Planning
- Asbestos removal

Implementation

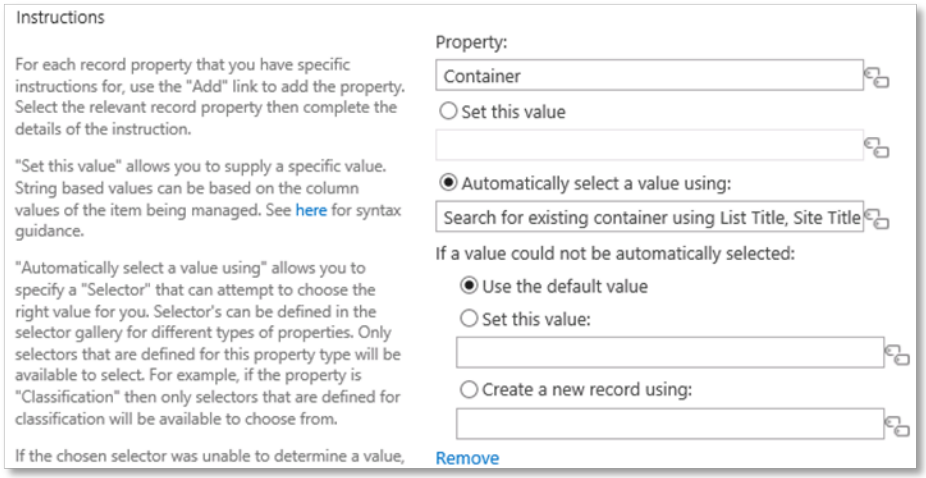
A management rule is created to identify these items using the criteria:

- The content type of the item is “Document”
- The title of the site is either
  - Strategic Planning
  - Asbestos removal



A management instruction is created for use with this rule with the following instruction:

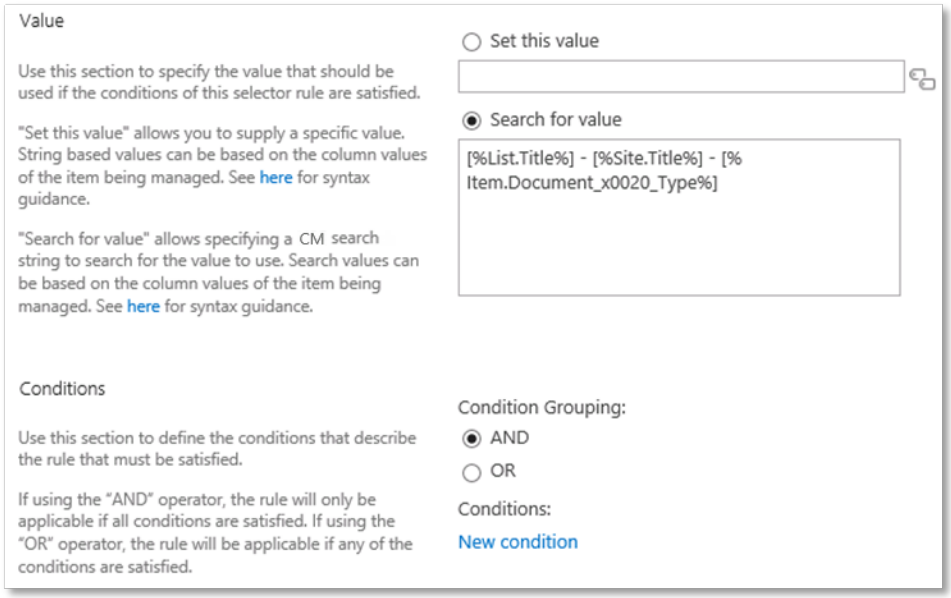
- Use a selector to identify the correct container to use



A selector is created for use with this instruction to identify the correct container to use. It is a search based selector searching Content Manager for a container that has a title based on the syntax:

```
List Title – Site Title – Document Type
```

Selectors allow the use of list, site and item properties in the search term. During search, these values are replaced with the value of the site, list and item being managed.



In this scenario, if the following are true:

- List title = 123 Hindley St
- Site title = Asbestos Removal
- Document type = Correspondence

At the time of management, the selector in will look for a container with the following title:

```
123 Hindley St – Asbestos Removal – Correspondence
```

Using selectors to locate containers allows the identification of the correct container based on the attributes of the item being managed at the time.

Example 6: Creating a new container with automatically generated title and specified retention schedule

This example demonstrates how management rules can be used to generate containers on demand. It also demonstrates the use of SharePoint item properties in the generation of text fields, in this example, the title of the created container.

Situation

The finance department receives invoices into a document library on their site. These invoices come from various sources. Invoices use the “Invoice” content type in SharePoint therefore they can be identified as invoices simply by determining the content type.

The document library includes a field “Invoice Date” that contains the date that the invoice was issued.

When invoices are put in to Content Manager, the finance department requires that there is a container for each month of invoices. These containers are named based on the month and year of the invoices that they hold. For example:

```
Invoices March 2015
```

Invoice containers in this organization are assigned the retention schedule “Financial Documents”

The finance department wants these containers to be created automatically as they are required so that they don’t have to remember to do it.

Implementation

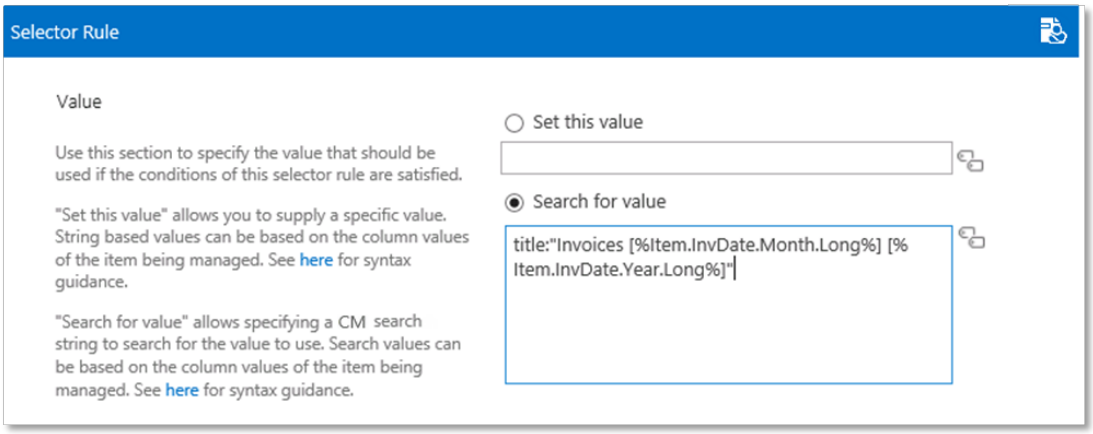
A management rule is created to identify these items using the criteria:

- The content type of the item is “Invoice”

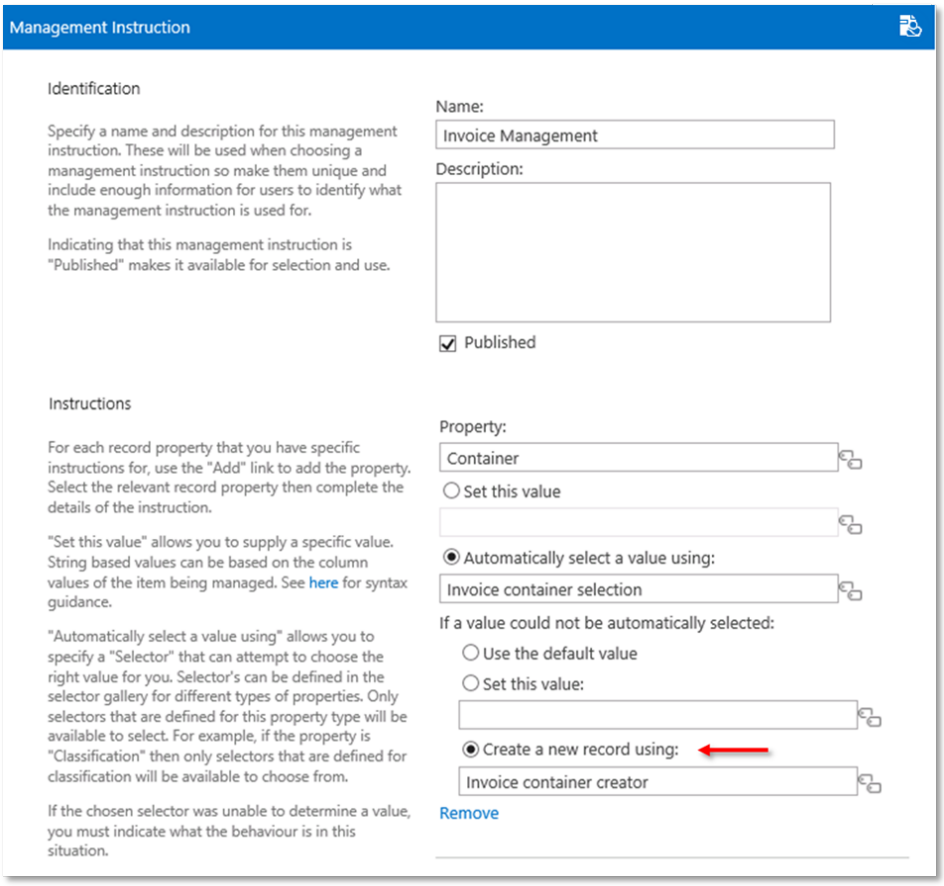
A management instruction is created for use with this rule with the following instruction:

- Search for the container to use based on the month and year of the invoice (using a selector)
- If the container is not found, create the container

The selector searching for the right container looks for a container with the title based on the long version of the invoice date and the long version of the invoice year.

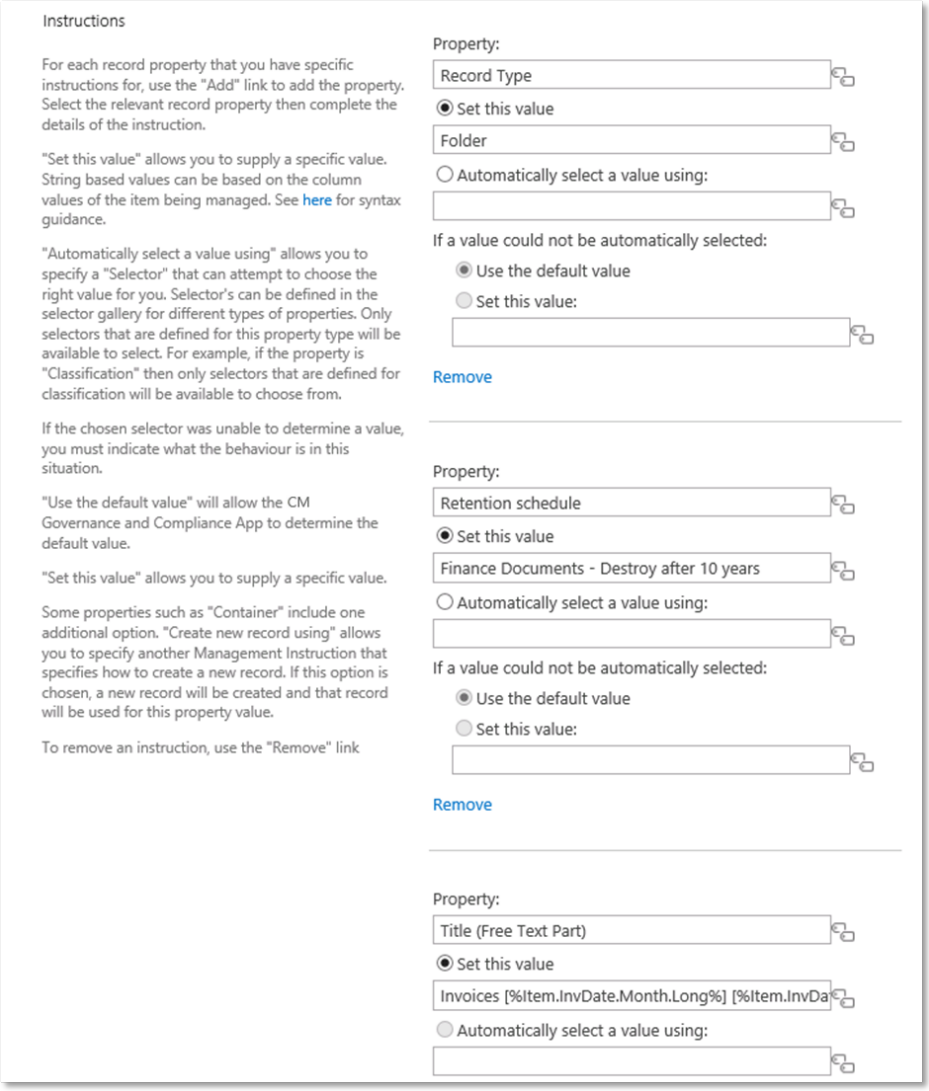


In the case of instructions that set records, an additional option is shown allowing the creation of a new record to use. The instructions for creating this new record are just another management instruction.



The instruction in this example has the following instructions:

- Set the record type to “Folder”
- Set the retention schedule to “Finance Documents”
- Set the title of the container to be based on the long month of the invoice date and the long year of the invoice date



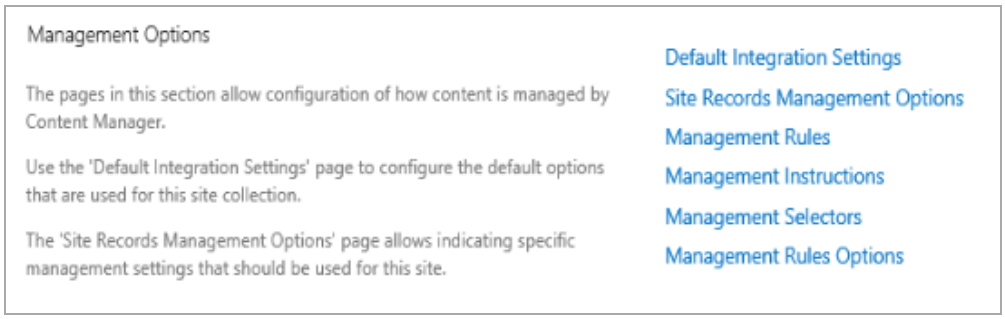
Consider when the first invoice for May 2015 is managed. The instruction associated with the management rule will search for a container called “Invoices May 2015” but will not find it as the container has not yet been created.

The instruction will be called to create the “Invoices May 2015” container. This newly created container will be used as the container for the invoice record.

When a subsequent invoice for May 2015 is managed, the instruction associated with the management rule will search for a container called “Invoices May 2015” and will find it (as it was created when the first item was managed). This container will be used as the container for the invoice record.

9.2 Content Manager Management Options

You can access the **Management Rule**, **Management Instructions**, and **Management Selectors** from **Management Options** section of the Content Manager app start page.



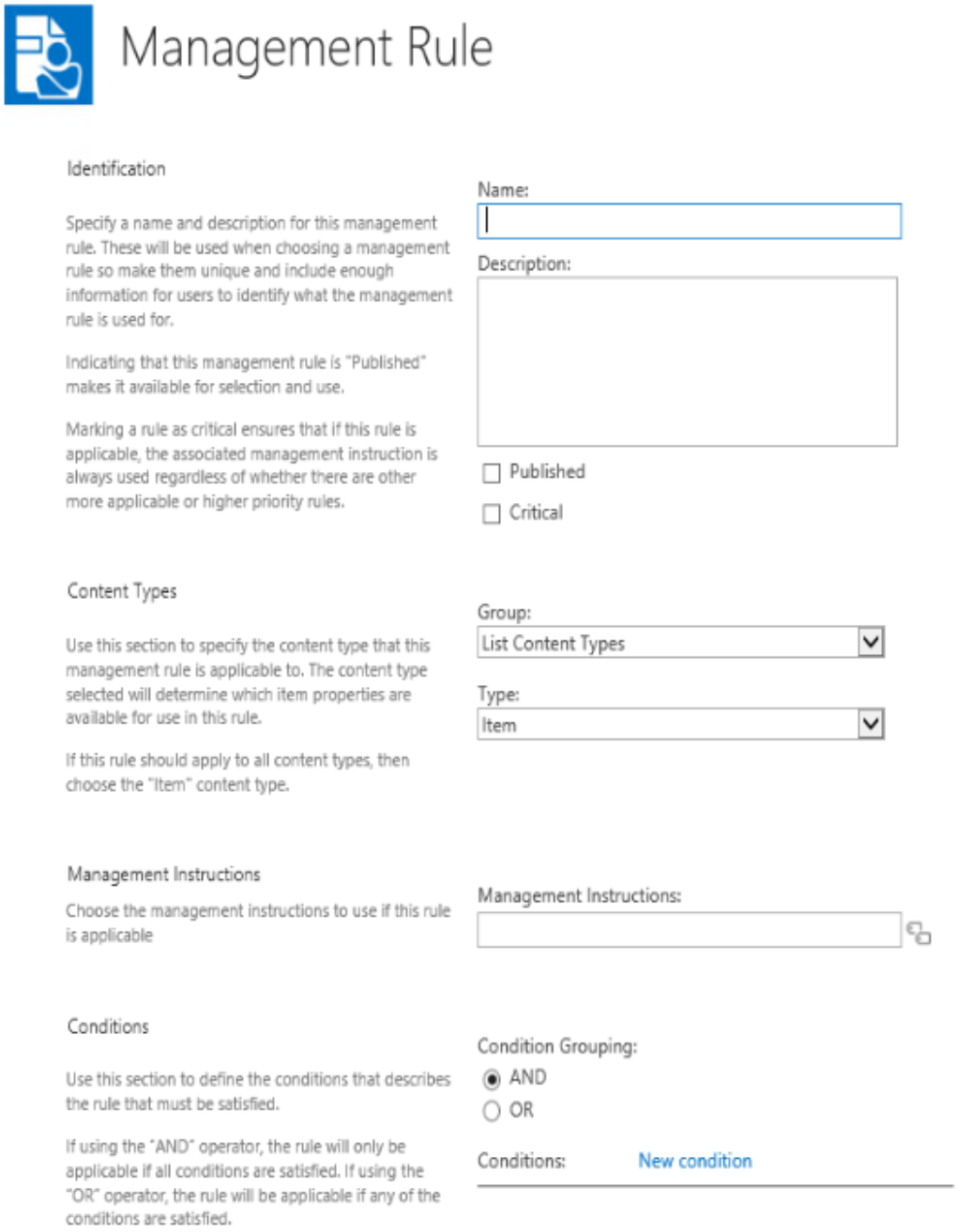
> You must be a site collection administrator to access these pages.

9.2.1 Creating and editing management rules

Management rules are specified for the site collection. Regardless of what site you access the app start page from, you will always be taken to the management rules gallery for the site collection.

9.2.1.1 Creating a new management rule

From the **Management Rules** page, click **Create New**. The **Management Rule** window is displayed.



Identification

The **Identification** section of the page is used to provide detail used to identify the management rule and indicate whether it can be used.

The **Name** of the rule is used for displaying the rule in the management gallery. It is important to provide a good name that will allow you to differentiate between rules in the gallery.

The **Description** of the rule is also displayed in the management rules gallery. Again, it is important to provide a good description that will allow you to identify and differentiate between rules in the gallery.

Marking a rule as **Published** makes the rule active. If a rule is not marked as published then it will be ignored during management. This allows you to design rules without them being used until you have completed the design.

Marking a rule as **Critical** affects the priority that is given to a rule. See the Applying management rules section for how this setting affects priority.

Content Types

The **Content Types** section of the page allows specifying the content type that this rule will apply to.

For a management rule to be considered during management of a SharePoint item, the item must use the content type specified here, or use a content type that inherits from this content type. Because content type inheritance is used, if you specify a content type of ***Item***, as this is the base content type for all others, the rule will be considered for all items.

Management Instructions

The **Management Instructions** section of the page allows you to specify the management instruction that must be used if this rule is found to be applicable during management.

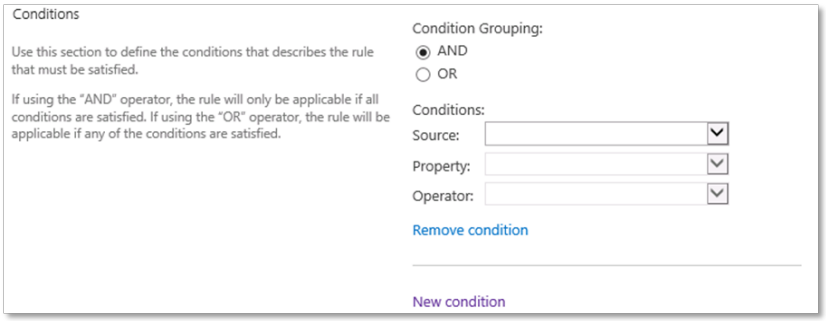
Click the icon to display **Select a Management Instruction** window. You can choose from existing management instructions or alternatively, click **Create** to create new Management Instruction.

Conditions

The conditions section allows the specification of the conditions that must be true for a management rule to be considered applicable.

Conditions can use either the AND or OR grouping. If AND is used, then all conditions that you specify must be true for the rule to be applicable. If OR is used, then if any one of the conditions is true, then the rule is considered to be applicable.

To create a condition, click the **New condition** link. This adds an empty condition to the page.



The **Source** dropdown allows you to choose the source of the property that will be used for the container. You can choose from:

- Site
- List
- Item

The properties that are available to select in the **Property** drop down will depend on the selection made in the source dropdown. Additionally, if you select Item as the source, the properties available will be based on the content type selected in the **Content Types** section.

The **Operator** dropdown provides the list of comparators that will be used against the selected property. The available operators will depend on the data type of the property that is selected.

Some operators require you to specify a ***Value*** to compare with. For example, if the condition includes a text field the operator may require entry of a value to compare with.

It is permissible to add multiple conditions. To add further conditions, click the **New condition** link. Continue adding the required number of conditions.

To remove a condition, click the **Remove Condition** link under the condition to be removed.

List specific properties

For properties of a list, there are some properties that require further clarification.

Template ID

The template ID allows specifying the list template that is in use. This allows assigning conditions that will only ever mature if the list is of a particular type. For reference, see Template ID

Custom templates

When you save a list as a template in SharePoint, the template ID is always the same, therefore it is impossible to differentiate custom templates based on the template ID. Instead, the ***Description*** of the list should be used.

Any syntax that suits your organization can be used to identify that a list is of a particular template. For example, the description of all announcements lists on the SharePoint farm might begin with:

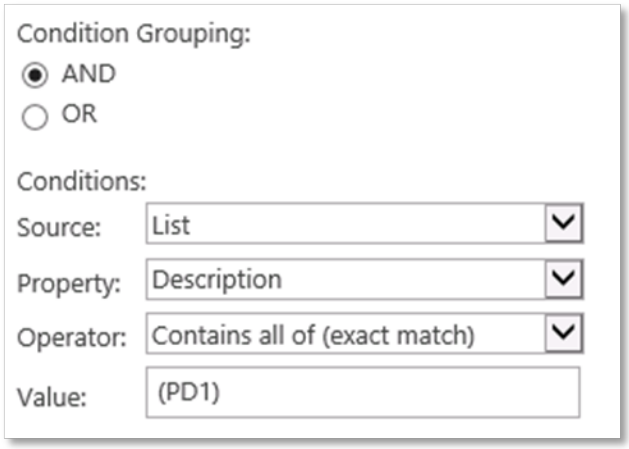
This list contains announcements about…

Unfortunately, description is not a property that is saved to list templates. Therefore, if using custom list templates, it will be necessary to ensure that the identifier is included in the description of each created list. When saving site templates however, description is included with the site lists and is therefore automatically added to new lists when a site of that template is created.

A management rule condition can then be defined identifying that if the description starts with this text, consider it to contain announcements.

Alternatively, it is possible to embed your own template identifier in the description. For a document library containing project documents, for example, use a custom identifier ***(PD1)***. The template could include in the standard description instructions to retain this identifier:

A management rule condition could search the list description for the value ***(PD1)***.



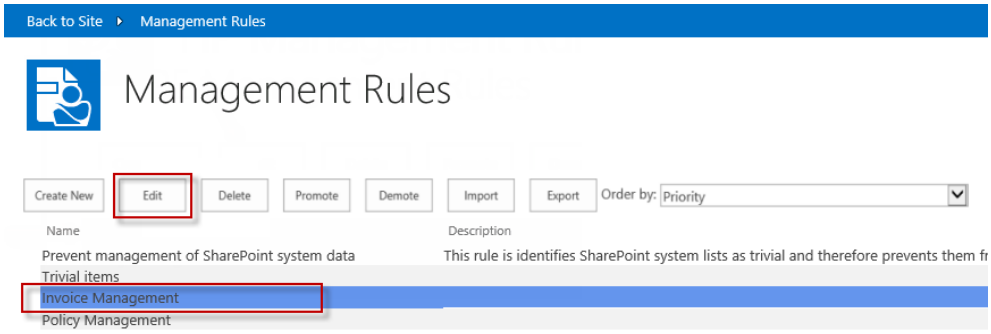
Saving the rule

Click **OK** to save the management rule. If the values entered are valid, the rule will save and will appear in the management rules gallery. If any data is invalid, a message will be displayed on the page identifying the issue.

Click **Cancel** to close the page without saving the management rule.

9.2.1.2 Editing an existing management rule

To edit an existing management rule, navigate to the management rules gallery, select the rule to be edited then click **Edit**.



9.2.1.3 Deleting a management rule

To delete an existing management rule, navigate to the management rules gallery, select the rule to be deleted then click **Delete**.

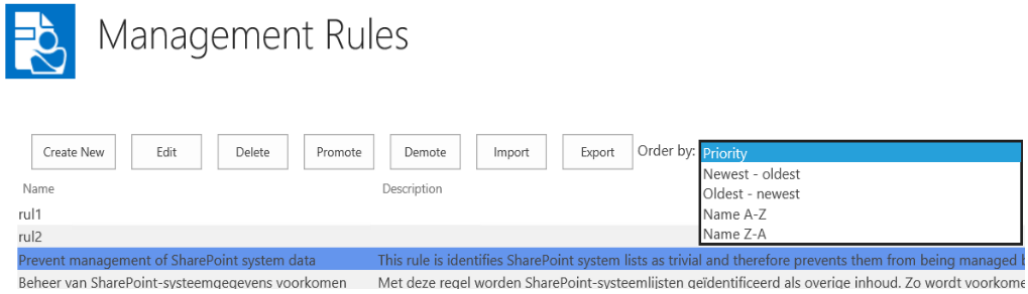
9.2.1.4 Ordering management rules

The management rules gallery allows ordering the view of management rules by:

- Priority
- Newest – oldest
- Oldest – newest

- Name A-Z
- Name Z-A

Select the order clause from the **Order by** dropdown on the management rules gallery.



9.2.1.5 Changing the management rule priority

When there are multiple applicable rules found during management, the priority of a rule can determine whether it is used in precedence to others. How priority is used is covered later in this chapter.

It is possible to change the priority of management rules using the management rules gallery.

Select the rule to change the priority on, then use the **Promote** or **Demote** buttons to increase or decrease the priority. The higher up the list that the rule is, the higher its priority.

> Priority can only be changed if the gallery is ordered by priority.

9.2.1.6 Importing and exporting management rules

Importing management rules

To import a management rule, perform the following:

1. Navigate to the management rules gallery and click **Import**.
2. Go to the location where you have saved the management rule, select the one you want to import and click **Open**.

   Once imported, a status message is displayed. The newly imported rule will be listed in the management rules gallery.

Exporting management rules

To export management rules, perform the following:

1. Navigate to the management rules gallery and click **Export**.
2. In the **Export Management Rule** dialog, select the rule(s) you want to export, and then click **Export**.

   The rule(s) will be exported as XML file with the file format as **SPI_Rules_<*Auto gen***

number>*.XML** where ***Auto gen number is the unique automatically generated number.

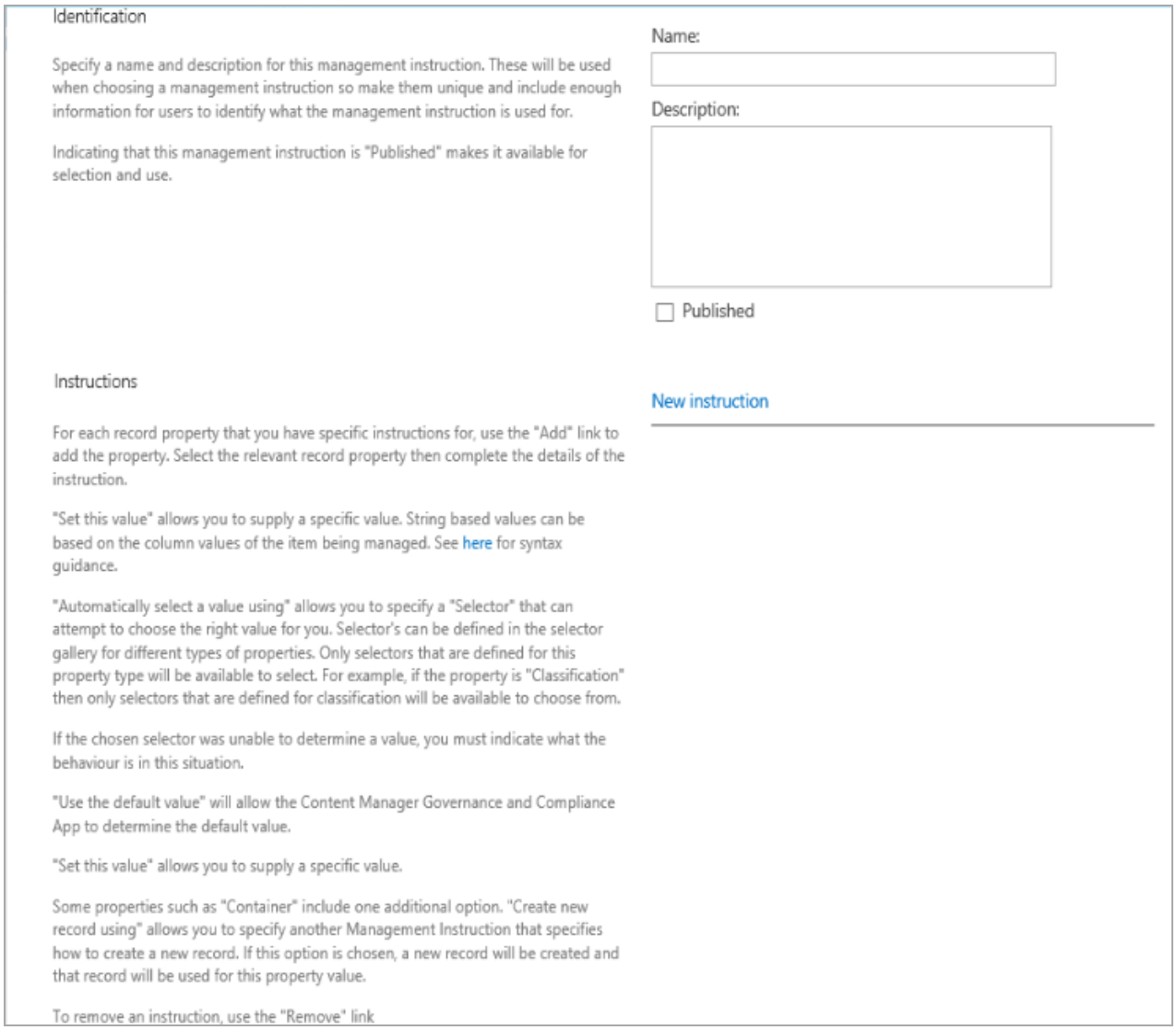
3. Click **Open** or **Save** to export the rule(s) to the desired location in your system.

9.2.2 Creating and editing management Instructions

Management instructions are specified for the site collection. Regardless of what site you access the app start page from, you will always be taken to the management instruction gallery for the site collection.

9.2.2.1 Creating a new management instruction

There are two ways to access the creation of management instructions. From the **Management Instruction Gallery**, click the **Create New** to open a pop up window.



Alternatively, from the **Management Rule** page when selecting the instruction to use, the **Select a Management Instruction** dialog includes a **Create** button that can be used to access the creation page. For more details, see Management Instruction.

Identification

The **Identification** section of the page is used to provide detail used to identify the management instruction and indicate whether it can be used.

The **Name** of the instruction is used for displaying the instruction in the management instructions gallery. It is important to provide a good name that will allow you to differentiate between instructions in the gallery.

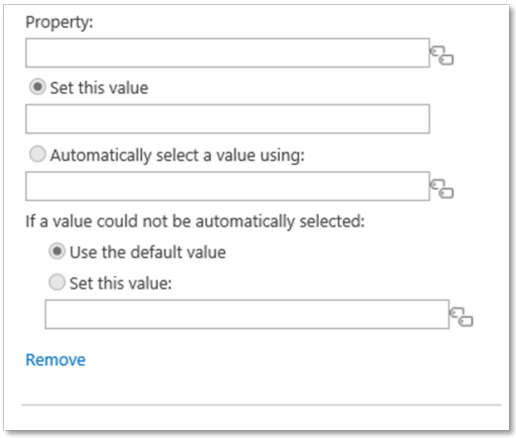
The **Description** of the instruction is also displayed in the management instructions gallery. Again, it is important to provide a good description that will allow you to identify and differentiate between instructions in the gallery.

Marking an instruction as **Published** makes the instruction available for selection in rules. If an instruction is not marked as published then it will not be available to be selected for management rules. This allows you to design instructions without them being used until you have completed the design.

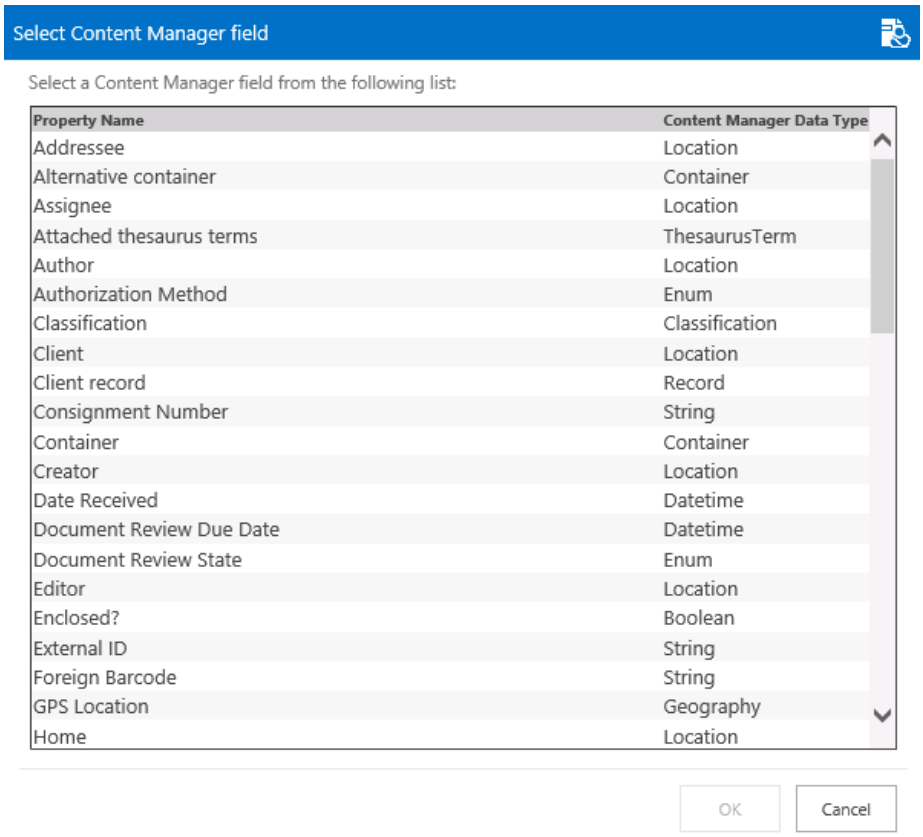
Instructions

The ***Instructions*** section of the page is where you define the record properties and the values to use during management. For a new instruction, the list of instructions is empty. To create a new instruction, click the **New instruction** link.

An empty instruction is added to the page.



Start by selecting the Content Manager ***Property*** that the instruction will set. This will display a dialog that contains the list of all Content Manager properties that are available to be set by instructions.



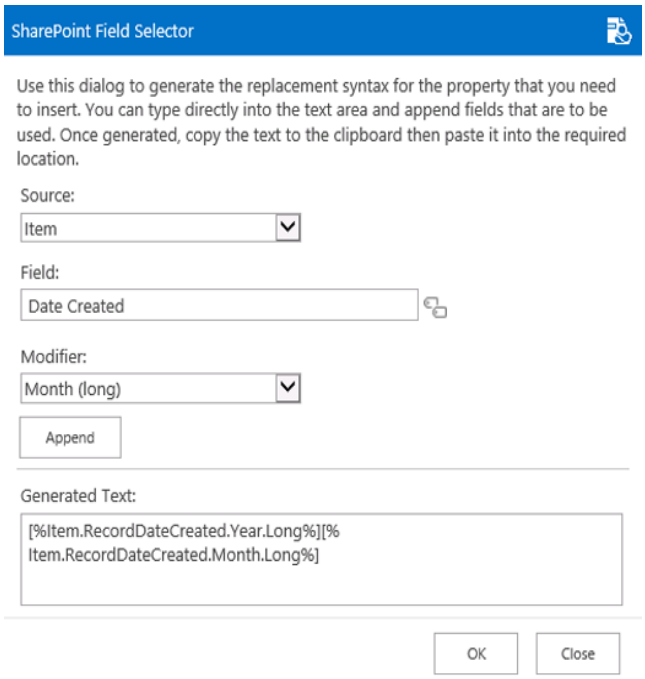
Once a property has been selected, the value selection options are enabled.

Use ***Set this value*** to select a specific value to set. Clicking the selection button next to the text box will show the appropriate dialog for selecting a value. For example, if the selected property is Classification then the dialog will allow selection of a Content Manager classification.

Text based properties

If the property is a text based property, you can enter a value directly into the text box. Text based properties allow you to use substitution syntax so that during management, the value is replaced with the value of a property of a site, list or the item itself.

The description of the instruction section includes a link to display the supported replacement syntax. Alternatively, clicking the selection button next to the text box will show a dialog that allows you to construct the full value of the text.



For properties that are of the following type, the **Automatically select a value using** option is available:

- Classification
- Location
- Record
- Container
- Record type
- Retention schedule
- Security caveat
- Security level
- Thesaurus term
- Jurisdiction

Selecting this option allows you to select a management selector that will attempt to choose the correct value.

When using this option, you must specify what value to use if the selector was unable to determine a value to use. The option **Use the default value** indicates to use the value that the app and/or Content Manager determines as the default. This is the value that would have been set for this property if you did not have an instruction.

The option **Set this value** allows selecting a specific value to set if the selector cannot determine a value. For example, if the selector attempted to choose a classification but could not find one, you

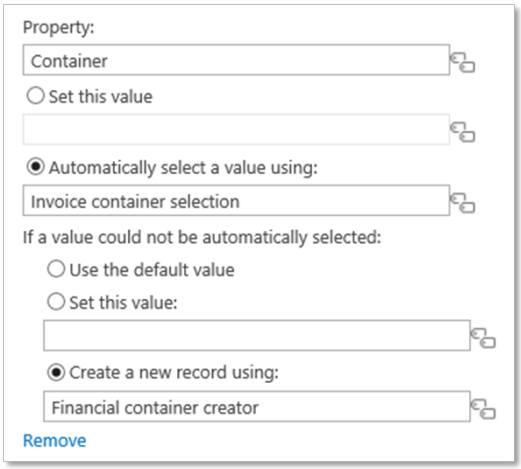
could specify a default classification that you monitor looking for records that need manual classification.

Multiple instructions can be added. Click the **New instruction** link to add additional instructions.

To remove an instruction, click the ***Remove*** link under the instruction to be removed.

Record based properties

If the property selected in the instruction is a record (for example Container) then an additional option is included in the instruction.



The **Create a new record using** option allows you to specify that when a selector cannot find a record, that a new one should be created and used. Select the management instruction that should be used to create this record.

When using this option, be sure that the management instruction used to create the record provides at a minimum the following:

- The record type to use
- The title of the record

Without this minimum information, the record will not be successfully created.

Thesaurus based properties

When selecting a term that is based on a Thesaurus value, a dialog permits the selection of the thesaurus value to use. There is a known issue with specifying a thesaurus value that is a child of a node label. Although you will be permitted to select it, during management an error will occur.

```
Error while saving mapped properties. Details of the problem are: 'Term1' must be a
narrower thesaurus term of 'TopTerm' for this titling method.
```

This reflects that if using ***Thesaurus Term – ISO*** as the title method on a record type, that the hierarchy cannot contain any labels. If you experience this issue, you will need to correct the thesaurus terms used in your organization.

Saving the instruction

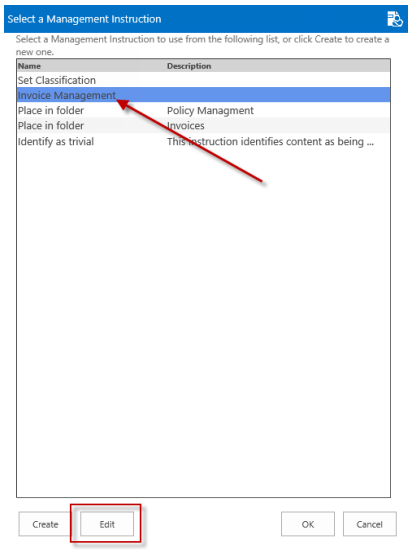
Click **OK** to save the management instruction. If the values entered are valid, the rule will save and will appear in the management instructions gallery. If any data is invalid, a message will be displayed on the page identifying the issue.

Click **Cancel** to close the page without saving the management instruction.

9.2.2.2 Editing an existing management instruction

There are two ways to access the editing of existing management instructions. From the management instruction gallery, select the instruction to be edited then click the ***Edit*** button to open the management instruction dialog.

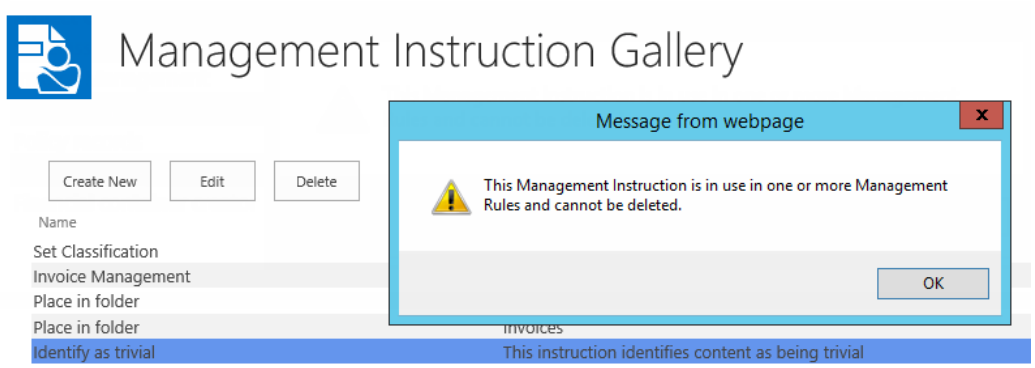
Alternatively, from the management rule page when selecting the instruction to use, the selection dialog includes an **Edit** button that can be used to edit the selected management instruction.



9.2.2.3 Deleting a management instruction

To delete an existing management instruction, navigate to the management instructions gallery, select the instruction to be deleted then click then **Delete** button.

If the instruction is in use by a management rule, the delete will be prevented. You must first remove the instruction from all management rules before you will be permitted to delete it.



9.2.2.4 Importing and exporting management instructions

Importing management instructions

To import a management instruction, perform the following:

1. Navigate to the management instructions gallery and click **Import**.
2. Go to the location where you have saved the management instruction, select the one you want to import and click **Open**.

   Once imported, a status message is displayed. The newly imported instruction will be listed in the management instructions gallery.

Exporting management instructions

To export management instruction, perform the following:

1. Navigate to the management instructions gallery and click **Export**.
2. In the **Export Management Instructions** dialog, select the instruction(s) you want to export, and then click **Export**.

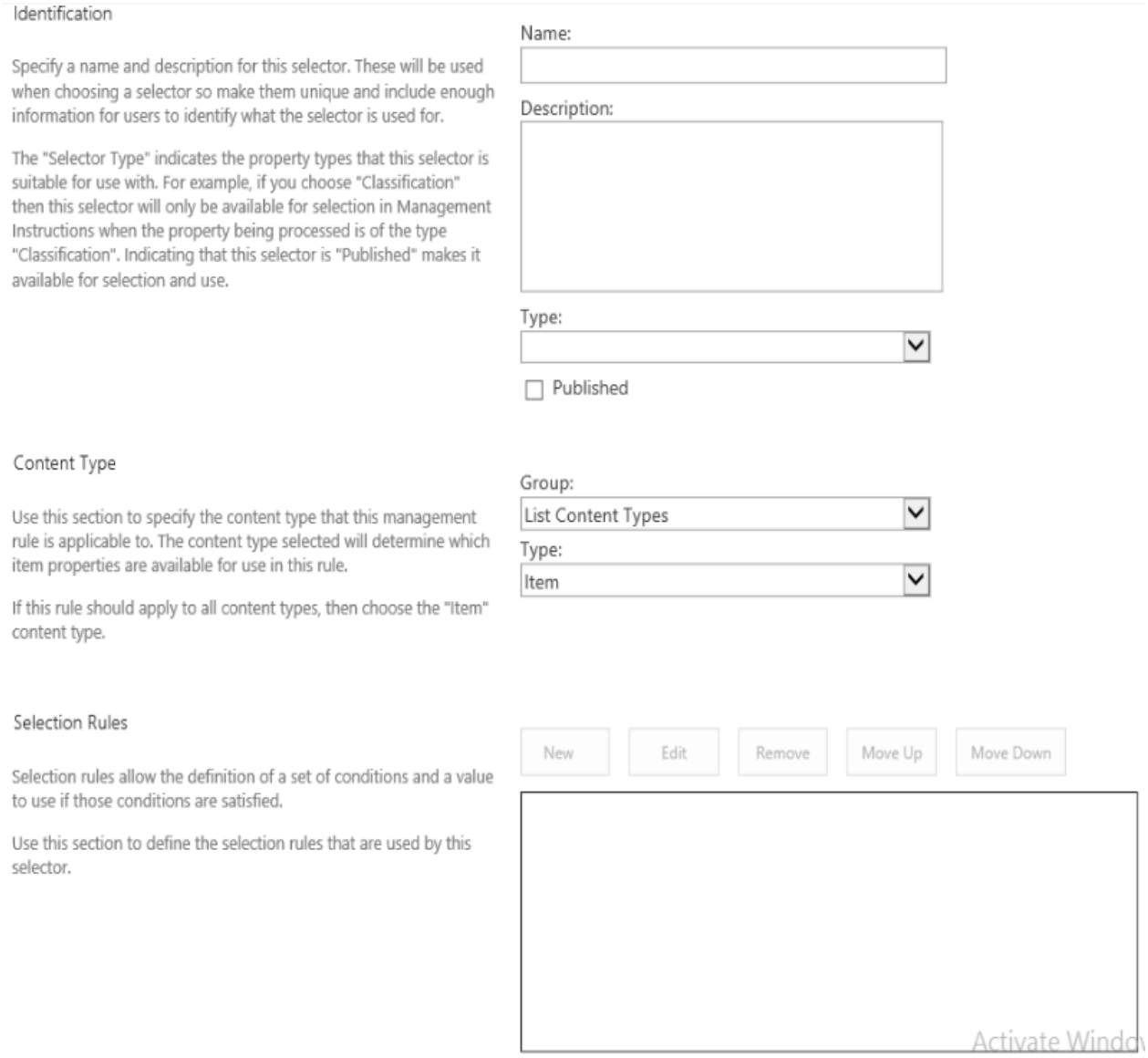
   The instruction(s) will be exported as XML file with the file format as **SPI_Instructions_<*Auto gen number*>.XML** where ***Auto gen number*** is the unique automatically generated number.
3. Click **Open** or **Save** to export the instruction(s) to the desired location in your system.

9.2.3 Creating and editing management selectors

Management selectors are specified for the site collection. Regardless of what site you access the app start page from, you will always be taken to the management selector gallery for the site collection.

9.2.3.1 Creating a new management selector

From the **Management Selector Gallery**, click **Create New** to open pop up window to create the new management selector.



Identification

The **Identification** section of the page is used to provide detail used to identify the management selector, indicate whether it can be used and what type of object it is used to select.

The **Name** of the selector is used for displaying the selector in the management selector gallery. It is important to provide a good name that will allow you to differentiate between selectors in the gallery.

The **Description** of the selector is also displayed in the management selector gallery. Again, it is important to provide a good description that will allow you to identify and differentiate between selectors in the gallery.

The **Type** drop down allows you to specify what type of value that this selector is designed to retrieve. You can choose from the following options:

- Classification
- Location
- Record
- Container
- Record Type
- Retention Schedule
- Security Caveat
- Security Level
- Thesaurus Term
- Jurisdiction

The type that you specify will determine when the selector can be used by management instructions. For example, if you define a selector for choosing a security level, this selector will not be available for use when setting the classification property in an instruction.

Marking a selector as **Published** makes the selector available for selection in instructions. If a selector is not marked as published then it will not be available to be selected for management instructions. This allows you to design selector without them being used until you have completed the design.

Content Type

This **Content Type** section allows specifying which content type the selector is to apply to. This will govern the properties of the item that you will permitted to select when creating rules.

Selection Rules

The **Selection Rules** section of the page allows specifying the rules that the selector will use for selecting a value.

To add a new rule, click **New**.

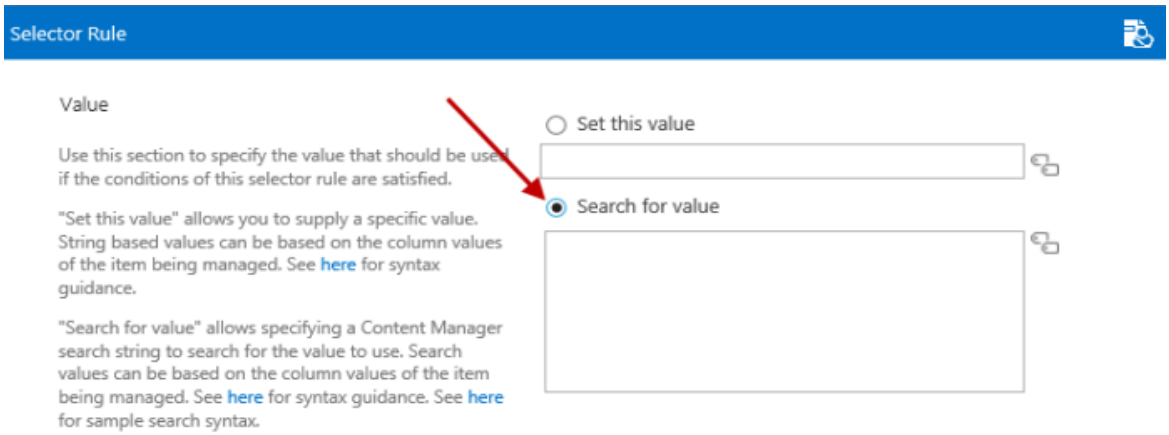
> **NOTE:** The New option will not be enabled unless a type has been specified for the selector.

There are two types of selector rules that can be created. A search based selector rule performs a search of Content Manager looking for a specific value. A condition based selector rule specifies a set of conditions and a value that should be used if those conditions are satisfied.

For condition based selector rules, it is expected that multiple rules will be included.

Creating a search based selector rule

Select the **Search for value** radio button on the selector rule dialog.



The text area associate with this option allows the entry of a Content Manager string based search. The description text on the page includes a link that provides basic syntax guidance.

Refer to Content Manager product documentation for the full description of string based searches.

The construction of Content Manager searches also supports the use of the replacement syntax to substitute the values of site, list and item properties at the time of searching. For example, if the selector rule needed to find a container that had a title based on the month and year of a column called InvDate, the search might be:

```
title:”Invoices [%Item.InvDate.Month.Long%] [%Item.InvDate.Year.Long%]”
```

If the item had a value in this column of 1 May 15, the actual search that will be performed is:

```
title:”Invoices May 2015”
```

The description text on the page includes a link that provides details of the replacement syntax. To the right of the text area is an edit button that displays a dialog that will allow the construction of the string without needing to understand the syntax.

Once the search based selector rule is complete, click ***OK*** to save the rule. The selection rule will appear in the list as:

Creating a condition based selector rule

Select the **Set this value** radio button on the selector rule dialog. Click the icon next to the value text box, select the value that should be set in this scenario from the dialog that displays.

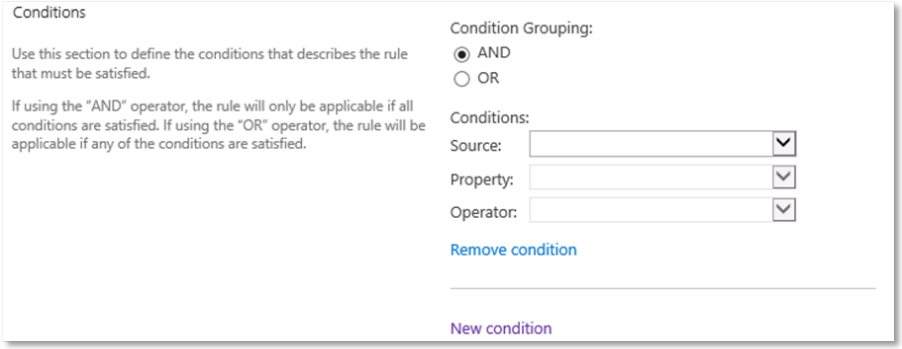
The values that you can select will be based on the type of selector that is being created. For example, if the selector is to choose a classification, then the dialog will only allow you to choose a classification.

A set of conditions must be specified in the **Conditions** section of the dialog. These conditions describe under what circumstances that the value chosen should be assigned.

To add a condition, click the **New condition** link.

Conditions can use either the AND or OR grouping. If AND is used, then all conditions that you specify must be true for the selector rule to be applicable. If OR is used, then if any one of the conditions is true, then the selector rule is considered to be applicable.

To create a condition, click the **New condition** link. This adds an empty condition to the page.



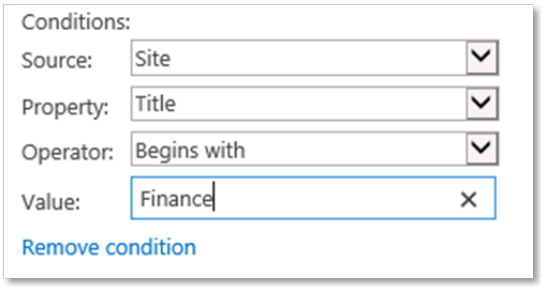
The **Source** dropdown allows you to choose the source of the property that will be used for the container. You can choose from:

- Site
- List
- Item

The properties that are available to select in the **Property** drop down will depend on the selection made in the source dropdown. Additionally, if you select Item as the source, the properties available will be based on the content type selected in the **Content Types** section.

The **Operator** dropdown provides the list of comparators that will be used against the selected property. The available operators will depend on the data type of the property that is selected.

Some operators require you to specify a **Value** to compare with. For example, if the condition includes a text field the operator may require entry of a value to compare with.



It is permissible to add multiple conditions. To add further conditions click the ***New condition*** link. Continue adding the required number of conditions.

To remove a condition, click the **Remove Condition** link under the condition to be removed.

Once the search based selector rule is complete, click **OK** to save the rule. The selection rule will appear in the list as (where the value is the value being set by the selector rule):

Saving the selector

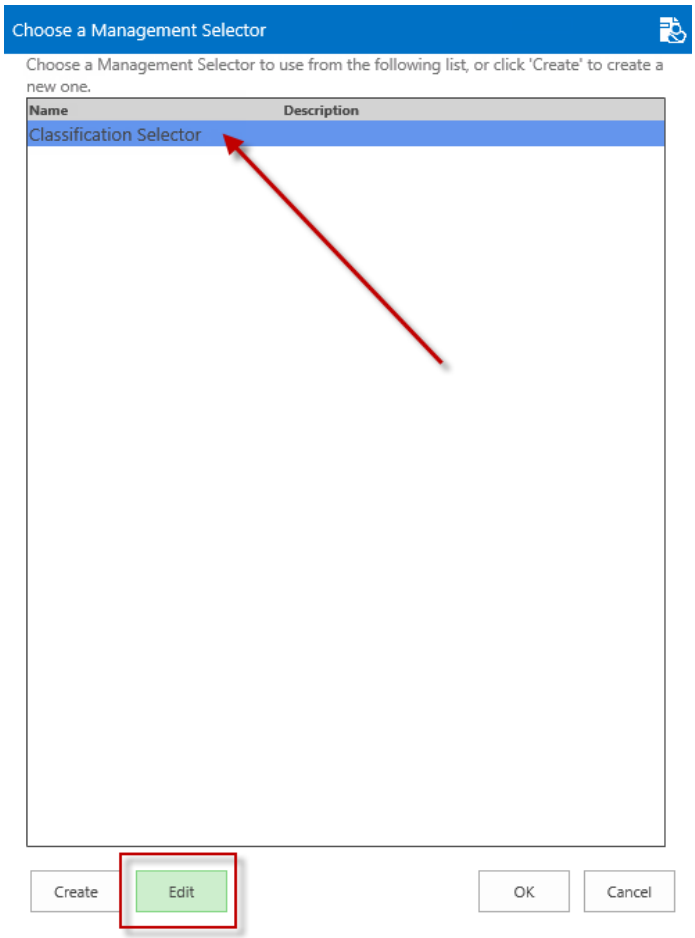
Click **OK** to save the management selector. If the values entered are valid, the rule will save and will appear in the management selector gallery. If any data is invalid, a message will be displayed on the page identifying the issue.

Click **Cancel** to close the page without saving the management selector.

9.2.3.2 Editing an existing management selector

There are two ways to access the editing of existing management selectors. From the management selector gallery, select the selector to be edited then click the ***Edit*** button to open the management selector dialog.

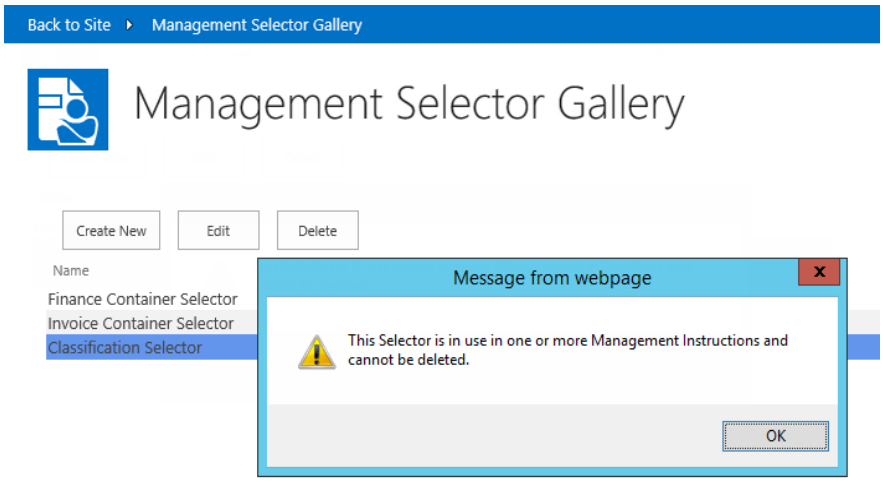
Alternatively, from the management instruction page when selecting the selector to use, the selection dialog includes an **Edit** button that can be used to edit the selected management selector.



9.2.3.3 Deleting a management selector

To delete an existing management selector, navigate to the management selector gallery, select the selector to be deleted then click then **Delete** button.

If the instruction is in use by a management rule, the delete will be prevented. You must first remove the instruction from all management rules before you will be permitted to delete it.



9.2.3.4 Importing and exporting management selector

Importing management selector

To import a management selector, perform the following:

1. Navigate to the management selector gallery and click **Import**.
2. Go to the location where you have saved the management selector, select the one you want to import and click **Open**.

   Once imported, a status message is displayed. The newly imported selector will be listed in the management selector gallery.

Exporting management selector

To export management selector, perform the following:

1. Navigate to the management selector gallery and click **Export**.
2. In the **Export Management Selector** dialog, select the selector(s) you want to export, and then click **Export**.

   The selector(s) will be exported as XML file with the file format as **SPI_Selector_<*Auto gen number*>.XML** where ***Auto gen number*** is the unique automatically generated number.
3. Click **Open** or **Save** to export the selector(s) to the desired location in your system.

9.2.4 Management rules options

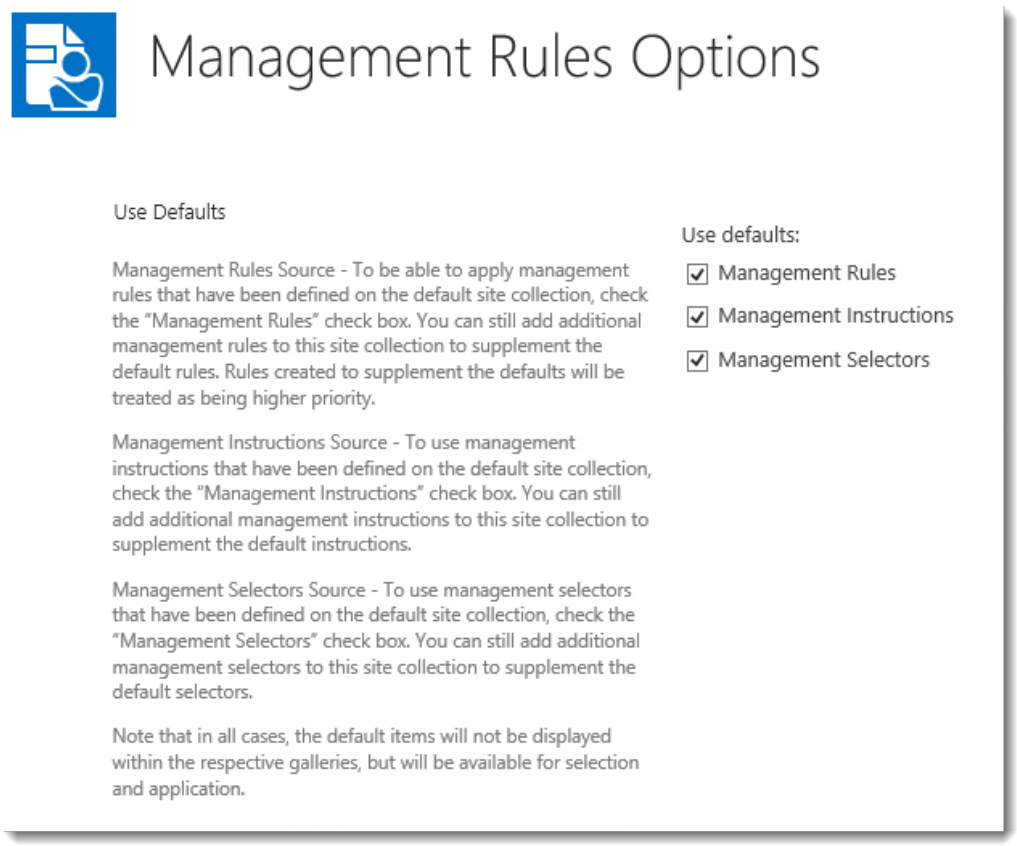
Management rules, management instructions and management selectors that are defined for the default site collection can be reused on other site. The **management rules options** page allows specifying which configuration is defined for the local site collection and what will be sourced from the default site collection.

Unlike other configuration that consumes the values from the default site collection, for management rules, instructions and selectors, this configuration can be supplemented on a site collection that uses the defaults.

For example, it is possible to have a set of core management rules that are defined on the default site collection and have another site collection using these rules, along with other rules that are defined for use on that site collection only.

9.2.4.1 Specifying use of values from the default site collection

The management rules options page allows you to specify individually whether management rules, management instructions or management selectors will use the values configured on the default site collection.



9.3 Applying management rules

It is possible that more than one management rule will be applicable to content when it is managed. It is also possible that the applicable management rules try to set the same Content Manager property with differing values.

This section describes how values are determined in these circumstances.

9.3.1 Applicable rules

A rule is considered to be ***Applicable*** if the conditions specified for that management rule are satisfied. In the case of conditions that us the AND grouping, then all conditions must be met for a rule to be applicable. If the management rule uses the OR grouping for conditions, then if any one of the conditions is met, the rule is considered applicable.

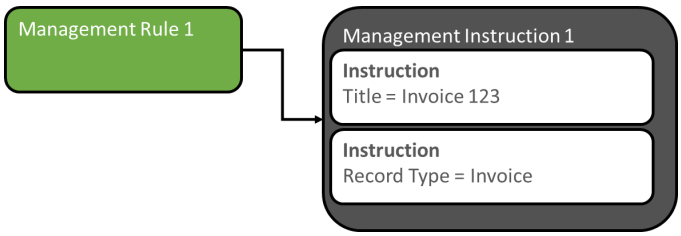
During management, only management rules that are found to be applicable are considered.

It is possible that there will be multiple management rules that are applicable to an item during management.

9.3.2 Constructing the collection of applicable instructions

Ultimately, the individual instructions associated with the management instructions that are associated with all the applicable management rules are what determine how the record is managed in Content Manager.

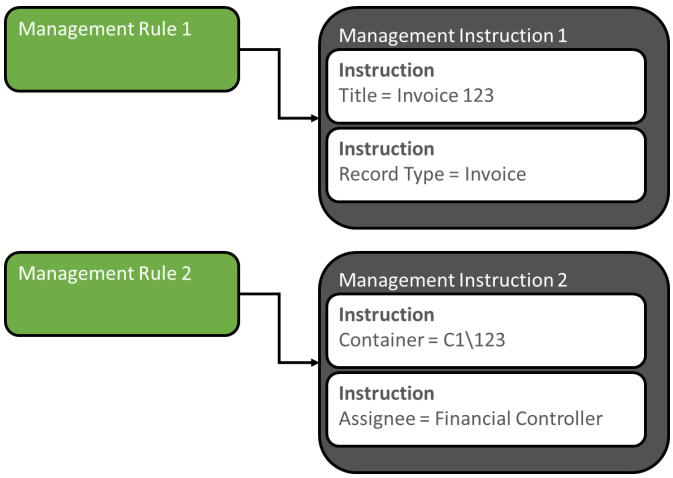
For example, consider the scenario where ***Management Rule 1*** is associated with ***Management Instruction 1*** as shown in the following diagram.



If management rule 1 is the only applicable management rule, then the list of instructions that are applicable are:

- Title = Invoice 123
- Record Type = Invoice

If there are multiple management rules that are applicable though, then the instructions associated with all rules are applicable. Consider the following example where management rule 1 and 2 are both applicable.

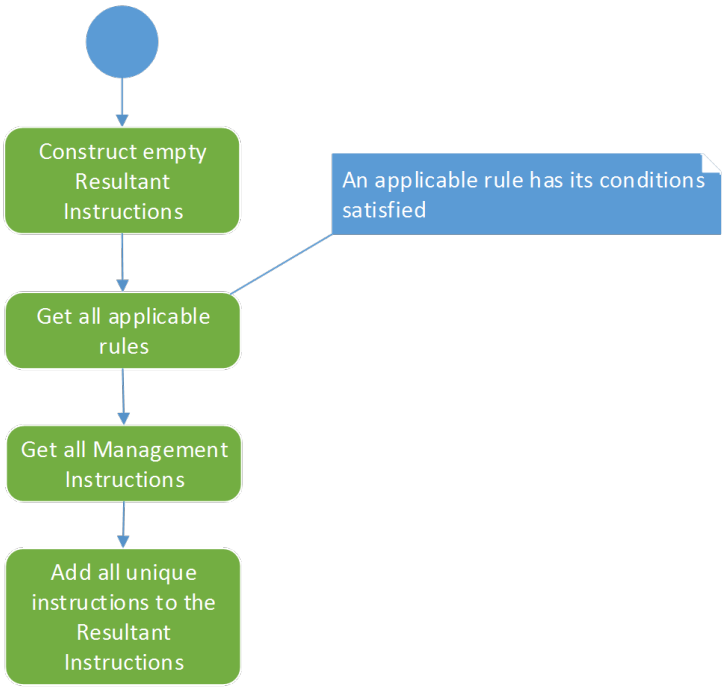


In this scenario, the list of instructions that are applicable are:

- Title = Invoice 123
- Record Type = Invoice
- Container = C1\123
- Assignee = Financial Controller

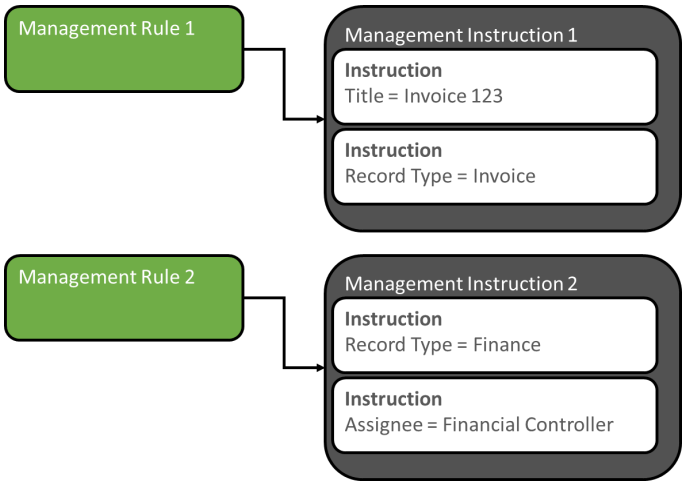
During management of the item, all four of these instructions would apply to the item.

The process of identifying the list of applicable instructions during management can be summarized as:



9.3.3 Handling duplicate instructions

There are situations where there may be duplicate instructions. Consider the scenario where the following two management rules are applicable:



In this scenario, there are two instructions specifying the value for Record Type. As it is only possible to set the value of a property once, a process is used to determine which of the duplicate instructions to use.

The attributes that are used to determine which to use are based on:

- Is the management rule associated with the instruction marked as ***critical***
- How many conditions are associated with the management rule
- What is the priority that has been given to the management rule

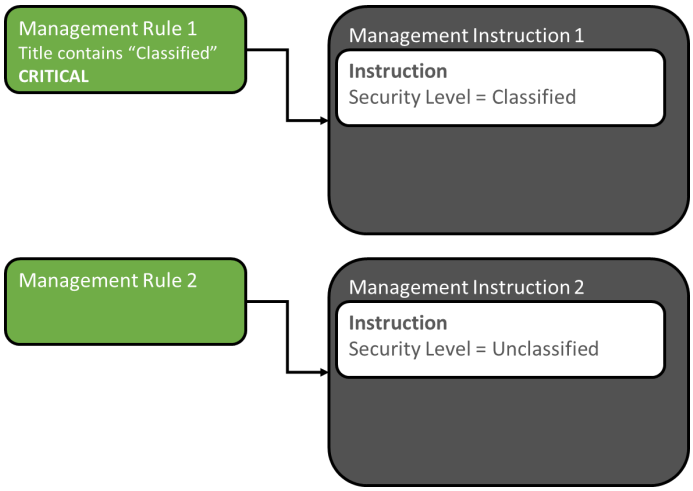
Critical management rules

During the definition of a management rule, the rule can be marked as Critical. By marking a management rule as being critical, you are effectively indicating that regardless of any other rules, the instructions associated with this management rule must always be applied.

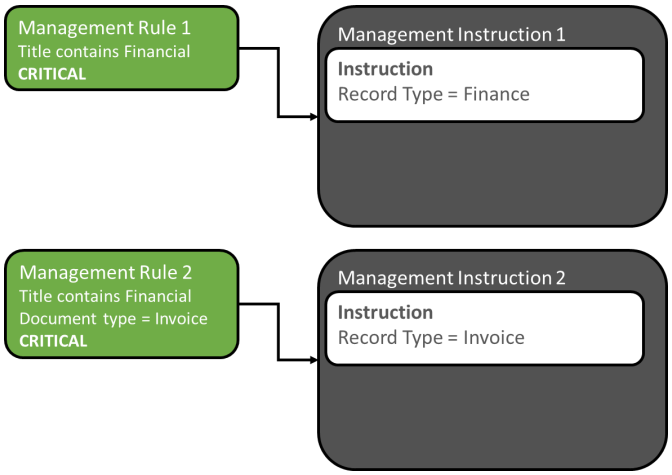
For example, your organization may have a policy that if the title of an item includes the word “Classified” in it, then the record created in Content Manager must always have a security level of “Classified”.

By defining a management rule that is marked as critical, when this rule is applicable, the instruction will always be applied.

In the example below, management rule 2 is not marked as critical. Both management rules are attempting to set the security level. The instruction associated with management rule 1 will always be used in preference as it is marked as being critical.



There can of course be scenarios where there are multiple applicable rules with duplicate instructions and all rules are marked as critical. Consider the following scenario:



In this case, two critical management rules are attempting to set the record type. In this scenario, the management rule with the most conditions will be used i.e. in this example, the record type will be set to "Invoice".

This reflects that a management rule with more conditions is more highly specialized and more likely to reflect the correct value to select.

If there is no difference in the number of conditions used by the applicable management rules, then the management rule that has the highest priority in the management rules gallery is used.

Management rules with the most conditions

When there are duplicate instructions coming from management rules that are not marked as critical, the number of conditions on the management rule is used to determine which instruction to use. The instruction associated with the management rule that has the most number of conditions is used.

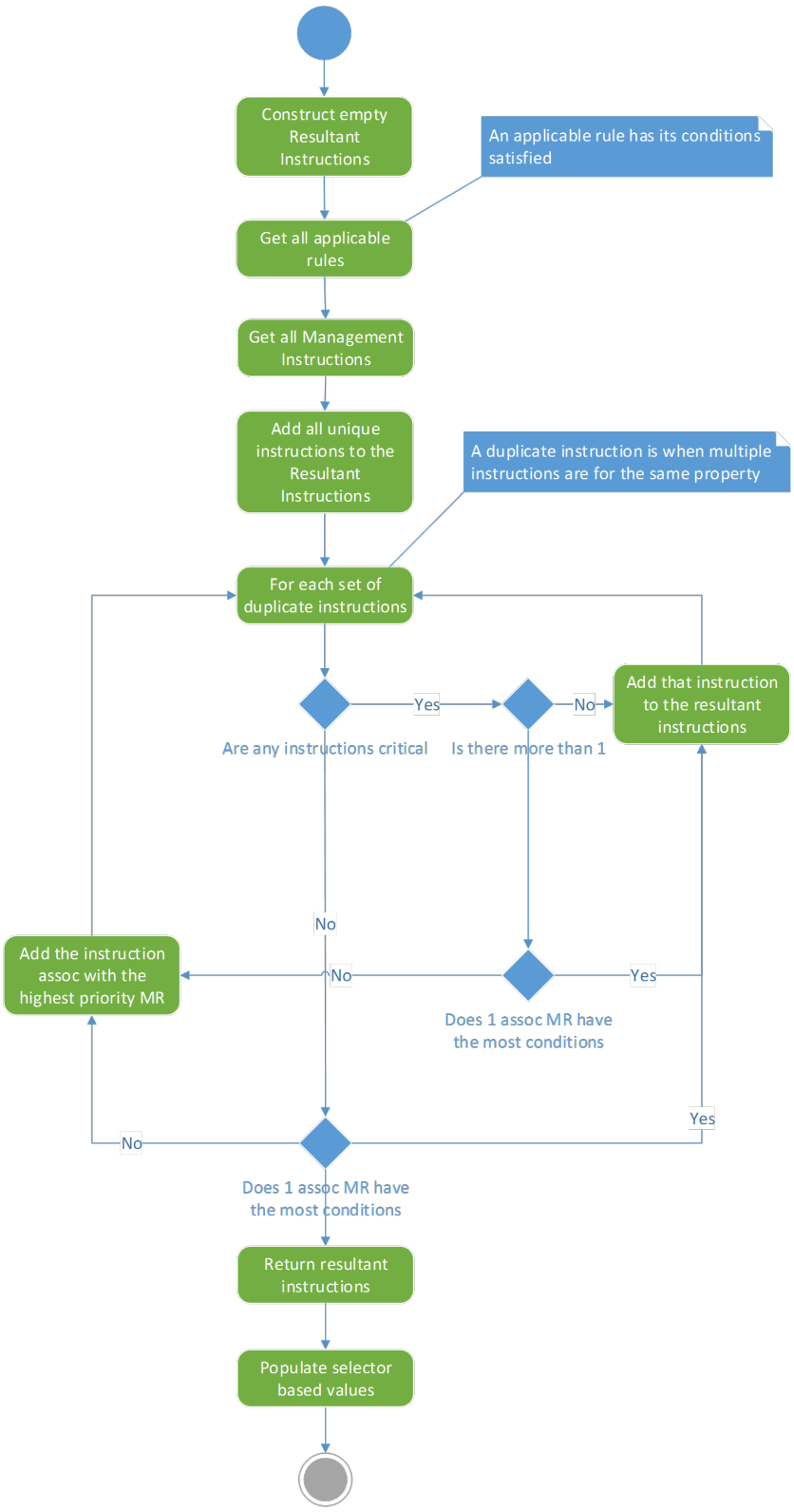
Management rule priority

When there are duplicate instructions coming from management rules that are not marked as critical and they have the same number of conditions on the associated management rule, the instruction

associated with the highest priority management rule is used.

9.3.4 Summary of management rule selection process

The following diagram summarizes the processes used to select the list of applicable instructions to apply during management.


Construct empty Resultant Instructions
An applicable rule has its conditions satisfied
Get all applicable rules
Get all Management Instructions
Add all unique instructions to the Resultant Instructions
A duplicate instruction is when multiple instructions are for the same property
For each set of duplicate instructions
Yes
No
Add that instruction to the resultant instructions
Are any instructions critical
Is there more than 1
No
Add the instruction assoc with the highest priority MR
No
Yes
Does 1 assoc MR have the most conditions
Yes
No
Does 1 assoc MR have the most conditions
Return resultant instructions
Populate selector based values

10 Manually managing content

The Content Manager Governance and Compliance app provides two main mechanisms for managing content:

1. Manually, through user instigation
2. Automatically, through the use of ***Lifetime Management Policies***

Note that these are not mutually exclusive, there will be many organizations choosing to use a mixture of automatic and manual management across their SharePoint landscape.

This chapter focuses on manual management, and is recommended reading for anyone who will be required to manually manage SharePoint content, for capture into Content Manager.

Some examples:

- Any users who are working with SharePoint content as part of their day-to-day processes, where the organization requires content to be managed in Content Manager as part of business process
- SharePoint site administrators who may need to manage, finalize, relocate, or archive lists and sites as part of ongoing site management
- Content Managers, Information Officers, and Compliance Officers, who may need to perform manual management to maintain existing content

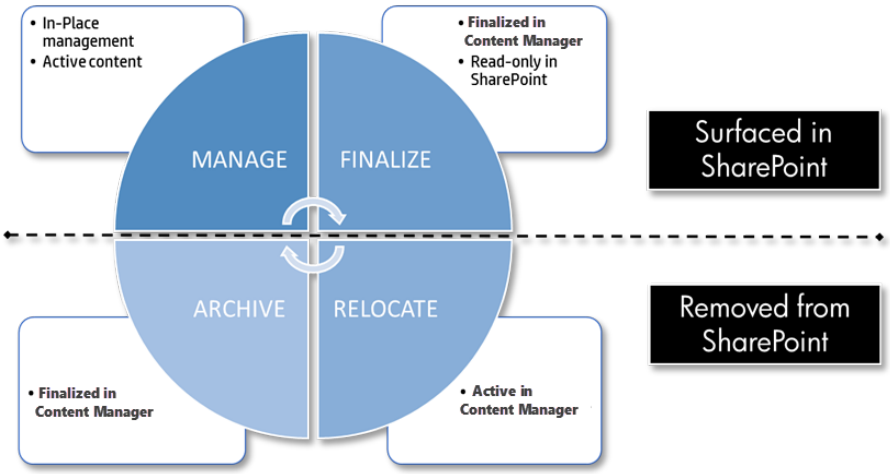
In short, unless you are aware that your organization does not allow manual management of content, you should read this chapter to familiarize yourself with the various management options

Permissions to perform manual management

To perform manual management actions, you must have minimum **Edit** permission.

10.1 Core actions

The Content Manager Governance and Compliance app provides four core actions for managing SharePoint content, these are available for both policy-driven and manual actions.



These core actions can be applied to all types of SharePoint content:

- Individual list items and documents
- Multiple items and documents
- Document Sets
- Folders
- Lists and libraries
- Sites, including all contained content

For more details, see the section The four core actions for managing content above.

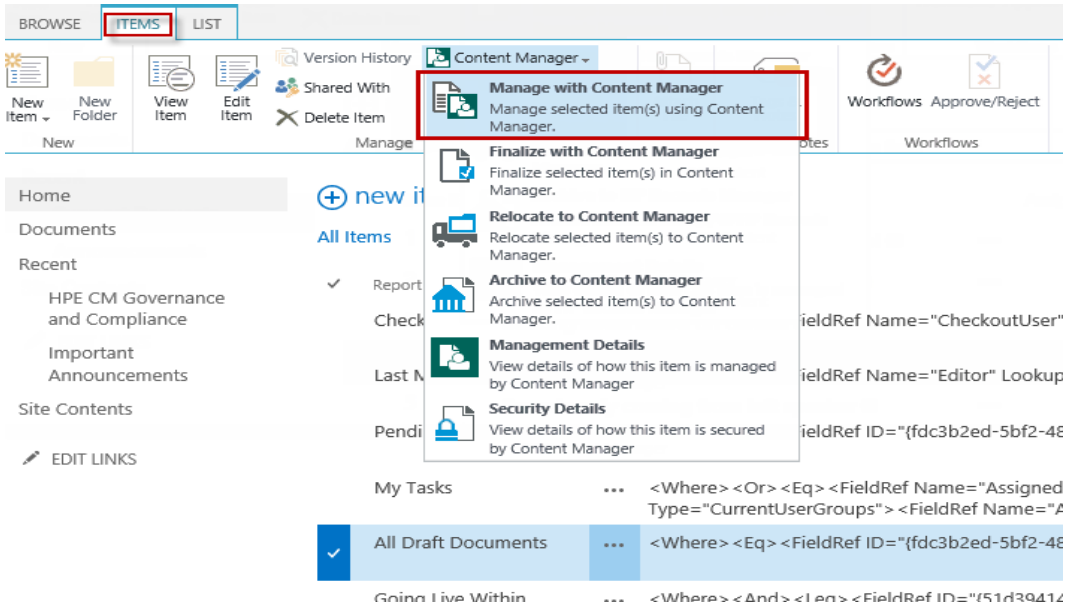
10.1.1 The 'Manage' action

This section describes the various ways of manually instigating the **Manage** action. Managing content will create a corresponding record in Content Manager, but the content will remain active, and in SharePoint.

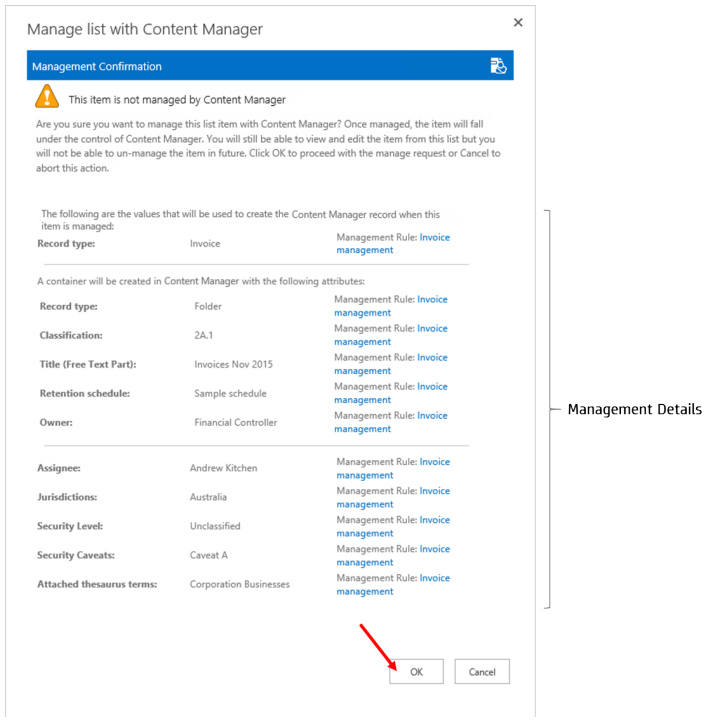
10.1.1.1 Manage an item or document

To manage either a single document or list item, perform the following steps:

1. Navigate to the list or library, and select the required item in the list.
2. Expand the **Items** ribbon, and from the **Manage** section click on the **Content Manager** dropdown.
3. Click on **Manage with Content Manager** to instigate the action.



4. Read the confirmation dialog, which explains what will happen to the item once managed, and then click **OK** to complete the **Manage** action. Choosing **Cancel** will return you to the list with no action taken. The dialog will include details of how the item will be managed by Content Manager.

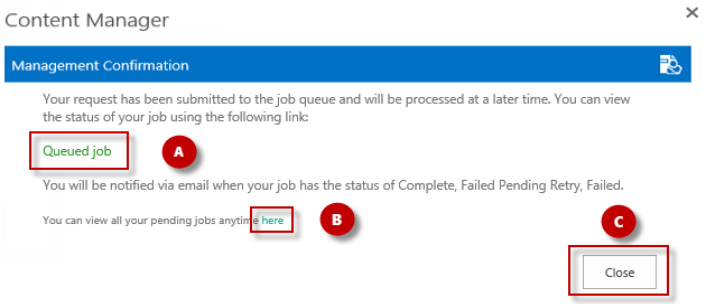


5. The next dialog confirms the action has been sent to the job processing queue. From here you can:

   a. View the details of the submitted job

   b. View all of your pending jobs in the queue

c. Close the confirmation and carry on working



> **NOTE:** All actions are submitted to a central job processing queue, and are processed sequentially. Your job may not be processed immediately, depending on current workload. You will be notified by email when your job has been completed. For more details on the job queue, please see *Chapter 20 - Understanding the job queue*.

How documents are managed

When SharePoint documents or list items with attachments are managed, the record created in Content Manager initially does not have the document attached to it. The document remains in SharePoint until the item is relocated or archived to Content Manager.

The document can still be viewed in Content Manager. Double clicking a record representing a document list item in SharePoint will retrieve the document from SharePoint and display it to the user.

When the item is relocated or archived, the document is moved to the Content Manager record. If the Capture all versions option is checked on the default integration settings page, then all versions of the document will be captured as revisions on the record. If this options is unchecked, then only the latest version of the document will be captured.

Use of the SharePoint Folder content type

The SharePoint ***Folder*** content type behaves somewhat differently to other content types. For example, it is not possible to modify the properties that are included on the folder.

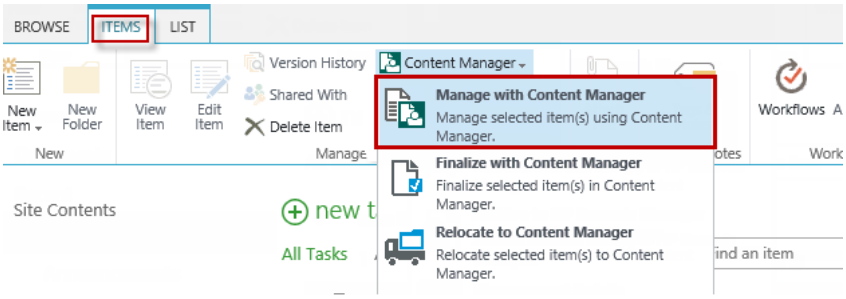
Consider the scenario where you want to display the record number of the record that represents a managed folder in SharePoint. This is not possible using the out of the box Folder content type.

Although the folder content type is supported, it is recommended that you create a customer Folder content type that derives from Folder. This will allow the inclusion of additional columns if required.

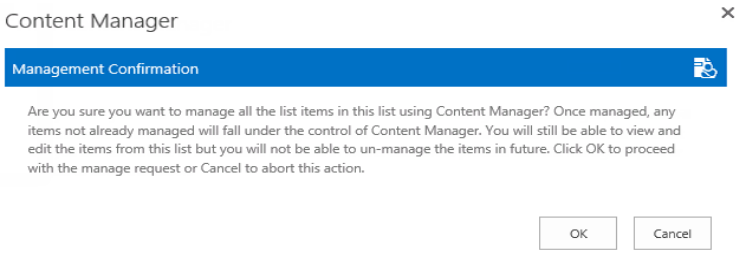
10.1.1.2 Manage multiple items or documents

To manage multiple documents or list items, perform the following steps:

1. Navigate to the list or library, and select the required items in the list.
2. Expand the **Items** ribbon, and from the **Manage** section click on the **Content Manager** dropdown.
3. Click on **Manage with Content Manager** to instigate the action.



4. Read the confirmation dialog, which explains what will happen to the items once managed, and then click **OK** to complete the **Manage** action. Choosing **Cancel** will return you to the list with no action taken.

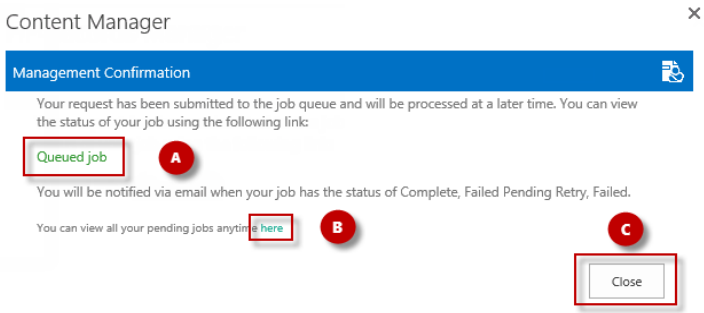


5. The next dialog confirms the action has been sent to the job processing queue. From here you can:

   a. View the details of the submitted job

   b. View all of your pending jobs in the queue

   c. Close the confirmation and carry on working



> **NOTE:** All actions are submitted to a central job processing queue, and are processed sequentially. Your job may not be processed immediately, depending on current workload. You will be notified by email when your job has been completed. For more details on the job queue, please see Chapter 19 - Exposing existing Content Manager records into SharePoint.

10.1.1.3 Manage a document set

Document sets are a collection of documents with some common metadata. Document Sets, including their contents, can be managed in one action. The document set will be tracked as a record,

along with the contained documents as related records.

To manage a document set/s, perform the following steps:

1. Navigate to the library, and select the required document set/s in the list.
2. Expand the **Files** ribbon, and from the **Manage** section click on the **Content Manager** dropdown.
3. Click on **Manage with Content Manager** to instigate the action.
4. Read the confirmation dialog, which explains what will happen to the items once managed, and then click **OK** to complete the **Manage** action. Choosing **Cancel** will return you to the list with no action taken.
5. The next dialog confirms the action has been sent to the job processing queue. From here you can:
   a. View the details of the submitted job
   b. View all of your pending jobs in the queue
   c. Close the confirmation and carry on working

> **NOTE:** All actions are submitted to a central job processing queue, and are processed sequentially. Your job may not be processed immediately, depending on current workload. You will be notified by email when your job has been completed. For more details on the job queue, please see *Chapter 20 - Understanding the job queue*.

10.1.1.4 Manage a folder

Document libraries can contain folders, which are sometimes used to organize information in a library. It is possible to perform integration actions directly on single and multiple folders.

The folder will be tracked as a record, along with the contained documents as related records.

> **NOTE:** Managing a top level folder will also manage all sub-folders and their content too.

To manage a folder/s, perform the following steps:

1. Navigate to the library, and select the required folder/s in the list.
2. Expand the **Files** ribbon, and from the **Manage** section click on the **Content Manager** dropdown.
3. Click on **Manage with Content Manager** to instigate the action.
4. Read the confirmation dialog, which explains what will happen to the items once managed, and then click OK to complete the **Manage** action. Choosing Cancel will return you to the list with no action taken.
5. The next dialog confirms the action has been sent to the job processing queue. From here you can:
   a. View the details of the submitted job
   b. View all of your pending jobs in the queue

c. Close the confirmation and carry on working

> **NOTE:** All actions are submitted to a central job processing queue, and are processed sequentially. Your job may not be processed immediately, depending on current workload. You will be notified by email when your job has been completed. For more details on the job queue, please see *Chapter 20 - Understanding the job queue*.

10.1.1.5 Manage a list or library

Sometimes business process can require bulk actions to be performed. A document library containing hundreds of contract documents may need to be captured to ensure compliance. The integration provides a mechanism for performing actions against an entire list, regardless of how many items/documents are in that list.

> **NOTE:** You can still use list/library management, even if some content has already been managed, the process will automatically skip any previously managed items.

To manage a list or library, perform the following actions:

1. Navigate to the list and expand the **Library** or **List** ribbon.
2. From the **Connect & Export** section, click on the **Content Manager** dropdown.
3. Click on **Manage list with Content Manager** to instigate the action.
4. Read the confirmation dialog, which explains what will happen to the items once managed, and then click OK to complete the **Manage** action. Choosing Cancel will return you to the list with no action taken.
5. The next dialog confirms the action has been sent to the job processing queue. From here you can:
   a. View the details of the submitted job
   b. View all of your pending jobs in the queue
   c. Close the confirmation and carry on working

> **NOTE:** All actions are submitted to a central job processing queue, and are processed sequentially. Your job may not be processed immediately, depending on current workload. You will be notified by email when your job has been completed. For more details on the job queue, please seeChapter 20 - Understanding the job queue.

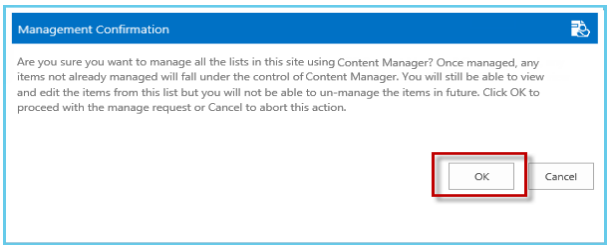
10.1.1.6 Manage a site

Sometimes business process can require bulk actions to be performed. A site containing numerous lists and large volumes of content may need to be captured to ensure compliance. The integration provides a mechanism for performing actions against an entire site, regardless of how many lists, items, and documents are contained within that site.

> **NOTE:** You can still use site management, even if some content has already been managed, the process will automatically skip any previously managed items.

To manage a site, perform the following actions:

1. Navigate to the site, click on the **Site Contents** link, then click on the **Content Manager Governance and Compliance** app icon to open the app start page.
2. Under the **Site Management** section on the app start page, click on **Manage this site** to instigate the process.
3. Read the confirmation dialog, which explains what will happen to the items once managed, and then click OK to complete the **Manage** action. Choosing Cancel will return you to the site with no action taken.



4. The next dialog confirms the action has been sent to the job processing queue. From here you can:
   a. View the details of the submitted job
   b. View all of your pending jobs in the queue
   c. Close the confirmation and carry on working

> **NOTE:** All actions are submitted to a central job processing queue, and are processed sequentially. Your job may not be processed immediately, depending on current workload. You will be notified by email when your job has been completed. For more details on the job queue, please see Chapter 20 - Understanding the job queue.

10.1.2 The 'Finalize' action

The process for instigating **Finalize** is exactly the same as when managing content. Please refer to 10.1.1 The 'Manage' action, on page 117 for details, noting that the **Finalize** action on menus should be chosen in place of **Manage**. Finalizing content will create a corresponding record in Content Manager, and will prevent any further changes to that content. The content will still be visible in SharePoint.

10.1.3 The 'Relocate' action

The process for instigating **Relocate** is exactly the same as when managing content. Please refer to 10.1.1 The 'Manage' action, on page 117 for details, noting that the **Relocate** action on menus should be chosen in place of **Manage**. Relocating content will create a corresponding record in Content Manager, and will move the content from SharePoint into Content Manager. The content will no longer be stored, nor be visible, in SharePoint.

10.1.4 The 'Archive' action

The process for instigating **Archive** is exactly the same as when managing content. Please refer to 10.1.1 The 'Manage' action, on page 117 for details, noting that the **Archive** action on menus should be chosen in place of **Manage**. Archiving content will create a corresponding record in Content

Manager, and will move the content from SharePoint into Content Manager, and finalize it, preventing any further changes. The content will no longer be stored, nor be visible, in SharePoint.

11 Determining the management status of content

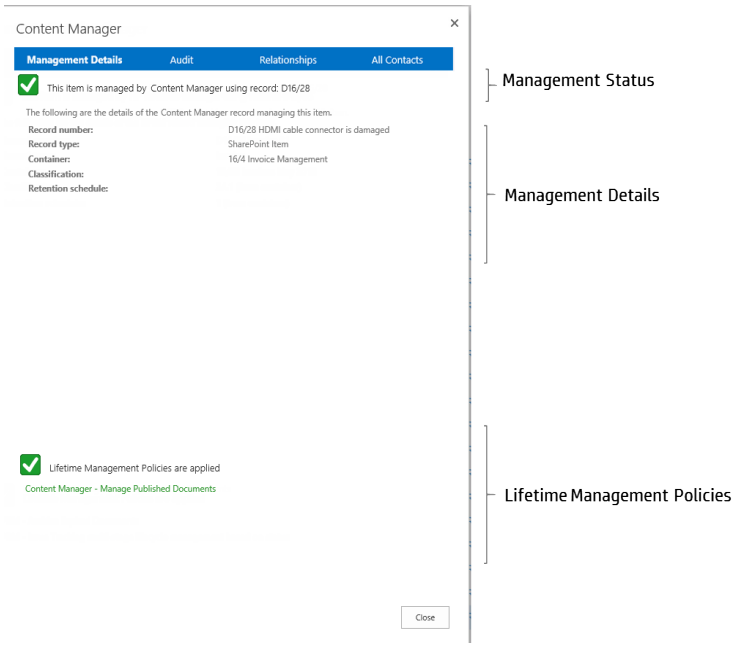
It may be necessary in certain scenarios to understand whether SharePoint content is managed by Content Manager. You may need to know how it is managed and perhaps, how it will be managed sometime in the future.

This chapter describes the functionality that is available to determine this information.

11.1 Management details page

The management details page can be accessed for individual items. This is available whether the item is managed or not. The page consists of the following details:

- Management status
- Management details
- Lifetime management policies



11.1.1 Accessing the page

To access **Management Details**:

1. Select the relevant list item.
2. Expand the **Items/Files** ribbon, and from the **Manage** section click on the **Content Manager** dropdown.
3. Click on **Management Details**.
4. The **Management Details** dialog is shown, click **Close** to return without refreshing the SharePoint page. If the top right corner X button is used to close the dialog then the

SharePoint page will be refreshed.

> **NOTE:** The management details page can also be accessed from the context drop down on the item itself.

11.1.2 Management status section

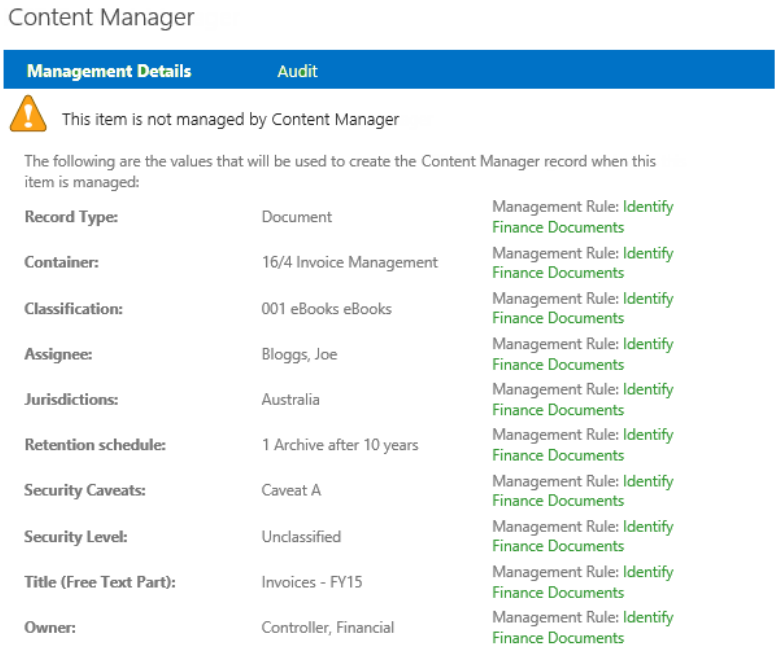
At current management status of an item is indicated at the top of the page. If the item is managed, the record number of the Content Manager record is displayed:

If the item is not managed, a caution is shown:

11.1.3 Management details section

Unmanaged items

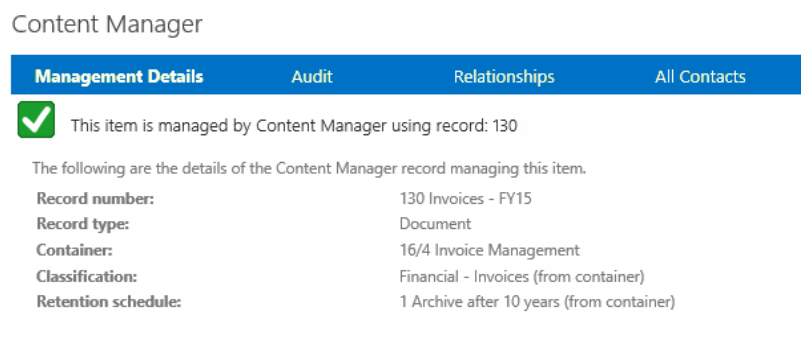
If the item is not currently managed, the page displays how the content will be stored in Content Manager, if and when the content becomes managed.



Where a record value has been determined by configuration values of the Content Manager Governance and Compliance app, a link to that configuration is included.

Managed items

If the item is managed by Content Manager, the page displays pertinent details of the Content Manager record used.



If the Content Manager web client is available, and the URL of the web client has been configured in the Content Manager system options, the record number and the container record number will appear as links to those records in the web client.

11.1.4 Lifetime management policies

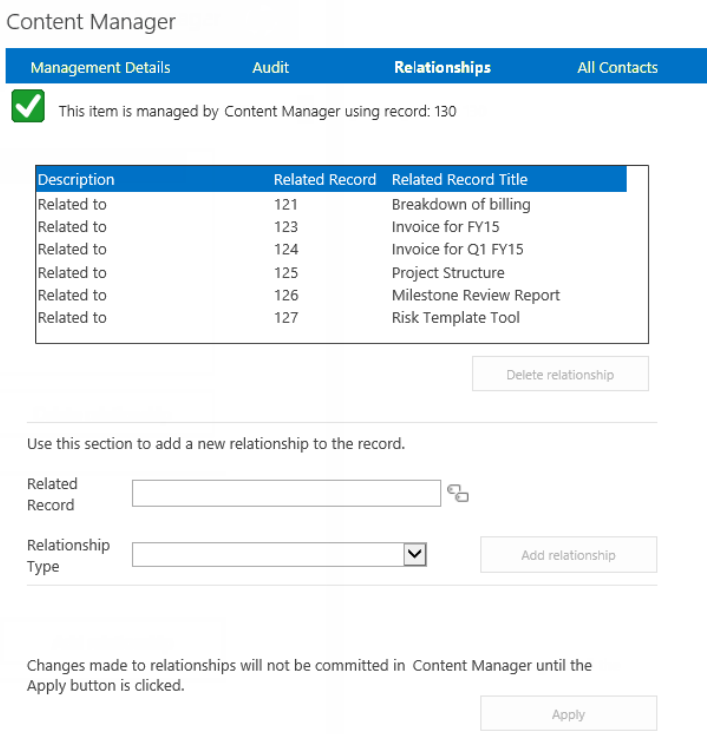
The Management Details page also displays a list of any Lifetime Management Policies that are in effect against this individual item. This can aid in troubleshooting, when trying to understand which policies are in effect, and why content has or has not been managed in a particular way.

A status is also included indicating whether there are lifetime management policies that may manage this content.

11.1.5 Relationships link

For items that are managed, a **Relationships** link is included in the page header to display all relationships associated with that record:

When clicked, the list of related records are displayed:

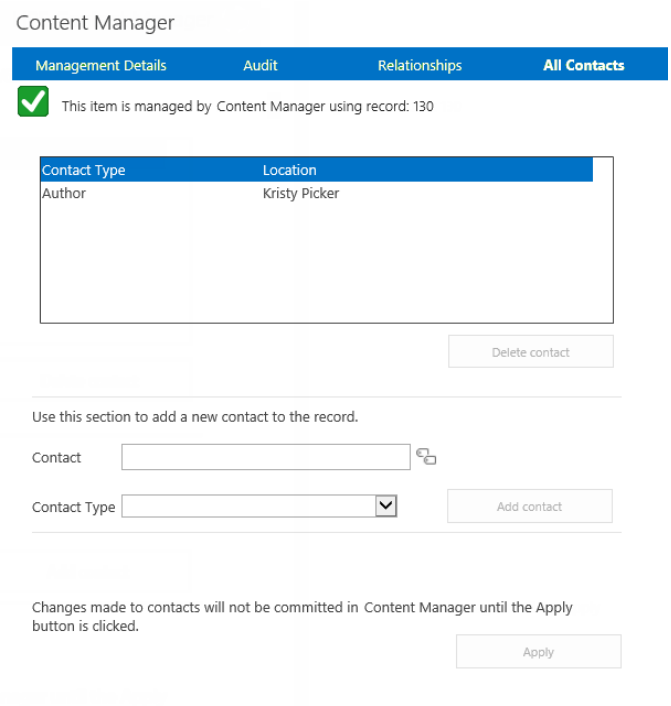


New relationships can be added and existing relationships deleted. Any changes made though are not committed in Content Manager until the ***Apply*** button is clicked.

11.1.6 All Contacts link

For items that are managed, an **All Contacts** link is included in the page header to display all contacts associated with that record:

When clicked, the list of contacts are displayed:

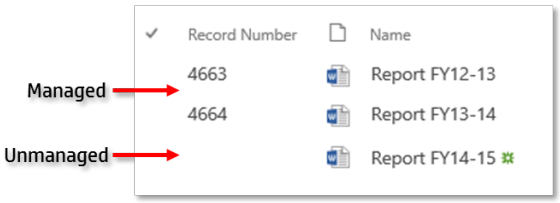


New contacts can be added and existing contacts deleted. Any changes made though are not committed in Content Manager until the ***Apply*** button is clicked.

11.2 Using column values to illustrate management status

Although the management details page can indicate whether content is managed or not, it requires examining each item individually to view the details. In the scenario where the user should be able to determine at a glance which items in a list are managed and which are not, another approach is required.

As all managed list items have a corresponding record in Content Manager, and every record has a record number, by adding the record number field to the list view, it becomes simple to identify items that are managed. If the item has a record number it is managed, if it doesn't then it is not managed.

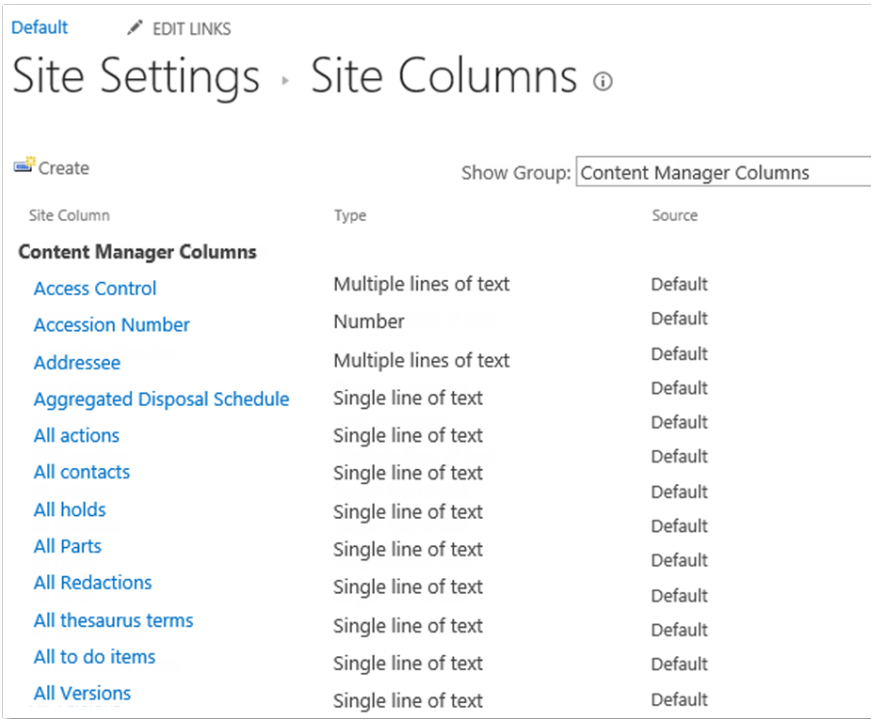


Use SharePoint list functionality to include the **Record Number** field found in the **Content Manager** column group.

> **NOTE:** If the record number field has had its caption changed in Content Manager to another term, the name of the column will be the same as that caption.

Site Columns

Record number is not the only column that can be used. The ***column generation tool*** that was run during installation and configuration creates a set of columns that represent fields (including additional fields) in Content Manager. These are created as site columns and appear under the group Content Manager.



NOTE: If you have upgraded from a previous version, the column names will not have changed to Content Manager to ensure backwards compatibility. As in the figure above.

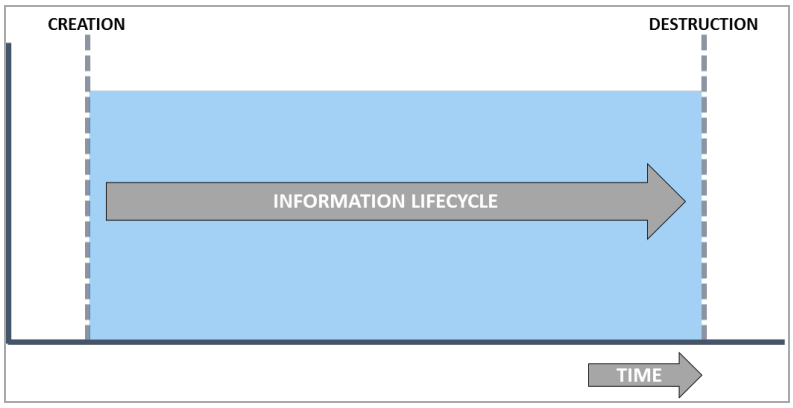
Any of these columns can be added to lists to display the value of that record property.

12 Automating governance and compliance

12.1 Overview

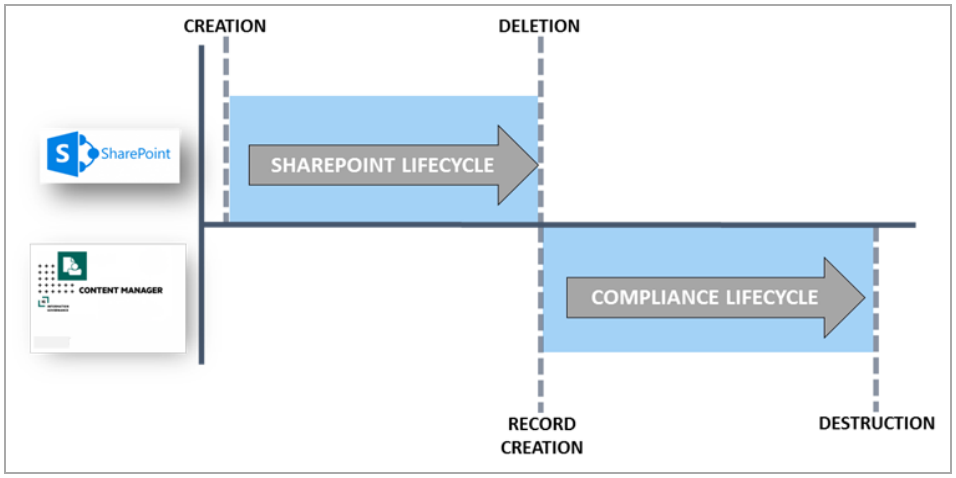
12.1.1 Automate information lifecycle

The information lifecycle is the period of time from when a piece of content is created, until that content is destroyed.



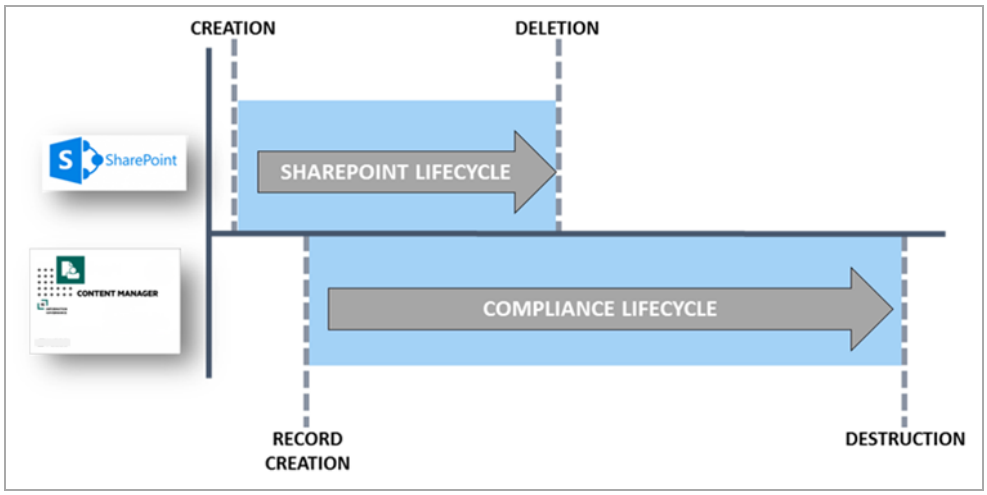
This diagram though does not reflect where that content resides at any point during its life. By including the system that contains content on the Y axis of this graph, it becomes clear that information lifecycle can be split into two distinct parts.

When considering an organization that requires “completed” content to be “moved” out of SharePoint and into a compliance system such as Content Manager, we could describe the information lifecycle as follows:



The period of time from when content is created in SharePoint until it is removed from SharePoint is considered the “SharePoint lifecycle”. The time beginning when a record is created in Content Manager until that record is destroyed is considered the “compliance lifecycle”.

The previous diagram reflects only one scenario though. Consider the scenario where content is created in SharePoint, that content must be stored as a record in order to be compliant with relevant legislation, but access to the content via SharePoint must be continued, despite the fact that a record is created.



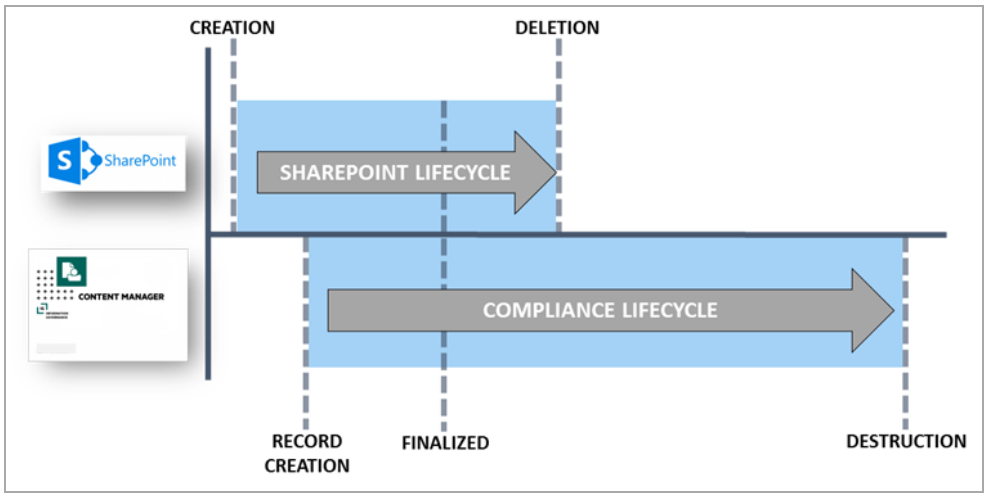
In this scenario, the content is deleted from SharePoint before the record is destroyed. This is reflective of the fact that content must often be retained for far longer than it is regularly accessed.

It is important to understand that not all organizations agree on what the definition of a record is. One of the key areas of difference that tends to stem from geographical differences in records management, is whether a record should be editable once it has been created/declared.

Some organizations consider a record to be “final” and therefore “finalized” such that no changes can be made to it.

Other organizations capture records representing work that is in-progress or underway. At some point, when the content is considered complete, the record is finalized but this does not occur automatically when the record is created.

The following diagram extends the previous example to include finalization:



Although the Information lifecycle is made up of the SharePoint and Compliance lifecycles, it is very important to recognize that these two parts of the information lifecycle are typically unrelated and are driven by different requirements. The SharePoint lifecycle is driven by the requirements of the SharePoint users. They are the ones that dictate what content should be accessible through SharePoint and for how long. It is compliance requirements such as legislation and company specific requirements that decide the compliance lifecycle.

Lifecycle decisions

There are a series of decisions that need to be made during the information lifecycle. These may include:

- When should the content be deleted from SharePoint?
- When should a record be created to represent the content?
- When should the record be finalized?
- When should the record be destroyed?

Consequences of not making lifecycle decisions

Requiring a user to make lifecycle decisions introduces human error as well as training requirements. A user who creates and consumes information through SharePoint is inevitably not interested in governance and compliance. Diligently making these decisions is perceived as an imposition to their daily duties, not part of them.

There are consequences for not having these decisions made correctly and in a timely manner.

In regards to the SharePoint lifecycle the primary consequence is the storage of content in high cost storage un-necessarily. If content is not removed when it is no longer used, the size of SharePoint infrastructure will continue to increase, along with support and storage costs.

In regards to the compliance lifecycle, there are several consequences including:

- Information not retained in accordance with applicable legislation or company policy. This includes retaining information for too long as well as not retaining it long enough
- Exposure during litigation or request-for-information exercises

In addition to users failing to make lifecycle decisions, poorly made decisions will also result in the same set of consequences.

Automating lifecycle decisions

Information management can be a difficult subject to understand. Requiring end users to have the necessary understanding as well as the inclination to make correct lifecycle decisions for your organization requires diligence on behalf of the organization to not only provide adequate training to staff, but also to supervise and enforce correct application of policy.

In many cases, there are well-defined and understood rules for making lifecycle decisions. These sets of rules are usually referred to as an organization's "information management policies".

Information management policies are used to manage the information lifecycle for an organizations content. These typically include policies governing information compliance that are usually designed by the records manager or compliance officer for an organization.

Information management policies may also include procedures for the removal of obsolete content in an organization. These parts of policies are typically system specific and are often designed by the IT department. These could include for example, policies regarding how long email content should be retained in employee's mail boxes. This retention time though is not a result of legislation, rather it may be an attempt to save storage costs.

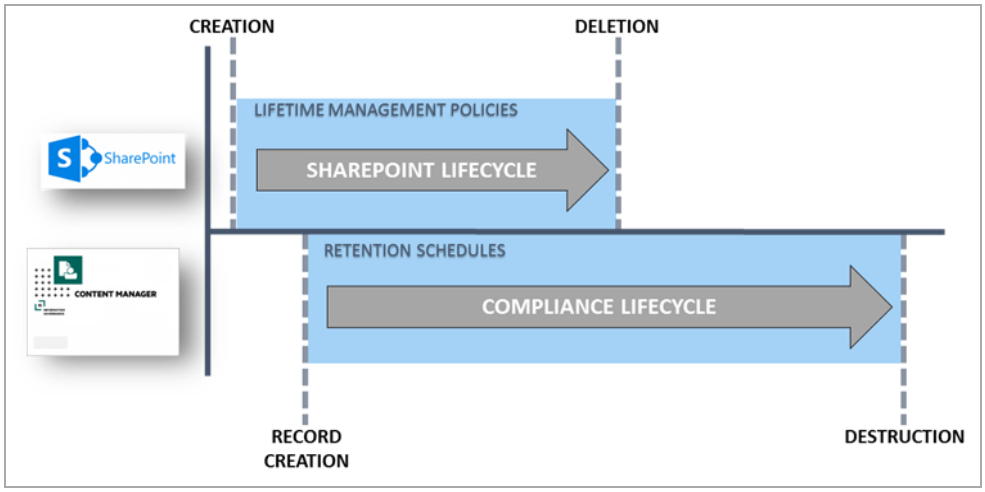
We can consider that the information management policy for an organization comprises two parts:

- Governance and Compliance policies: what must the organization do to comply with relevant legislation as well as internal business practices.
- Application specific policies: how long does the organization store information in a specific system before removing it to reduce maintenance and storage costs.

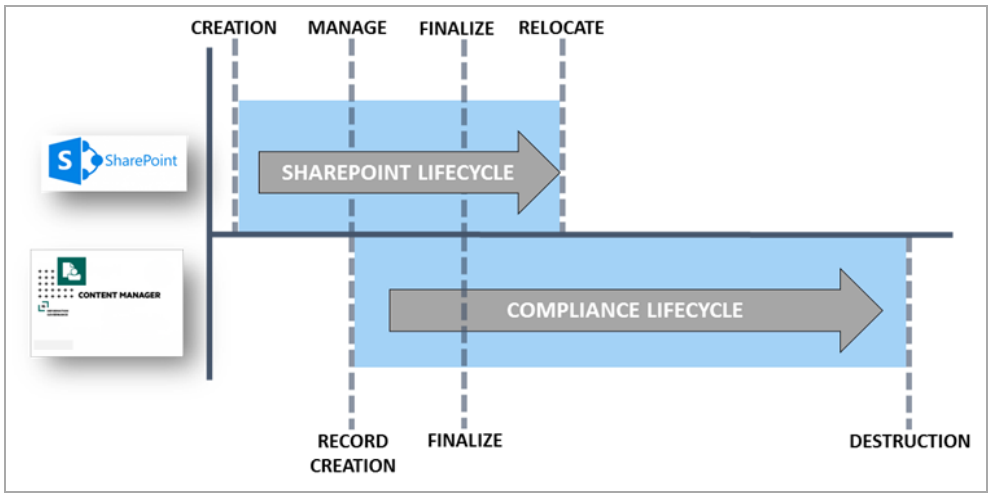
When equating to SharePoint, these two policies equate to management of the SharePoint and Compliance lifecycles.

Content Manager provides ***Retention Schedules*** for management of the compliance lifecycle. See the Content Manager documentation for details regarding retention schedules.

Content Manager for SharePoint provides ***Lifetime Management Policies*** (LMPs) for management of the SharePoint lifecycle.



LMPs include the ability to trigger the compliance lifecycle. The core processes (***manage-finalize-relocate-archive)*** can all be triggered by the LMP.



Lifetime management policies allow the automation of the application specific policy for SharePoint as well as automating the commencement of the compliance lifecycle. This allows lifecycle decisions to automatically be made based on the rules specific to an organization. Removing the requirement for SharePoint users to make these decisions removes the potential for human error and significantly reduces the likelihood of the adverse consequences associated with them.

12.1.2 Lifetime management policies (LMPs)

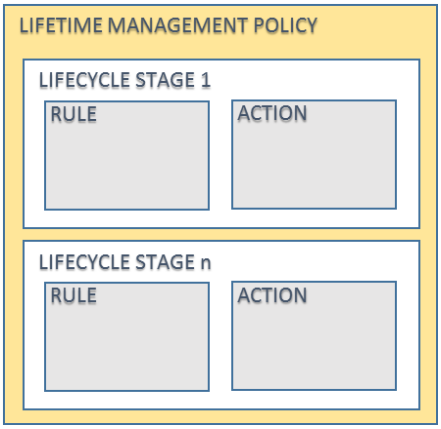
A lifetime management policy is used to define:

- When the compliance lifecycle should start
- How long content should be retained in SharePoint

It is a collection of rules that can be thought of as set of conditions that when true, initiate a specific action. For example, when a document in a document library has not been modified for more than a month, manage it with Content Manager.

Lifecycle stages

Each set of conditions and actions is called a ***Lifecycle Stage*** (LS). An LMP must have at least one LS but can have many.



Lifecycle stages are processed sequentially. The second LS will not be processed until the first LS has been completed. If the first LS never completes, then any subsequent LS will not be processed.

Rules

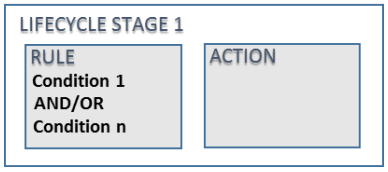
Each LS includes a rule. A rule can consist of zero to many conditions. These conditions can use the AND or the OR grouping. When the AND grouping is used, all conditions must be met for the rule to be considered "matured". For example, a rule with the following conditions would not be considered mature unless both conditions were true:

```
Title Begins with "Policy" AND Date Last Modified Older than 2 weeks
```

When the OR grouping is used, the rule is considered "matured" if any of the conditions are true. For example, a rule with the following conditions would be considered mature as soon as either of the conditions were true:

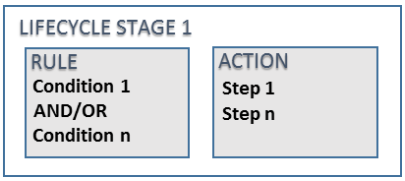
```
Title Begins with "Policy" OR Date Last Modified Older than 2 weeks
```

It is also acceptable to not specify any conditions for the rule. A rule with no conditions will be considered immediately mature. This is useful if the LMP being defined needs to immediately execute an action.



Actions

When a rule is mature, the action associated with the LMP is processed. An action can contain one or many steps. Each step that is specified is executed in the order that it appears on the LS.



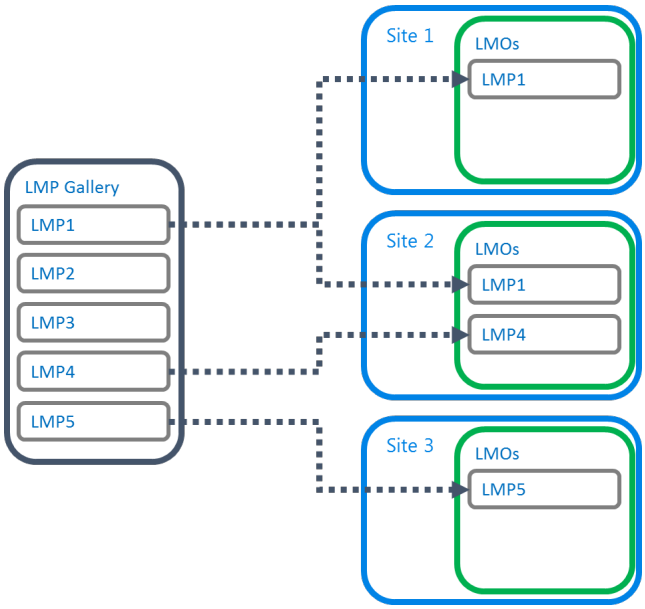
The LMP gallery

The collection of LMPs available for use in the site are defined in the ***Lifetime Management Policies Gallery,*** accessed from the app start page. This gallery is used to manage the creation, editing and deletion of LMPs used by your organization.

12.1.3 Applying LMPs

Defining a LMP in the LMP gallery does not apply the LMP to any content in SharePoint. The LMP gallery is merely the collection of LMPs that you can apply.

Lifetime Management Options (LMOs) are where you apply LMPs. LMOs can be set at site or list level and can contain multiple LMPs that have been defined in the LMP gallery.



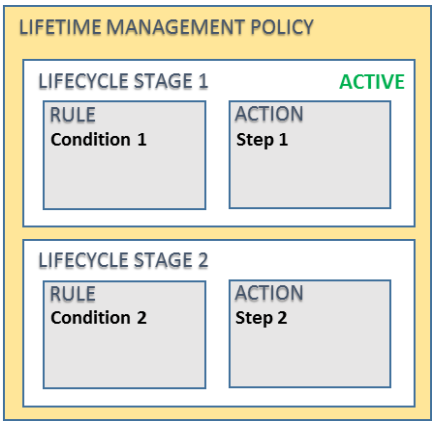
Only the locations where you add a LMP to the LMOs will the LMP be executed.

For more detail on how to apply LMPs to child sites and lists without having to specifically set LMOs, see Applying LMPs to sites and Applying LMPs to lists.

12.1.4 How LMPs are executed

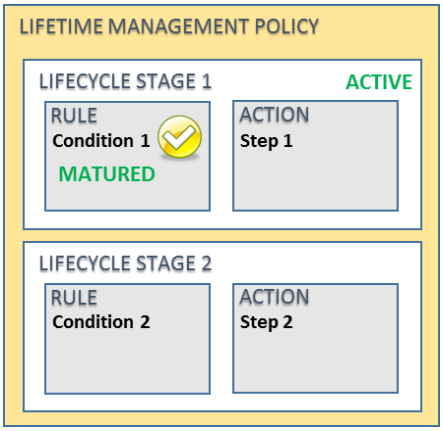
When a LMP is applied to content, it is applied in a logical and predictable way. Understanding how LMPs are applied can assist in the design of LMPs.

Consider the following LMP with two lifecycle stages:



When first applied, the first lifecycle stage is considered to be the ***Active*** stage. Only this stage is examined.

The condition/s associated with the rule are examined and if they are met, the rule is considered to be ***matured***.

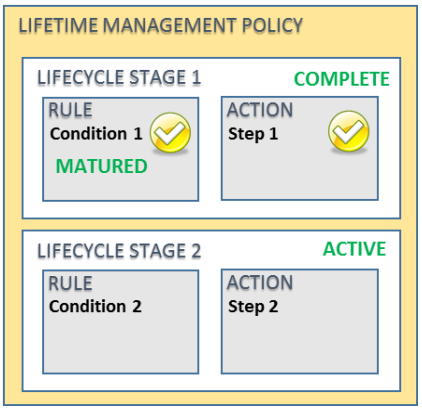


If at the time of examining the rule, conditions are not met, one of the following occurs:

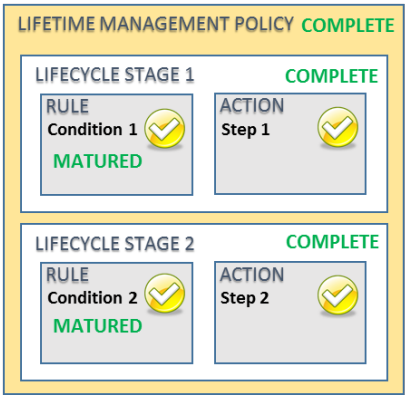
In the case that the conditions do not include date or time based conditions, the maturity of the rule is not assessed again until something changes. For example, if the rule contained the condition "***Title contains all of Policy***", then there is no reason to reassess the condition until the title changes.

If the conditions include date or time-based conditions, a task is recorded to reassess the maturity of the rule in future. For example, consider the case where the rule contained a condition "***Date Created Older than 3 months***". If the date created is *1 Aug 2014* and todays date is *1 Sep 2014*, then the item is only 1 month old. It will not be older than 3 months until *2 Nov 2014*. There is therefore no point in checking the maturity of this rule again until that date.

When a rule is found to be mature, the steps defined in the action are executed. Once all steps in the action have been executed, the lifecycle stage is considered ***complete***. The next lifecycle stage in the LMP becomes the ***active*** stage.



This lifecycle stage is processed in the same manner as the previous stage until it is complete. Once all lifecycle stages for a LMP are completed, the LMP is considered to be complete.



12.2 Defining a LMP

12.2.1 The LMP gallery

The LMP gallery contains the collection of LMPs that are available for use and application.

Accessing the gallery

From the app start page, access the **Lifetime Management Policies** link in the **Lifetime Management** section.

> **NOTE:** You must have **manage site** permission to access the LMP gallery.

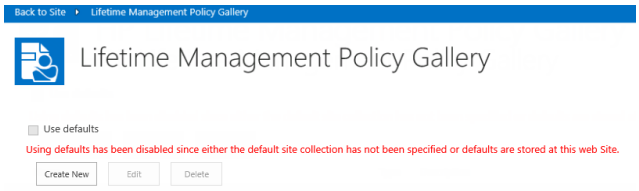
The LMP gallery page is displayed:

Using defaults

The LMP gallery is suitable for publishing from the default site collection. If **Use defaults** is checked, then only the LMPs defined in the default site can be used. It is not possible to edit LMPs or add new LMPs if using defaults.

If you deselect **Use defaults**, a copy of all default LMPs will be placed into the LMP gallery for this site. Editing existing LMPs and creating new LMPs is permitted if not using the defaults.

If you are viewing the LMP gallery on the default site collection, the **Use defaults** checkbox will be disabled.

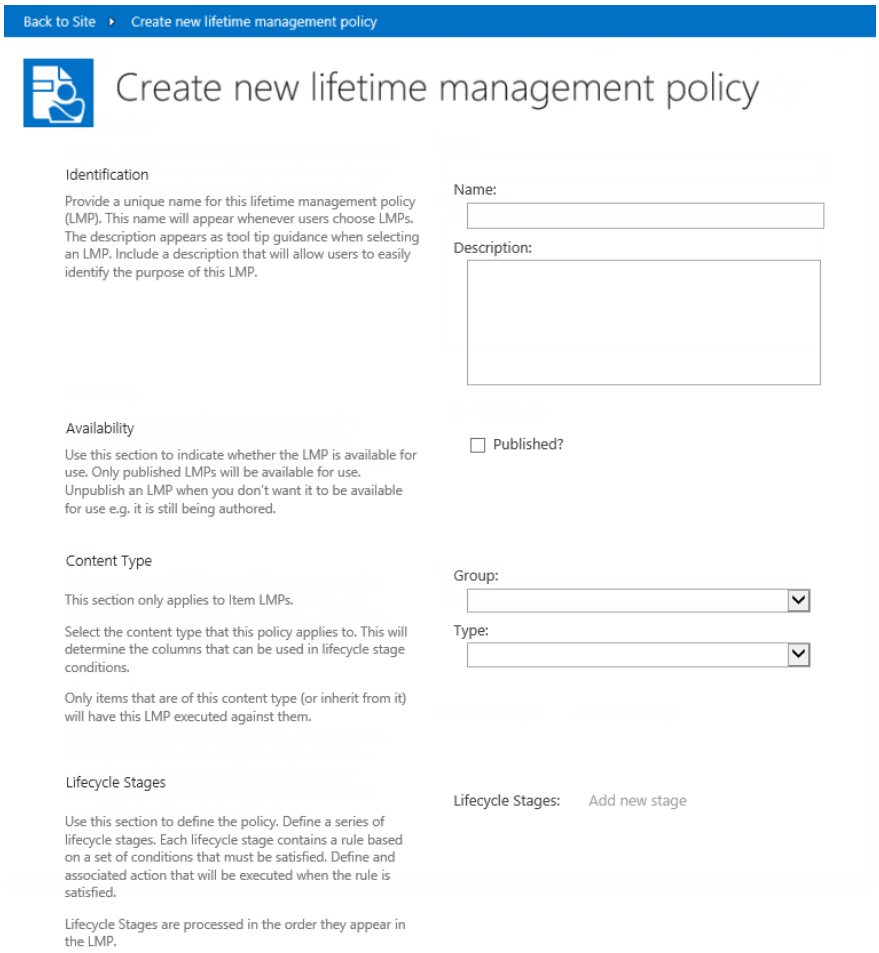


12.3 Creating a LMP

To create a new LMP, follow these steps:

In the LMP gallery page, click **Create New**.

The **Create new lifetime management policy** page is displayed.



12.3.2 Identification

The identification section of the page includes the values that will be used to identify a LMP.

The name of the LMP will be used to identify the LMP in the LMP gallery and also in dialogs that allow selecting LMPs. Use a name that will allow users to readily identify the correct LMP to use.

> **NOTE:** Duplicate names for LMPs are not prevented.

The description is used as the description in the LMP gallery as well as the tool tip used in dialogs that allow selecting LMPs. Provide a descriptions that will allow users to understand the intention of the LMP so that users can readily identify the correct LMP to use.

12.3.3 Availability

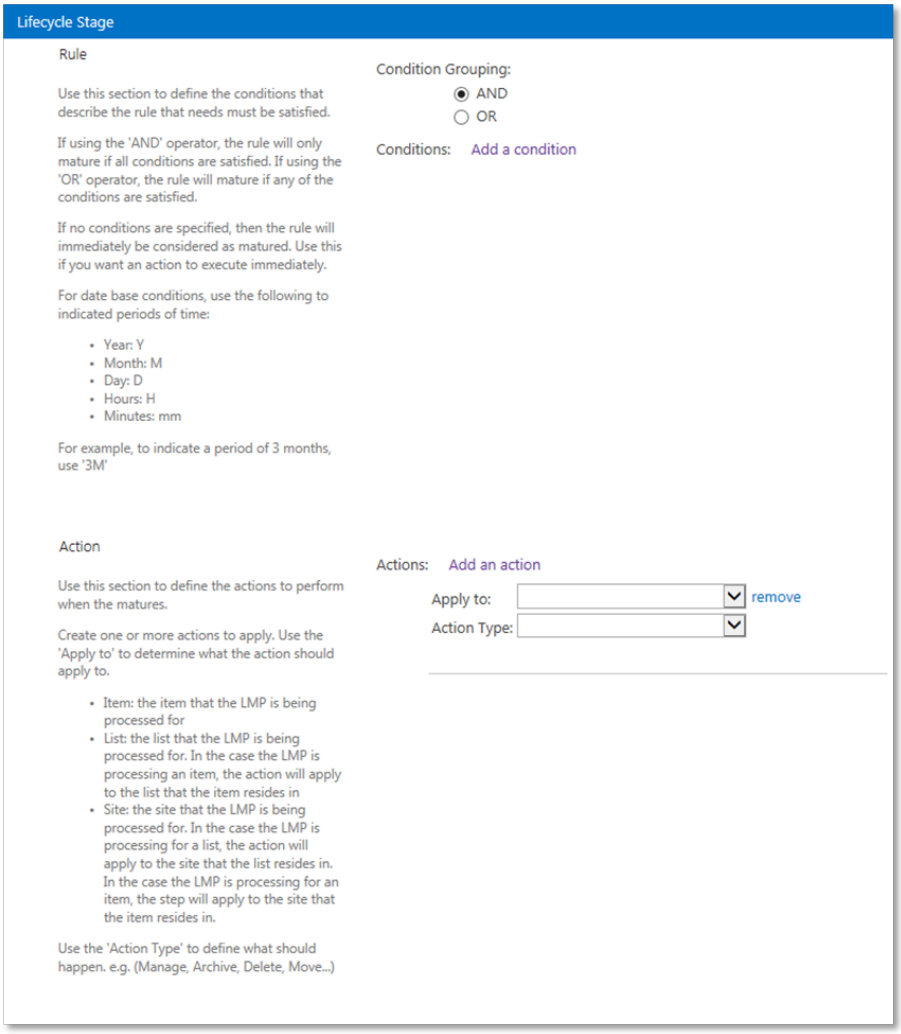
The availability section of the page is used to indicate if a LMP in the gallery is available for use. Only if the **Published?** checkbox is checked will this LMP be made available for selection.

All LMPs, regardless of the value of this checkbox are visible in the LMP gallery.

12.3.4 Adding a lifecycle stage

Once a LMP type has been selected (as well as content type if the ***Item*** LMP type is selected) on the **Create new lifetime management policy** page, The **Add new stage** link is enabled.

Clicking this link displays the **Lifecycle Stage** dialog.



12.3.5 Defining a rule

Each lifecycle stage includes a rule. Only when the rule has been satisfied will the associated action for that stage be executed.

> **NOTE:** When all conditions are satisfied, the rule is said to be "**matured**".

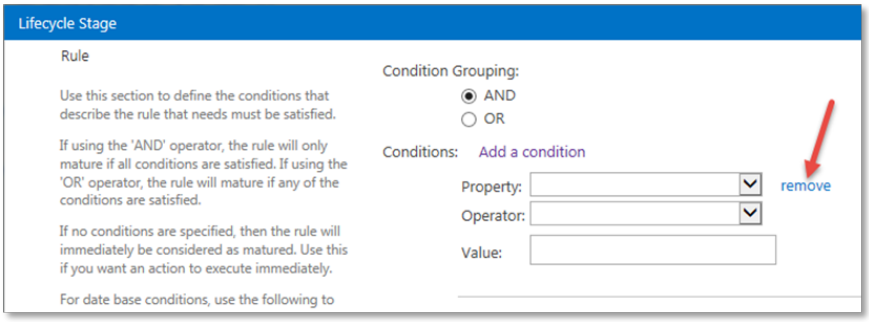
A rule can have zero to many conditions that make up to rule. These conditions are grouped either as ***AND*** conditions or ***OR*** conditions. If ***AND*** is used, then all conditions defined must be satisfied for the rule to be matured. If ***OR*** is used, if at least one of the conditions is satisfied, the rule is considered to be matured.

The condition grouping is set using the radio buttons at the top of the page.

To add a condition to the rule, click the **Add a condition** link.

To add additional conditions, click the **Add a condition** link again.

To remove a condition from the rule, click the **Remove** link.



A condition consists of three elements:

1. Property: what property should be examined to determine the current value
2. Operator: how should the selected property value be compared
3. Value: what value should the selected property value be compared to

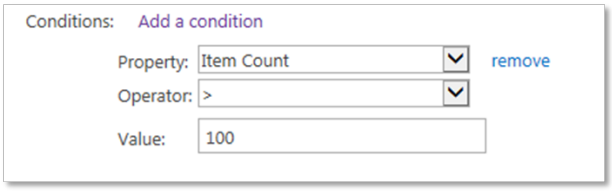
For example, if the condition required is that the list must have more than 100 items in it, this could be written as:

```
Item count > 100
```

In this example the three elements of the condition are:

1. Property = Item count
2. Operator = greater than (>)
3. Value = 100

The condition would therefore be as follows:



NOTE: The subsequent sections cover the properties that are available.

The values available for selection will vary depending on the data-type of the selected property.

Understanding when rule maturity is calculated

Rule maturity for the current lifecycle stage is checked in the following scenarios:

1. When the LMP is initially applied to content
2. When an item is added
3. When an item is modified
4. At a calculated time that time based conditions may have matured

Date based conditions

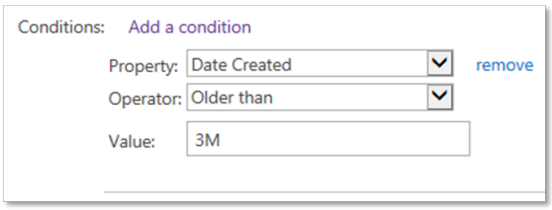
Date based properties provide the following operators that can be used:

- Older than
- Younger than
- =

When using the ***Older than*** or ***Younger than*** operators, you must specify a duration. For example, if the requirement was:

```
Item is more than 3 months old
```

This would equate to the following condition:



Use the following characters to indicate the units of time that a duration represents:

- Year: Y
- Month: M
- Day: D
- Hours: H
- Minutes: mm

If using the **=** operator, then the value specified must be an exact date. The format of the date must be:

```
dd mmm yyyy
```

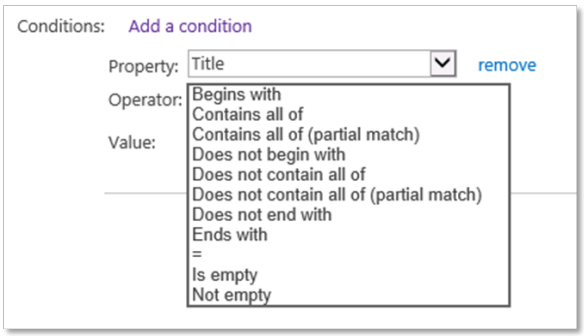
For example:

```
14 Apr 2014
```

> **NOTE:** In the current version, when exact dates are entered, they must use the format specified in the regional settings that the OS is configured to use on the Content Manager server. Dates entered in other formats will not be correctly recognized.

Text based conditions

Text based conditions have special text based operators.



Most of these operators are self explanatory. An operator that uses ***partial match*** will return true if the value partially matches it. For example, consider the following condition:

```
Title Contains all of (partial match) with
```

This condition will return true if the title contains words such as:

- With
- Withheld
- Withhold
- With
- Herewith

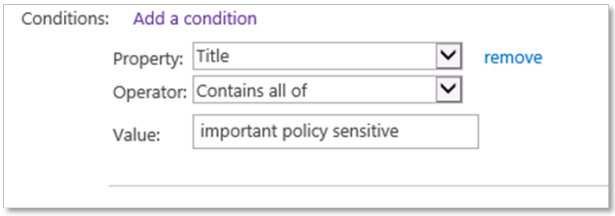
Whereas consider the condition:

```
Title Contains all of with
```

This condition will return true if the title contains the exact word “with”

Text based conditions allow the entry of multiple words into the value.

When a value contains multiple words, these words should be separated by a space. For example, for a condition where the title contains the words “important” and “policy” and “sensitive” the condition would look like:



Managed metadata based conditions

Managed metadata based columns allow the entry of one or more values. These values must be separated by a semicolon. This is different to text based fields as it is possible that a managed metadata term actually contains a space.

Using the "=" operator with management metadata actually executes the ***Contains all of*** operator. This is to account for the fact that when selecting multiple metadata values, the user can select in any order. For example, if selecting from a list of colors, "red;blue" is the same as "blue;red". If a true "=" comparison was used, these would not be equated as the same thing.

People or group base conditions

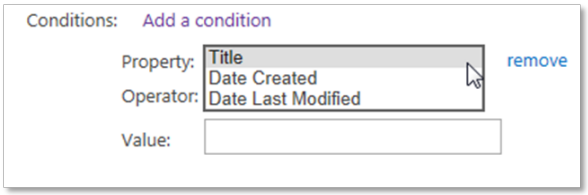
When creating conditions based on columns that use the ***People or Group*** type, the following rules should be applied when entering the value:

- AD groups must be entered in the format ***domain\group***
- AD users must be entered in the format ***username***
- SharePoint groups must have the group title entered

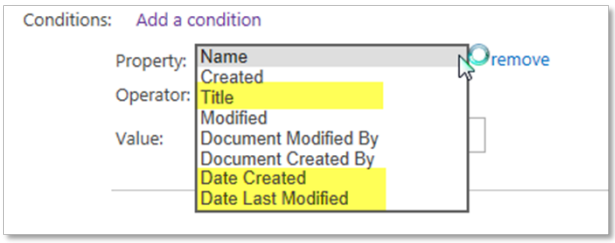
Item properties

The properties that are available for selection in the property dropdown for an Item LMP are based on the content type that was selected for the LMP. All properties for a content type will be available, including inherited properties.

For example, the following properties are available if the ***Item*** content type is selected:



If the ***Document*** content type is selected, because this inherits from the ***Item*** content type, the properties of the ***Item*** content type are available for selection:



It is important to choose the right content type if this LMP is an ***Item LMP***. Not only does this determine which list items the LMP will apply to, but it determines what properties you can create conditions based on.

List properties

If the LMP being authored is a ***List LMP***, then the properties available for use in conditions are a subset of the properties of the list itself. The following sections describe the properties that are available.

Title

The title is the name of the list. The name of a list can be found by accessing list settings through SharePoint then choosing the ***List name, description and navigation***.

> **NOTE:** You use this property, unlike other non-date-based properties, the condition maturity is based on the value of the title at the time the LMP is applied to the list. If the title is subsequently changed, this will not trigger reassessment of the condition.

Date Created

This is the date that the list was first created. For example, this property could be used to archive lists that are older than 12 months.

Date Last Modified

This is the last date that any list item in the list was added, deleted or modified. For example, this property could be used to archive lists that have not been modified for 12 months.

Item Count

This property is based on the number of list items that reside in a list. For example, this property could be used to archive lists once they exceed 10,000 items.

Custom templates

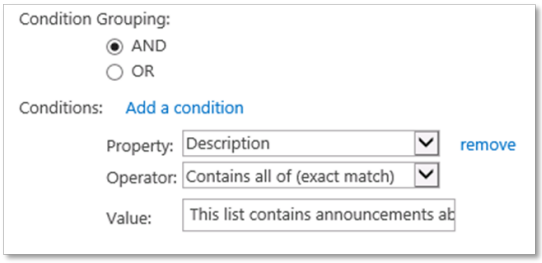
When you save a list as a template in SharePoint, the template ID is always the same, therefore it is impossible to differentiate custom templates based on the template ID. Instead, the ***Description*** of the list should be used.

Any syntax that suits your organization can be used to identify that a list is of a particular template. For example, the description of all announcements lists on the SharePoint farm might begin with:

This list contains announcements about…

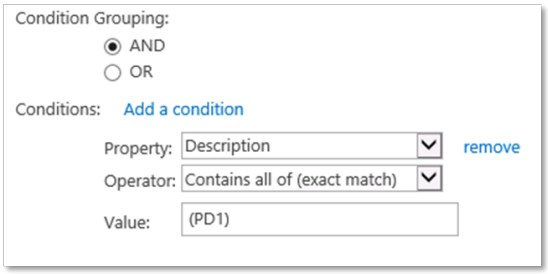
Unfortunately, description is not a property that is saved to list templates. Therefore, if using custom list templates, it will be necessary to ensure that the identifier is included in the description of each created list. When saving site templates however, description is included with the site lists and is therefore automatically added to new lists when a site of that template is created.

An LMP can then be defined identifying that if the description starts with this text, consider it to contain announcements.



Alternatively, it is possible to embed your own template identifier in the description. For a document library containing project documents, you could for example use a custom identifier ***(PD1)***. The template could include in the standard description instructions to retain this identifier:

An LMP condition could search the list description for the value ***(PD1)***.



Template ID

The template ID allows specifying the list template that is in use. This allows assigning conditions that will only ever mature if the list is of a particular type. For reference, the following is the list of standard templates that are in use in SharePoint:

AccessRequest	**Access Request List.**	**160**
AdminTasks	Administrator Tasks	1200
Agenda	Agenda (Meeting)	201
Announcements	Announcements	104
CallTrack	Call Track	404
Categories	Categories (Blog)	303
Circulation	Circulation	405
Comments	Comments (Blog)	302
Contacts	Contacts	105
CustomGrid	Custom grid for a list	120
DataConnectionLibrary	Data connection library for sharing information about external data connections	130

AccessRequest	**Access Request List.**	**160**
DataSources	Data sources for a site	110
Decision	Decisions (Meeting)	204
DeveloperSiteDraftApps	Draft Apps library in Developer Site	1230
DiscussionBoard	Discussion board	108
DocumentLibrary	Document library	101
Events	Calendar	106
ExternalList	External	600
Facility	Facility	402
GanttTasks	Project Tasks	150
GenericList	Custom list	100
HealthReports	Health Reports	1221
HealthRules	Health Rules	1220
HelpLibrary	Help Library	151
Holidays	Holidays	421
HomePageLibrary	Workspace Pages (Meeting)	212
IMEDic	IME (Input Method Editor) Dictionary	499
InvalidType	Not used	-1
IssueTracking	Issue tracking	1100
Links	Links	103
ListTemplateCatalog	List template gallery	114
MaintenanceLogs	Maintenance Logs Library	175
MasterPageCatalog	Master Page gallery	116
MeetingObjective	Objectives (Meeting)	207
Meetings	Meeting Series (Meeting)	200
MeetingUser	Attendees (Meeting)	202
NoCodePublic	No Code Public Workflow	122
NoCodeWorkflows	No Code Workflows	117

AccessRequest	Access Request List.	160
NoListTemplate	unspecified list type	0
PictureLibrary	Picture library	109
Posts	Posts (Blog)	301
SolutionCatalog	Solutions	121
Survey	Survey	102
Tasks	Tasks	107
TasksWithTimelineAndHierarchy	Tasks with Timeline and Hierarchy	171
TextBox	Text Box (Meeting)	210
ThemeCatalog	Themes	123
ThingsToBring	Things To Bring (Meeting)	211
Timecard	Timecard	420
UserInformation	User Information	112
WebPageLibrary	Wiki Page Library	119
WebPartCatalog	Web Part gallery	113
WebTemplateCatalog	Site template gallery	111
Whereabouts	Whereabouts	403
WorkflowHistory	Workflow History	140
WorkflowProcess	Custom Workflow Process	118
XMLForm	XML Form library	115

Site properties

If the LMP being authored is a “Site” LMP, then the properties available for use in conditions are a subset of the properties of the site itself. The following sections describe the properties that are available.

Title

The title is the name of the list. The name of a list can be found access list settings through SharePoint then choosing the “List name, description and navigation”.

> **NOTE:** You use this property, unlike other non date based properties, the condition maturity it is based on the value of the title at the time the LMP is applied to the list. If the title is subsequently changed, this will not trigger reassessment of the condition.

Date Created

This is the date that the site was first created. This property could be used for example to archive sites that are older than 12 months.

Date Last Modified

This is the last date that any list item in the site was added, deleted or modified. This property could be used for example to archive sites that have not been modified for 12 months.

Web Template

The web template is the ID of the site template that was used to create the site. The following table lists that template IDs used for standard SharePoint sites:

> **NOTE:** A known issue in 8.1 causes these template IDs to not be recognized correctly. This is fixed in the 8.1ML release.

Template ID	Title
GLOBAL#0	Global template
STS#0	Team Site
STS#1	Blank Site
STS#2	Document Workspace
MPS#0	Basic Meeting Workspace
MPS#1	Blank Meeting Workspace
MPS#2	Decision Meeting Workspace
MPS#3	Social Meeting Workspace
MPS#4	Multipage Meeting Workspace
CENTRALADMIN#0	Central Admin Site
WIKI#0	Wiki Site
BLOG#0	Blog
SGS#0	Group Work Site
TENANTADMIN#0	Tenant Admin Site
APP#0	App Template
APPCATALOG#0	App Catalog Site
ACCSRV#0	Access Services Site

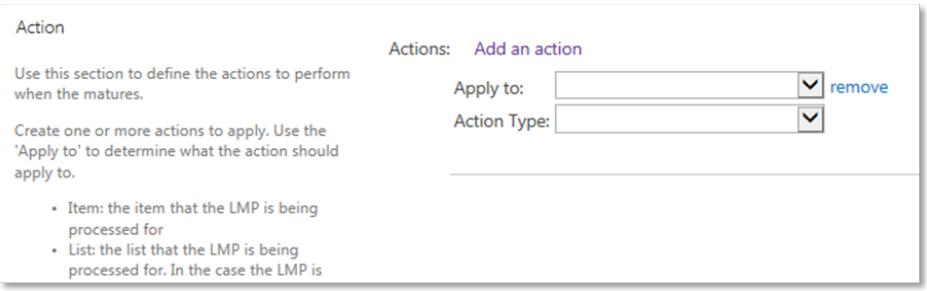
Template ID	Title
ACCSRV#1	Assets Web Database
ACCSRV#3	Charitable Contributions Web Database
ACCSRV#4	Contacts Web Database
ACCSRV#5	Projects Web Database
ACCSRV#6	Issues Web Database
ACCSVC#0	Access Services Site Internal
ACCSVC#1	Access Services Site
BDR#0	Document Center
DEV#0	Developer Site
DOCMARKETPLACESITE#0	Academic Library
EDISC#0	eDiscovery Center
EDISC#1	eDiscovery Case
OFFILE#0	(obsolete) Records Center
OFFILE#1	Records Center
OSRV#0	Shared Services Administration Site
PPSMASite#0	PerformancePoint
BICenterSite#0	Business Intelligence Center
SPS#0	SharePoint Portal Server Site
SPSPERS#0	SharePoint Portal Server Personal Space
SPSPERS#2	Storage And Social SharePoint Portal Server Personal Space
SPSPERS#3	Storage Only SharePoint Portal Server Personal Space
SPSPERS#4	Social Only SharePoint Portal Server Personal Space
SPSPERS#5	Empty SharePoint Portal Server Personal Space
SPSMSITE#0	Personalization Site
SPSTOC#0	Contents area Template
SPSTOPIC#0	Topic area template
SPSNEWS#0	News Site

Template ID	Title
CMSPUBLISHING#0	Publishing Site
BLANKINTERNET#0	Publishing Site
BLANKINTERNET#1	Press Releases Site
BLANKINTERNET#2	Publishing Site with Workflow
SPSNHOME#0	News Site
SPSSITES#0	Site Directory
SPSCOMMU#0	Community area template
SPSREPORTCENTER#0	Report Center
SPSPORTAL#0	Collaboration Portal
SRCHCEN#0	Enterprise Search Center
PROFILES#0	Profiles
BLANKINTERNETCONTAINER#0	Publishing Portal
SPSMSITEHOST#0	My Site Host
ENTERWIKI#0	Enterprise Wiki
PROJECTSITE#0	Project Site
PRODUCTCATALOG#0	Product Catalog
COMMUNITY#0	Community Site
COMMUNITYPORTAL#0	Community Portal
SRCHCENTERLITE#0	Basic Search Center
SRCHCENTERLITE#1	Basic Search Center
SRCHCENTERFAST#0	FAST Search Center
visprus#0	Visio Process Repository

12.3.6 Adding an action

When a rule is considered mature, the corresponding action is executed. This action can contain one or more steps. Each step requires specifying what action to take and what to apply the action to.

For a new lifecycle stage, a blank action will be placed in the “Action” section of the page.



Use the **Add an action** link to add new steps to the action.

Use the **remove** link to remove a step from the action.

Apply to

The selection made in the **Apply to** drop down, governs what the action will be applied to.

- Item: the action will be performed on the item that this LMP is executing on
- List: the action will be performed on the list that the LMP is executing on, or the list that the item the LMP is executing on resides in.
- Site: the action will be performed on the site that the LMP is executing on, or the site that the item the LMP is executing on resides in.

Action Type

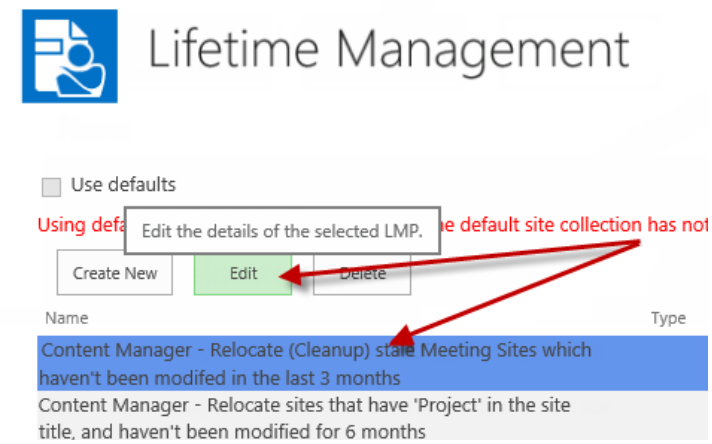
The selection made in the **Action Type** drop down governs what action will actually be performed.

- Manage: the object selected in the **Apply to** drop down will be managed
- Finalize: the object selected in the **Apply to** drop down will be finalized
- Relocate: the object selected in the **Apply to** drop down will be relocated
- Archive: the object selected in the **Apply to** drop down will be archived
- Delete permanently: the object selected the **Apply to** drop down will be deleted permanently (this action is only available for items, not for lists or sites)

12.4 Modifying a LMP

12.4.1 Editing an existing LMP

In the case where an existing LMP must be modified, this can be done from the LMP Gallery. Select the LMP to modify and click **Edit**.



The **Edit lifetime management policy** page is displayed. Use this page to modify the details of the LMP and save it when completed.

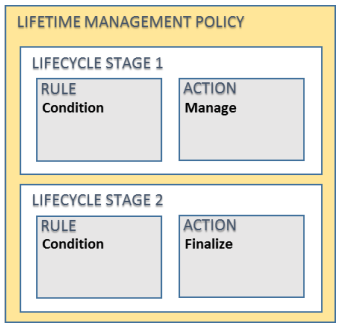
> **NOTE:** You are not permitted to change the type of a LMP after it has been saved. Create a copy of the LMP instead and modify the type on the copy.

12.4.2 Implications of changing an existing LMP

If you change an existing LMP that is currently not applied to any lifetime management options, there are no implications to consider.

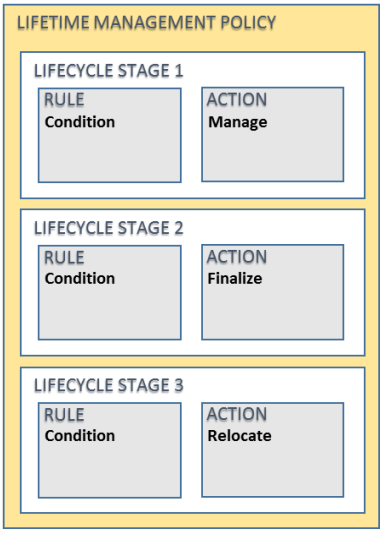
However, if a LMP is already applied to lifetime management options, the LMP may already be in progress. The modified LMP behavior may appear to be applied inconsistently depending on what lifecycle stage the LMP is up to.

For example, consider a LMP that has two lifecycle stages.



This LMP is applied to items in a list. Item 1 has completed both lifecycle stages and has been finalized. The execution of the LMP against that item is completed.

The LMP is then modified to include a new lifecycle stage that relocates items.

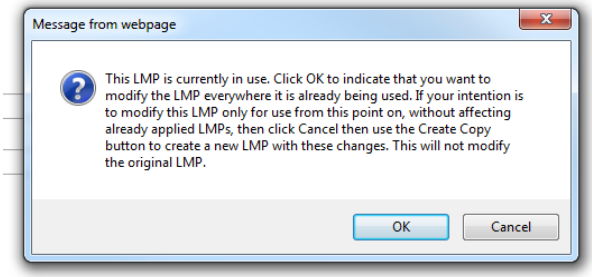


Any new items added to the list, or items that have not yet completed lifecycle stage 2 will be relocated. Any items that have had the LMP previously completed, will not have the new lifecycle stage retrospectively applied and will therefore not be relocated.

Similarly, if changes to the conditions on lifecycle stage 1 were modified, any item that had previously completed lifecycle stage 1, will not be reprocessed using the updated rules.

It is important to recognize this behavior when modifying a LMP.

If you attempt to modify a LMP that is being used, you will be prompted:



See Copying a LMP for details of the copy process. By copying the LMP and creating a new one based on this original LMP, the updated LMP can be applied where necessary without affecting LMPs that have already been applied.

If you do not receive this prompt, this indicates that the LMP has not been added to any lifetime management options.

12.4.3 Considerations if using the defaults

If the site is configured to use the LMP gallery from the default site collection, there are some considerations.

Unchecking “Use defaults”

By unchecking the **Use defaults** option, this indicates that this site should have its own set of LMPs that are not the ones specified in the default site collection. When doing this, a copy of all the LMPs in

the default site collection LMP gallery is made in the site's LMP gallery.

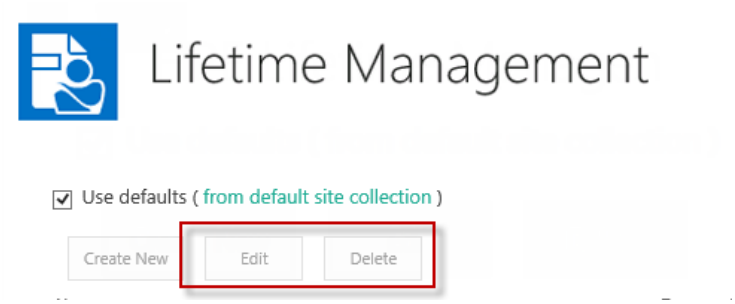
These copies are independent of the LMPs defined in the default site collection and can be deleted or modified without affecting applications of the LMP.

Creating new LMPs

You cannot create new LMPs from the LMP gallery for a site that is using defaults. If new LMPs are required, they must be added to the default site collection LMP gallery. A link to the default site collection is included after the **Use defaults** check box. This takes the use to the default site collection, not directly to the LMP gallery for that site.

Modifying existing LMPs

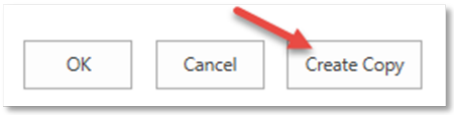
The **Edit** and **Delete** buttons are disabled in this scenario.



To modify or delete LMPs, you must navigate to the LMP gallery for the default site collection. Be aware, that this will affect any site that is using these values.

12.5 Copying a LMP

When editing a LMP, the page includes **Create Copy** button that allows you to copy the current LMP to a new LMP but does not save it. The name of the copied LMP by default will be the original name with "***- Copy***" appended to it.

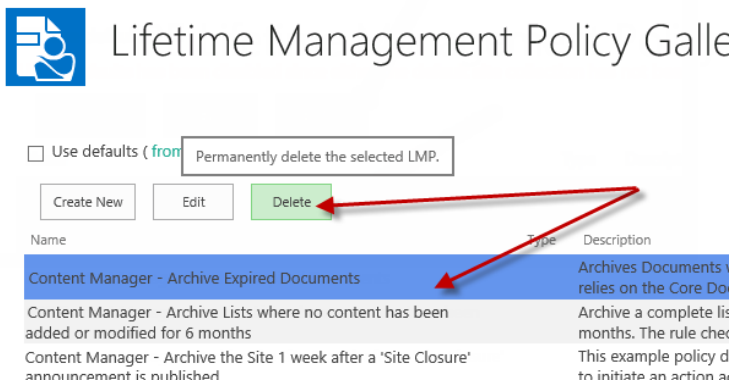


Once the copy has been modified as required, save the LMP to the gallery.

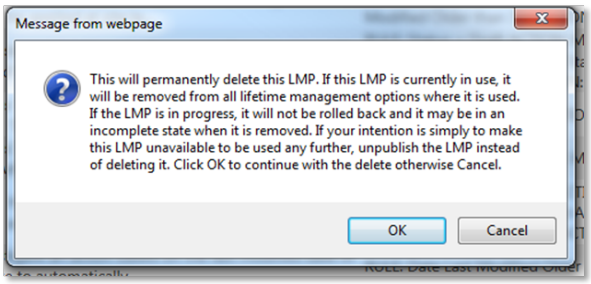
The copy functionality allows you to create new LMPs based on existing LMPs, without affecting the original one.

12.6 Deleting a LMP

It is possible to delete a LMP from the LMP gallery. Select the LMP and click **Delete**.



You will be asked to confirm the delete and provided the implications of doing this.



12.7 Included LMPs

The LMP gallery includes a number of standard LMPs. You can do the following with these LMPs:

- Use them as they are
- Modify them to suit the requirements of your organization
- Use them as samples for creating other LMPs (via Create Copy)
- Delete them if they are not required

> **NOTE:** The standard LMPs are created whenever a publish is performed using the configuration tool. See the installation guide for further details.

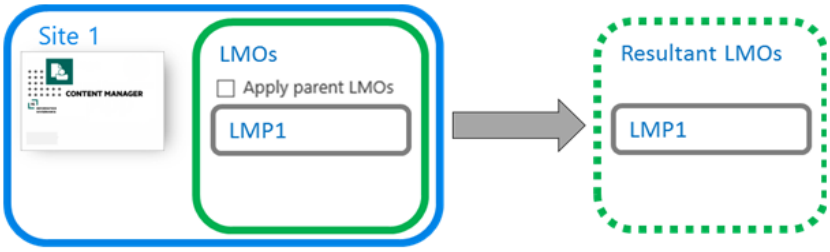
12.8 Applying LMPs to sites

12.8.1 Understanding site Lifetime Management Options (LMOs)

Specific LMOs

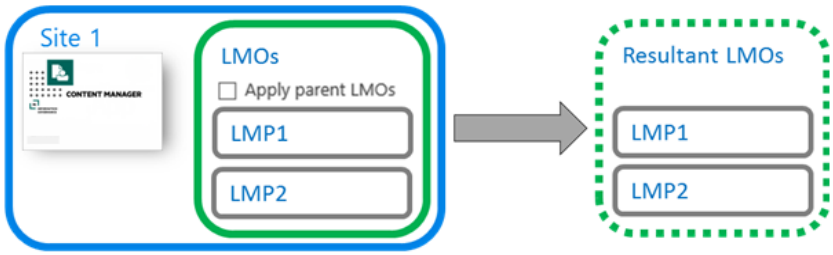
The LMP gallery allows the definition of LMPs. **Lifetime Management Options** (LMOs) allows you to indicate the content that LMPs should be applied to.

Using site LMOs, you can specify that one or more LMPs defined in the gallery should be used. For example, if the site LMOs have LMP1 added, then the result is that LMP1 will be applied to all content in the site.

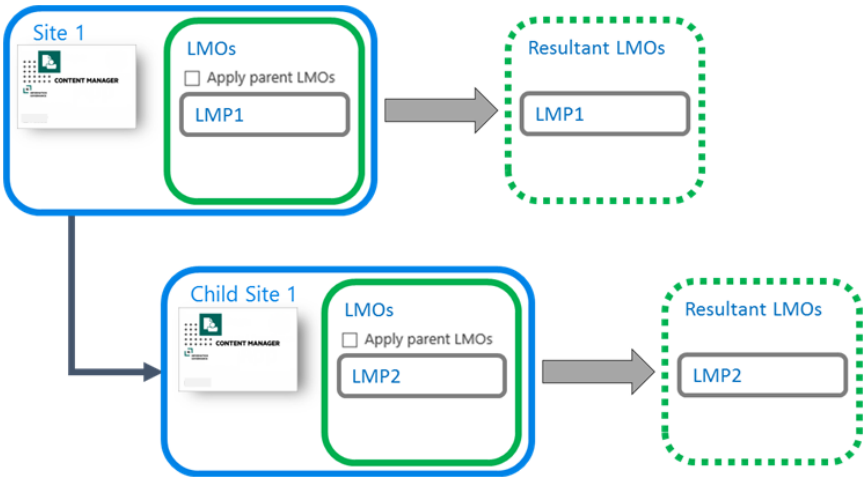


NOTE: Remember that just because a LMP is applied, it doesn't mean that it will actually perform an action on content. The content must satisfy the conditions of that LMP before the action is applied. It is therefore possible to apply LMPs at site level that will only affect a subset of content.

If multiple LMPs are added to the LMOs, all of them apply to the content of the site.

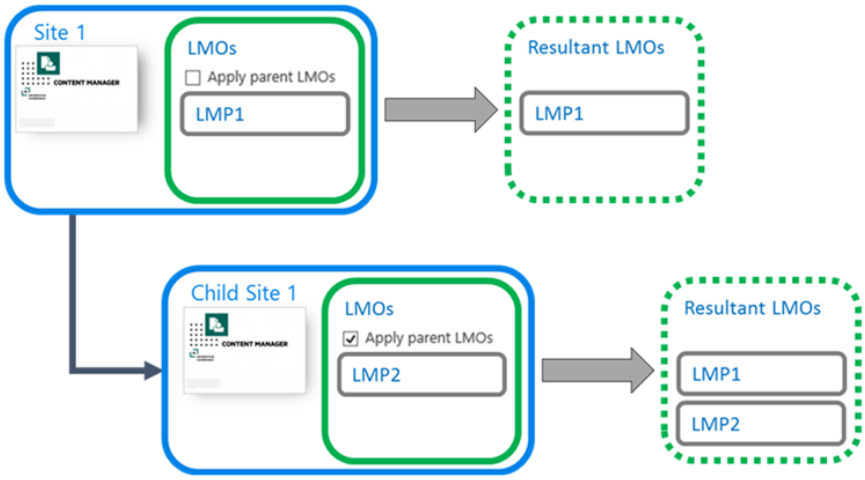


A child site can itself specify its own LMOs. In the scenario below, the child site has LMP2 applied to its LMOs. The result is that LMP2 will be applied to content on child site 1.

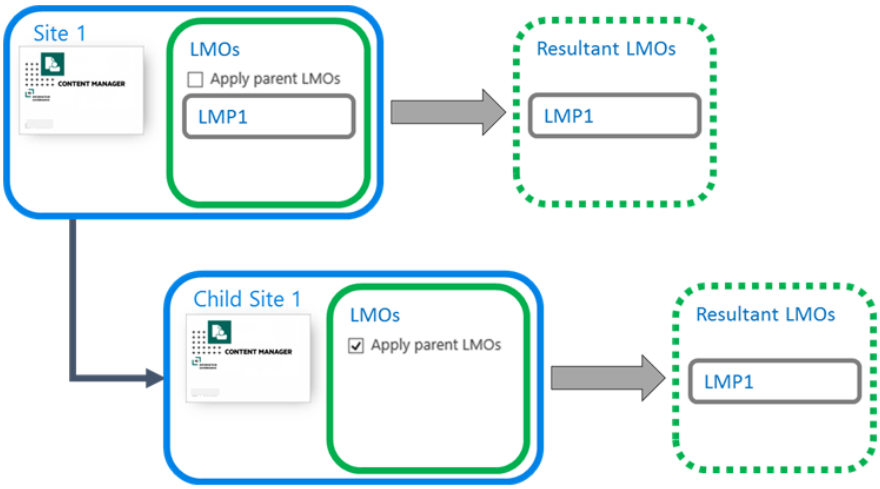


NOTE: You must have the app activated on a child site in order to edit the LMOs.

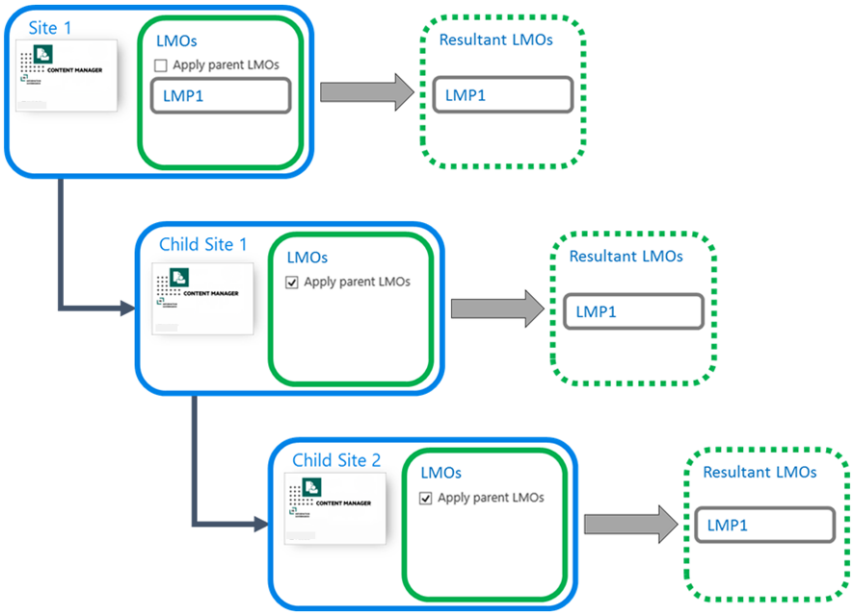
LMOs include a setting **Apply parent LMOs**. If ticked, this indicates that not only should the LMPs defined on the LMOs for the site be applied, but the LMPs defined on the parent site should also be applied.



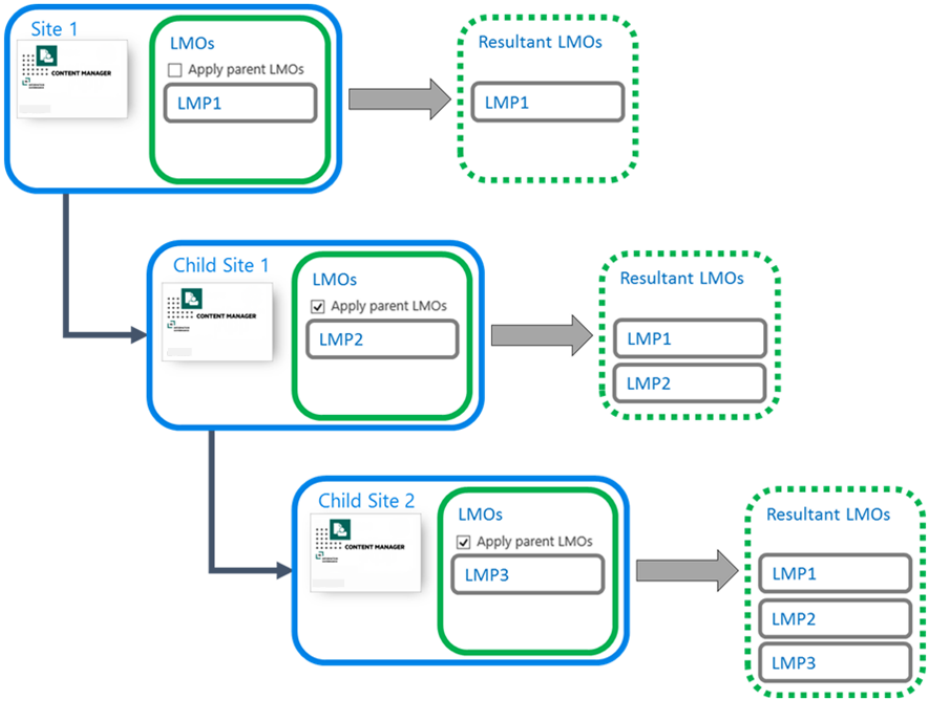
If no LMPs are included on the LMOs for a site, and **Apply parent LMOs** is ticked, the result is that only the LMPs from the parent site are applied.



The application of parent LMOs applies across multiple levels. It is not limited to just the immediate parent. Consider the following examples. In this first scenario, none of the children have any LMPs added to the LMOs. The net result is that the LMP applied at the top level is applied to all child sites.



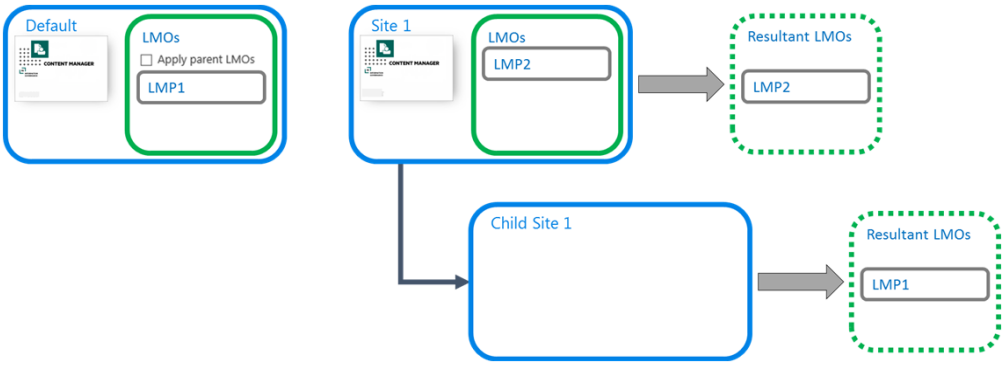
In the next scenario, each child site includes application of a LMP on the site LMOs.



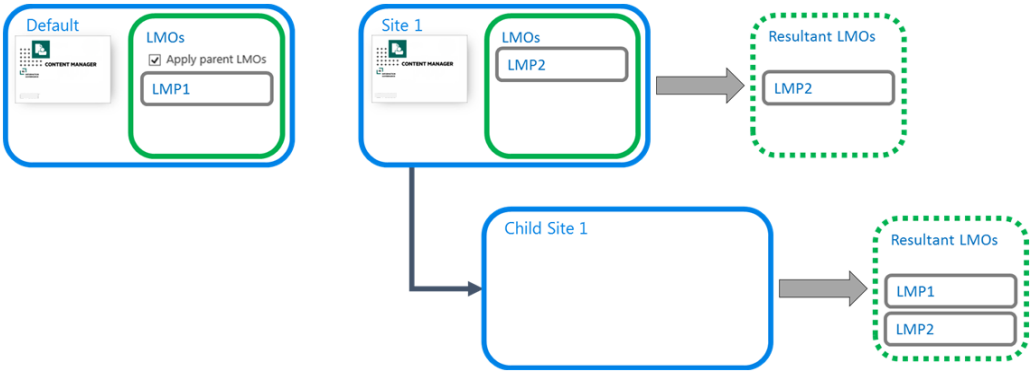
Defaulted LMOs

The LMOs for a site can also be provided by the default site collection. In this example, site 1 is set to **Use defaults**. The defaults are provided by the **Default** site collection.

If Site 1 has a child site that does not have the app added, this child site uses the default site LMOs. If the "**Apply parent LMOs**" check box is unchecked on the defaults, the LMOs of the parent site are ignored.



If the "**Apply parent LMOs**" check box is checked on the default LMOs, then the LMOs of the parent are applied.



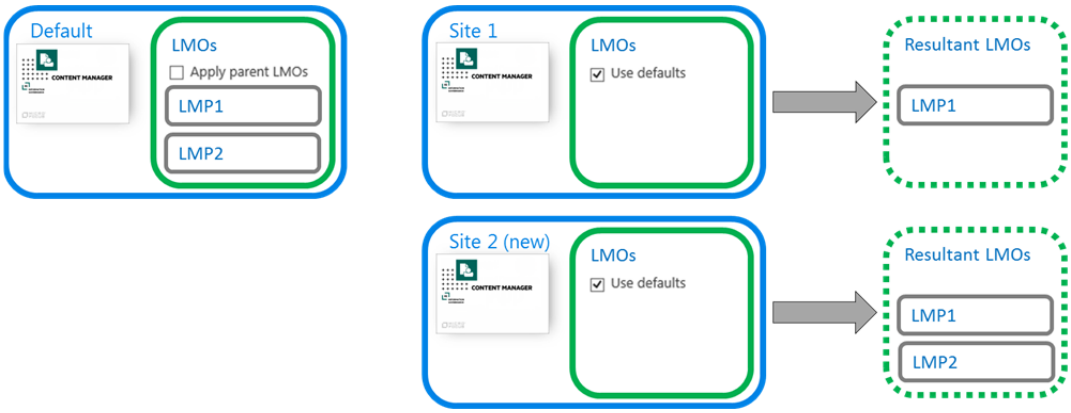
Applying changes made to default site LMOs

Consider the scenario where a site is using the default site RMOs. In this example, a single LMP has been applied to the default site LMOs.

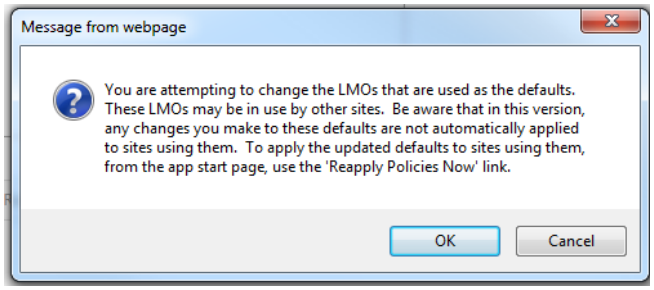
If the default site LMOs are modified e.g. a new LMP added, it may be expected that these modified LMOs are applied to sites that already have the app activated i.e.

This is not what happens

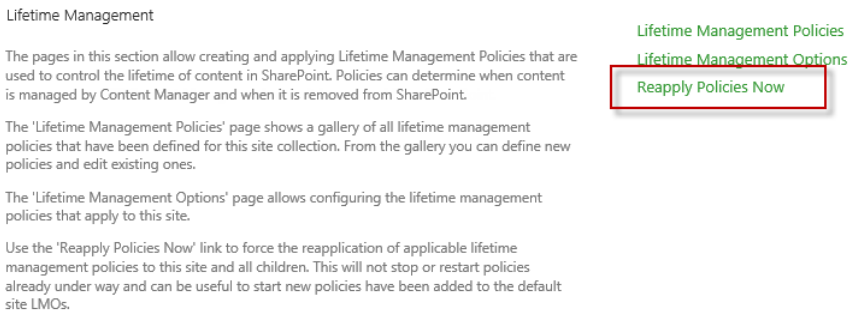
In this version of the product, any new sites will use the updated site LMOs, but sites that already had the app activated will not have the new LMOs applied.



If an attempt is made to update the default site LMOs, the user is shown the following prompt warning them of this situation.



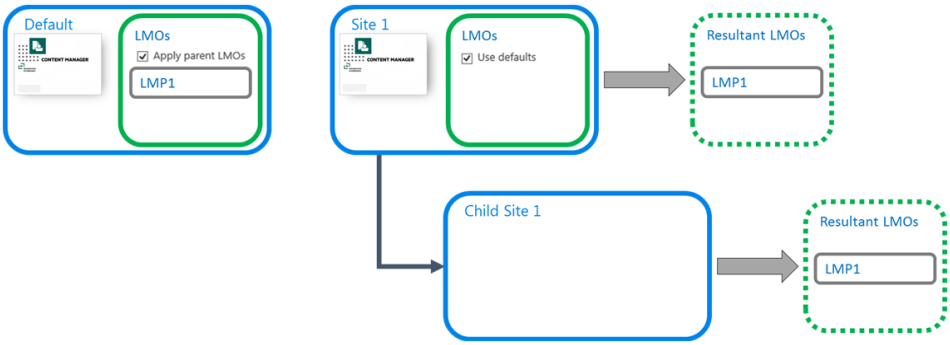
In this version, application of any changes to site LMOs in this scenario must be instigated manually. Navigate to the app start page. In the **Lifetime Management** section of the page is a link **Reapply Policies Now.**



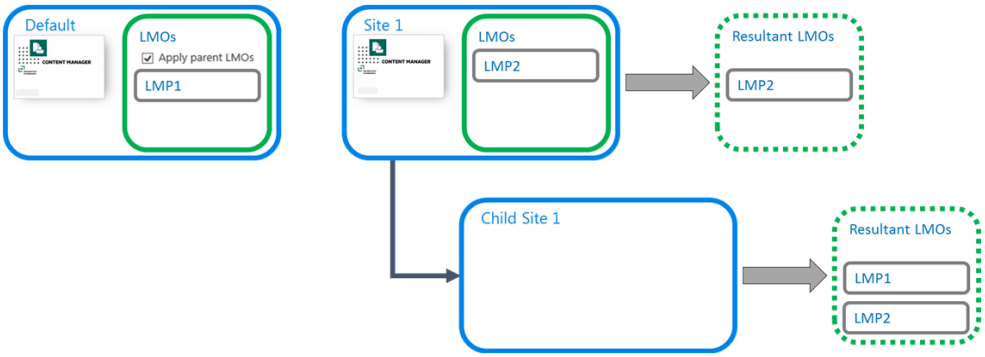
Inherited LMOs

The diagrams in this section so far have all indicated that the app is added to the child sites. This is only necessary if you intend to modify the LMOs. Without the app for example, you would not be able to add a LMP to the LMOs of a child site.

Site LMOs can be defaulted to use the LMOs specified by the default site collection. In this example, child site 1 does not have the app added therefore this child site does not have specific LMOs (as they are only available if the app is added). The resultant LMOs are the LMOs for the default site collection.

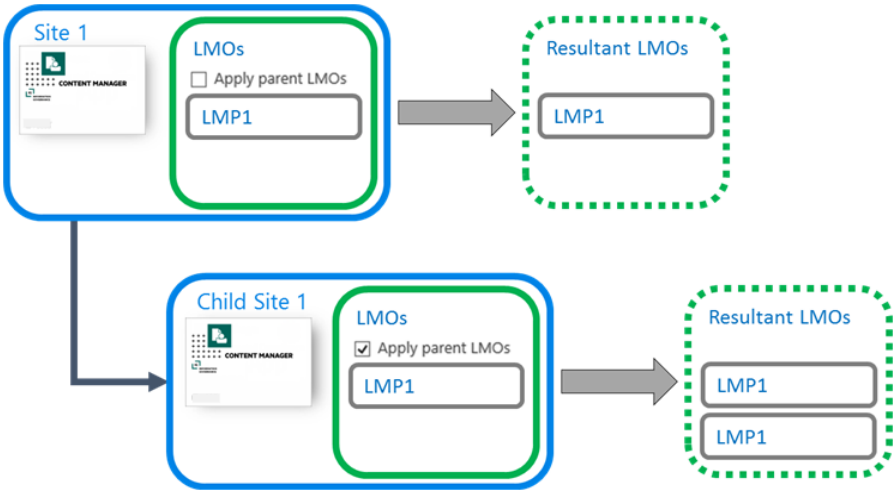


If in the previous scenario, site 1 had specified LMOs, then child site 1 would use an aggregate of the default site collection and site 1 as the resultant LMOs because the default LMOs have the ***Apply parent LMOs*** option checked.

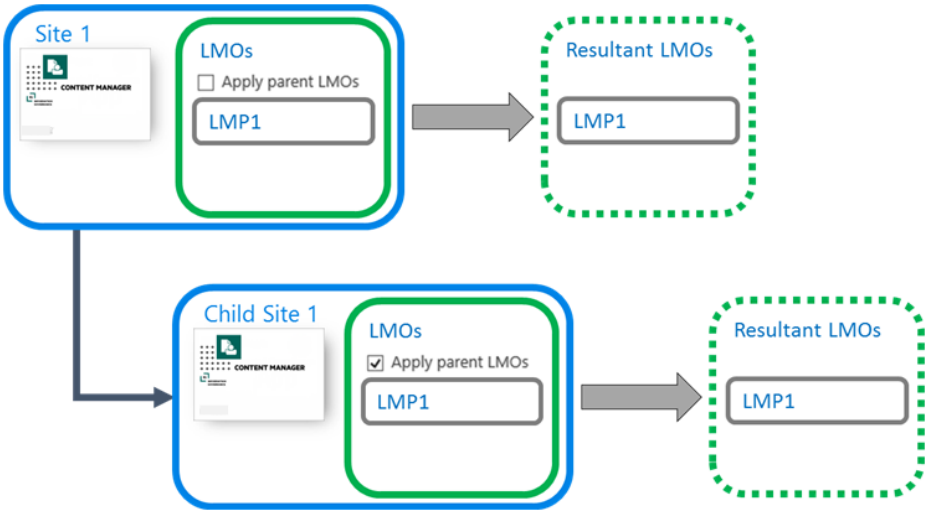


Duplicate LMPs

There are scenarios where the resultant LMOs would include the same LMP applied multiple times. For example:



Whenever a LMP would be applied multiple times, it is restricted to only allow a single application. The resultant LMPs are therefore:



Recommendations

There is not a one size fits all strategy when it comes to application of policies to content in a SharePoint farm. These recommendations are guidelines that will provide a starting point for you to determine the how content is manage for your organization. Sticking as closely as possible to these recommendations will provide clarity to others as to how content is being managed.

1. **Recommendation 1**

   Always try to apply LMPs that apply to your organization on the LMOs of the default site collection. This ensures that any new site collections that are created in future, automatically have these LMPs applied to all content in that site collection.

   This is the simplest way of ensuring that all site collections in your farm, have a common set of policies applied to all content. It also provides a central place to manage polices applied to the SharePoint farm.

2. **Recommendation 2**

If different site collections require different policies from those specified on the default site collection LMOs, it will be necessary to define specific LMOs for these site collections.

In this scenario, always try to apply the LMPs that apply to this site collection on the top level site of the site collection. This ensures that all existing content is managed in accordance with your policies. It also ensures that any new sites or lists that are subsequently created are also subject to these LMPs.

3. **Recommendation 3**

   Only create unique LMOs for a site if there is a special requirement for that particular site (and possibly children) that it does not make sense to have applied at site collection level.

4. **Recommendation 4**

   If it is necessary to create unique LMOs for a site, always use the ***Apply parent LMOs*** unless it does not make sense to do so. This ensures that any top level policies required by your organization are applied to the content of this site, despite it having unique LMOs.

5. **Recommendation 5**

   If creating unique LMOs, document the business reason for doing this. This will assist with any fault finding and business justification in future.

6. **Recommendation 6**

   Use site and list template filtering in LMPs. This ensures that policies applicable to a particular type of content are not applied to other types of content. For example, if your organization has a policy regarding management of leave applications, ensure that the LMP designed to apply this policy is designed to only work with the **leave application** content type.

12.8.2 Setting site LMOs

Accessing site LMOs

> **NOTE:** You must have **manage site** permission to access the site LMO page.

Access to edit site LMOs is only available for sites that have the Content Manager Governance and Compliance app added.

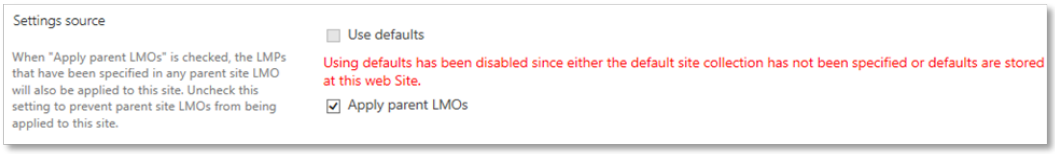
Access the app start page. Click the **Lifetime Management Options** link in **Lifetime Management** section.

This will take you to the site LMO page.

Use defaults

The **Settings source** section of the page allows specifying where the LMOs are derived from. Checking the **Use defaults** check box indicates that the site RMOs should use those specified on the default site collection. You will be unable to use any other controls on the page if this check box is checked.

If you are setting the LMOs for the default site collection, this option will be disabled.



When **Use defaults** is checked, the values of the default site collection site LMOs will be displayed on the page.

If this option is subsequently unchecked, the values from the default site collection are copied to the page as the starting settings.

Apply parent LMOs

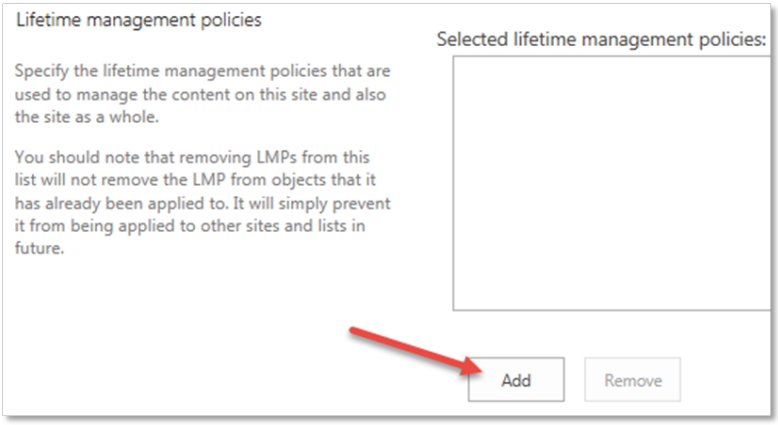
The **Settings source** section of the page includes the **Apply parent LMOs** checkbox.

Checking this option ensures that any LMOs applied to the parent site are applied to this site as well. See the Inherited LMOs section for further details.

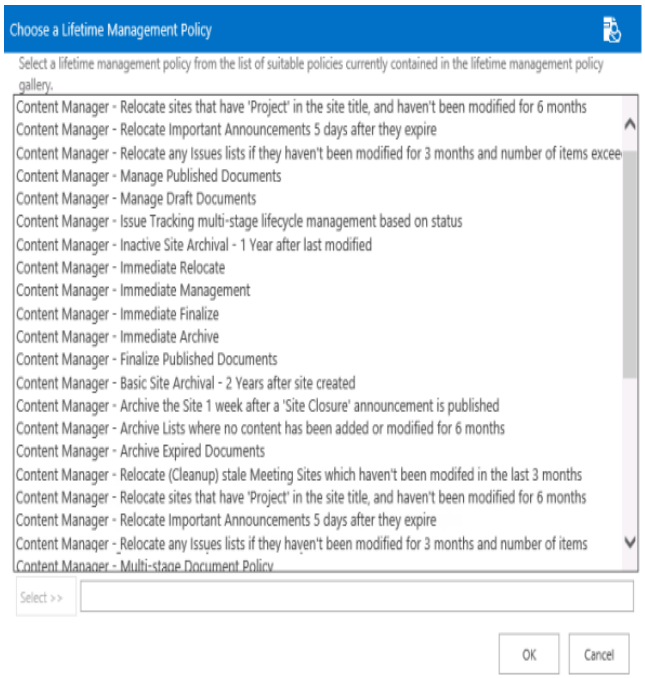
Managing the list of LMPs

The **Lifetime management policies** section of the site LMOs page allows the management of the LMPs that are to be applied to the site.

To add a LMP, click **Add**.

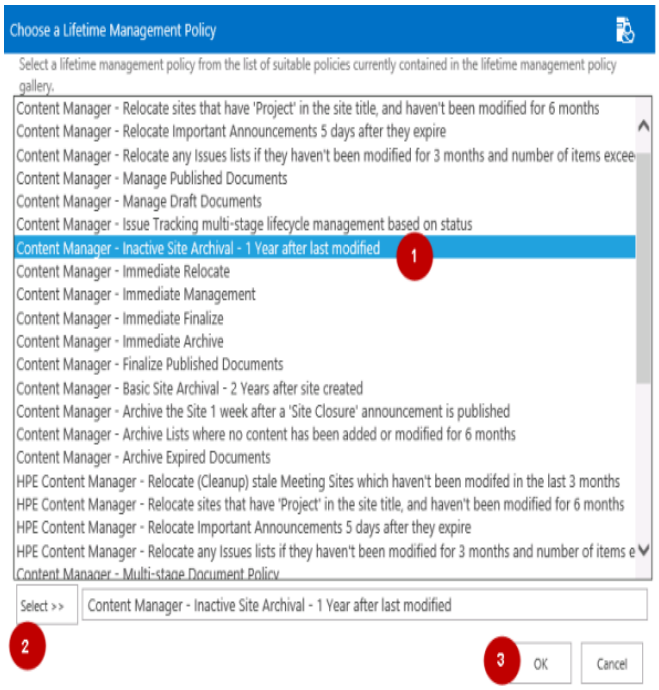


The **Choose LMP** dialog is shown allowing selection of all suitable LMPs.



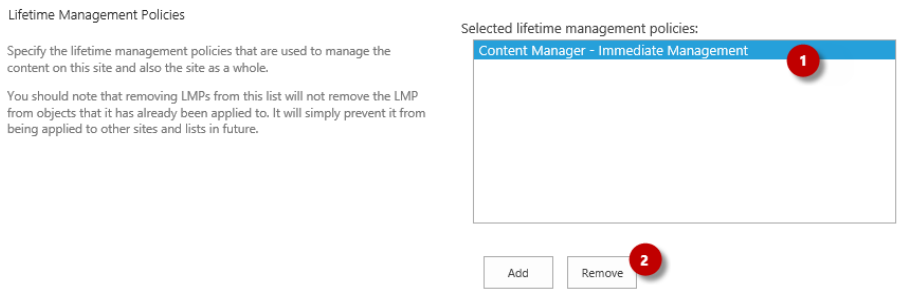
NOTE: An LMP is considered suitable to appear in this dialog if it is published.

To select a LMP to add, select it in the list, click **Select** then click **OK**.



The LMP will now appear in the list of LMPs

To remove a LMP from the list, select it, then click **Remove**.



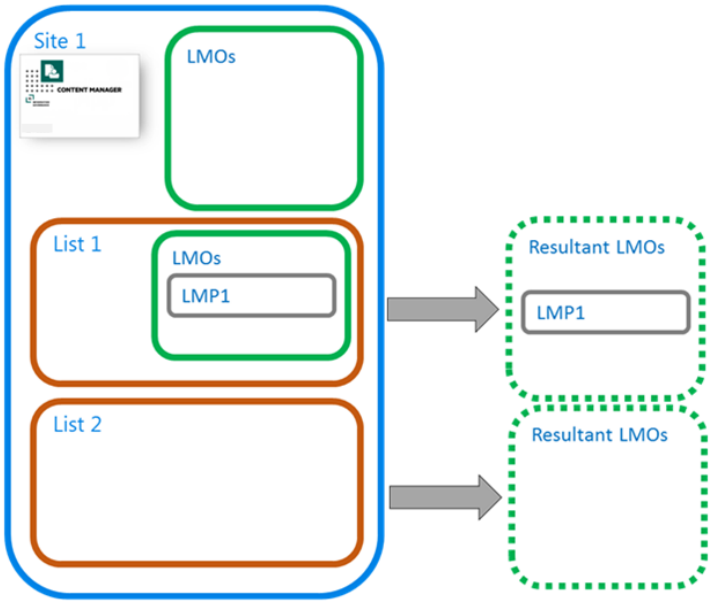
Saving the LMOs

Once the lifetime management options have been set correctly, click **OK** to save the settings.

12.9 Applying LMPs to lists

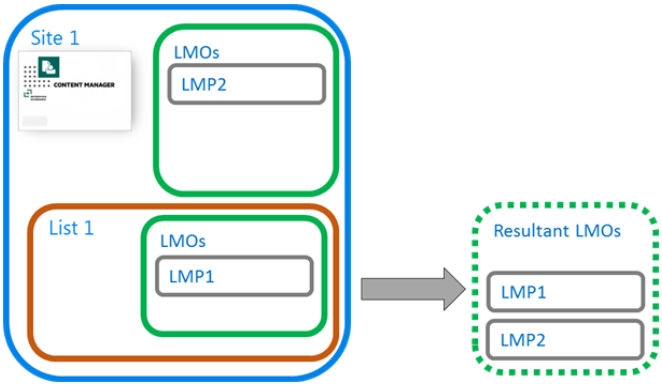
12.9.1 Understanding list Lifetime Management Options (LMOs)

List lifetime management options allows the application of LMPs to a particular list without applying it other lists. In the following example, the list 1 LMOs have LMP1 applied. The resultant LMPs that will be applied to list 1 will be LMP1.



Other lists on the site such as list 2 in this example, do not have LMP1 applied.

Site LMPs are applied in addition to list LMPs. In the following example, both LMP1 and LMP2 would be applied to the content in List 1



12.9.2 Setting list LMOs

Accessing list LMOs

> **NOTE:** You must have Edit list permission to access the list LMO page.

Access to edit list LMOs is only available for sites that have the Content Manager Governance and Compliance app added.

Navigate to the list that the LMOs are to be set for. From the ribbon select the ***LIST*** tab, the right ***most Content Manager*** drop down button then click **Lifetime Management Options**.

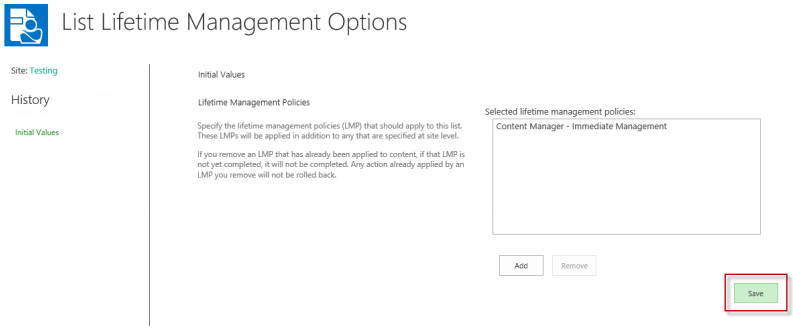
Managing the list of LMPs

See the site LMO section managing the list of LMPs

> **NOTE:** Only Item and List LMPs will be displayed as suitable LMPs for selection. Site LMPs will not be available for application to list LMOs.

Saving the LMOs

Once the **lifetime management options** have been set correctly, click **OK** to save the settings.



13 Preventing management of trivial content

Not everything in SharePoint needs to be retained in a compliant manner. Whilst there may be content in SharePoint that is subject to compliance requirements, there will be content that does not have this requirement.

Consider an image library that contains photos of social events. Typically, this type of information is not subject to legislation or internal policy that specifies it should be retained for any formal period of time.

Content that does not need to be managed as a record is referred to as “trivial” content. This is not to imply that the content is of no worth, it is simply the term that has been used to indicate that the content should not be managed by Content Manager.

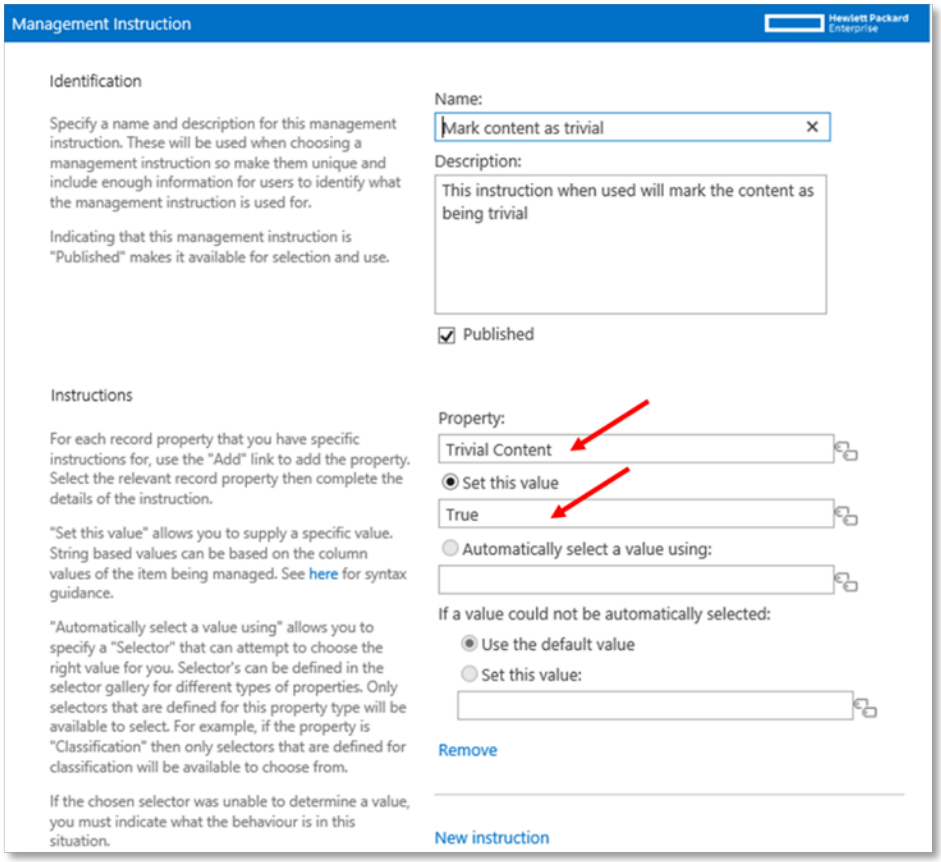
How do you identify trivial content so that it is not managed by Content Manager? Without a mechanism to identify this content, manual or automated management processes may inadvertently create unwanted records.

For example, consider a list that contains corporate documents as well as documents that are not required to be managed by Content Manager. Should a user specify that the list, or even the site be managed by Content Manager, all content in the list will be managed, including the trivial content.

13.1 Identifying content as trivial

Management Rules are used to identify content as trivial. As with any management rule, a set of conditions are defined to indicate content that should be considered as trivial.

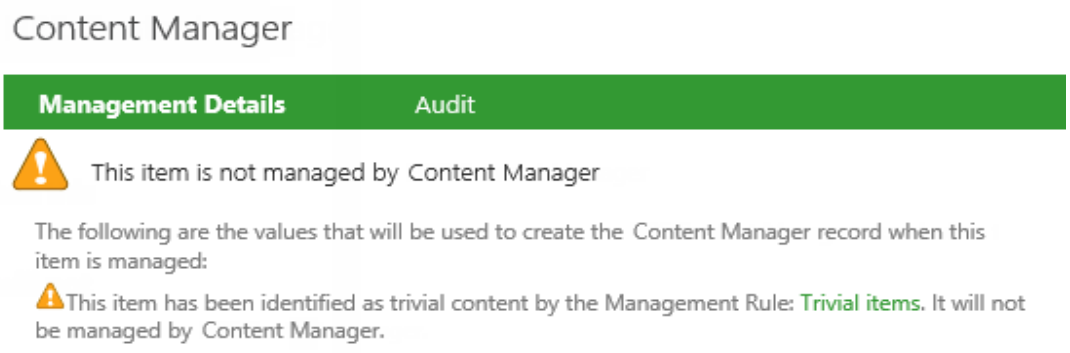
A management instruction must be defined that indicates that information is trivial. A management instruction used to indicate content is trivial must set the value of the ***Trivial Content*** property to ***True***.



13.1.1 The effect of the trivial identification

Whenever a management rule sets the ***Trivial Content*** value to ***True*** for an item, the manage, finalize, relocate and archive processes will not execute on that content.

Looking at the management details page for trivial content, regardless of any other configuration or management rules, the following is displayed:



Although a user can attempt to manage trivial content, when the job executes, the content will not be managed. Similarly, if a LMP attempts to manage trivial content, it will not be managed.

13.1.2 Overriding the trivial identification

There are situations where, although in most cases, a piece of content is to be considered trivial, that in specific circumstances it should be managed.

An organization has defined custom content type called ***Corporate Images*** that includes custom checkbox column ***Important Image***. They consider all photos on a particular site to be trivial, except if the custom property ***Important Image*** check box is checked.

A management rule has been defined that causes all items of the content type ***Corporate Images*** to be identified as trivial.

A second management rule has been defined that causes all items of content type ***Corporate Images*** with the ***Important Image*** column value equal to ***Yes*** to have Trivial Content set to ***False***.

The second rule is marked as being ***Critical***. This causes this second rule to always override the first rule and therefore prevent important images from being considered trivial. See Summary of management rule selection process for further details.

13.1.3 Practical examples

This section provides guidance for implementing some practical examples around trivial content.

Preventing folders from being managed

In this scenario, the organization does not want records to be created for folders in SharePoint.

- Create a management rule that applies to the ***Folder*** content type with no other conditions
- For this rule use an instruction that marks the ***Trivial Content*** property to ***True***

Preventing certain types of lists from being managed

In this scenario the organization wants image libraries to not be managed.

- Create a management rule with the condition that the list template ID is 109 (Picture library) see Template ID for list template IDs
- For this rule use an instruction that marks the ***Trivial Content*** property to ***True***

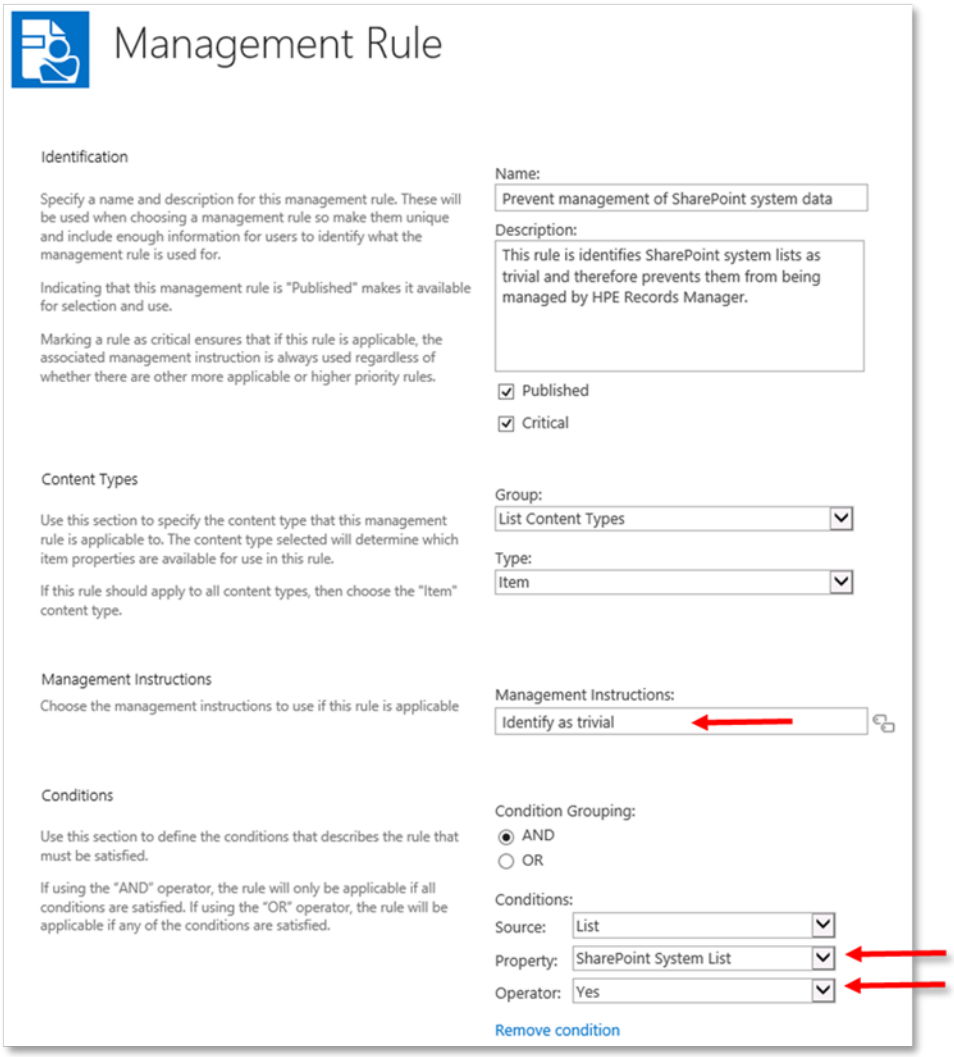
13.2 Preventing management of system lists

There are a number of lists that are used by SharePoint to manage system data. Typically these do not contain information that an organization is not required to capture in Content Manager.

Managing a site will however manage all lists that are on a SharePoint site. This can lead to unwanted records in Content Manager, and in some cases, errors in the system log and difficulty relocating SharePoint sites.

It is possible to exclude the management of system lists by marking them as trivial using management rules.

To do this, define a management rule with a condition that if the list ***SharePoint System List*** property is ***True***, then use a management instruction to indicate that the content is considered trivial.



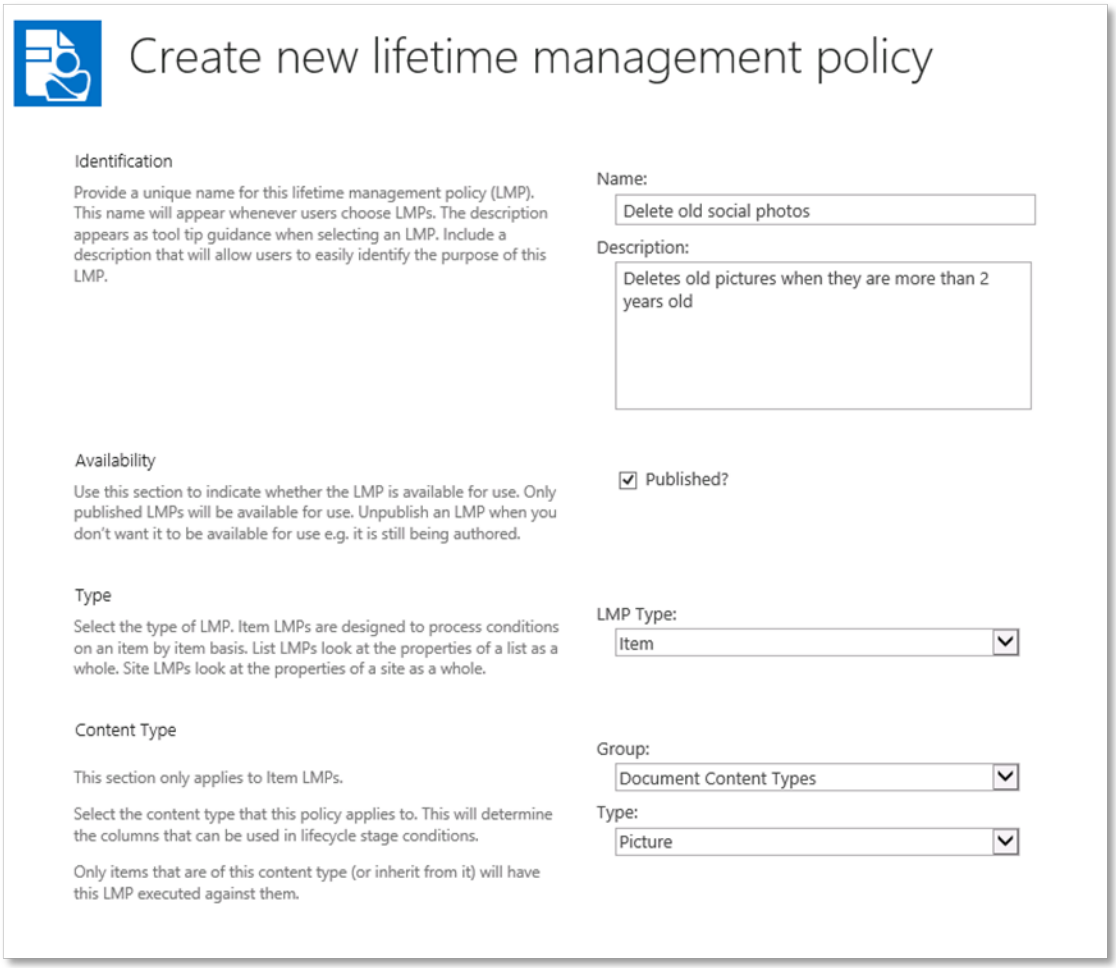
It is recommended that unless there is a specific reason to manage SharePoint system lists, that all implementations include a management rule that indicates that system lists are trivial.

By default, the management rules gallery will include a standard rule to do this. If this rule is unwanted, mark it as unpublished to prevent it from being used. If you delete it, it may be recreated next time a publish of configuration data is performed.

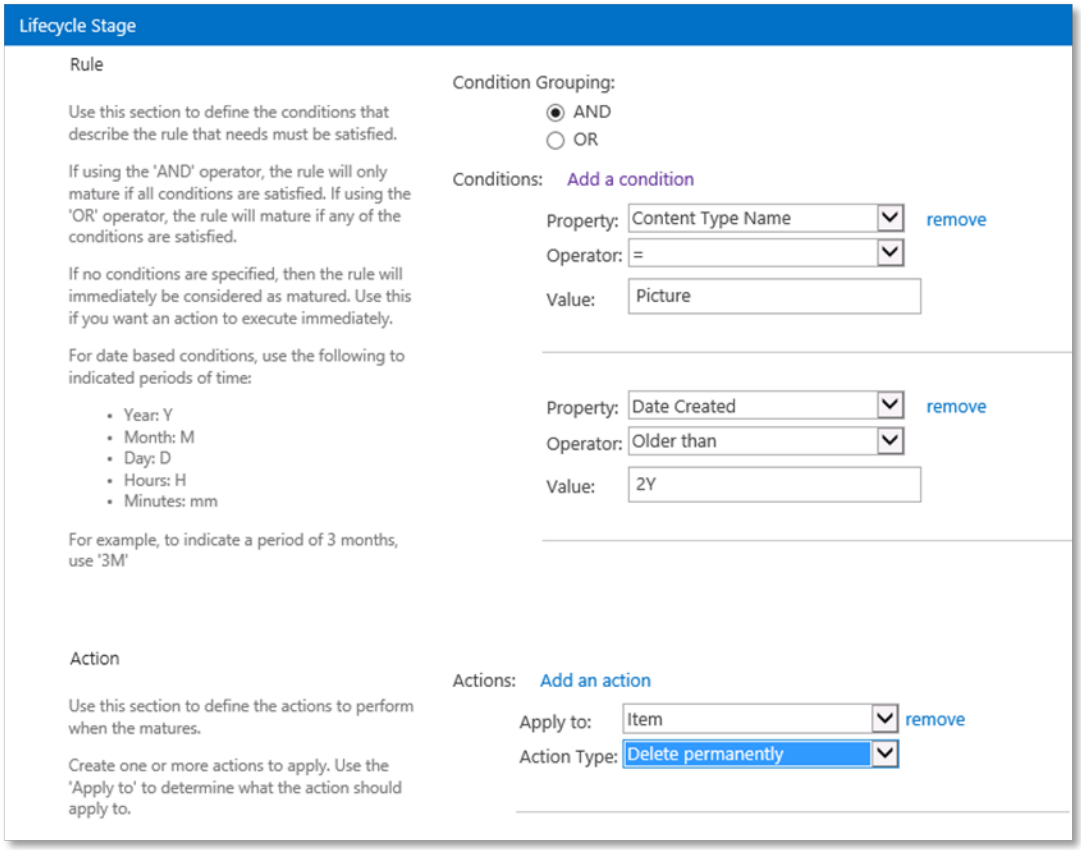
13.3 Deleting trivial content

Lifetime management policies allow defining that content that satisfies a set of conditions should be deleted from SharePoint.

For example, to delete images on a picture library called ***Social Outings***, when they are more than two years old define a LMP as follows:



Include a lifecycle stage as follows:



Apply this LMP to the ***Social Photos*** list. Pictures that are older than two years old will automatically be deleted permanently from the picture library.

14 Securing SharePoint content with Content Manager

14.1 Security and access control features

Content Manager includes powerful security and access control features. The Content Manager Governance and Compliance app can be used to ensure that any security or access control applied to records in Content Manager, are correctly respected by SharePoint. In many scenarios, the default security provided by SharePoint itself will be satisfactory for the requirements of an organization. Where more granular restrictions are required, the security capabilities of the app can satisfy this requirement.

In order to understand how security is applied, it is important to understand how both SharePoint and Content Manager restrict access to information. This chapter begins by explaining the basics of the models used by each system.

14.1.1 Information security in SharePoint

SharePoint allows granting permissions for individual users or groups of users to sites, lists, and individual items.

SharePoint includes granular permissions that can be used to determine what a user can and cannot do with content. These permissions can include the ability to create, view, edit and delete content.

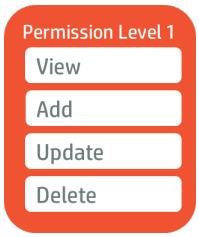
Permissions themselves are not directly assigned. Instead, “Permission Levels” are created, which group together one or more individual “permissions”.

For example, permission levels provided by SharePoint OOB include:

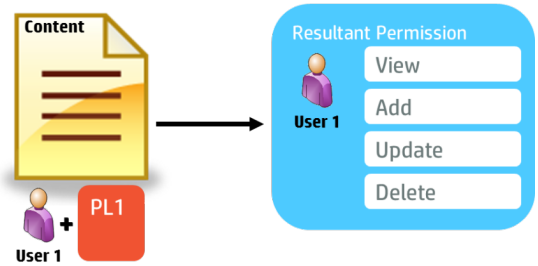
- Full Control - Has full control.
- Design - Can view, add, update, delete, approve, and customize.
- Contribute - Can view, add, update, and delete list items and documents.
- Read - Can view pages and list items and download documents.
- View Only - Can view pages, list items, and documents. Document types with server-side file handlers can be viewed in the browser but not downloaded.

In order to specify the permissions a user has to have content (e.g. site, list or list item), users are assigned permission levels for that content.

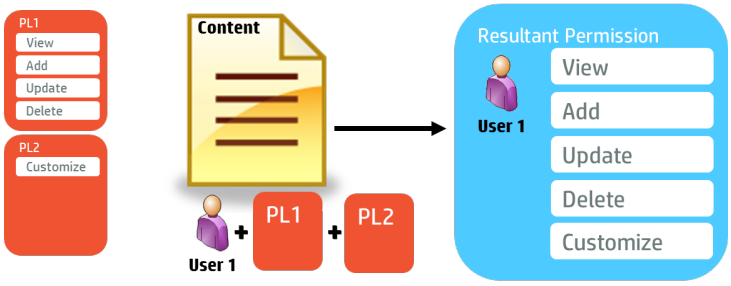
Consider the following permission level, Permission Level 1 or PL1.



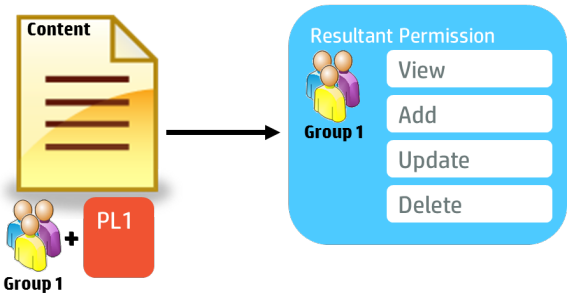
If User 1 is assigned PL1 for content in SharePoint, then User 1 has view, add, update, and delete permission to that content.



If User 1 is assigned PL1 and an additional permission level PL2, the user's resultant permission is the sum of all unique permissions contained in PL1 and PL2.



Permission levels can be assigned to groups of users as well as to individual users. These groups can be Active Directory groups or SharePoint groups.



Inherited permissions

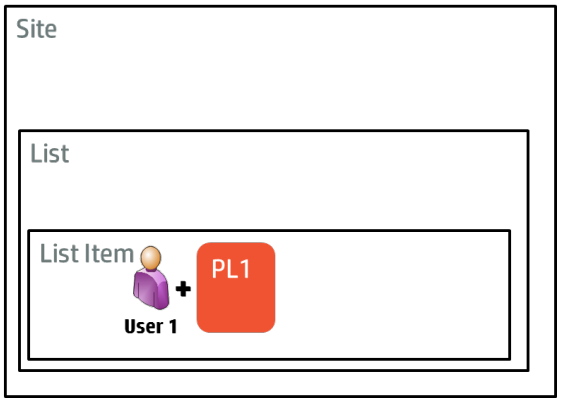
If specific permissions are not applied to a site, list or item in SharePoint, the resultant permissions are the permissions applied to the container. In other words, without specified permissions, the following rules are used to determine the resultant permissions to an item:

- List item: the list permissions
- List: the site permissions
- Site: the parent site permissions

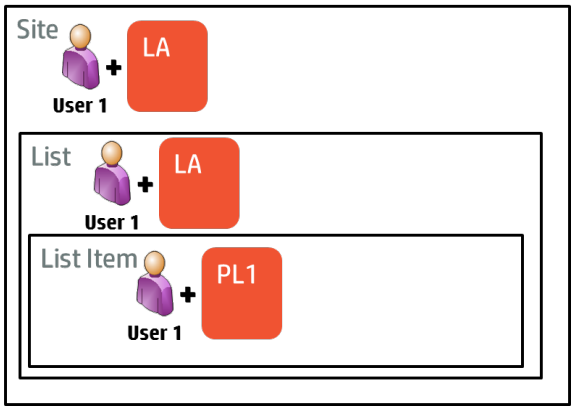
Permissions determined in this manner are said to be "inherited".

Limited Access

Permission levels can be assigned for a user to a site, a list or an individual item. However, if a user is assigned permissions to a list item, but not to the list in which the item resides, or to the site in which the list resides, this user would not be able to access the list item regardless of their permission to the item.



To solve this problem, SharePoint uses a special permission level called “Limited Access” (LA). LA gives the user the necessary permissions to access the items that they have access to. In the previous example, User 1 would automatically be granted LA to the list and the site the item resides in.



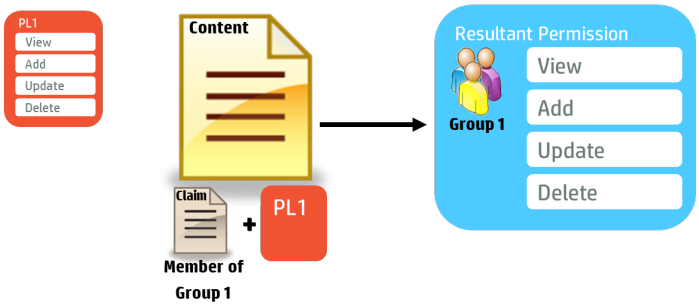
14.1.2 Claims based authentication

SharePoint supports a number of different authentication models including claims based authentication. In claims based authentication, when a user authenticates to SharePoint, the user is given a series of claims. For example, if User 1 is a member of Group 1, the user will be assigned claims that state:

- This user is User 1
- This user is a member of Group 1

> **NOTE:** These claim names are used for illustrative purposes, only.

When applying permission levels to content, the levels are assigned for users who have particular claims. For example, if Permission Level 1 is assigned to members of Group 1, this claim would translate to "Users who have the claim “This user is a member of Group 1” will get the permissions of Permission Level 1".



NOTE: Claims based authentication is the default and recommended authentication mechanism for SharePoint.

14.1.3 Information Security in Content Manager

Information security can be thought of as controlling access to information and controlling what can be done with that information if you are permitted to access it.

Content Manager has three mechanisms for controlling access to information:

- Security levels
- Security caveats
- Access controls

Depending on an organization’s requirements, all of these mechanisms may be used, or just a selection. Note that if multiple mechanisms are used, they apply collectively. For example, if content requires a particular security level, security caveat, and group membership, all three of these requirements must be met, not just one.

Security Levels

Security levels indicate the security level that a user must have in order to access a record.

NOTE: In the case of security levels, “accessing a record” refers to the ability to identify that the record exists. It is important to understand that access controls will determine whether a user can view and/or edit the record.

Security levels are definable in Content Manager; therefore it is unlikely that the levels used by one organization will necessarily apply to another organization. For illustrative purposes in this section, we will assume the organization has defined the following security levels starting at the most secure through to the least secure:

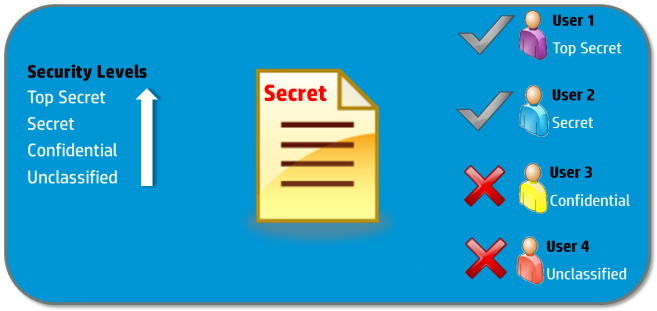
- Top Secret
- Secret

- Confidential
- Unclassified

Security levels are hierarchical. Users assigned to a particular security level have access to all security levels beneath. For example, if User 3 is assigned the “Secret” security level, they can see records that have security levels of:

- Secret
- Confidential
- Unclassified
- No security level

Users who do not have a security level equivalent to, or higher than, that of a record are not permitted to access that record.



A user and a record can only ever have one security level assigned.

Security Caveats

Security caveats indicate additional requirements that a user must have in order to access a record.

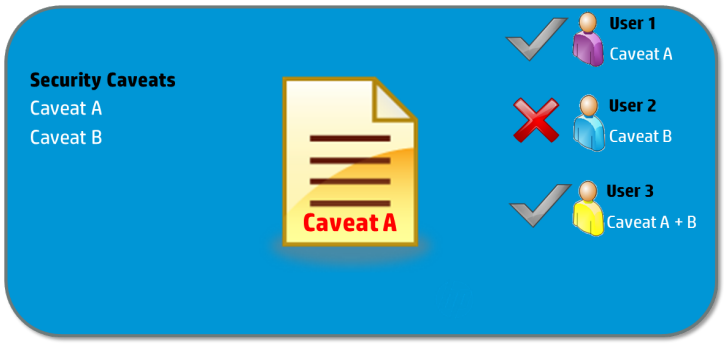
> **NOTE:** In the case of security caveats, “accessing a record” refers to the ability to identify that the record exists. It is important to understand that access controls will determine whether a user can view and/or edit the record.

For example, medical records could have a caveat of “Medical in Confidence,” indicating that regardless of any other access controlling mechanisms, only users such as Doctors who have the “Medical in Confidence” security caveat are permitted to access the information.

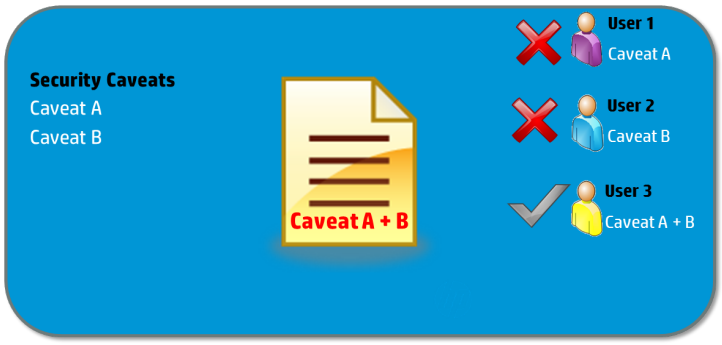
Security caveats are definable in Content Manager therefore it is unlikely that the caveats used by one organization will apply to another organization. For illustrative purposes in this section, we will assume the organization has defined the following security caveats:

- Caveat A
- Caveat B

Unlike security levels, caveats are not hierarchical. If Caveat A is required to access a certain record, the only acceptable caveat to satisfy this requirement is Caveat A.



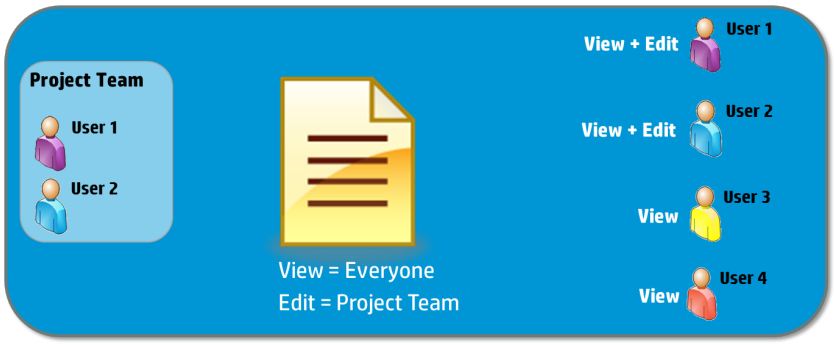
Users and records can be assigned multiple caveats. If a record has multiple caveats, then a user must have all caveats to be eligible to access the record.



Access Controls

Access controls are used to restrict what a user can do with a record. Largely, access controls can be used to control which users and groups of users can view and edit a record.

In the following example, everyone is permitted to view the record (i.e. no access controls are placed on viewing the record) but only members of the Content Manager group called “Project Team” are permitted to edit the record.



Content Manager access controls are more granular than just view and edit, allowing you to assign separate access to the metadata and the document. It is therefore possible to give user permission to view the metadata, but not to view the document. This would allow the user to access the record, but not view the contents of it.

User Permissions

Content Manager users are represented as user type locations in Content Manager. What a user is permitted to do in Content Manager can be set on the user's profile. These permissions include the ability to edit records. In all cases, if the user's permissions are more restrictive than the access controls on a record, the more restrictive permissions are used.

For example, if User 1 does not have the "Modify Records" permission on their user location in Content Manager, User 1 will not be permitted to make modifications, even if the record access controls permit User 1 to modify the record.

Referenced access controls

Access controls can be applied specifically to a record. They can also be derived based on the record type, classification, and parent container of the record. These types of access controls are known as "referenced access controls".

For example, the default access controls of a record type "Record Type 1" (RT1) is set to allow only users in the Content Manager group "Project Team" to edit the records. Because of these referenced access controls, all records using RT1 will be editable only by members of the "Project Team" group.

This example can be extended to classifications and parent containers.

14.1.4 Content Manager security applied to managed SharePoint content

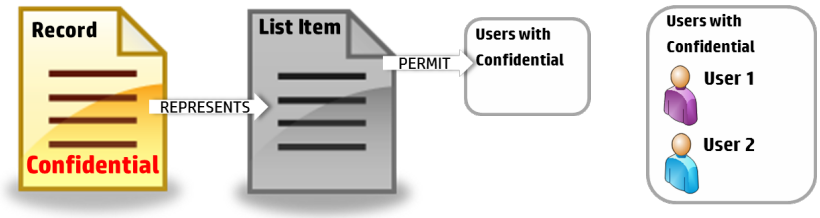
Application of Content Manager security and access controls to SharePoint content is off by default. Access to SharePoint items will only be restricted if you configure the Content Manager Governance and Compliance app to respect these values.

This section describes the underlying mechanics of how access is restricted. A subsequent section in this chapter describes how to enable and configure security to be used when and where it is required.

Content Manager Security Groups

The security features of the Content Manager Governance and Compliance app utilizes SharePoint authentication to enforce the security and access controls applied to the relevant Content Manager record. In order to do this, SharePoint groups are created to represent the collection of users who satisfy the relevant security attributes represented by that group.

For example, consider a record that has a security level of "Confidential". If this record represents a managed list item in SharePoint, the access to that list item is restricted to only members of the SharePoint group that contains all users that have the Content Manager security level of "Confidential".



Therefore, in this example, only user 1 and user 2 will have access to this list item

SharePoint groups created to represent collections of users with specific security and/or access control attributes are referred to as “Content Manager Security Groups”.

CM Permission Levels

Content Manager access controls allow differentiating between users that can view a record and those that can edit a record. In order to replicate this capability in SharePoint, groups of users must be allocated permission levels that represent the ability to view and the ability to edit an item.

The following permission levels are created when the security features are first used

- View CM Secured Item
- Edit CM Secured Item
- CM Limited Access
- Administer CM Secured Item

When a Content Manager security group is used to control access to a SharePoint list item, it is one of these permission levels that is assigned to the group.

The permission levels have the following permissions included:

Permission	View CM Secured Item	Edit CM Secured Item	Administer CM Secured Item	CMLimited Access
Override List Behaviors			✓	
Add Items		✓		
Edit Items		✓		
Delete Items		✓		
View Items	✓			
Approve Items			✓	
Open Items	✓			
View Versions	✓			
Delete Versions		✓		
Create Alerts	✓			
View Application Pages	✓			
Manage Permissions			✓	
View Pages	✓			
Enumerate Permissions			✓	

Permission	View CM Secured Item	Edit CM Secured Item	Administer CM Secured Item	CMLimited Access
Manage Alerts			✓	
Use Client Integration Features	✓			
Open	✓			

NOTE: Permissions that are not applicable to item level operations are not listed in the above table as they are not included in any of the CM permission levels.

Modifying the CM permission levels

These permission levels have been designed specifically to work with the Content Manager Security feature. It is strongly recommended that you do not change these permission levels.

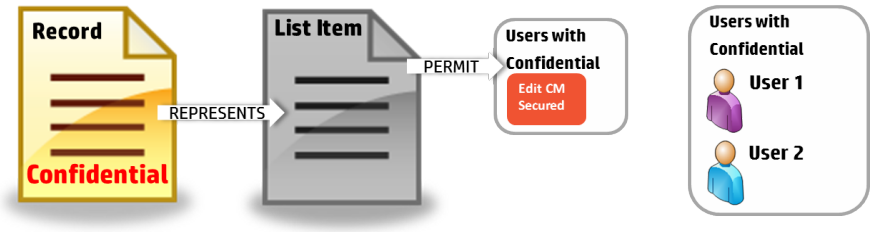
You must consider carefully the implications of changing these permission levels if you have a requirement to modify them.

CAUTION: You should never under any circumstance modify the CM Access permission level.

Controlling access to a list item

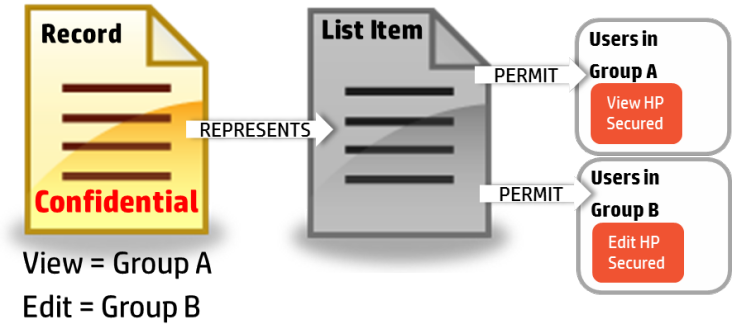
Controlling access to a list item is achieved using Content Manager Security Groups in combination with CM Permission levels.

Consider the scenario where a record has a security level of “Confidential” and there are no access controls on the record. Content Manager will grant anyone permission to view and edit the record as long as they have the Confidential security level or higher. To represent this on a list item represented by the record, the Content Manager Security Group that contains all users with Confidential or higher is granted the “Edit CM Secured Item” permission level.



In a scenario where edit and view permissions are different however, multiple assignments can be made. For example, consider a record that allows members of Group A to edit and members of Group B to edit the record.

To represent this access control, the Content Manager security group containing members of Content Manager Group A is assigned the “View CM Secured Item” permission level and the Content Manager security group for Group B is assigned “Edit CM Secured Item” permission level.



This is the underlying principle for application of Content Manager security and access controls to SharePoint items.

Converting access controls to permissions

Equivalent permission levels

Where a Content Manager security group is determined to have permission to view the list item, the ***View CM Secured Item*** permission level is granted.

Where a Content Manager security group is determined to have permission to edit the list item, the ***Edit CM Secured Item*** permission level is granted.

Determining permissions to apply

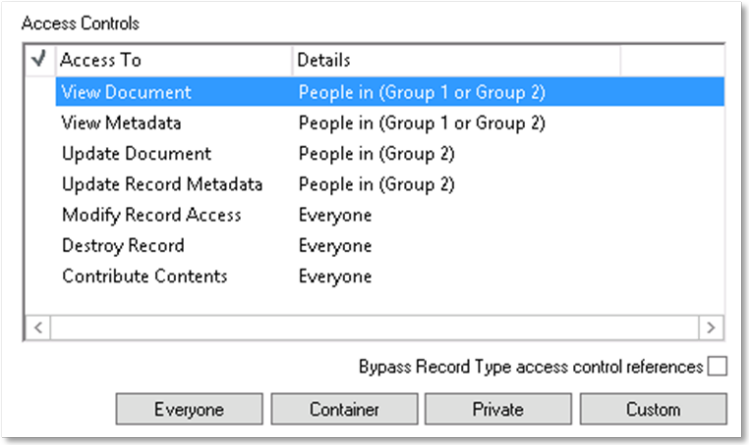
A number of different types of access controls are available in Content Manager; however only the following four are used to determine a Content Manager security group’s permission level:

- View Document
- View Metadata
- Update document
- Update Record Metadata

The following table describes how the resultant permission level is calculated.

Access control		
View Document	✓	✓
View Metadata	✓	✓
Update Document		✓
Update Record Metadata		✓
Resultant Permission Level	View CM Secured Item	Edit CM Secured Item

For example, consider the following record access controls in Content Manager:



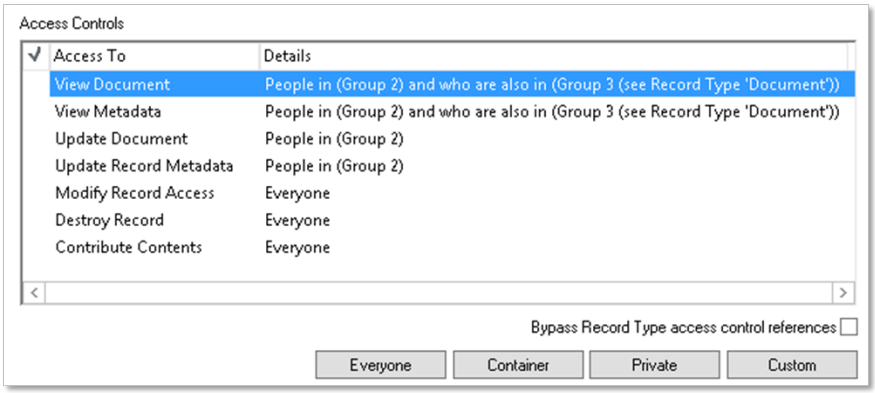
List items represented by this record would have the following claims assigned:

- Group 1 granted the ***View CM Secured Item*** permission level
- Group 2 granted the ***Edit CM Secured Item*** permission level

Referenced access controls

Referenced access controls, regardless of where they are referenced from (record type, classification, or container), are considered when calculating the resultant access controls on a record.

For example, consider the following record access controls in Content Manager, noting that the “View Document” and “View Metadata” access controls use referenced access controls from the record type “Document”:



List items represented by this record would have the following claims assigned:

- Group 3 granted the ***View CM Secured Item*** permission level
- Group 2 granted the ***Edit CM Secured Item*** permission level

Despite the fact that Group 3 obtained the “View Document” and “View Metadata” access controls via record type referenced access controls, these access controls are used to determine the resultant permissions in SharePoint.

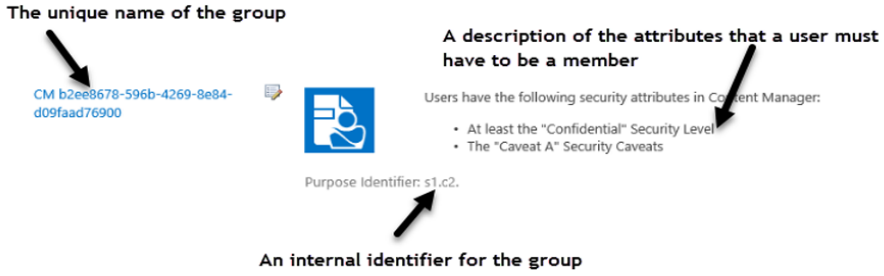
Creation of Content Manager Security Groups

Content Manager Security Groups are only created as they are needed. If no SharePoint content is secured using a particular security or access control attribute (or combination of attributes) then a Content Manager Security Group will not exist to represent these users. This is done deliberately to reduce the number of SharePoint groups created.

As Content Manager Security Groups are SharePoint groups, they can be accessed from the **People and Groups** option under **Site Settings**.

A group has the following attributes:

1. Unique name of the group
2. Description of the security attributes a user must have
3. internal identifier for the group



Initial population of Content Manager Security Groups

When a Content Manager security group is first created, it is initially empty. The group is populated asynchronously with the eligible members. This task is performed by a job in the job queue:

PopulateSecurityGroup.

This job identifies the eligible members and adds them to the newly created group. Therefore, it is important to recognize that when a group is created and used to restrict permissions on a list item, until the PopulateSecurityGroup job has finished running, eligible users may not have access to the item.

Only user's with active locations in Content Manager are placed into these groups.

The following rules are used to calculate Content Manager security group membership:

Security levels

When a group is used to represent all users with a particular security level, all users with that security level, and all users with a higher security level are included in the group.

Security caveats

When a group is used to represent all users with a particular security caveat, only the users that have that security caveat in Content Manager are included in the group.

Group locations

When a group is used to represent all users that are members of a Content Manager group location, only users that are members of that group location are placed in the Content Manager security group.

User locations

When a group is used to represent a Content Manager user location, only the user who that user location represents is placed into the group.

Inclusion of Content Manager user permissions

When a group is used to represent Content Manager users who have a particular security attribute, and their user location has permission to edit records, the Content Manager security group will include all users who have the relevant security attribute (security level, security caveat or location membership) AND their account allows them to modify records.

For the purpose of calculating if a user can modify records, the corresponding location in Content Manager must have at least one of the following permissions:

- Modify records OR
- Document update

Combinations of attributes

When a group is used to represent all users that have multiple attributes, for example:

- A security level and one or more caveats
- Multiple caveats
- A security level and a member of a group location

Only users who have all of the attributes will be included in the group.

Maintenance of group memberships

From time to time, the membership of a Content Manager security group will change. This can occur when:

- A user's security level is changed
- A user's caveats are changed
- A user's group membership is changed
- A user is made inactive
- A user is made active

When these types of events occur, a ***RefreshSecurityGroups*** job will be added to the job queue. This job is responsible for updating the membership of relevant Content Manager security groups.

Until this job is completed, the user's access to SharePoint list items may be incorrect.

Preventing malicious group modification

Were a malicious user able to gain access to SharePoint and add themselves to Content Manager security groups that represent security attributes that the user does not have, this would allow them to grant themselves higher access to information than they should have.

The Content Manager Governance and Compliance app prevents this type of action. If the membership of a Content Manager security group is manually modified by a user, the action will be prevented and the user presented with the message:

This group is used by Content Manager to secure managed content in SharePoint. Only Content Manager is permitted to modify the memberships of this group. Your requested change has therefore been prevented

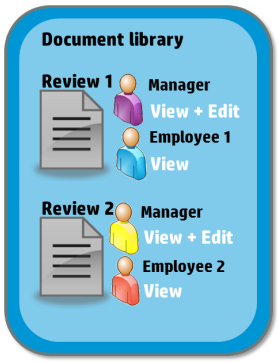
If an attempt made by a user to delete a group, the action will be prevented and the user presented with the message

This group is used by Content Manager to secure managed content in SharePoint. You are not permitted to delete this group therefore your request to delete has been prevented.

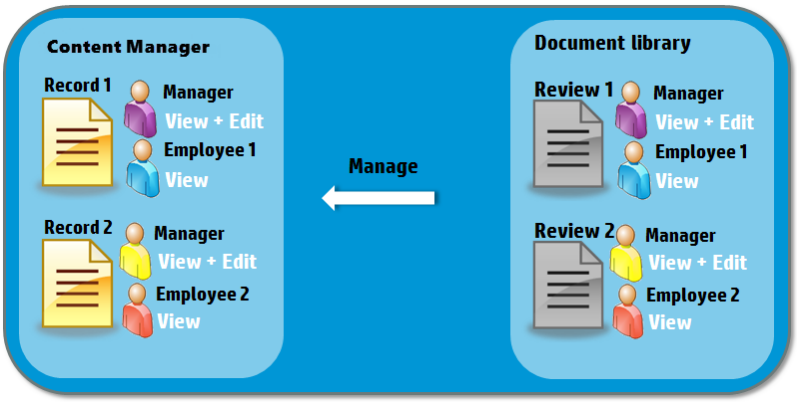
14.1.5 Capturing access controls

SharePoint allows specifying unique permissions at item level. This allows restricting the information to a specific set of users. This permits the storage of many items in a list or site, while only allowing particular users access to a subset.

For example, an organization uses a document library to create and store reviews of employees. Each review is secured using SharePoint permissions so that only the employees' manager can edit the reviews, and each employee can only view their own review and not those of their colleagues.



When these reviews are managed with Content Manager, the resultant records must be locked down in a similar way; that is, only the manager should be able to edit the records and employees should only be able to view their own reviews. The mechanism used to apply these restrictions in Content Manager is access controls.



The Content Manager Governance and Compliance app provides the ability to capture SharePoint permissions applied at site, list or item level as access controls on the record in Content Manager.

> **NOTE:** This is a configuration option that can be turned on or off at site level to meet organizational requirements.

Converting Permissions to Access Controls

To determine the equivalent access controls to apply to a record, requires examining the permissions that are assigned to the list item and determining equivalency. The ability to view and/or edit a list item determines the access control in Content Manager.

When determining if a user has permission to view a list item, SharePoint uses the following definition of view - View items in lists, documents in document libraries, and view Web discussion comments.

When determining if a user has permission to edit a list item, SharePoint uses the following definition of edit - Edit items in lists, edit documents in document libraries, edit Web discussion comments in documents, and customize Web Part Pages in document libraries.

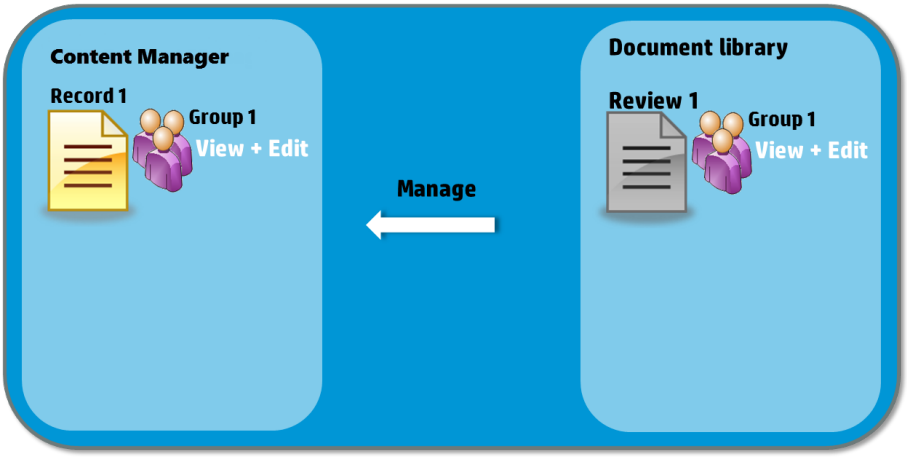
Permission	Resultant Access Control

View	View Document + View Metadata
Edit	View Document + View Metadata + Update Document + Update Record Metadata

> **TIP:** When capturing permissions as access controls is enabled, take note that the items permissions will not be altered on the item in SharePoint. Content Manager will use the access controls on the record to lock down access to the data.

Capture of groups

SharePoint allows the use of both SharePoint and AD based groups to secure information. In the following example "Group 1" is used to secure access to the document, therefore this group is used to secure access to the record.



Automatic creation of groups

Capture of groups works well when there exists a group location in Content Manager already that matches the SharePoint or AD group called Group 1. If there is no location that matches however, it would not be possible to apply the correct access controls.

To alleviate this issue, when a SharePoint or AD group is used that has no matching group location in Content Manager, a location is created. The group is created as an internal location. If it is based on an AD group, the name of the group will be:

```
AD Group Name + "(AD:" + Domain name + ")"
```

For example, if the name of the group was "Financial Services Team" and the domain was called "Production" then the group will be named:

```
Financial Services Team (AD:Production)
```

If the location is based on a SharePoint group, the name of the group will be:

```
SharePoint Group Name + "(SP:" + Site collection name + ")"
```

For example, if the name of the group was "Human Resources" and the site collection was called "Onboarding" then the group will be named:

```
Human Resources (SP:Onboarding)
```

Initial population of group locations

When a group location is automatically created, an asynchronous job is created to populate the group. This job is called ***PopulateGroup***

Maintenance of group locations

From time to time, the members of the AD and SharePoint groups that automatically created group locations are based on may change. When they do change, the memberships of the group locations in Content Manager need to be updated.

For SharePoint groups, this update is performed in response to the event raised by SharePoint indicating the group membership change.

For AD groups, the ***MaintainGroups*** job is run on an hourly basis to correct any group membership changes.

14.2 Enabling security

14.2.1 Enabling Options and Considerations

Enabling options

Application of Content Manager security and access controls to SharePoint is not turned on by default. You must enable security where it is needed.

You can enable at the following levels:

- On the default site collection so that all other site collections using the defaults are also enabled
- On a site collection by site collection basis
- For a specific site

Considerations

SharePoint has recommended limits around the use of SharePoint groups and as the security functionality utilizes SharePoint groups, it is important to consider these limits.

Typically these limits are not “hard” limits and Microsoft simply advise that exceeding these values may have performance implications in areas of SharePoint.

Remember when considering the number groups you will have, Content Manager security groups are only created if they are required. Consider an organization that has two security levels (SL1 and SL2) and two caveats (C1 and C2). The possible combinations of these are:

1. SL1
2. SL1 + C1
3. SL1 + C2
4. SL1 + C1 + C2

5. SL2
6. SL2 + C1
7. SL2 + C2
8. SL2 + C1 + C2
9. C1
10. C2
11. C1 + C2

Although these are the possible combinations, the organization only has records secured using the following combinations:

1. SL1
2. SL1 + C1
3. SL1 + C2
4. SL2
5. SL2 + C2

Therefore, only five groups will be created, not eleven.

1. **Consideration**

   Do you have a large number of combinations of security levels, caveats and groups that you regularly use?

   Possible impact

   This may result in a large number of SharePoint groups being created. Microsoft recommends creating no more than 10000 groups per site collection.

2. **Consideration**

   Will there be Content Manager security groups created that will have more than 5000 eligible users?

   Possible impact

   Microsoft recommends putting a maximum of 5000 members in a SharePoint group. If you have Content Manager security and access control combinations that more than 5000 users are eligible for, there may be a possible performance impact.

3. **Consideration**

   Do you have users that will be eligible for membership in more than 5000 groups?

   Possible impact

   Microsoft advise limiting the number of groups that a user belongs to 5000.

4. **Consideration**

   Will a single list have more than 5000 items that have completely different security and access control combinations?

Possible impact

Microsoft advise that you should limit the number of unique permissions in a list to ideally 5000 with a maximum limit of 50000.

Retrospective application of access controls

Enabling security will implement this behavior only from that point on. Security and access controls are not applied to existing managed list items retrospectively (unless a change is made to the list item or the record).

14.2.2 Content Manager Security Settings page

The Content Manager Security Settings page is the page that is used to enable security for SharePoint content.

Accessing the Security Settings page

You can access the **Security Settings** page from the **app start page > Security** section.

Settings source section

The ***Settings source*** section of the security settings page is used to specify how the security settings are derived.

Use defaults

Checking the ***Use defaults*** check box indicates that this site should use the security settings that have been specified for the default site collection.

If this is checked, all other controls on the page are disabled.

Inherit security settings from the parent site

Checking the ***Inherit security settings from the parent site*** check box indicates that the security settings should be based on the security settings of the site that is this sites parent. If this site is the top level site on the site collection, this check box will be disabled (as there is no parent to inherit from).

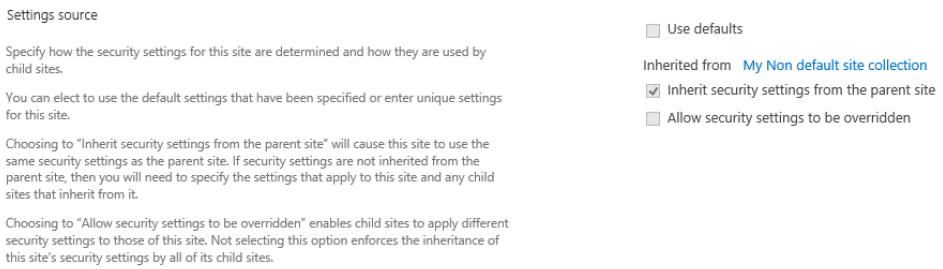
If this is checked, all other controls on the page are disabled.

Allow security settings to be overridden

Checking the ***Allow security settings to be overridden*** check box indicates that child sites can modify the enablement of security. This would allow the situation where security is enabled for a site, but for the child sites security has been disabled.

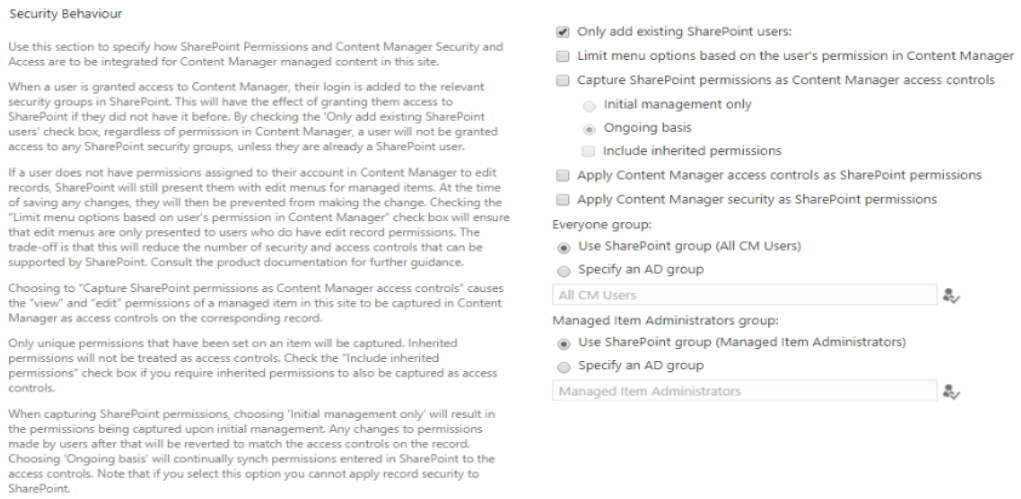
Leave this check box ticked if you want the security enablement to be applied to this site as well as any child sites.

The security settings for a child site of this one will have the following set in the settings source section.



Security behavior section

The ***Security behavior*** section of the security settings page is used to indicate that how security is actually applied to the site.



Only add existing SharePoint users

If the ***Only add existing SharePoint users*** check box is checked, whenever Content Manager security groups are populated, in addition to having the Content Manager security attributes required for the group, a user will only be placed in the group if they already have permission to this site. With this option checked, Content Manager users need to be explicitly granted permission to a SharePoint site before they will begin appearing as members of the Content Manager security groups applicable.

If the option is unchecked, then all eligible Content Manager users will be added to the group regardless of whether they already have access to the SharePoint site. This therefore has the effect of granting them access to the SharePoint site if they didn't have it before

Limit menu options based on the user's permission in the Content Manager

The Inclusion of Content Manager user permissions section of this document describes the ability to consider the user's permissions in Content Manager when determining the permission they are assigned to a list item. This is only considered if the ***Limit menu options based on the user's permission in Content Manager*** check box is checked.

Although it may seem attractive to enable this option, there is a consideration when doing so. This will double the number of Content Manager security groups that are created. Consider a list item that the corresponding record has a security level of "Confidential". In order to limit access to the item,

users who have the Confidential security level and the ability to modify records should be granted permission to edit the item, but users who have the Confidential security level but no permission to modify records should only be granted permission to view the item.

In this example a group would be created to represent users with Confidential and edit permission and another group would be created to represent users with Confidential but without edit permission.

If after looking at the considerations earlier in this section, the doubling of group numbers will not cause issues, then it is recommended to check this option to improve the user experience.

Capture SharePoint permissions as Content Manager access controls

The Capturing access controls section of this document described applying access controls to represent the SharePoint permissions applied to an item. This will only occur if the ***Capture SharePoint permissions as Content Manager access controls*** check box is checked.

While this option is turned on, the following options, **Apply Content Manager access controls as SharePoint permissions** and the **Apply Content Manager security as SharePoint permissions** have no effect on SharePoint item permissions, i.e. the SharePoint permissions will remain unchanged.

Include inherited permissions

The ***Include inherited permissions*** check box is only enabled if the ***Capture SharePoint permissions as Content Manager access controls*** check box is checked.

If this option is not checked, when capturing SharePoint permissions as Content Manager access controls, only list items with specific permissions are considered. If a list item is inheriting permissions from the site or the list, then the access controls for the record in Content Manager will be set to “Everyone”.

If this option is checked though, then the access controls for the record will be set based on the permissions that the item is inheriting from the list or site.

Apply Content Manager access controls as SharePoint permissions

The Content Manager security applied to managed SharePoint content section of this document described applying Content Manager access controls as permissions on a SharePoint list item. This will only occur if the ***Apply Content Manager access controls as SharePoint permissions*** check box is checked.

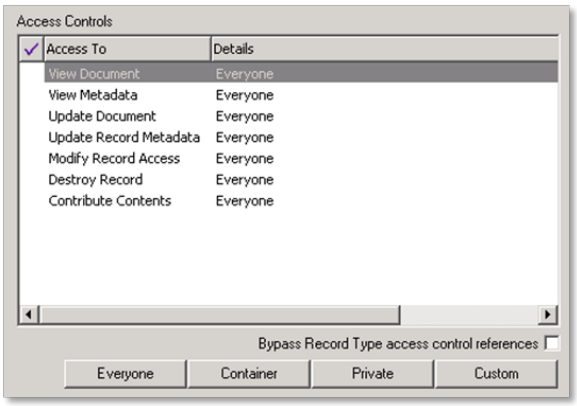
Apply Content Manager security as SharePoint permissions

The Content Manager security applied to managed SharePoint content section of this document described applying Content Manager security levels and caveats as permissions on a SharePoint list item. This will only occur if the ***Apply Content Manager security as SharePoint permissions*** check box is checked.

Everyone group

When there are no restrictions on accessing a record in Content Manager (either from security or access controls), a record is considered to be available to everyone. This means that it is available to everyone who has an active user location in Content Manager.

The use of “everyone” is most prevalent when examining the access controls for a record. If no specific access controls are applied, the access controls will display “Everyone”.



In Content Manager “Everyone” refers to all users with an active user location. By default, there is no equivalent group to this in Active Directory or SharePoint. To assign permissions to a list item in SharePoint where it has been determined that everyone should have access, an Active Directory or SharePoint group must be created to represent these users.

The ***Everyone group*** picker in the security behavior section of the page allows specifying the Active Directory group that represents “Everyone” in Content Manager. This group is granted permission to the item in cases in which everyone should have access to the item.

The simplest example of using the “Everyone group” is in the case where a record has no security level or caveats and no access controls. Everyone who can access Content Manager has permission to access the record.

If a group called “All Content Manager users” is specified as the “Everyone group,” then this group will be granted the “View Secured Item” and “Edit Secured Item” permission levels for any list item representing the record (assuming that the security settings are configured to apply permissions).

Using a SharePoint group instead of an AD group

In scenarios where an AD group is not suitable, a fixed SharePoint group can be used. ***Selecting Use SharePoint group (All Content Manager Users)*** indicates that users who are a member of the SharePoint group ***All Content Manager Users*** should be considered as everyone.

If there is already a group created with this name, it will be used. If the group does not exist, it will automatically be created the first time it is required.

> **NOTE:** A group will be created on each site collection as needed. Although these groups have the same name, they are considered different groups by SharePoint. Bear this in mind as you may need to populate this group with the relevant users in multiple places. This provides the flexibility however to have different users with everyone access on different site collections.

Considerations for the “Everyone Group”

You should ensure that the ***Everyone group*** chosen contains all Content Manager users. If a user does not appear in this group, then regardless of their rights in Content Manager, they may not be able to access permitted content in SharePoint.

Note that all members of the “Everyone group” will be able to access a list item that uses this group in permissions, even if the user does not have a valid location in Content Manager. If this is not the

desired behavior, then it is important to ensure that only valid Content Manager users belong to this group.

> **NOTE:** Remember that a member of the everyone group who does not have a valid Content Manager location will not be able to modify content even if they can access it.

If there is a requirement to use a different group for each site, this can be achieved by saving the security settings for that site with the required site specific group entered as the everyone group.

Managed Item Administrators group

Using the Content Manager Security feature, there are scenarios where the permissions to a list item are so restrictive that no user can access the item and/or no user is able to modify the permissions to the item. To prevent inadvertent item “lock outs” such as these, a group known as the “Managed Item Administrators group” is always granted permission to list items.

The ***Managed Item Administrators group*** picker in the security behavior section of the page allows specifying the group of users who should always be granted this access.

For every list item where permissions are set by the Content Manager Security feature, the group specified will be granted the permission level ***Administer Secured Item***. This permission level includes that ability to manage permissions.

Using a SharePoint group instead of an AD group

In scenarios where an AD group is not suitable, a fixed SharePoint group can be used. ***Selecting Use SharePoint group (Managed Item Administrators)*** indicates that users who are a member of the SharePoint ***group Managed Item Administrators*** should be considered as users with this permission.

If there is already a group created with this name, it will be used. If the group does not exist, it will automatically be created the first time it is required.

> **NOTE:** A group will be created on each site collection as needed. Although these groups have the same name, they are considered different groups by SharePoint. Bear this in mind as you may need to populate this group with the relevant users in multiple places. This provides the flexibility however to have different users with manage item administrator access on different site collections.

Considerations

Members of this group will be permitted to see all managed items in SharePoint regardless of their security in Content Manager. It is important therefore that you carefully consider who the members of this group are. Consider this group to be equivalent to a site collection administrator in SharePoint or an administrator in Content Manager.

It is possible to specify a different group to use for each site. This would limit the ability for members of this group to access content on other sites and in highly sensitive implementations, may provide added protection from inadvertent exposure of sensitive content.

14.3 Setting security and access control using SharePoint

Security levels, security caveats, and access controls can of course be set on a record using the Content Manager client. This cannot be done though until the record actually exists and it requires the user to have access to the Content Manager client.

Several SharePoint columns are included with the Content Manager Governance and Compliance app that can be used with content types, or directly on lists and libraries to allow security levels, security caveats and access controls to be set for a list item just as any other list item properties are set.

These columns are created by the column creation feature found in the configuration tool. This is described in the product installation guide. If this tool has not been run, these columns will not be available. The remainder of this section assumes that this tool has been run.

14.3.1 Security columns

Security level

The ***Content Manager Security Level*** site column is available in the ***Content Manager Columns*** group of site columns.

This column uses the ***Security Levels*** synchronized term set to allow users to select a value from the security levels used by Content Manager.

> **NOTE:** A security level column only has the effect of restricting access to a list item if:

- The item is managed by Content Manager
- The Content Manager Security Settings have the “Apply Content Manager security as SharePoint permissions” option checked

Security caveat

The ***Content Manager Security Caveats*** site column is available in the ***Content Manager Columns*** group of site columns.

This column uses the ***Security Caveats*** synchronized term set to allow users to select a value from the security caveats used by Content Manager.

Note that a security caveat column only has the effect of restricting access to a list item if:

- The item is managed by Content Manager
- The Content Manager Security Settings have the “Apply Content Manager security as SharePoint permissions” option checked

Access control columns

Two columns are available in the ***Content Manager Columns*** group of site columns. These columns are designed to allow viewing and editing the access controls for a list item using SharePoint.

Both of these columns can be added to a list or content type.

The ***Content Manager View access controls*** column allows viewing and specifying the user's and groups who have view permission to the list item and record.

The ***Content Manager Edit access controls*** column allows viewing and specifying the user's and groups who have edit permission to the list item and record.

Eligibility to be displayed

Only the users who have view access controls should be displayed in the "View access control" column. Only the users who have edit access controls should be displayed in the "Edit access control".

Remembering that Content Manager has multiple view and edit access controls, the following rules are used to determine which users and groups are eligible to be displayed.

View: users who have all of the following:

- View Document
- View Metadata

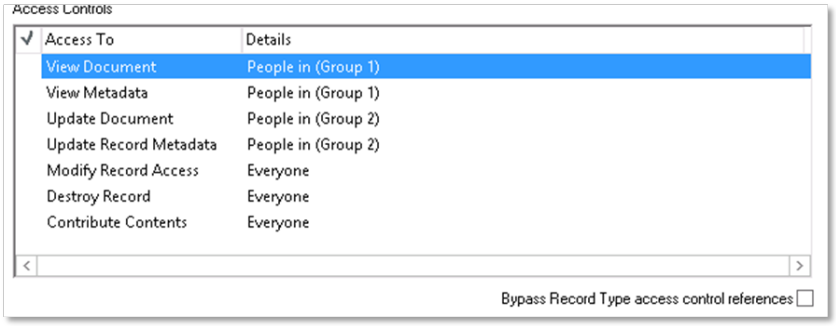
Edit: users who have all of the following:

- Update Document
- Update Metadata

Filtering the locations that are displayed

The premise of the access control columns is that the users and groups applied to access controls for the Content Manager record are shown in the field.

For example, if the access controls on the record were:



The access control columns for any associated list item would show:

Name	Configuration Tool.log
Title	
Record Number	D18/8
CM Security Level	Confidential
CM Security Caveats	Caveat A;
CM View access control	SPQA4\group1
CM Edit access control	SPQA4\group2

Version: 5.0
Created at 7/10/2018 11:40 PM by spadmin
Last modified at 7/11/2018 12:12 AM by spadmin

Close

However, what if a location used in Content Manager for access control did not have an associated Active Directory or SharePoint group or user? If in the previous example, ***Content Manager Group 1*** is added to the view access controls. This group is only a location in Content Manager and has no associated Active Directory or SharePoint group.

Access Controls

Access To	Details
View Document	People in (Group 1 or HPRM Group 1)
View Metadata	People in (Group 1 or HPRM Group 1)
Update Document	People in (Group 2)
Update Record Metadata	People in (Group 2)
Modify Record Access	Everyone
Destroy Record	Everyone
Contribute Contents	Everyone

Bypass Record Type access control references

Because this group does not have an associated Active Directory or SharePoint group, it is not possible to represent in the access control columns. Therefore, the access control columns in this scenario will continue to display:

Name	Configuration Tool.log
Title	
Record Number	D18/8
CM Security Level	Confidential
CM Security Caveats	Caveat A;
CM View access control	SPQA4\group1
CM Edit access control	SPQA4\group2

Version: 5.0
Created at 7/10/2018 11:40 PM by spadmin
Last modified at 7/11/2018 12:12 AM by spadmin

Close

Similarly, group locations that are based on SharePoint groups are site collection specific. Consider a record that is exposed on two different site collections. On site collection 1 (SC1) a user restricts

the edit access control to “SharePoint Group 1”. This group is specific to SC1 and cannot be represented on SC2.

When viewing the edit access controls on SC1, “SharePoint Group 1” would be displayed.

When viewing the edit access controls on the record in Content Manager, “SharePoint Group 1” would be displayed.

However, when viewing the edit access controls on SC2, the user would not see “SharePoint group 1”.

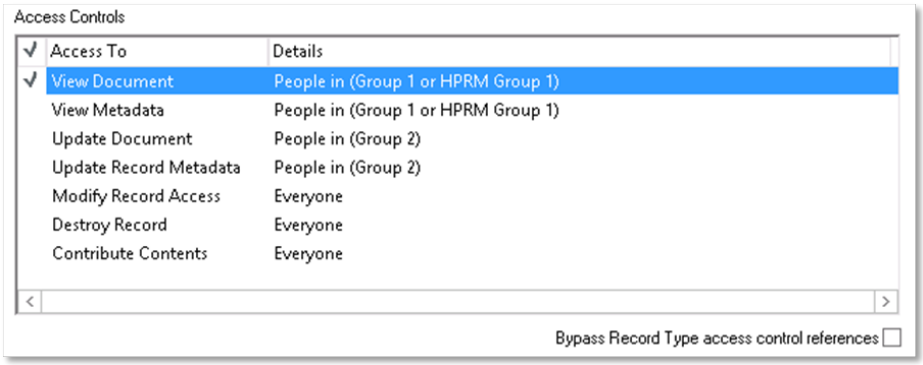
The values displayed in the access control columns are filtered to only show users and groups that have Active Directory accounts or SharePoint groups that originate on that particular site collection.

Filtering of referenced access controls

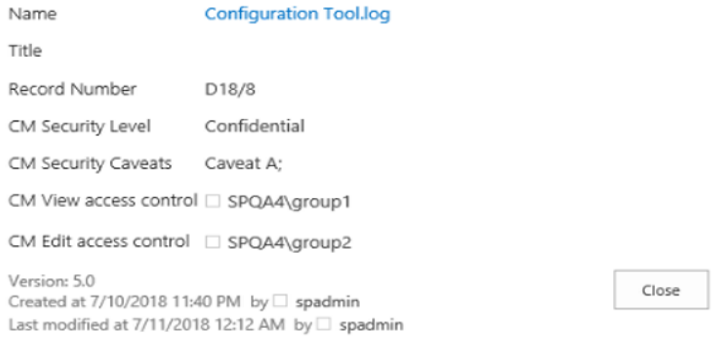
When a record has referenced access controls (from record type, container or classification), these access controls will not be displayed in the access control columns.

Saving when locations have been filtered

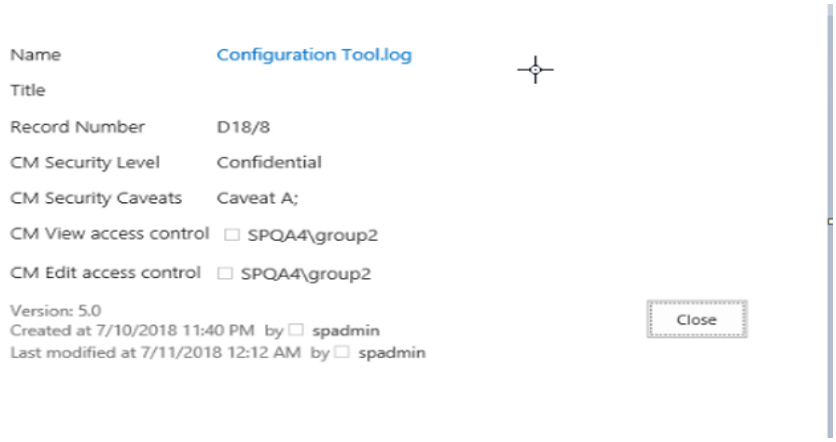
In the scenario where one or more locations have been filtered from display in an access control column, changing the access control in the column will not remove the locations that have been filtered. For example, if the current access controls include the “Content Manager Group 1” location that has no mapped Active Directory or SharePoint group:



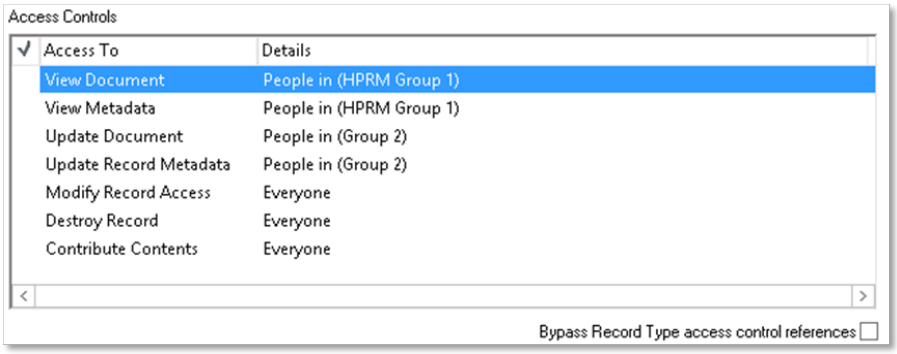
We have already seen that the access controls that are displayed will filter this group:



Consider the scenario where a user modifies the view access control to make the item available to “Group 2” to view and removes the ability for “Group 1” to view:



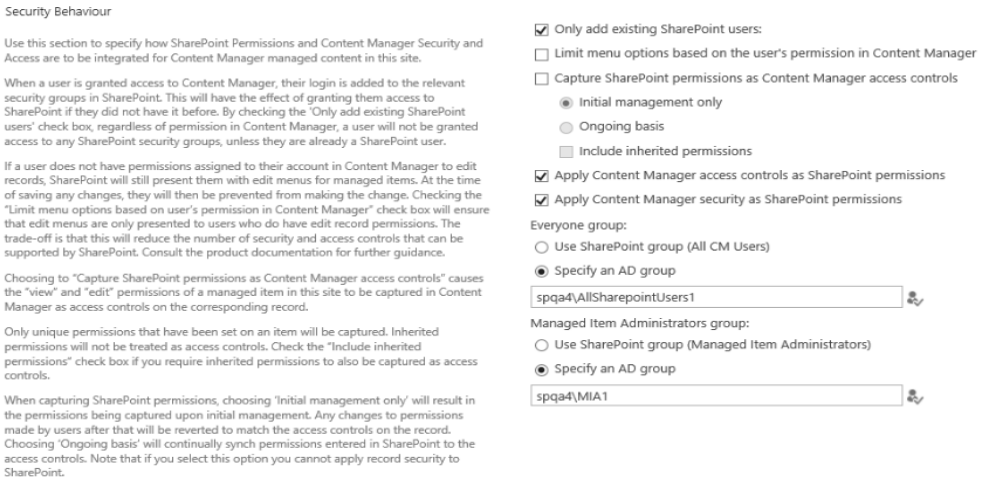
The resultant access control on the record still includes the filtered group “Content Manager Group 1” despite implementing the changes made by the user in SharePoint.



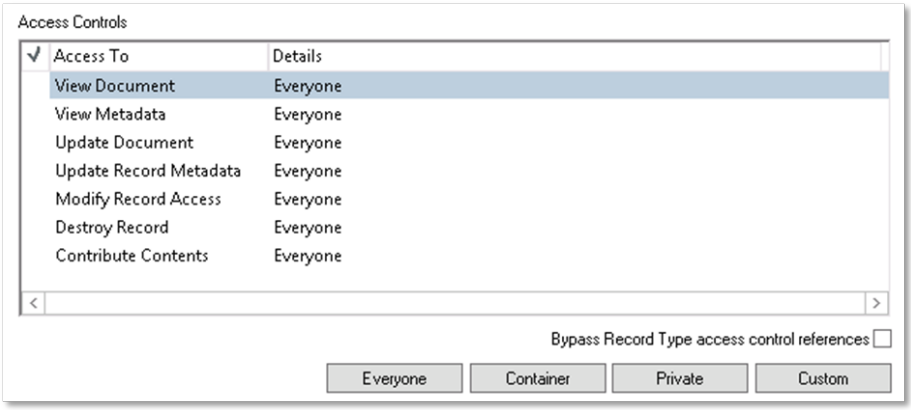
Displaying “Everyone” access controls

In the scenario where the access controls are “Everyone”, an access control column will display the group that is specified in the Content Manager Security settings as the “Everyone” group.

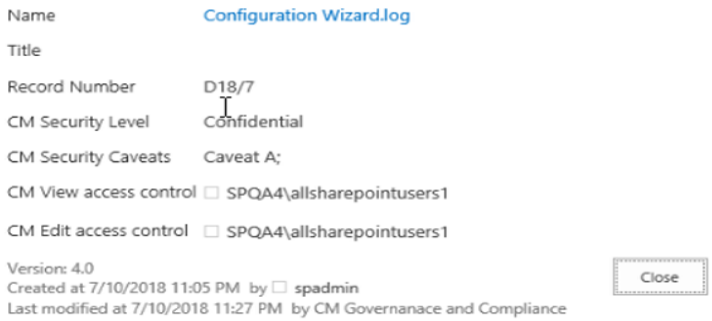
In the following example, the “Everyone” group has been specified as “AllSharePointUsers1”.



There are no specified access controls on the record therefore all access controls are “Everyone” in Content Manager.



Any list item representing the record will have the “All Users (windows)” shown in the relevant access control columns.

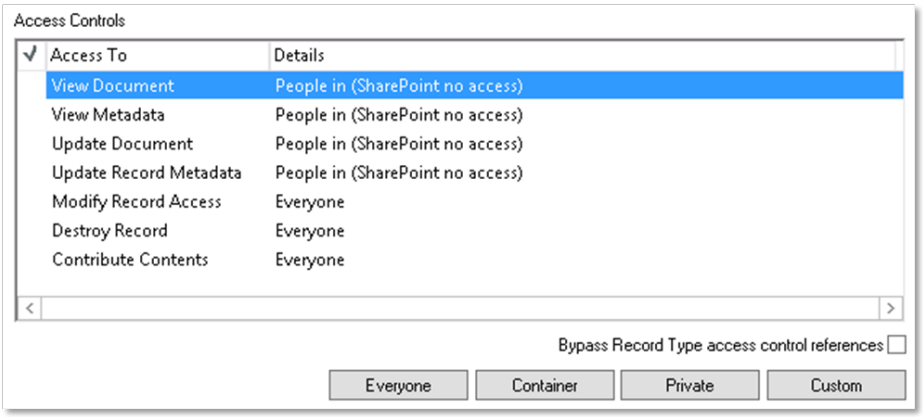


Similarly, if the group entered into an access control column corresponds to the “Everyone” group, the resultant access control will be set the “Everyone”. If the “Everyone” group is included along with other users and groups, access control will still be set to “Everyone”.

Behavior when no entry is made

If no entry is made in an access control column, the access controls on the corresponding record are set to “Everyone” during initial management of the list item. However, once managed, changing the column to have no entry will result in the access control becoming either:

- Any filtered locations that exist on the record, or
- If there are no filtered locations and this change would result in no users or groups having access, the ***SharePoint no access*** group will be granted access.



Restricted groups

You will not be permitted to enter special Active Directory groups such as “All Authenticated Users” into access control columns.

Attempting to use these special group will result in an error.

Behavior when “Capture SharePoint permissions as Content Manager access controls” is checked

Checking “Capture SharePoint permissions as Content Manager access controls” on the Content Manager Security Settings indicates that the permissions assigned to a list item should be used to determine the access controls. This setting will take precedence even if values are specified in access control columns.

These controls are not designed to be used in conjunction with the “Capture SharePoint permissions as Content Manager access controls” setting. You should choose either method for assigning access controls, not both. If using both, the capture of SharePoint permissions will always take precedence.

Automatic location creation

If a group or user that does not have a location in Content Manager is entered in an access control column, the automatic location creation process is used to create a location to match. See the “**Error! Reference source not found.**” section earlier in this chapter for details.

14.3.2 Immediate lock down of secured items

SharePoint list items do not have the permissions restricted in accordance with security and access control until that item is managed. While an item is unmanaged, it is the permissions that have been set in SharePoint that will determine who can access a list item.

Consider the situation though where a user uploads a document to SharePoint and marks it as having the “Confidential” security level. If the permissions were not restricted on this list item until it were managed, there will be a period where users without the “Confidential” security level may be able to access the document using SharePoint.

To prevent this situation, in certain circumstances, the list item will be immediately locked down to the following users:

- The user who created the list item
- The managed item administrators group

These groups are granted the permission: ***Interim edit CM Secured Item***

This lock down will happen immediately rather than when manage occurs. As soon as the item is managed, the permissions will be corrected to represent the security level, caveats and access controls on the record.

This immediate lock down occurs when:

- The ***Apply Content Manager security as SharePoint permissions*** option is checked on the security settings page, AND
- A value is entered in either
  - Content Manager Security Level OR
  - Content Manager Security Caveats

It will also occur when:

- The ***Apply Content Manager access controls as SharePoint permissions*** option is checked on the security settings page, AND
- A value is entered in either
  - Content Manager edit access controls
  - Content Manager view access controls

14.4 Determining the security of an item

It is often required to determine what the security of an item is. This may involve identifying the security and access control applied to the Content Manager record, or it may involve identifying how the permissions in SharePoint have been set.

There are several options available to surface the details of the security of an item.

14.4.1 Standard Content Manager columns

There are several columns that are created by the column creation tool that can be used to display the current security and access controls of the associated record. By adding these to your content types or lists, the Content Manager values will be displayed. These columns include:

- Access control
- Security
- Security Caveats
- Security Level
- Security Locks

14.4.2 Security and access control specific columns

Earlier in this chapter, four columns were described that were specific to security and access control. Adding these columns to content types of lists allows the viewing and editing of these values:

- Content Manager Security Level
- Content Manager Security Caveats
- Content Manager Edit Access Controls
- Content Manager View Access Controls

14.4.3 Security details page

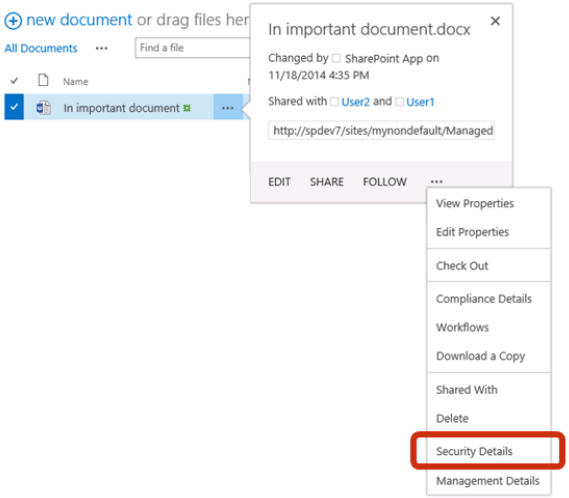
A dedicated page is provided to allow you to see in one view:

- The security and access controls applied to the Content Manager record
- The permissions on the SharePoint list item

This page is known as the ***Security Details*** page. Click **Close** to return to the list without refreshing the SharePoint page. If the top right corner X button is used to close the dialog then the SharePoint page will be refreshed.

Accessing the page

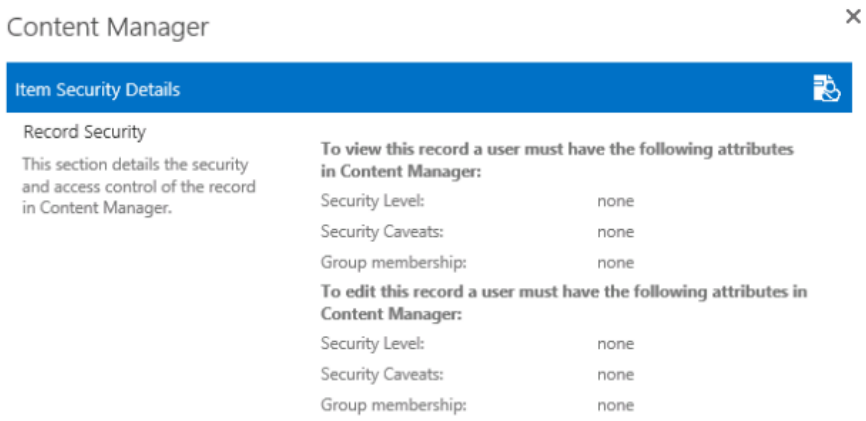
The ***Security Details*** page is accessible from the ribbon and the context menu dropdown for a particular item.



Record security

The first section on the Security Details page describes the security and access controls of the associated record. If the SharePoint item is not yet managed, there will not be an associated record therefore the page is unable to display details in this section.

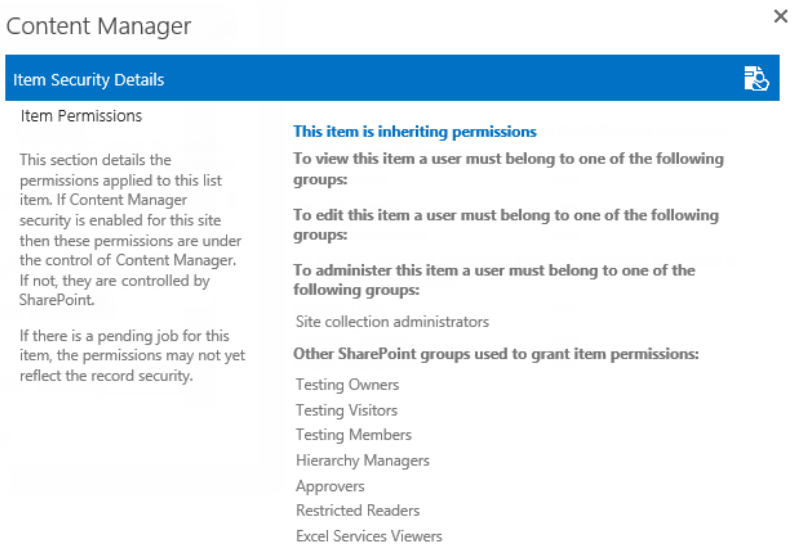
This section allows the viewing of both the security level and caveats applied to the record. It also summarizes the access controls identifying which Content Manager group locations a user must be a member of in order to view and/or edit the record.



This section of the page is populated directly from the Content Manager record. It will always reflect the actual values set on the Content Manager record at that time i.e. the values here are ***real time*** values.

Item permissions

The second section of the page describes the SharePoint permissions that are set on the item.



These permissions are divided into the following categories:

- Permissions required to view the item
- Permissions required to edit the item
- Permissions required to administer the item
- Other permissions

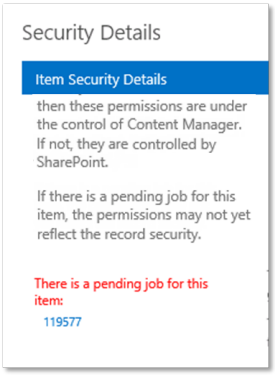
From a permissions perspective, this equates to the following permission levels:

Permission Category	Actual permission level
Permissions required to view the item	View CM secured item
Permissions required to edit the item	Edit CM secured item
Permissions required to administer the item	Administer CM secured item OR Site collection administrator
Other permissions	Any other permission level

Pending jobs

Using the security details page, in some scenarios, the permissions applied to the SharePoint item may appear not to match the security and access controls of the record itself. Assuming that the security settings are configured to apply security and access controls, this situation typically arises because there is a change that has been made to the Content Manager record and the job responsible for updating the list item has not yet processed.

In this situation, a warning is included on the page indicating that there is a pending job.



The job can be accessed directly from the link shown.

14.5 Configuration Access Controls

The Configuration Access Controls page is used to specify which users can perform specific configuration tasks. The different configuration access controls are:

- Configuration administrator - people in this role can manage any configuration - including the ability to define role membership
- Default Integration Settings - people in this role can manage the default integration settings
- Site RMO’s - people in this role can manage site RMO’s
- List RMO’s - people in this role can manage list RMO’s
- Site LMO’s - people in this role can manage site LMO’s
- List LMO’s - people in this role can manage list LMO’s

- Management rules - people in this role can manage management rules, management selectors and management instructions
- LMP's - people in this role can manage LMP's
- Monitoring - people in this role are permitted to view all jobs in the job queue
- Mappings - people in this role can manage CT2RT and column mapping
- Search Settings - people in this role can manage search settings
- Exposure Settings - people in this role are permitted to modify exposure settings
- Security - people in this role can manage security settings
- Auditing - people in this role can see site and site collection auditing. Anyone can see list auditing
- System Roles - these roles are used by the system:
  - Document Viewer - people in this role are permitted to view SharePoint documents on behalf of Content Manager user.
  - Search Administrators - people in this role must belong to search administrator role. People in this role are permitted to execute federated searches.
  - Default Search Location - people in this role are permitted to perform anonymous searches.

    > **NOTE:** Make sure that the account nominated for Default Search Location is at least an Inquiry User in Content Manager. Also have security level, caveats, and access control relevant to the content that should be returned in an anonymous search.

As a Configuration administrator, which is set in the Content Manager SharePoint Configuration Tool, it is possible to add either Active Directory users or Active Directory Groups to the specific Configuration Access Control group.

Once the user or group has been added to the Configuration Access Control group they will be granted access to modify SharePoint Integration configuration settings, as outlined above.

14.6 Troubleshooting

Occasionally, users may feel that security has been applied incorrectly. It can in some scenarios be tricky to confirm the correctness of application of security and demonstrate to a user that the security is correct.

This section describes some tools and techniques for troubleshooting in these scenarios.

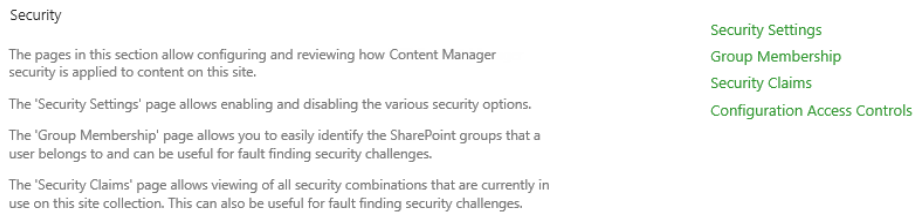
14.6.1 Security details page

The security details page (described in an earlier section) is the primary fault finding tool. It illustrates what Content Manager considers the security and access control to be for a record, and what the corresponding permissions are that have been applied in SharePoint.

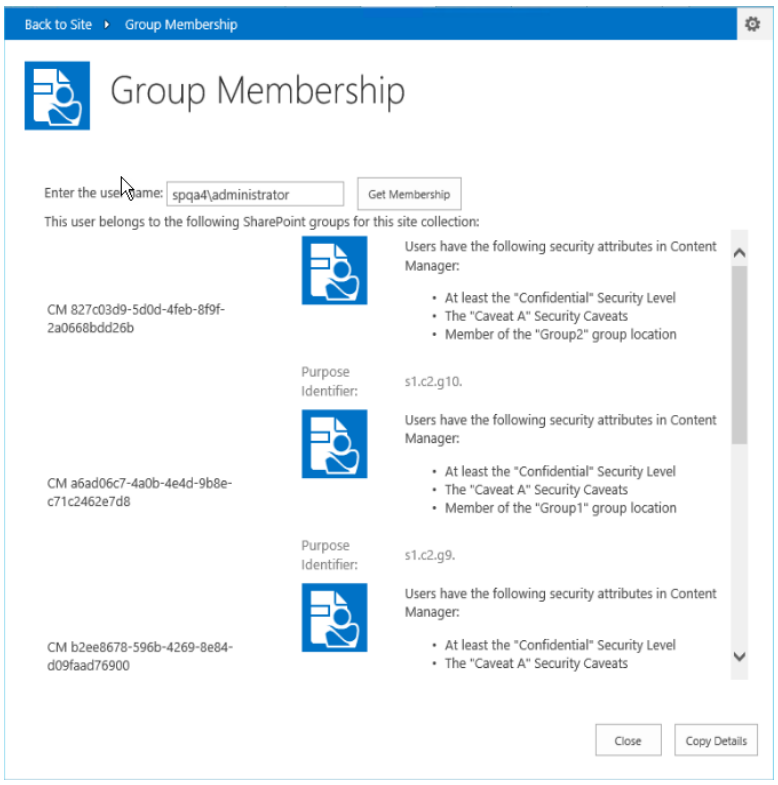
Often simply referring to this page clarifies why security has been applied as it has.

14.6.2 Group Membership page

From the app start page, under the ***Security*** section is a link to the ***Group Membership*** page.



The group membership page is a simple tool that allows the retrieval of all SharePoint groups that a particular user belongs to. Enter the user name and click the ***Get Membership*** button to retrieve all groups.



> **NOTE:** This will retrieve the list of all SharePoint groups, not just Content Manager security groups.

SharePoint allows you to examine a particular group to determine who the members are, but it does not provide you a tool to detail all groups that a user belongs to. This tool is designed to fill that void. This information can be invaluable when trying to determine why a user can or cannot access a particular item.

14.6.3 Fault finding techniques

This section details some common scenarios along with steps for fault finding;

You have set a security level and/or caveat on an item, but a user who has that security level and/or caveat cannot see/edit the item in SharePoint or a user who does not have the security level and/or caveat can see/edit it

1. Look at the security details page
2. Confirm that the record security section correctly reflects the security level and/or caveat:
   a. If no: confirm that the columns used to apply security level and caveat are mapped correctly on the column mapping page. If not, this is the issue.
   b. If yes: Confirm that there is not a pending job for this item (there will be a warning under the item permissions description on the security settings page). If there is, wait for it to complete then go back to step 1.
3. Confirm that the item view and item edit permissions are locked down to a Content Manager group that represents the security level and/or caveat.
   a. If no: confirm that the ***Apply Content Manager Security as SharePoint permission*** option is checked on the security settings for the site. If not, this is the issue.
4. Using the ***Group Membership*** page, confirm that the user in question belongs to the groups used to secure the item.
   a. If they belong to the group and you believe they shouldn't: using Content Manager, confirm that the user has all the security attributes described in the group description.
      i. If they do, then this is correct
      ii. If they don't, then check to see if there is a ***PopulateSecurityGroup*** or ***RefreshSecurityGroups*** job pending in the job queue. Wait for this to complete then repeat step 4
   b. If they don't belong to the group and you believe they should: using Content Manager, confirm that the user has all the security attributes described in the group description.
      i. If they don't, then this is correct
      ii. If they do, then check to see if there is a ***PopulateSecurityGroup*** or ***RefreshSecurityGroups*** job pending in the job queue. Wait for this to complete then repeat step 4

You have set and access control on a record, but a user who should have permission cannot see/edit the item in SharePoint or a user who does not have permission can see/edit it

1. Look at the security details page
2. Confirm that the record security section correctly reflects the resultant view and edit groups:
   a. If no: confirm that the columns used to apply access controls are mapped correctly on the column mapping page. If not, this is the issue.

   b. If yes: Confirm that there is not a pending job for this item (there will be a warning under the item permissions description on the security settings page). If there is, wait for it to complete then go back to step 1.

3. Confirm that the item view and item edit permissions are locked down to a Content Manager group that represents the access controls.

   a. If no: confirm that the ***Apply Content Manager access controls as SharePoint permission*** option is checked on the security settings for the site. If not, this is the issue.

4. Using the ***Group Membership*** page, confirm that the user in question belongs to the groups used to secure the item.

   a. If they belong to the group and you believe they shouldn't: using Content Manager, confirm that the user has all the security attributes described in the group description.

      i. If they do, then this is correct

      ii. If they don't, then check to see if there is a ***PopulateSecurityGroup*** or ***RefreshSecurityGroups*** job pending in the job queue. Wait for this to complete then repeat step 4

   b. If they don't belong to the group and you believe they should: using Content Manager, confirm that the user has all the security attributes described in the group description.

      i. If they don't, then this is correct

      ii. If they do, then check to see if there is a ***PopulateSecurityGroup*** or ***RefreshSecurityGroups*** job pending in the job queue. Wait for this to complete then repeat step 4

14.7 Implementation considerations

This section describes considerations for utilizing the Content Manager Security feature.

14.7.2 Site Collection Administrators

Users who are site collection administrators (SCA) have access to all list items regardless of the permissions that are set on the site, list, or list item. In essence, an SCA bypasses security in much the same way that an administrator in Content Manager does.

Note that regardless of security level, security caveats, or access controls that are applied by the Content Manager Security feature, a site collection administrator will have access to all list items.

14.7.2 Web Application User Policies

Users who are granted "Full Control" or "Full Read" permission through a web application user policy will have access to all list items regardless of the permissions that are set on the site, list or list item. In essence, users with these permissions bypass security in much the same way that an administrator in Content Manager does and in the same way that and SCA does.

Note that regardless of security level, security caveats or access controls that are applied by the Content Manager Security feature, a user granted “Full Control” or “Full Read” in a web application user policy will have access to all list items.

14.7.3 Synchronizing with existing Content Manager locations

The Content Manager Security feature creates Content Manager locations to represent Active Directory and SharePoint groups that are used in SharePoint to restrict permissions. However, your organization may already utilize a tool that has created locations in Content Manager based on Active Directory users and groups. This section describes the steps you may need to take to ensure that the security feature recognizes these existing locations and therefore does not create duplicate ones.

Active Directory users

When an Active Directory user is utilized in the permissions of a SharePoint item, during management, Content Manager locations are examined to see if a corresponding location already exists. The matching is performed based on the value of the network login for the location (found on the profile tab in Content Manager).

It is not important that the “Accept logins for this user, using login name” is checked. A location can be matched even if it is currently not accepting logins. What is important though is that the network login includes the full account name and the domain.

Active Directory groups

Matching of Active Directory groups is based on the value in the network login for the location in Content Manager. If you ensure that this has the network account name and the domain, then existing locations that correspond to Active Directory groups will be correctly identified and used.

SharePoint groups

If you have SharePoint groups that correspond to Content Manager group locations, it is also the network login of the location that is used to match these. In the case of SharePoint groups though, the value of the network login is the concatenation of the site collection ID and the group ID.

For example, if the ID of the site collection the group belongs to is “1b080d7a-c8ba-474c-8d1a-0c6861c3781c” and the ID of the SharePoint group is “28” then the network login for the corresponding Content Manager group location should be:

```
1B080D7AC8BA474C8D1A0C6861C3781C28
```

> **NOTE:** All hyphens from the site collection ID have been removed and all characters are in upper case.

To find the ID of the site collection, please consult stsadm documentation for SharePoint. A simple way to identify the ID of a SharePoint group is to navigate to the “People and Groups” page from “Site Settings” then click on the link to the group. The URL of the page will end with:

```
_layouts/people.aspx?MembershipGroupId=XX
```

where “XX” is the identity of the SharePoint group.

Special AD accounts

Do not use special AD accounts such as ***All authenticated users*** to secure content in SharePoint. This will result in a corresponding location being created in Content Manager that may never be successfully populated.

15 Auditing

Auditing of information is designed to illustrate:

- Whether an action has been performed against information, eg create, modify, view or delete
- When that action was performed
- Who performed the action

Each action is recorded as an individual audit entry. The collection of audit entries is referred to as the audit history.

Audit history is available at various levels in SharePoint:

- Item
- List
- Site
- Site collection

A parent object may display audit entries of the child object. For example, viewing the audit history of a site, will include the audit history of all lists on that site.

15.1 Audit sources

Audit entries that are applicable to an object in SharePoint may come from one of three different sources:

1. Record

   Records in Content Manager include an audit history. Audit entries are for actions performed against that particular record.

2. SharePoint

   SharePoint audits actions performed against its items including when documents are viewed.

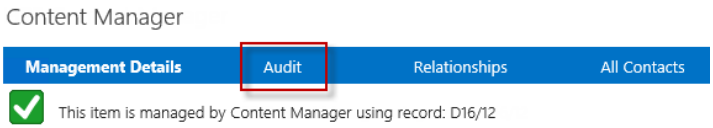
3. Configuration

   Changes to product configuration create audit entries in the configuration database. In this version the following configuration is audited:

   - Default Integration Settings
   - RMOs
   - LMOs
   - Column Mapping
   - Content type to Record Type mapping
   - Security
   - Exposure

15.2 Item audit history

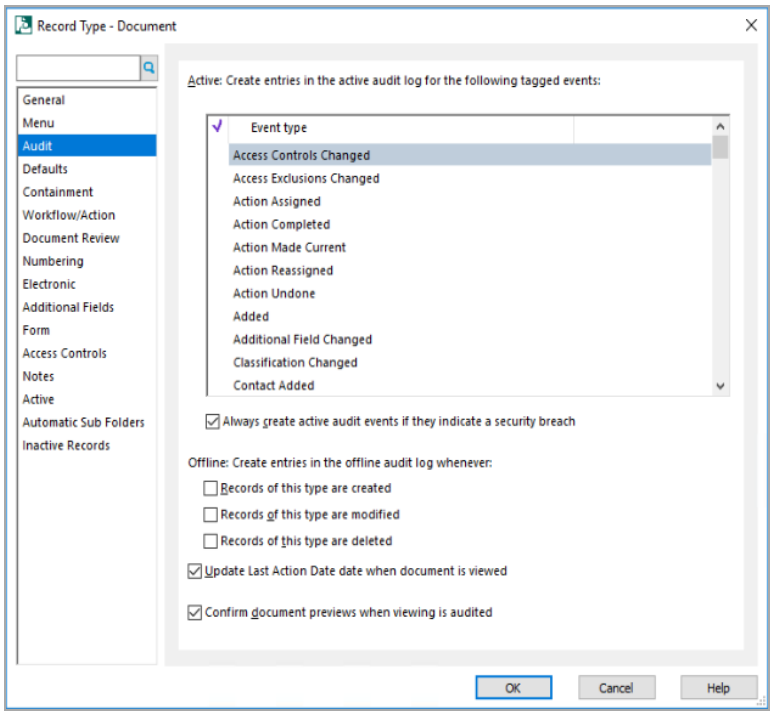
The audit history for a particular item can be accessed on the management details page. Items, whether they are managed or unmanaged, include the ***Audit*** link in the title bar of the management details page.



15.2.1 Enabling auditing events

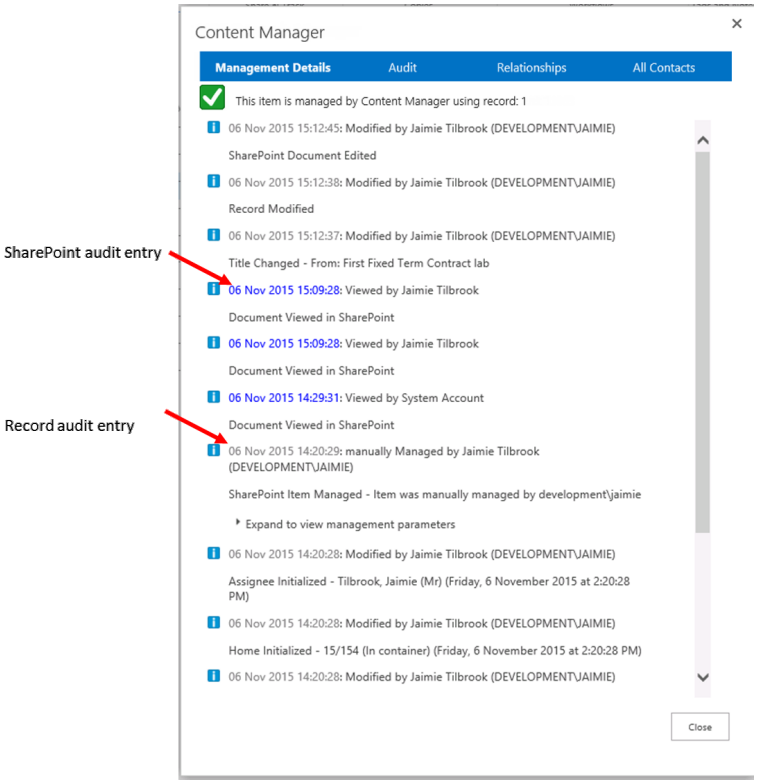
The audit events that are captured by Content Manager need to be configured. This section describes the events that relate to SharePoint only. For a description of all other audit events, please read the Content Manager help file.

SharePoint specific audit events are enabled on a per record type basis. Using the Content Manager desktop application, go to **Manage > Record Types > Audit tab**.



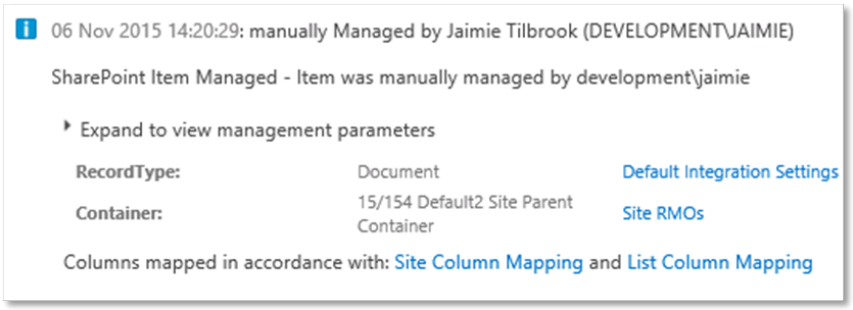
15.2.2 Audit history

The audit history displayed includes all applicable entries from the record, SharePoint and configuration. In the entry, the date and time is shown in blue if the source of the entry is SharePoint. Else, it is grayed if the source of the entry is record.



Management parameters

Audit entries indicating that an item was managed or finalized include the ability to view the configuration that was used during the management. Expanding the section ***Expand to view management parameters*** reveals the values and configuration that were used.



Following the links to the configuration will display the configuration values as they were at the time the process ran, even if they have been subsequently modified.

Status

Three status images are used to indicate the severity of an audit entry.

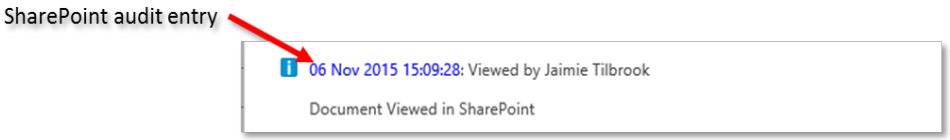
Image	Severity
	Information: This entry is information only entered as part of normal operations.
	Caution: Indicates that a problem has occurred that may require attention.
	Warning: Indicates that an error has occurred that requires attention.

15.2.3 Audit entries indicating document viewed in SharePoint

When a document is viewed in SharePoint, this event can be configured to be included in the audit history for an item.

> **NOTE:** Audit entries for document viewing events through SharePoint are only available if the auditing components have been installed. See the Installing the auditing components section of the installation guide.

When a document is viewed through SharePoint, an audit entry is created by SharePoint. If the item audit history is viewed shortly after the view occurred, this audit entry will be included in the history but indicated that it was sourced from SharePoint.



> **NOTE:** For a single view event, there may be multiple view entries in the history.

At this point, the audit entry is only in SharePoint and not on the record audit history.

Every five minutes, a job executes to place SharePoint view audit entries onto the relevant record. Once completed, although SharePoint still has the view audit entry, it will now be shown as being sourced from the record.

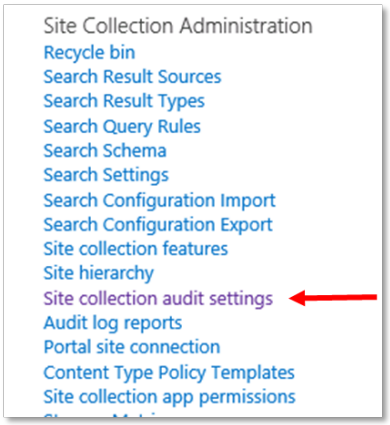
Examining the record through Content Manager, the audit entry can be seen in the history for the record.

Configuring “view” audit events in SharePoint

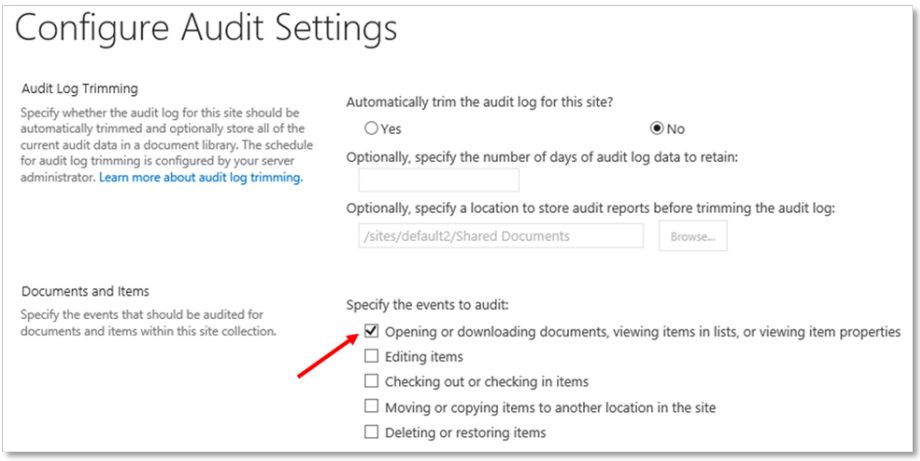
SharePoint by default does not capture audit entries when a document is viewed. This must be enabled for a site collection.

> **NOTE:** It is not possible to configure document view events in Office 365

Navigate to site settings then follow the link to ***Site collection audit settings***.



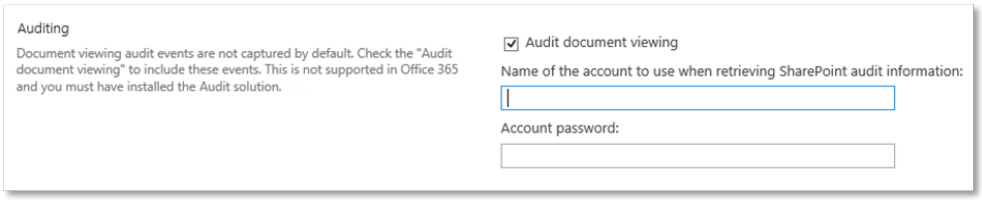
Ensure that the option shown in the screen shot below is checked then save the settings.



Indicating that view events should be included in history

By default, the app is not configured to include document view events in the audit history. This configuration is performed on the The Default Integration Settings (DISP) page.

The ***Auditing*** section of this page is used to configure the inclusion of these entries.



Check the ***Audit document viewing*** check box.

Retrieval of audit entries from SharePoint is performed as the account that is entered in the subsequent text boxes. This account typically needs to be a site collection administrator to retrieve these details.

> **NOTE:** If you are editing the default integration settings for the default site collection, this account should have the necessary permissions on all site collections that use these default settings.

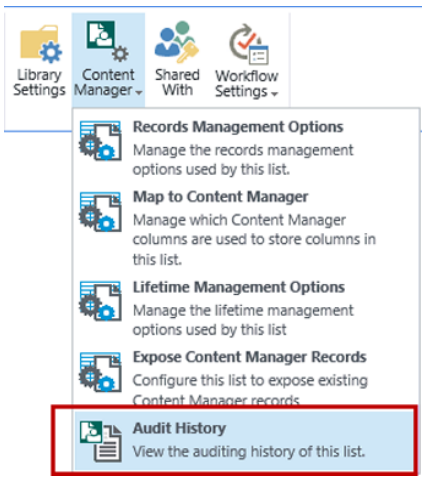
15.3 List audit history

It is often a requirement to view the audit history for a list. This may be to identify any issues that are occurring with a list or determine if and when configuration has been changed that may be affecting the expected behavior of the app on that list.

15.3.1 Accessing list audit history

From the ribbon menu for a list or library, select the **list** or **library** tab and locate the **Content Manager** button in the **Settings** section of the ribbon.

Expand this button and select the **Audit History** option.



15.3.2 Inclusions in list audit history

Viewing the audit history for a list will show the following audit entries that are applicable to this list:

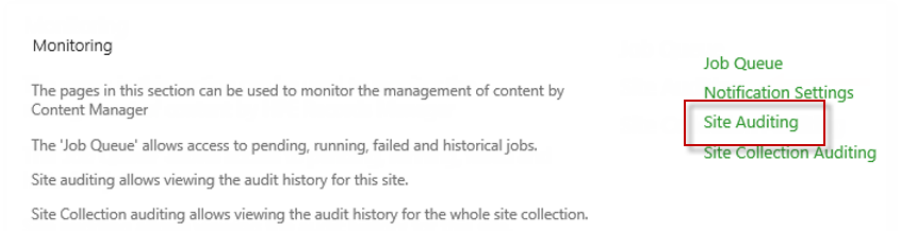
- Any warning or caution entries that apply to any item in the list
- Any configuration changes to the Content Manager Governance and Compliance app that have been made that apply to this list specifically

15.4 Site audit history

It is often a requirement to view the audit history for a site. This may be to identify any issues that are occurring with a site or determine if and when configuration has been changed that may be affecting the expected behavior of the app on that site.

15.4.1 Accessing site audit history

Site audit history is accessed from the app start page. Click the **Site Auditing** link located in the **Monitoring** section of the page.



15.4.2 Inclusions in site audit history

Viewing the audit history for a site will show the following audit entries that are applicable to this site:

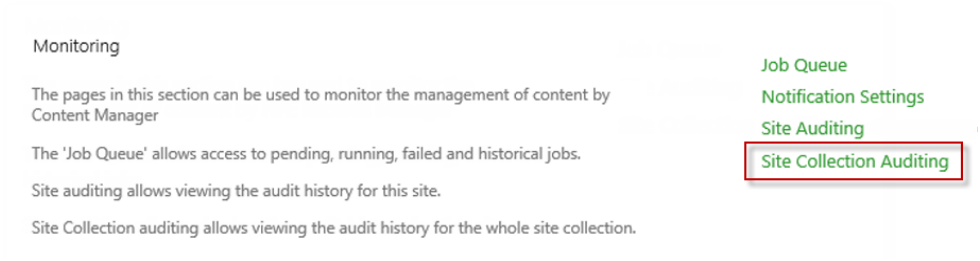
- Any warning or caution entries that apply to any item in the site
- Any configuration changes to the Content Manager Governance and Compliance app that have been made that apply to:
  - This site specifically
  - Any list on this site

15.5 Site collection audit history

It is often a requirement to view the audit history for a site collection. This may be to identify any issues that are occurring with a site collection or determine if and when configuration has been changed that may be affecting the expected behavior of the app on that site collection.

15.5.1 Accessing site collection audit history

Site collection audit history is accessed from the app start page. Click the **Site Collection Auditing** link located in the **Monitoring** section of the page.



15.5.2 Inclusions in site collection audit history

Viewing the audit history for a site collection will show the following audit entries that are applicable to this site collection:

- Any warning or caution entries that apply to any item in the site collection regardless of the site or list they are on.
- Any configuration changes to the Content Manager Governance and Compliance app that have been made that apply to lists and sites on the site collection including site collection changes themselves.

16 One Drive for Business

One Drive for Business (ODB) provides cloud hosted file storage for businesses. The underpinning technology used by ODB is SharePoint. A user's drive in ODB is simply a SharePoint document library.

Because SharePoint is used for ODB, the Content Manager Governance and Compliance app can also be used.

All features of this app works with ODB including Lifetime Management Policies and custom columns. It is therefore possible to use the app to govern information that is stored in ODB.

1. **One Drive for Business file explorer extension**

   ODB can be accessed using a file explorer extension. This renders ODB as a location on the user's computer that files can be stored. Although accessible via the file explorer, the documents are actually stored in ODB.

   Files that are added, modified or deleted using this extension are still handled by the Content Manager Governance and Compliance app. Lifetime management policies are still applied to content, records are maintained when content is changed and items are disposed of by Content Manager.

2. **One Drive for Business mobile**

   ODB can be accessed through mobile applications. Files that are added, modified or deleted using these types of apps are still handled by the Content Manager Governance and Compliance app. Lifetime management policies are still applied to content, records are maintained when content is changed and items are disposed of by Content Manager.

> **NOTE:** There is a known issue in the current version. If the name of a file is changed on a mobile device, although it updates the document name in ODB, LMPs may not be triggered. This could affect governance of documents where the title is being used in the conditions of a LMP.

17 Searching for existing Content Manager records using SharePoint search

17.1 Federated searches

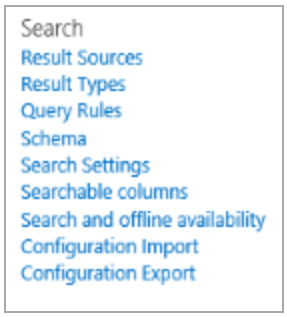
A federated search in SharePoint involves performing a search of an external system and optionally displaying these results with results from SharePoint itself.

How these results are displayed including their relevance to SharePoint results depends on how the federated search has been configured in your SharePoint farm.

The ability to search Content Manager as a federated search provider is included from version 8.2 onwards. Although the tools required to perform federated search have been included, the product does not automatically configure this federated search for you.

Every organization has differing requirements around federated search. Any attempt to automatically configure Content Manager search would be unlikely to be suitable for the majority of organizations.

This section describes how to configure SharePoint to perform a search of Content Manager records.



17.1.1 Result sources

SharePoint supports a concept called ***Result sources***. A result source is how you describe to SharePoint the existence of an external search source. It includes the ability to specify:

- The URL of the server that will supply the search results
- Any additional query terms that should be provided to the server
- The authentication to use when issuing the search to the server.

In the case of Content Manager, an RSS source is provided by the Content Manager Governance and Compliance App. This is the URL that is used by the result source.

17.1.2 Result types

Result types can be used to specify how specific types of results are displayed. For example, it is possible to configure results from one source to display differently to those from another source. This allows display of the properties of a search result that are pertinent to that type of result.

Result types uses ***display templates*** to control how results are rendered.

17.1.3 Query rules

A ***query rule*** is used to specify what content sources are searched when a search is executed. This is similar to search scopes that were available in previous versions of SharePoint.

17.2 Planning your search implementation

Planning search for SharePoint is an important topic. Chances are, if you are implementing the Content Manager Governance and Compliance app for SharePoint that you already have search implemented for SharePoint. If you are new to SharePoint search, the following article provides some good guidelines for implementing search:

https://technet.microsoft.com/en-us/library/cc263400.aspx

- Determining the search account

  The search account is the account that will be used to execute the search of Content Manager. This is just the identity of the process. The search results returned will still be specific to the user interacting with SharePoint.

  The account selected must be a member of the ***Search Account*** group nominated in the configuration tool.

  If you do not add this user to the search account group, when searches are performed, you may not see any results or the result will indicate that the process identity does not belong to this group.

  > **NOTE:** During the creation of the result source, you will indicate that this account must be used.

- Determine when the Content Manager results be displayed

  When a user performs a search in SharePoint, under what conditions should records that match in Content Manager be displayed to the user? In some organizations the answer will be “always” and in others “only when the user specifically asks for records”.

  The answer to this question will allow you to determine how to configure query rules on your SharePoint farm.

17.3 Including Content Manager in federated search results

17.3.1 Adding the app to your search site

After planning the search implementation, you will have decided whether search will be implemented at site level, site collection level or globally using a SharePoint search center. Whichever approach is taken, the Content Manager Governance and Compliance app must be added on the site in use.

See the Adding the app to a site section earlier in this document for details.

17.3.2 Creating a result source

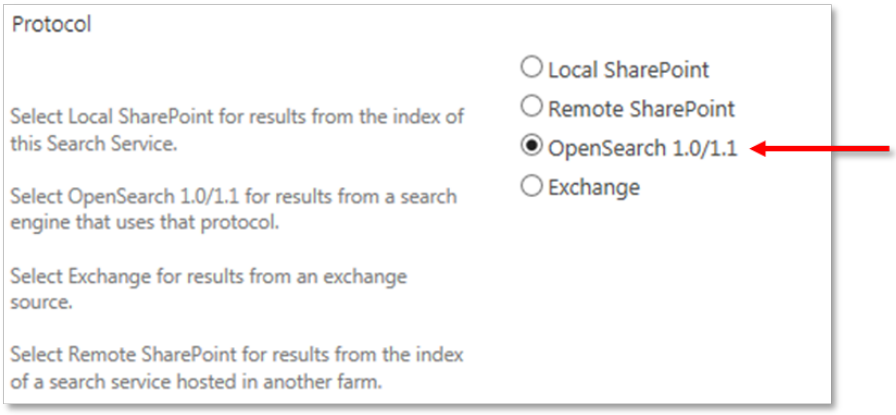
A Content Manager results source is required in order to include Content Manager records in SharePoint search results. Where you create the result source will depend on where you intend to allow the return of Content Manager records (see the planning your implementation section earlier in this chapter).

To create a result source for a site collection, go to **Site Settings > Site Collection Administration > Search Result Sources**. The **Manage Result Sources** page is displayed.

To create a result source for a site, go to **Site Settings > Search > Result Sources**. The **Manage Result Sources** page is displayed.

To create a result source for your search center, navigate to the search center then follow the instructions for creating a result source for a site.

1. In the **Manage Result Sources** page, click **New Result Source** to open the **Add Result Source** page.
2. Enter name and description for the result source.
3. **Protocol** - Choose the **OpenSearch 1.0/1/1** protocol.

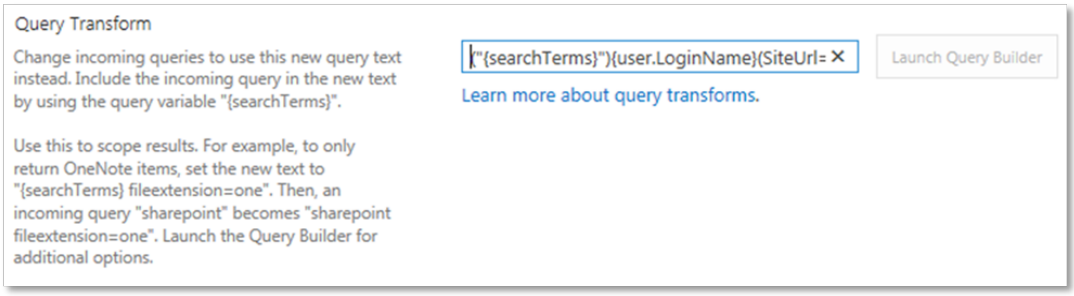


4. **Query transform**

   The query transform allows insertion of data into the query that is passed to the server executing the search.

   Enter the following text exactly into the Query Transform text box (for SharePoint online see the subsequent section).

   ```
   ("{searchTerms}"){user.LoginName}(SiteUrl={Site.URL})
   ```



5. **Source URL**

> **NOTE:** This section includes the simplest options for the source URL. More advanced options can be included in the source URL and are covered in the Modifying the search results section later in this chapter.

The source URL is the full URL to the RSS server for Content Manager. This is constructed as follows:

```
[your server URL]/ Pages/DataStoreSearchProvider.aspx?q={searchTerms}&pagesize=
{count}&start={startIndex}
```

The server URL is the URL that the Content Manager Governance and Compliance app server components were installed on your Content Manager server. Consult the installation guide for details of how to determine this.

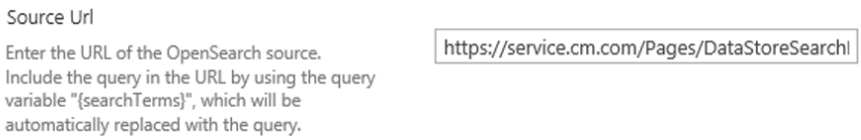
> **NOTE:** A simple way to determine this is to navigate to the app start page. The URL prior to /Pages is the full URL of the Content Manager server.

For example, if the URL of your server is:

```
https://service.cm.com
```

The full source URL would therefore be:

```
https://service.cm.com/Pages/DataStoreSearchProvider.aspx?q=
{searchTerms}&pagesize={count}&start={startIndex}
```



6. **Source URL for SharePoint online**

SharePoint online does not include the ability to replace the {Site.URL} component of a query string transform. Instead it is necessary to explicitly include the URL of the site collection that is being used for search.

Determine the full URL of the site collection that this result source is to be used on. For example:

```
https://YourSharePoint.com/sites/Search
```

URL encode the site collection URL. There are a number of tools freely available to this such as found at:

http://www.url-encode-decode.com/

http://www.urlencoder.org/

The example above after encoding becomes:

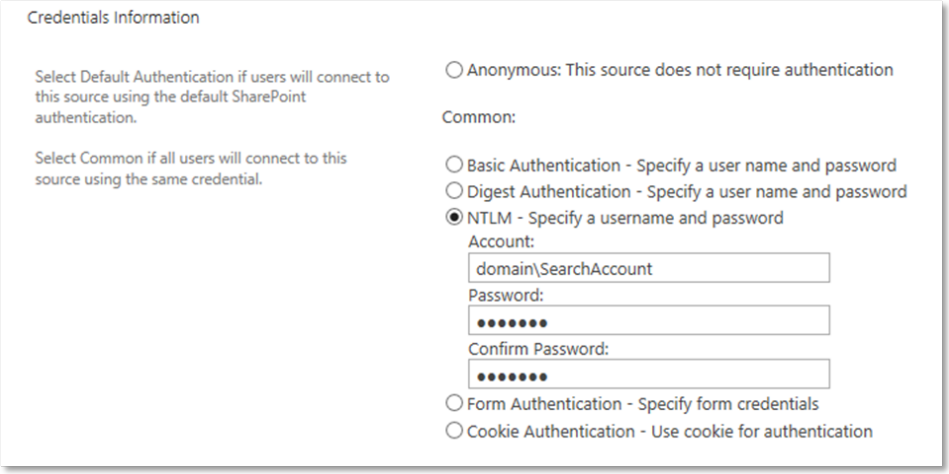
```
https%3A%2F%2FYourSharePoint.com%2Fsites%2FSearch
```

The resultant source URL to use in this scenario in SharePoint online would therefore be (using the previous example):

```
https://service.cm.com/Pages/DataStoreSearchProvider.aspx?q=
{searchTerms}&pagesize={count}&start={startIndex}&
SiteUrl=https%3A%2F%2FYourSharePoint.com%2Fsites%2FSearch
```

7. **Credentials**

   Lastly, specify the credentials that will be used for executing the search. This is the account that was determined in the Determining the search account section earlier in this chapter.



8. Click **Save** to save the result source.

In some implementations you may receive an **Access Denied** error when trying to save the query rule. It has been found that this is caused by the identity of the **search service application** requiring read permission to the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Tools\Web Server
Extensions\15.0\Secure\FarmAdmin
```

If you are unable to overcome this issue, then you must leave the credentials information as ***Anonymous*** and ensure that you have specified a ***default search account*** (covered in the installation guide). In SharePoint online, the credential information is set to ***Anonymous*** and you don't have any option to change it. So it is mandatory to specify a default search account for SharePoint online to get search results back from Content Manager. This account will be used to execute the search regardless of who the interactive user is if this approach is taken.

17.3.3 Creating a result type

A result type is used to specify rules around how a particular type of result should be displayed in search results. You can nominate specific handling for how a record is displayed. If you don't create a record result type, then SharePoint will display the content using the default item template.

Where you create the result source will depend on where you intend to allow the return of Content Manager records (see the planning your implementation section earlier in this chapter).

> **NOTE:** In order to use custom display templates, you must have the **SharePoint Server Publishing Infrastructure** feature activated at site collection level. This is typically activated already if you have used a search template for creating the site collection.

Uploading the Content Manager display template

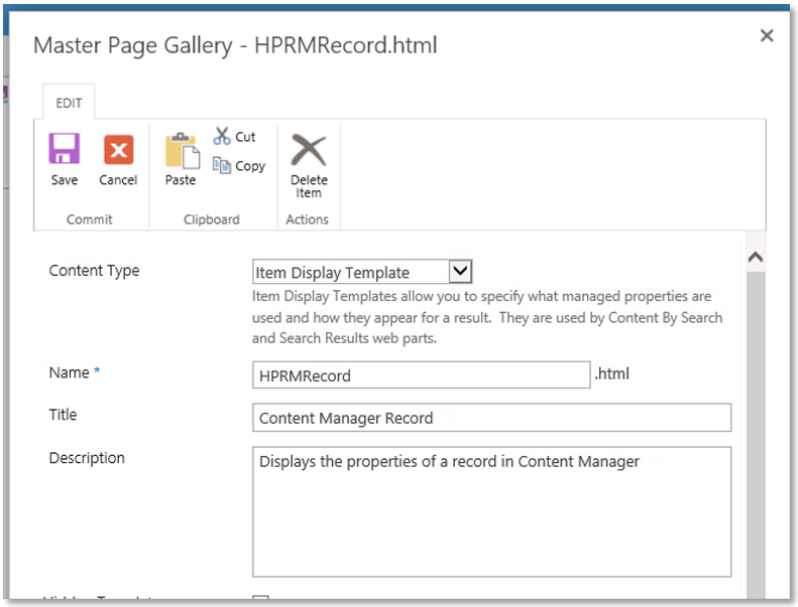
1. Before you create a result type, it is necessary to upload a display template that will be used.
2. Navigate to the **Site Settings > Web Designers Galleries > Master Pages** gallery for your site collection. You should perform these steps from the Content Manager server as you will need to upload a file that is installed there. The **Master Page Gallery** is displayed.

   > **NOTE:** Uploading the display template only needs to be performed once, not every time you create a result type.

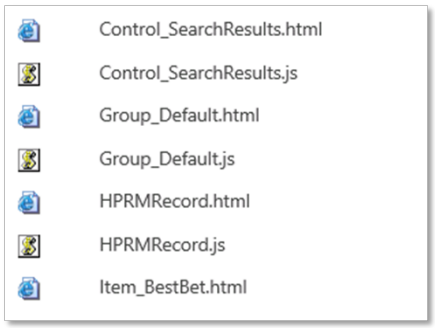
3. Open the **Display Templates** folder:
4. Open the **Search** folder. List of script files will be displayed.
5. From the **Files** ribbon, click **Upload Document**:
6. Using the Browse button, navigate to the location you installed the Content Manager Governance and Compliance App.

   > **NOTE:** This location is usually **C:\Program Files\Micro Focus\Content Manager\Content Manager SharePoint Integration**

7. Under the **Scripts** folder choose the `HPRMRecord.html` file. Click **OK** on the upload page.
8. Accept the default values on the **Master Page Gallery** page that displays:



If successfully added to the gallery, you will see both `HPRMRecord.html` and `HPRMRecord.js` files.



> **NOTE:** If you do not see the HPRMRecord.js file get created you must activate the **SharePoint Server Publishing Infrastructure** feature at site collection level and repeat these steps.

Creating the result type

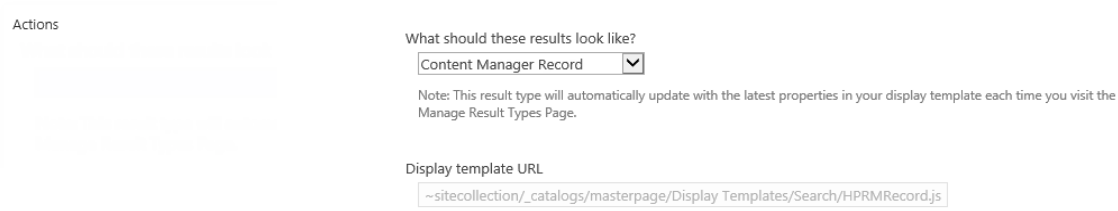
To create a result type for a site collection, go to **Site Settings > Site Collection Administration > Search Result Types**. The **Manage Result Types** page is displayed.

To create a result type for a site, go to **Site Settings > Search > Result Types**. The **Manage Result Types** page is displayed.

To create a result type for your search center, navigate to the search center then follow the instructions for creating a result type for a site.

1. In the **Manage Result Types** page, click **New Result Type** to open the **Add Result Type** page.

2. Enter a name for the result type.
3. In **Conditions**, indicate that this result type should be used for results that come from the query source that you have defined.
4. In Actions, select the ***Content Manager Record*** display template that has been installed by the Content Manager Governance and Compliance app.



5. Click **Save** to save the result type.

17.3.4 Creating a query rule

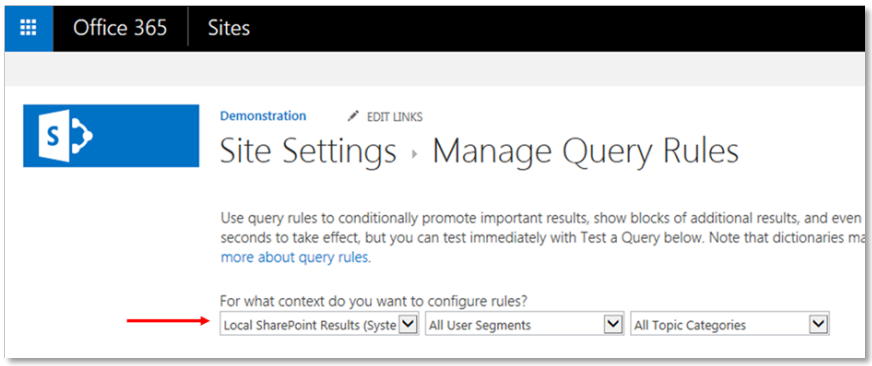
A query rule is used to determine what result sources are queried when a search is executed and how the results are included. In these steps, we will modify a query rule to include Content Manager search results in the search.

To access query rules for a site collection, go to **Site Settings > Site Collection Administration > Search Query Rules**. The **Manage Query Rules** page is displayed.

To access query rules for your search center, navigate to the search center the follow the instructions for creating a result source for a site.

Firstly you must identify the search context that you want to create a query rule for. In this example, we will configure the ***Local SharePoint Results*** context to include Content Manager records whenever a search of SharePoint is performed.

1. In the **Manage Query Rules** page, choose the context.

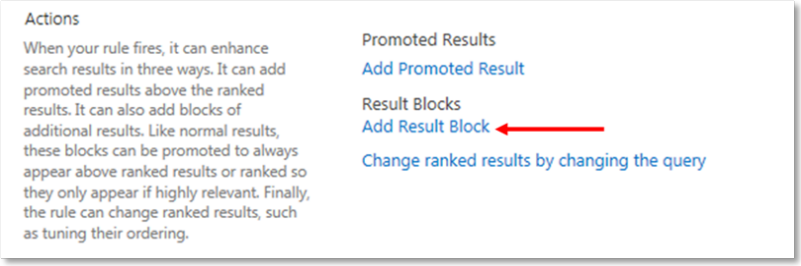


   The list of configured query rules for the context will be displayed.

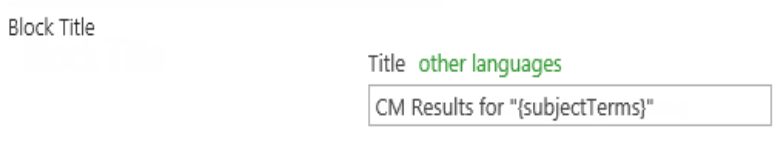
2. Select **Local SharePoint Results (System)** from the drop down and click **New Query Rule**.
3. Enter a name for the rule.
4. Under the **Query Conditions** section, remove the existing condition.

> **NOTE:** This assumes that you do not require any query conditions. See the SharePoint documentation for an explanation of this feature.

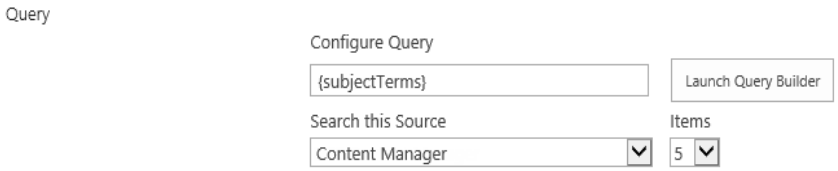
5. Lastly, a result block needs to be added. The result block describes the block of results that will be shown with the SharePoint results. Click the **Add Result Block** link to create a new block. The **Add Result Block** page is didplayed.



6. In the **Add Result Block** page, set the title as you would like it displayed in the block of results. Note that `{subjectTerms}` will be replaced by SharePoint search with the words that were searched for.



7. In **Query**, set the query to search the Content Manager result source and configure the query to display the number of items you want to show in the block.



8. Expand the **Settings**.

   Indicate whether you want the results from Content Manager to always be shown at the top of SharePoint results or whether you want SharePoint to rank them and place them accordingly with the SharePoint results. Note that this will only rank the block as a whole, not the individual results.

> **NOTE:** The Creating a more results page section describes how to create a page that can be used as the More link. You can edit this result block at a later time after that page has been created.

9. Save the results block then save the query rule.

17.3.5 Testing the federated results

If you have followed the steps till here, performing a SharePoint search of ***everything*** using a term that will return results from Content Manager will allow you to confirm that the search is working.

If you do not see results from Content Manager returned, try the following steps:

- Choose a search word that appears in the title of one or more records. If still not working, perform the search using the Content Manager client to ensure that results are actually returned
- Modify the result block you created to always put the block at the top. If this is not the case, results may be being returned but are just not considered relevant enough by SharePoint to show.

If you still do not see results, follow the steps later in this chapter in the Creating a more results page to create a page that only shows results from Content Manager. If there is an error occurring, the error will not be displayed in the ***everything*** view. On a page that only shows Content Manager results, the details of the error will be provided.

17.4 Modifying the search results

17.4.1 Suppressing SharePoint items

Records returned by search may represent list items in SharePoint. If conducting a search of both Content Manager and SharePoint, this could result in duplicate results. In this scenario, it is possible to suppress records from being returned that represent managed list items in SharePoint.

To prevent these types of records from being included in results, append the following to the source URL:

```
suppressmlis=true
```

For example:

```
https://service.cm.com/Pages/DataStoreSearchProvider.aspx?q={searchTerms}&pagesize=
{count}&start={startIndex}&suppressmlis=true
```

If this parameter is not included in the source URL, these types of records will always be returned.

> **NOTE:** Exposed items will still be returned even if this filter is applied.

17.4.2 The search settings page

The search settings page is used to specify the default settings that are used by the Content Manager federated search. This page is accessed from the app start page using the **Search Settings** link.

To access this page, the user must be a site collection administrator.

The following sections describe the sections on this page.

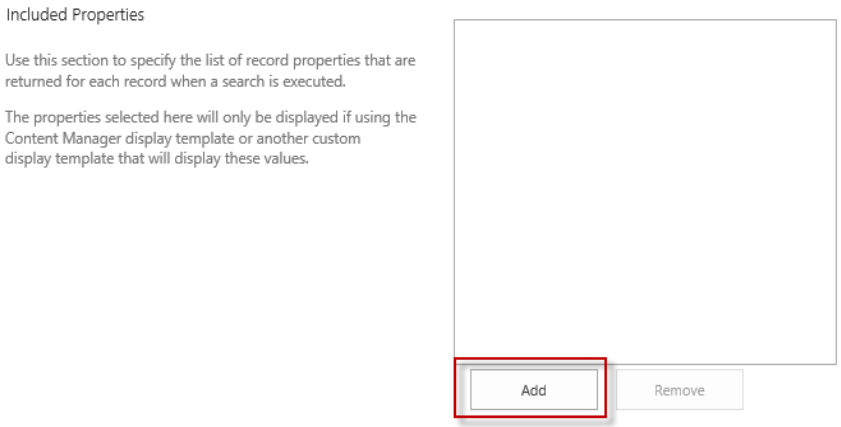
17.4.3 Selecting the columns to include

By default, if using the Content Manager display template, each search results will include the following properties:

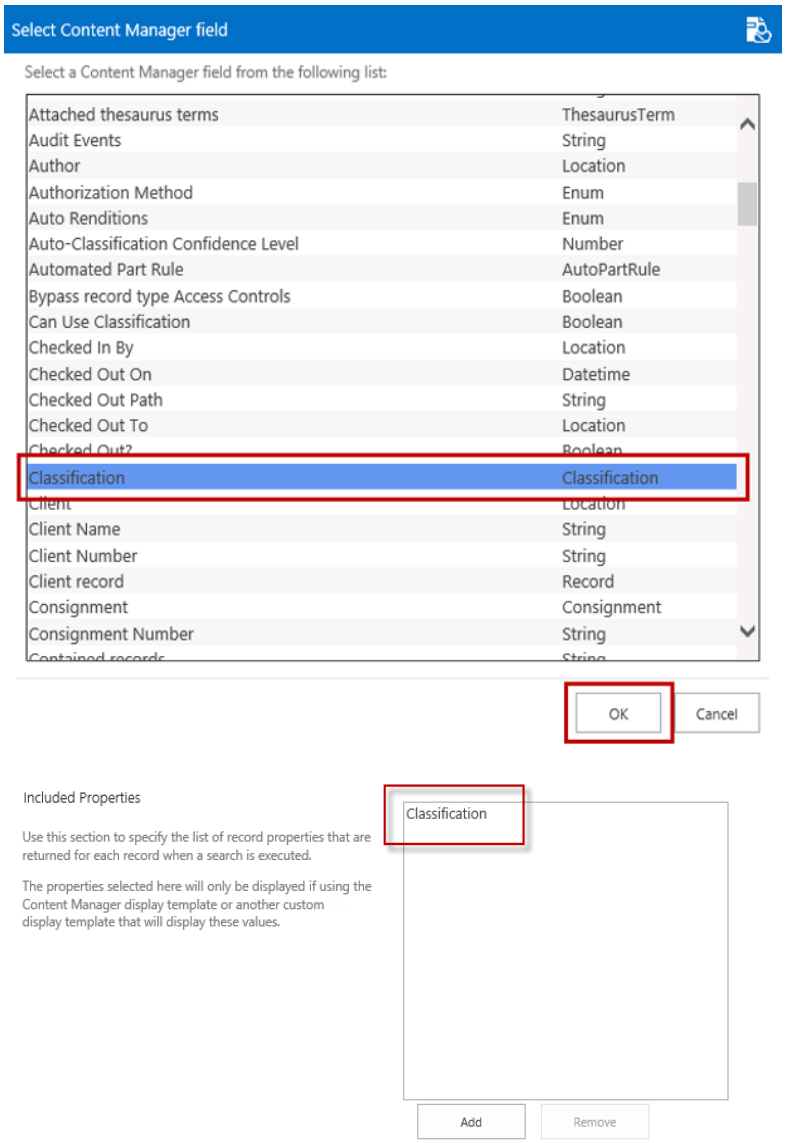
- Record title
- Record number
- Author
- Date created

Using the **Search Settings** page, it is possible to nominate additional properties that should be included in search results.

The **Included Properties** section of the page provides the ability to select properties to return in the search. Click **Add**:



This displays a dialog allowing you to select a Content Manager property to include.



Click **Add** to continue adding properties.

> **NOTE:** The order that you add the properties will be the order that they are displayed on the search result.

Once the page has been saved, the next time a search is performed, these properties will be included in the search results.

> **NOTE:** You cannot remove the standard properties. If you do not want one or more of the standard properties to be displayed then it will be necessary for you to create a custom display template. See the Changing how search results are displayed section for details.

17.4.4 Specifying what is searched by a keyword search

When performing a keyword search e.g. using the search box that appears on most SharePoint pages, a search of Content Manager is performed against a set of properties. By default, the properties that are searched for the keyword are:

- Title
- Notes
- Record number

Using the Search Settings page, it is possible to modify which properties are included in this search.

The **Default Keyword Search** section allows the definition of the **Search Template**. The Search Template is a Content Manager search with placeholders for the app to insert the search terms.

For example, the Content Manager string search of the title for the word “legal” is:

```
title:”legal”
```

The search template for this would be:

```
title:”[%SearchTerms%]”
```

When the search is executed, `[%SearchTerms%]` will be replaced with the keyword/s that are entered.

Therefore, to search title, notes and record number, the search template is:

```
title:"[%SearchTerms%]" or notes:"[%SearchTerms%]" or number:"[%SearchTerms%]”
```

Once the page has been saved, the next time a keyword search is performed, this template will be used.

17.5 Changing how search results are displayed

The ***display template*** selected is used to control how results are displayed. The display template includes html and javascript that controls how results are displayed. The instructions in the template tell SharePoint how to display a single result. These instructions are then applied to each and every result that should use the template.

The display template used is specified in one of two ways:

1. When defining a result type (see Creating a result type).
2. When defining a block in a query rule you can specify the display template to use.

It is possible to define your own display template to customize the look and feel of search results. There is a large amount of material available on the internet about customizing display templates for SharePoint search. The following sections provide some basic guidance but are designed to be read in conjunction with formal SharePoint guidance.

17.5.1 Creating a custom display template

The simplest way to create a custom display template is to begin with an existing one. The examples in this section are based on using the ***Content Manager Display Template*** and modifying it.

Create a copy of the Content Manager display template

Start by making a copy of the Content Manager display template. This can be found in the ***Scripts*** directory of the installation directory. The name of the file is:

```
HPRMRecord.html
```

> **NOTE:** It is strongly recommended to not modify the Content Manager display template directly. Changes will be overwritten during upgrades and retaining the original allows a point of reference to go back to should you make a mistake.

Customizing the display template

The subject of how to customize a display template is outside the scope of this document. A simple search engine search for the following terms will return a wealth of information on this topic:

```
customizing sharepoint display template
```

Using your custom display template

Once the custom display template has been uploaded, modify the result type created in an earlier step to use this custom template.

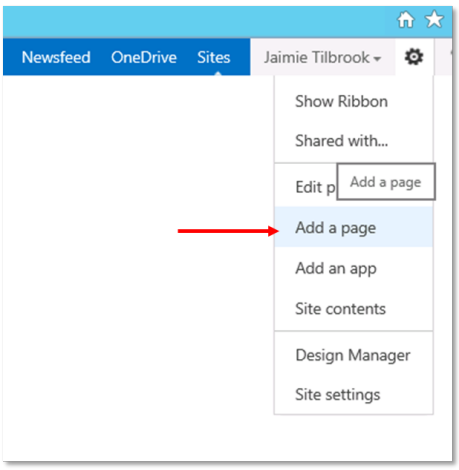
17.6 Using SharePoint search functionality to further refine search results

17.6.1 Creating a more results page

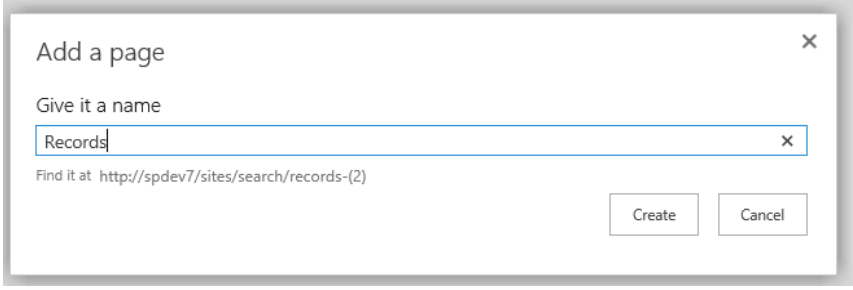
When displaying results from Content Manager in a results block, there may be more results than can be shown in the space available in the block. To allow users to view all results, you must implement a page that can be used to display all the results.

Create the page

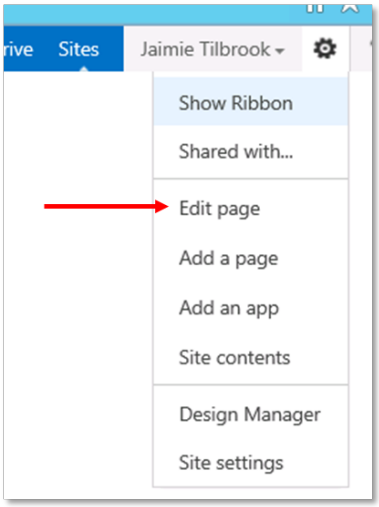
Create a new page in site pages. In this example, the page is being created on the search center in use. This ensures that the page includes the required web parts. If creating a page on a non site center, please consult SharePoint documentation for guidance.



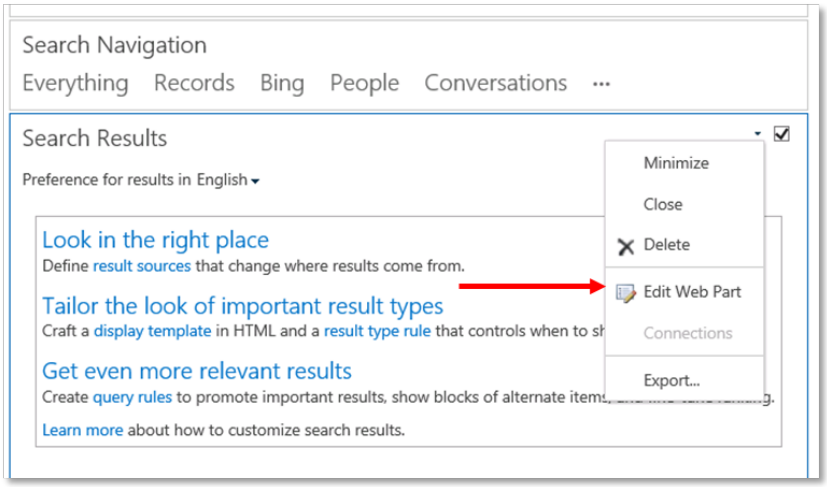
Name the page. In this example it is named **Records**.



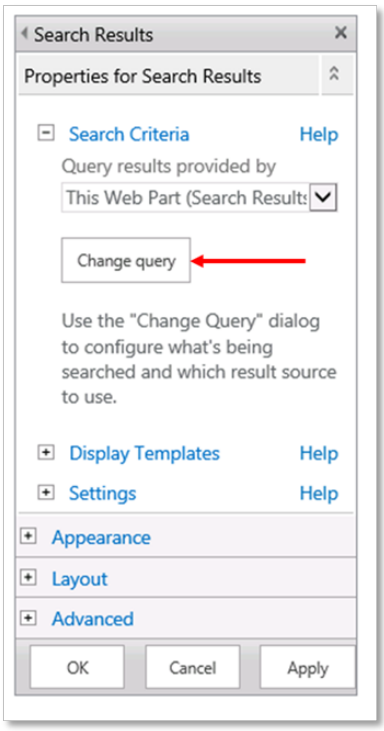
Place the page into design mode (note that typically SharePoint will place the page into design mode for you):



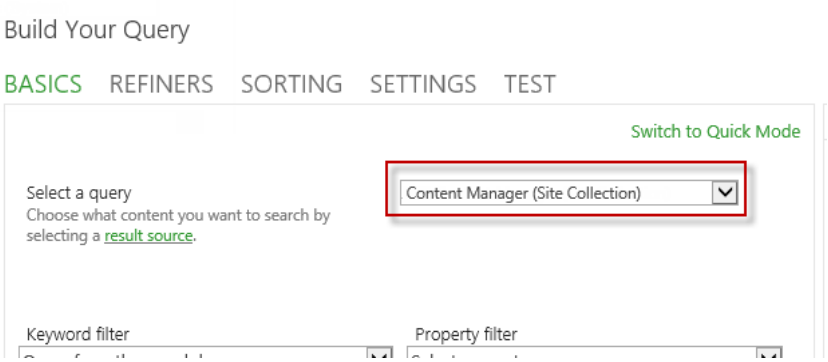
Edit the **Search Results** web part:



From the tool part, select the **Change Query** button:



In the Select a Query section choose the result source created earlier in this chapter. If the example was followed, it will be called **Content Manager**.



This step indicates that the search results should only be shown from the Content Manager result source and no other.

Save the changes to the page, check it in and publish it.

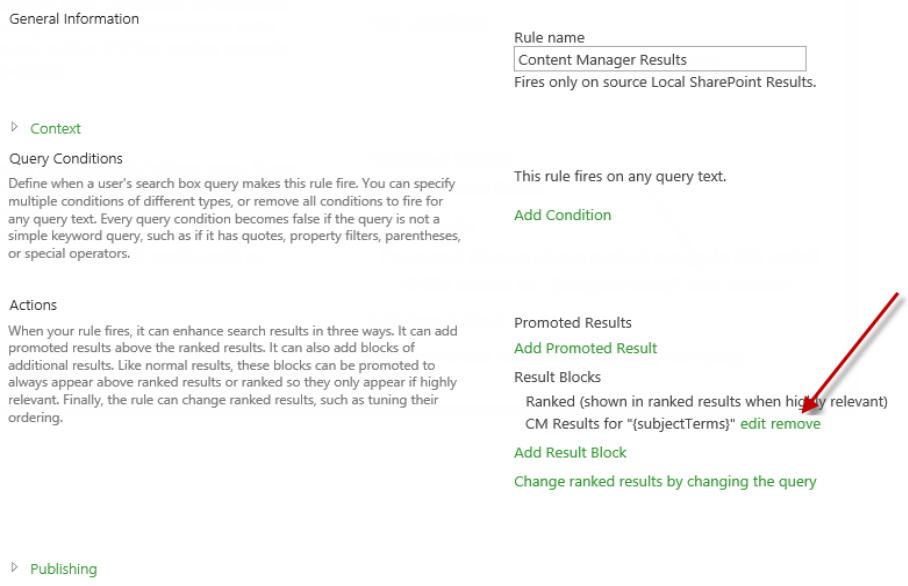
Test the page by entering a keyword into the search box and ensuring that only results from Content Manager are returned.

Note that if the returned results are more than can be shown on one page, SharePoint includes pagination controls.

Make the page available

To indicate that this page is to be used to show more results, the result block added in the query rule needs to be modified. To access the query rule, follow the steps in Creating a query rule.

Edit the result block that was created earlier in this chapter:



Expand the Settings section.

Check the **"More" link goes to the following URL** radio button.

Enter the full URL of the page created in the previous step with the following appended to the end:

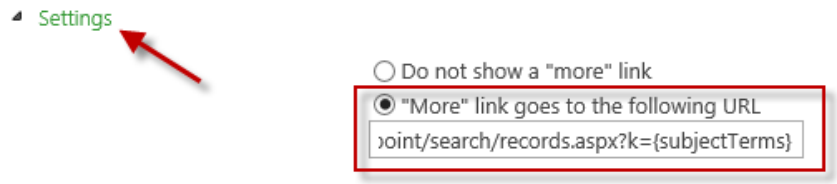
```
?k={subjectTerms}
```

For example, if the URL of the page was:

```
https://sharepoint/search/records.aspx
```

Then the full URL to enter will be:

```
https://sharepoint/search/records.aspx?k={subjectTerms}
```

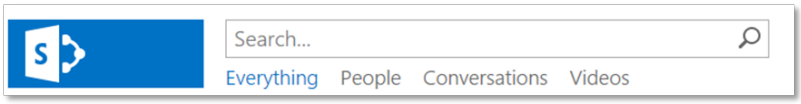


Click **OK** to result block and save the changes to the query rule.

Now when a search is performed, if there are more results than the result block can show, a **Show More** link will be included. When clicked, this will take you to the page created.

17.6.2 Viewing a records only subset of results

SharePoint includes the ability to include navigation links on search results page that allow users to see subsets of search results. For example, by default, SharePoint search center includes the following navigation links:



This section describes how to include a ***Records*** navigation link to allow users to view only search results that are records.

Create the page

The steps to create a page that display only records are the same as that in the previous section. See Create the page.

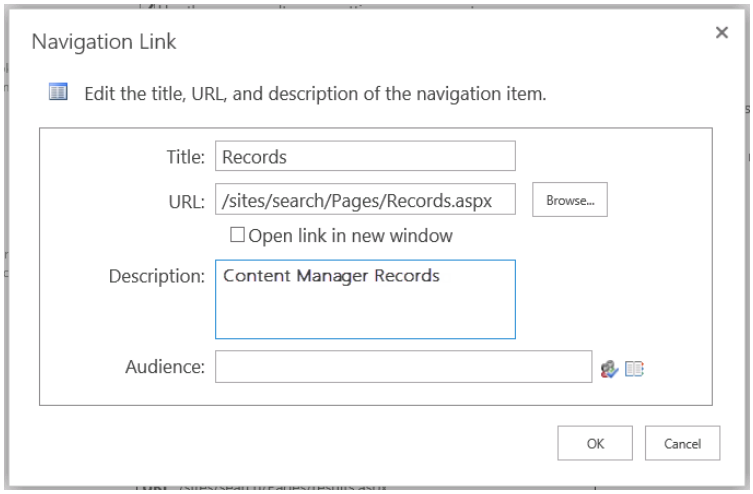
Add the navigation link

1. For the site providing the search, navigate to **Site settings > Search > Search Settings**.
2. On this page you can configure the search navigation. In the **Configure Search Navigation** section, click the **Add Link**.

   The dialog allows you to enter the details of the navigation link. The URL field requires you to enter the relative path to the page created in the earlier step. The following are suggested values for the other fields:

   Title: Records

   Description: Content Manager records

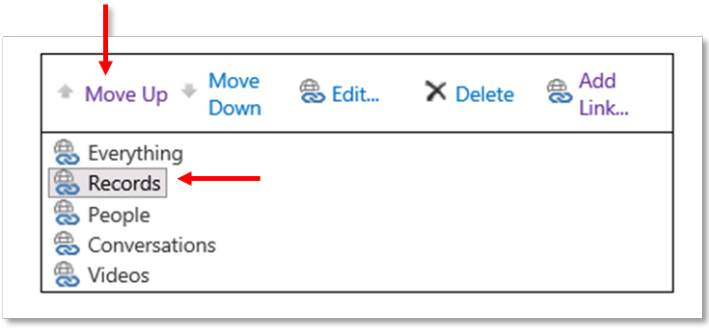


3. Click **OK** to add the link.

> SharePoint in some versions causes a javascript error to occur on the page when clicking OK. It has been found that ignoring these, the link still adds correctly.

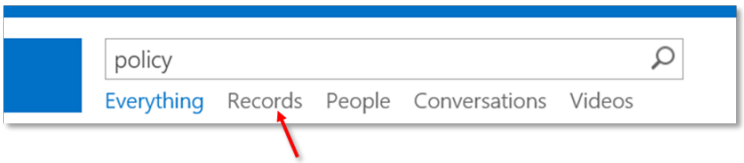
Setting the position of link in search navigation bar

The position of the link in the search navigation bar can also be set. For example, to move the **Records** link so that it appears next to the **Everything** link, select the **Records** link then click the **Move Up** link until the **Records** link is in the correct position.



Click **OK** on the **Search settings** page to save these changes.

To test the change, perform a search and note that the Records navigation link is now included.



Ensure that clicking on the Records navigation link that the results shown are only from Content Manager.

17.7 Using SharePoint advanced search

17.7.1 Overview

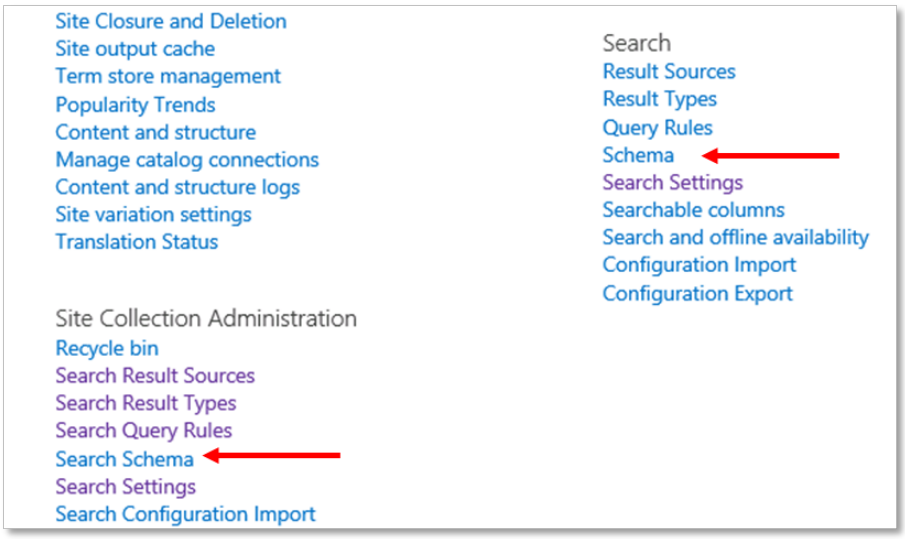
SharePoint includes the ability to perform advanced searches. These are searches that allow you to specify particular properties of an item to search. For example, this would allow you to search for all items where the author was a particular person.

A user navigates to the advanced search page (which includes an advanced search web part) and constructs the query to perform.

Managed properties

At the heart of advanced search are ***Managed Properties***. These represent the various properties of an item and can be used in SharePoint search syntax.

The managed properties defined for a site or site collection can be found through site settings:



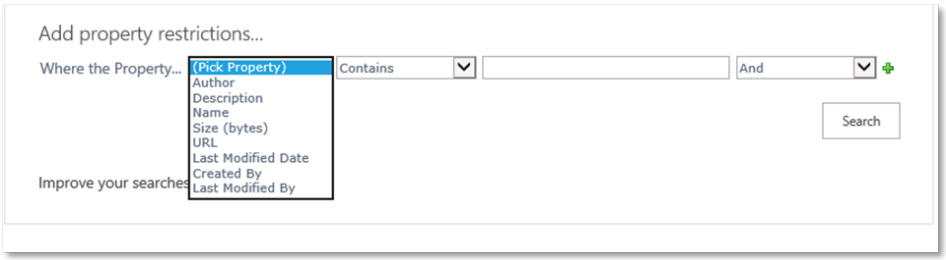
Although the advanced search web part is typically used by SharePoint users to conduct an advanced search, all this web part does is produce a search string that specifies the managed properties to search.

For example, to search for items with an author whose name is “Smith” the advanced search web part will produce the following search syntax:

```
Author:smith
```

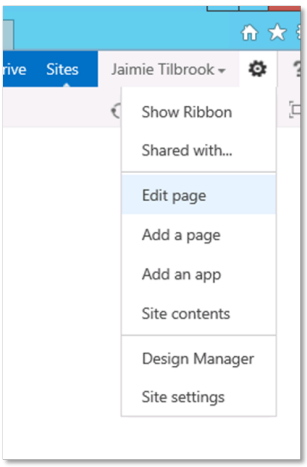
Configuring the advanced search web part

Out of the box, the advanced search web part is configured to allow search across the following managed properties:

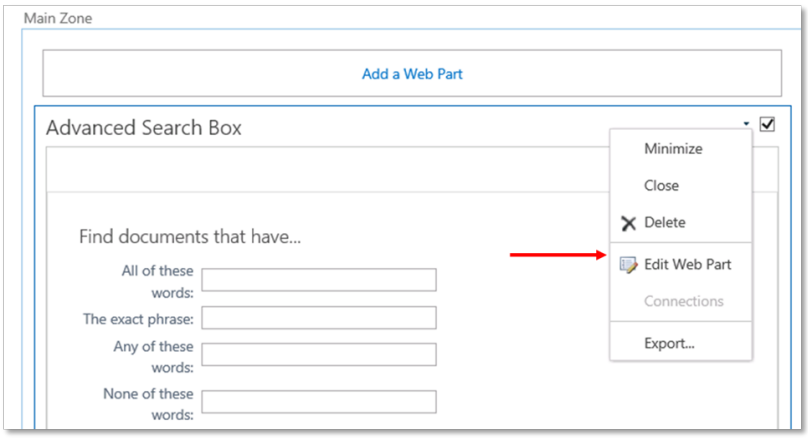


The properties that are available for use in advance search can be modified through configuration of the web part.

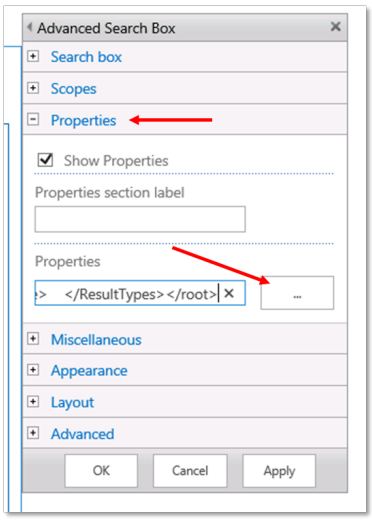
Put the advanced search page into design mode:



Edit the advanced search box.



Expand the **Properties** section then click the ellipse button next to the **Properties** text box.

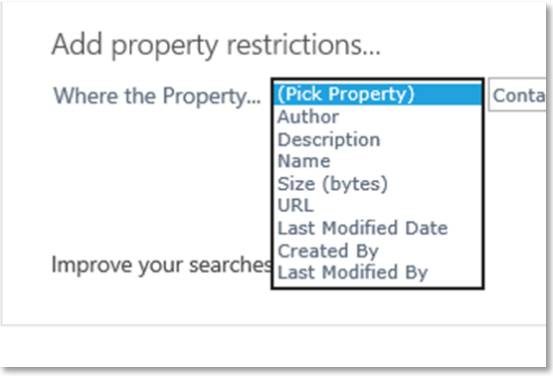


The text editor contains XML used to configure the web part. It is recommended that you copy this XML in its entirety and open it in a tool suitable for modifying XML.

There are several sections of the XML document:

- LangDefs
- Languages
- PropertyDefs
- ResultTypes

The **PropertyDefs** section is responsible for specifying which properties are available to appear in the following dropdown:



If the web part has not been modified, the XML in this section will be:

```
<PropertyDefs>
  <PropertyDef Name="Path" DataType="url" DisplayName="URL"/>
  <PropertyDef Name="Size" DataType="integer" DisplayName="Size (bytes)"/>
  <PropertyDef Name="Write" DataType="datetime" DisplayName="Last Modified Date"/>

  <PropertyDef Name="FileName" DataType="text" DisplayName="Name"/>
  <PropertyDef Name="Description" DataType="text" DisplayName="Description"/>
  <PropertyDef Name="Title" DataType="text" DisplayName="Title"/>
  <PropertyDef Name="Author" DataType="text" DisplayName="Author"/>
  <PropertyDef Name="DocSubject" DataType="text" DisplayName="Subject"/>
  <PropertyDef Name="DocKeywords" DataType="text" DisplayName="Keywords"/>
  <PropertyDef Name="DocComments" DataType="text" DisplayName="Comments"/>
  <PropertyDef Name="CreatedBy" DataType="text" DisplayName="Created By"/>
  <PropertyDef Name="ModifiedBy" DataType="text" DisplayName="Last Modified By"/>
</PropertyDefs>
```

Each PropertyDef element defines a property that can be included in the dropdown. Notice though that not all properties are currently displayed in the screenshot of the dropdown. The **ResultTypes** section of the XML is what determines which of these properties are shown based on the result type selected. In this case the **All Results** result type is selected.

The XML of the standard node describing the **All Results** result type is:

```
<ResultType DisplayName="All Results" Name="default">
  <KeywordQuery/>
  <PropertyRef Name="Author" />
  <PropertyRef Name="Description" />
  <PropertyRef Name="FileName" />
  <PropertyRef Name="Size" />
  <PropertyRef Name="Path" />
  <PropertyRef Name="Write" />
```

```
    <PropertyRef Name="CreatedBy" />
    <PropertyRef Name="ModifiedBy" />
  </ResultType>
```

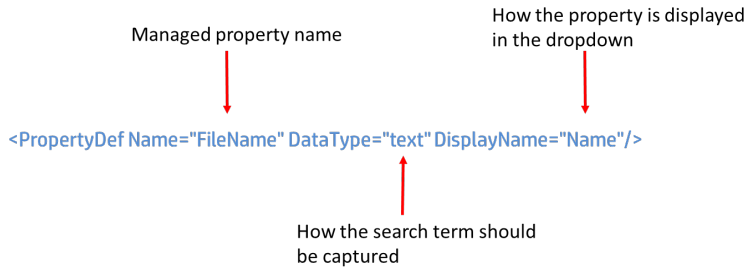
Each ***PropertyRef*** element refers to a ***PropertyDef*** element and indicates which of the properties should be shown in the dropdown.

> **NOTE:** The name of a property may be different to the display name.

To remove a property from being displayed, the relevant ***PropertyRef*** element should be removed from the ***ResultType*** node. For example, if we wanted to remove the ***Size*** property from the dropdown when ***All results*** is selected, the node would be modified to:

```
<ResultType DisplayName="All Results" Name="default">
  <KeywordQuery/>
  <PropertyRef Name="Author" />
  <PropertyRef Name="Description" />
  <PropertyRef Name="FileName" />
  <PropertyRef Name="Path" />
  <PropertyRef Name="Write" />
  <PropertyRef Name="CreatedBy" />
  <PropertyRef Name="ModifiedBy" />
</ResultType>
```

To make an entirely new property available to be searched, a new entry must be added to the ***PropertyDefs*** section. The following is the entry used to allow searching on the name property.



The managed property name is the name of the SharePoint managed property that should be searched when this property is used. Ultimately, it is used by the advanced search web part to determine the syntax of the search string. In this example, if searching for “housing policy”, the search performed by SharePoint would be:

```
FileName:"housing policy”
```

The data type tells the web part how to capture the search term. For example, if this was ***date***, then the web part would expect a date to be entered.

Lastly the display name is used to indicate how this property should be shown in the dropdown.

After adding the new ***PropertyDef*** element, decide which result types should be allowed to use this property and add ***PropertyRef*** elements to the relevant ***ResultType*** sections.

Once all changes have been made to the XML, copy it and paste it back into the properties field of the web part and apply the changes.

17.7.2 Advanced search without using managed properties

It is possible to perform searches of some Content Manager fields without the need to create managed properties. All that you need to know is the term used in a Content Manager string search to find that property.

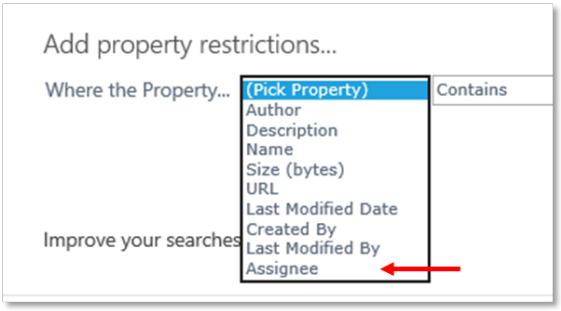
Consider the scenario where you need to be able to search for records with a particular assignee. In Content Manager, searching for assignee uses the search term:

```
assignee
```

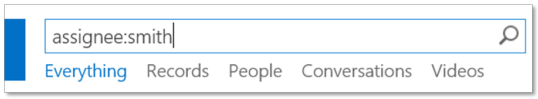
A PropertyDef entry is added to the advanced search web part properties XML as follows:

```
<PropertyDef Name="assignee" DataType="text" DisplayName="Assignee"/>
```

A ***PropertyRef*** entry is added to the relevant result type.



Performing a search for records with an assignee name of “smith” will result in a search term being created:



Not all properties support mapping in this way. If a property is not supported then, you must create a Content Manager managed property for the field (see Creating Content Manager managed properties).

17.7.3 Using standard mapped managed properties

There are managed properties in SharePoint that map well to fields in Content Manager. For example, a search for ***title*** in SharePoint brings back records that have that word in the title of the item. If searching Content Manager, this search would also equate to searching the title of a record.

However, there are less obvious equivalencies. For example, the managed property ***FileName*** is used to search the file name of a document in a library (as against the title). There is no differentiation between file name and title in Content Manager therefore title should be searched when file name is searched in SharePoint.

These obvious equivalencies have been provided already. The following are the SharePoint managed properties that are provided equivalency out of the box.

Managed property name	Purpose	Equivalent Content Manager search
Size	The size of the document	documentSize
Write	The last modified date	updated
FileName	The file name of a document	title
Description	Any notes relating to the item	notes
Title	The title of the item	title
Author	The author of the item	author
DocKeywords	Any attached thesaurus terms	keyword
CreatedBy	The person who created the item	creator
ModifiedBy	The person who last modified the item	updatedBy

These standard mappings are found in a file located in the installation directory called:

`StandardManagedPropertyMapping.xml`

If there are other standard mappings that need to be added in your organization, this file can be modified to include these.

Open the file in a program, such as notepad. There is a ***ManagedPropertyMap*** node created for each mapping of a managed property.

```
<?xml version="1.0" encoding="utf-16"?>
<ArrayOfManagedPropertyMap xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns
  <ManagedPropertyMap>
    <ManagedProperty>AttachedLabelsOWSTEXT</ManagedProperty>
    <SearchTerm>searchTerm</SearchTerm>
  </ManagedPropertyMap>
  <ManagedPropertyMap>
    <ManagedProperty>LastUpdatedByOWSTEXT</ManagedProperty>
    <SearchTerm>updatedBy</SearchTerm>
  </ManagedPropertyMap>
```

To add a new mapped managed property you must create a new ***ManagedPropertyMap*** node and insert it into the document. For example, if Content Manager assignee's should be searched when the SharePoint managed property called ***DocumentOwner*** is searched (this is not a real managed property name) then the new node would be:

```
<ManagedPropertyMap>
  <ManagedProperty>DocumentOwner</ManagedProperty>
  <SearchTerm>assignee</SearchTerm>
</ManagedPropertyMap>
```

The ***ManagedProperty*** element contains the name of the managed property to be mapped. The ***SearchTerm*** element contains the Content Manager string search term that should be used when searching for this property.

Once the change has been made, save the document then run the ***column creation tool*** again (see the installation document for details of using this tool). This tool updates the configuration database with the new mapping.

17.7.4 Creating Content Manager managed properties

Consider the scenario where you have added the ***Record Number*** column to one or more of your content types. Your staff want to be able to search for content by record number across both SharePoint and Content Manager. This allows them to find items that are still active in SharePoint as well as ones that have been relocated to Content Manager.

To search by record number in SharePoint, there must be a managed property created to allow this to happen. Fortunately, as soon as SharePoint has indexed any items that have this column, it will automatically create the managed property for us. Looking at the search schema, it is found that a managed property ***RecordNumberOWSTEXT*** has been automatically created.

The following search string will therefore return any items in SharePoint that have a record number of D15/58:

```
RecordNumberOWSTEXT:D15/58
```

In order to have Content Manager also searched for a record with this record number, a managed property mapping is required. See Using standard mapped managed properties for details regarding how to create these. For many Content Manager properties though, a standard mapping has already been included in the standard mappings. For record number you will find the following mapping in the mapping file:

```
<ManagedPropertyMap>
  <ManagedProperty>RecordNumberOWSTEXT</ManagedProperty>
  <SearchTerm>number</SearchTerm>
</ManagedPropertyMap>
```

> **NOTE:** Always search for a mapping before attempting to create a new one.

In most cases, if you include one of the Content Manager columns that was created by the column creation tool, the mapping will already be included. Therefore in order to search by these columns across Content Manager and SharePoint you should only need to:

1. Add the column to the required content type or list
2. Start an incremental reindex of SharePoint content or wait for the scheduled one to complete
3. Begin using the managed property

17.7.5 Using Content Manager managed properties in manual searches

The Content Manager search strings can be used directly in the SharePoint search box. For example, to search for records where the assignee has a surname of Smith, the following can be entered directly into the search text box:

```
Assignee:smith
```

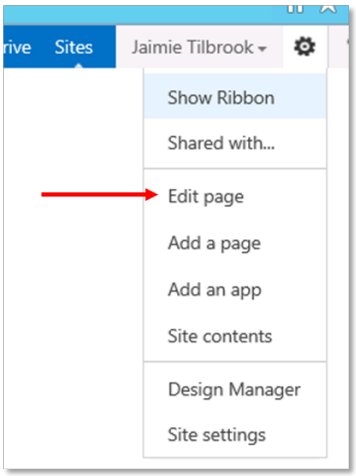
This will return all records that satisfy this requirement. This can be done without the need to create managed properties if there is a mapping in the XML file.

17.8 Fixed searches

There may be times where users want a particular search executed every time they navigate to a page. For example, users may want to see any records that have been assigned to them. It is possible to do this with the federated search provider.

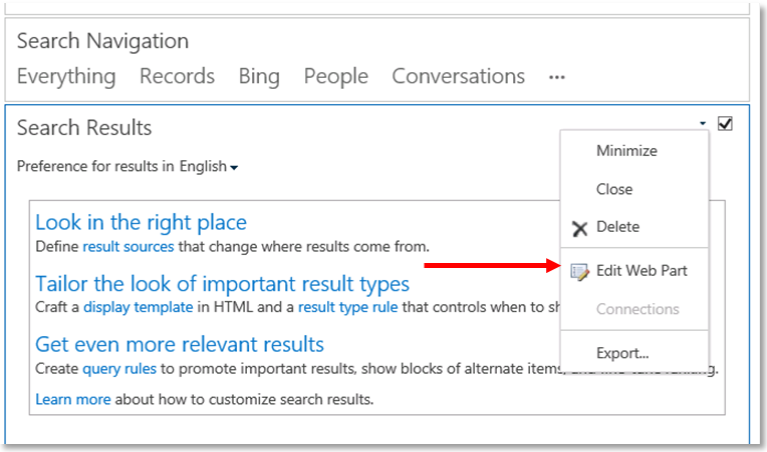
The example below assumes that you have the result source and result type configured already for the site or site collection. See the Including Content Manager in federated search results section for details.

On the page that the fixed search is required, put the page into edit mode.

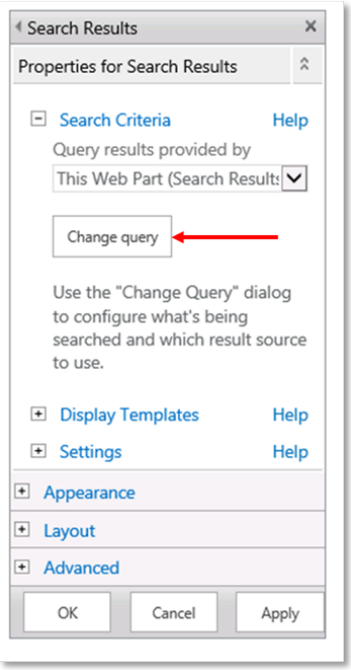


Add a **Search Results** web part to the page.

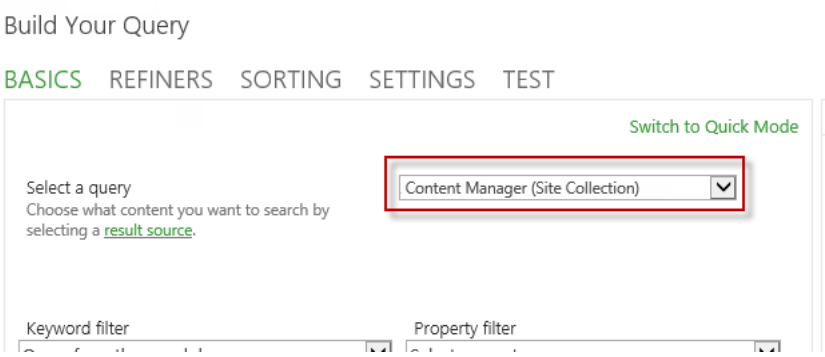
Edit the web part:



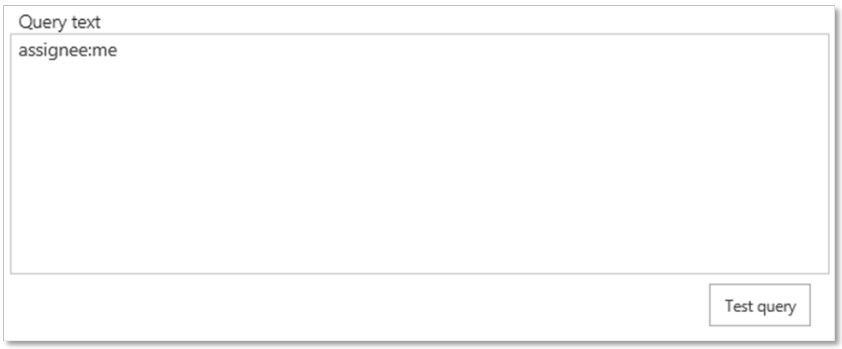
From the tool part, select the **Change Query** button:



In the Select a Query section choose the result source created earlier in this chapter. If the example was followed, it will be called ***Content Manager***.

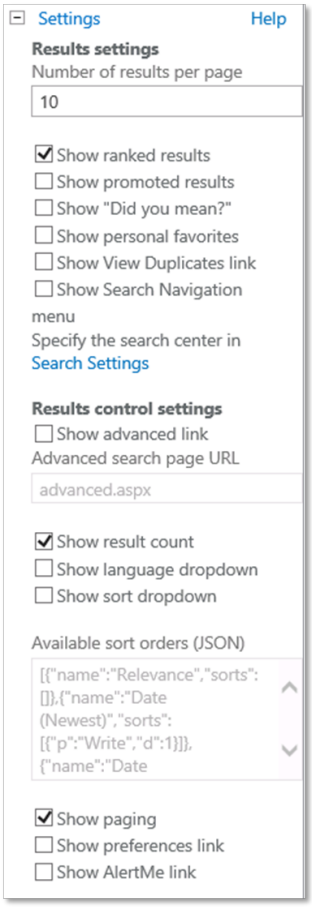


Modify the query text to include the exact query to always be executed. For this example, the intention is to show all records that are assigned to the current user.



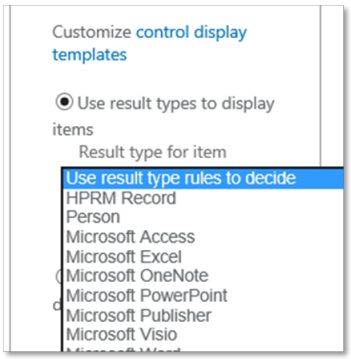
Click **OK** to change the query.

It may also be useful to remove everything from the web part except for the ranked results:



Save the web part and the page. Every time this page is visited, this fixed search will be executed.

The display template used for the display of Content Manager records may not be considered suitable for fixed searches. See Changing how search results are displayed for details on how to create a different template to be used. If a new template is created, modifying this search result web part will allow you to select that template to use:



17.9 Troubleshooting

Here are some common mistakes made when attempting to implement federated searching:

- The Content Manager governance and compliance app has not been added to the site that the searches are being performed on.
- The result source includes spelling mistakes, extra spaces or extra brackets.
- The SharePoint server has no access to reach the Content Manager server due to network issues.

18 Searching for existing Content Manager records using app parts

Content Manager search is delivered through app parts, which can be added to SharePoint pages where appropriate. A number of pre-configured search app parts, together with a free search input app part, are included. This allows users to display information stored in Content Manager directly alongside SharePoint content.

Search scenarios

The search capability is provided to enable the following scenarios:

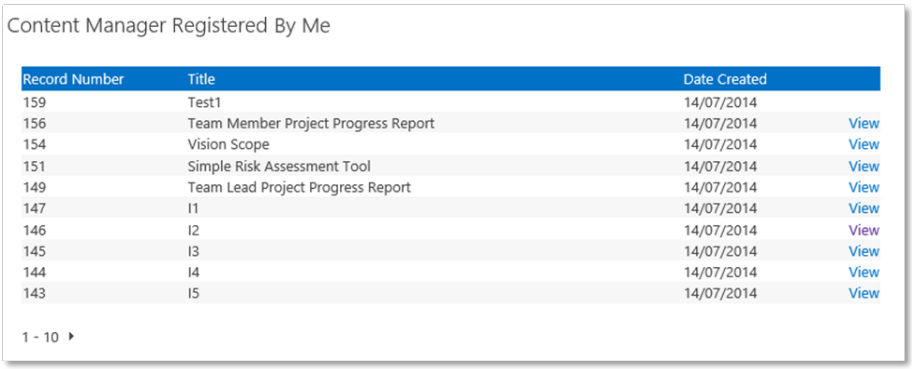
- Content relocated or archived from SharePoint to Content Manager can still be searched against and viewed.
- Content captured from elsewhere (LOB systems, Exchange, File Systems etc.) into Content Manager can be searched and viewed from SharePoint.
- Content captured from external SharePoint farms into Content Manager could be searched locally.

For content managed by Content Manager, but still stored in SharePoint, native SharePoint search can be used in the normal manner.

Search app parts

All the search app parts have the same basic anatomy. They provide a list of results in a simple grid format, with the following columns of information displayed:

- Record Number
- Title
- Date Created
- View Links



Documents and metadata items are treated in the same way, and by default 10 items are shown per page, with the ability to page through results using the arrow controls at the bottom of each page.

Clicking on the view link (where active) will behave differently depending on whether or not the item is still stored in SharePoint, and whether it is a list item or document.

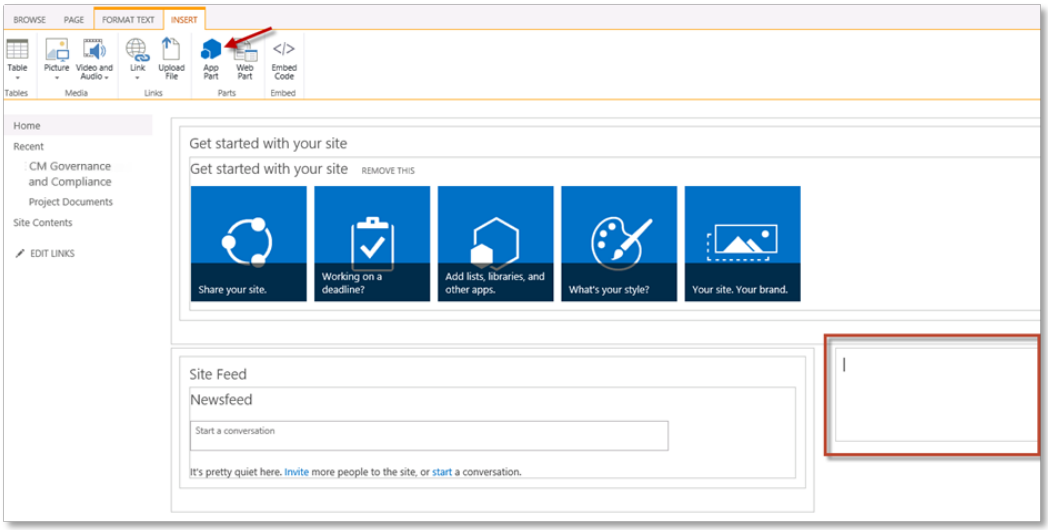
18.1 Adding pre-configured app parts

The Content Manager Governance and Compliance app includes a number of pre-defined search app parts. That is a number of different app parts with different search terms already populated in them.

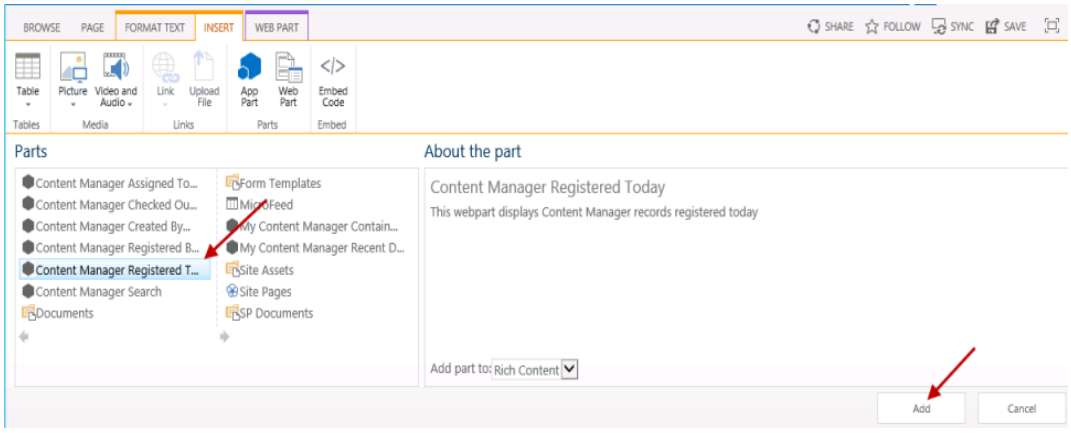
> **NOTE:** To perform the following you will require appropriate site permissions to edit pages in SharePoint.

To add a search app part to a page, perform the following steps:

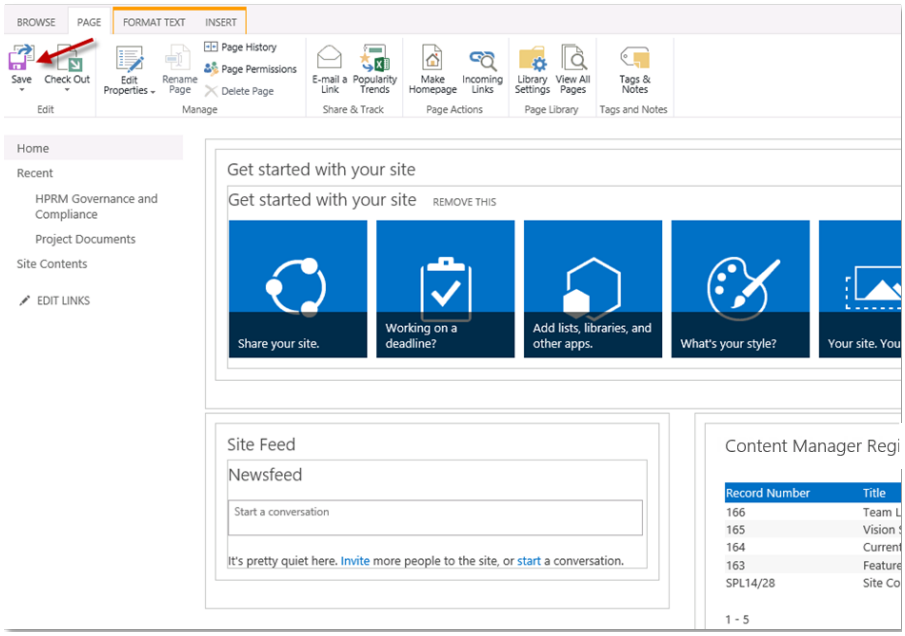
1. Navigate to the site you wish to add the app part to.
2. From the **PAGE** ribbon, click **Edit**.
3. Once the page is in edit mode, click into the zone you wish to add the search app part to. From the **INSERT** ribbon, click **App Part**. (In this example an app part is being inserted into the right-hand zone).



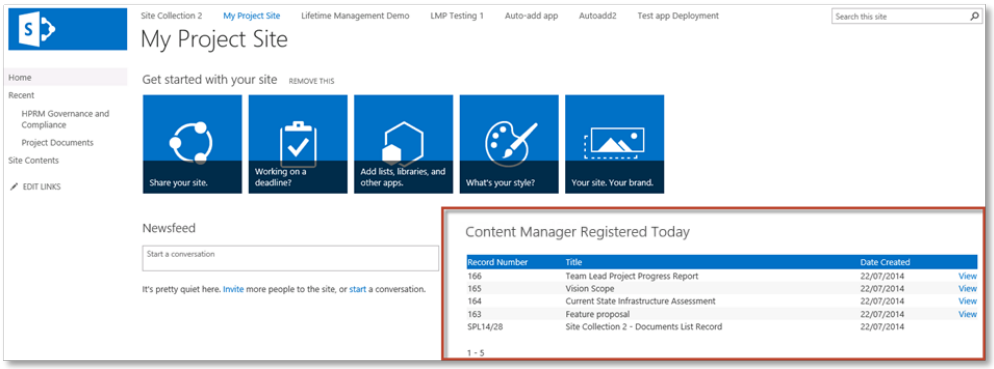
4. From the **Parts** pane, select the search part you wish to add then click **Add**. Repeat for other pre-defined parts if you wish to add more than one. In this example the **Content Manager Registered Today** search app part is being inserted.



5. Once you have added all required app parts, from the **PAGE** ribbon click **Save**.



The page will refresh and the selected app part will automatically retrieve and display any relevant results.



The following table describes the pre-configured search app parts:

NOTE: A number of these pre-configured searches are dynamic. That is, they are executed against the user currently logged into the SharePoint site. Different users will therefore see different results.

Title	Description
Content Manager Assigned To Me	Shows all records that have been assigned to the current user within Content Manager, typically to perform an action related to that record.
Content Manager Checked Out To Me	Shows all records that are checked out to the current user in Content Manager.
Content Manager Created By Me	Shows all records that were created in Content Manager by the current user.
Content Manager Registered By Me	Shows all records that were registered (Added) in Content Manager by the current user.
Content Manager Registered Today	Shows all records that were registered (Added) in Content Manager on today's date.
My Content Manager Containers	Shows containers in Content Manager that include records the current user has been using recently. Shows up to 25 containers.
My Content Manager Recent Documents	Shows up to the last 25 records the current user has created or worked on in Content Manager.

NOTE: The pre-defined search app parts automatically link the title in the chrome to the app start page. This is the nature of an app part, bear in mind that this may be confusing for some users.

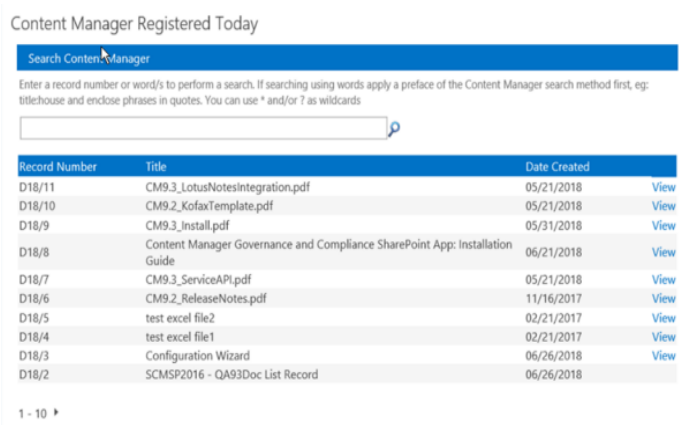
18.2 Creating your own pre-defined search app parts

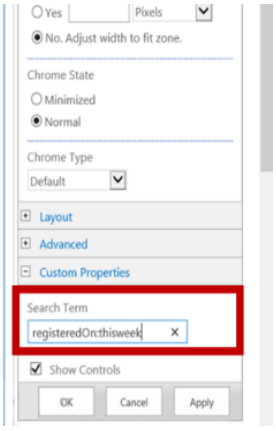
You may wish to provide other pre-defined search app parts to site consumers. It is possible to use an existing app part as the basis for a customized version, using your own search criteria, and then to share it in the **Parts** gallery.

NOTE: You will need to be a Site Collection Administrator to perform this task, as it involves saving a customized app part into a Web Designer Gallery

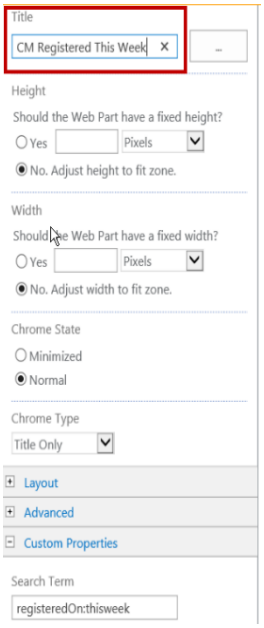
To create your own pre-defined search app parts, perform the following:

1. Edit the web part to access the configuration pane.
2. Add one of the existing pre-defined search app parts to a temporary site page location. For details on adding a search app part, see the 18.1 Adding pre-configured app parts, on page 255 section above.
3. Expand the custom properties section of configuration, and enter your required search parameter/s into the Search Term box. In this example, modifying the Content Manager Registered Today app part to show records registered this week.

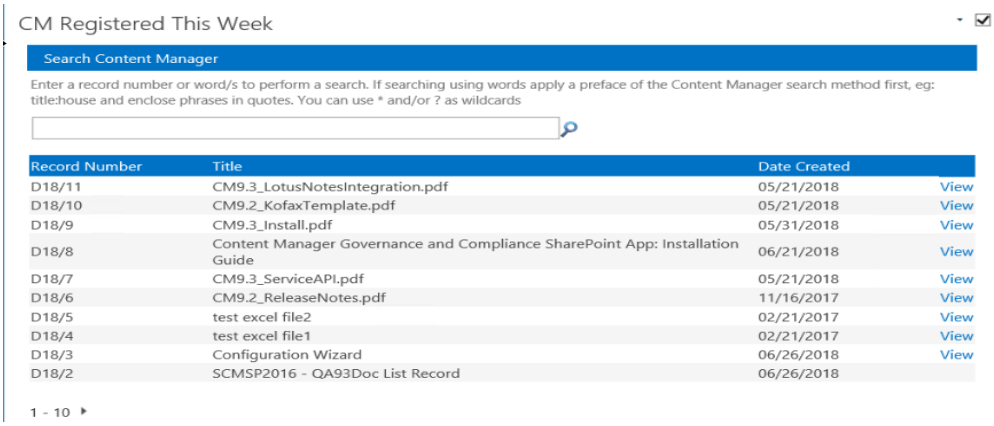




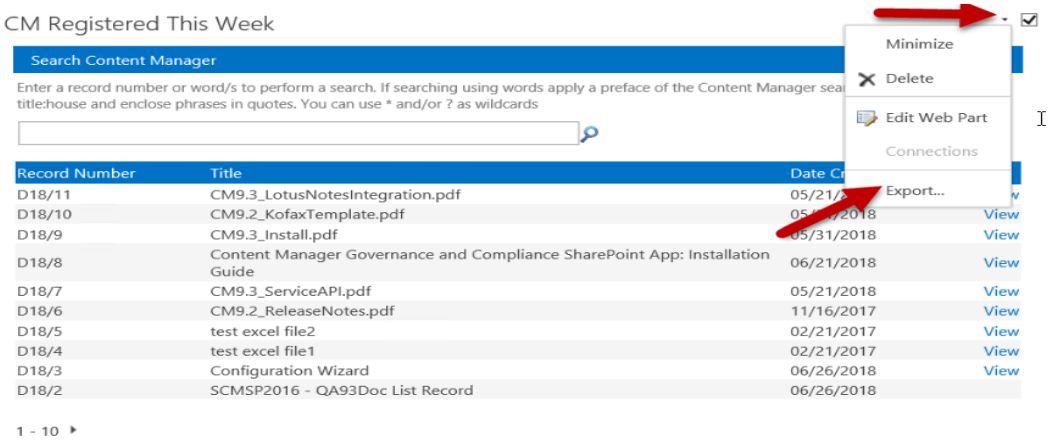
4. Under the **Appearance** section, modify the title to reflect your new search parameter/s.



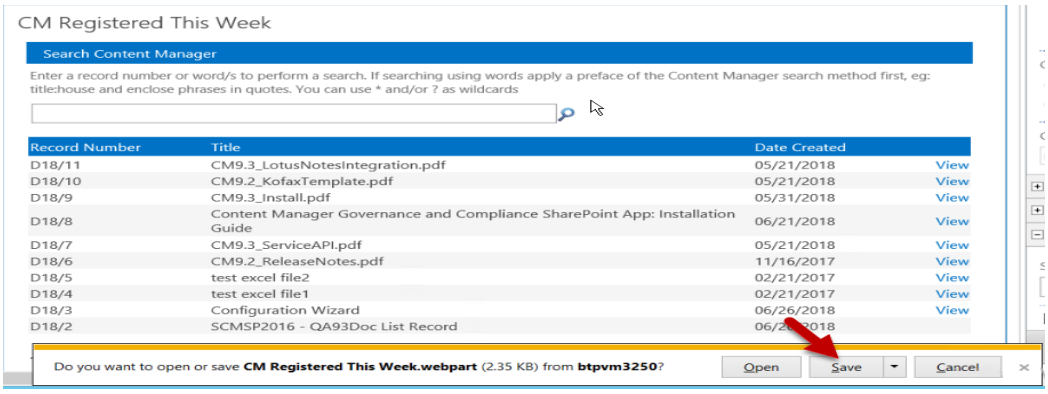
5. Expand the **Advanced** section, and change the **Export Mode** dropdown to **Export all data**. Click **OK** to apply all changes, and return to the page. The app part will refresh and display the results of your modified search parameter/s.



6. Now click on to the app art on the page, and from the drop down menu, choose **Export**.

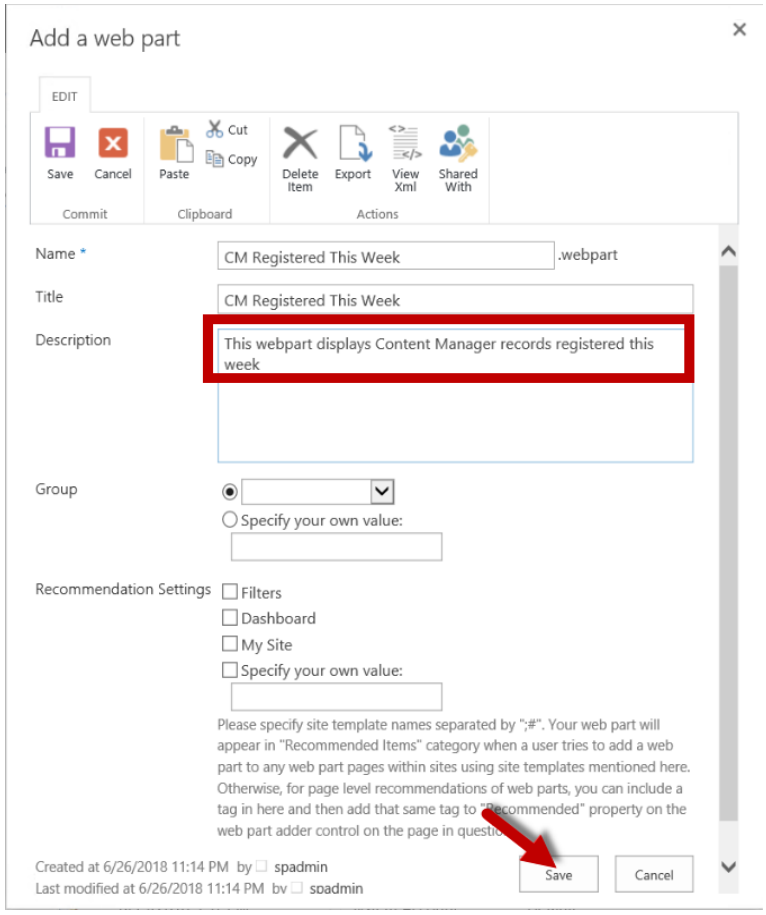


7. Choose to Save the **webpart** file, and save to a temporary location on the local machine (Your experience may vary depending on the browser being used).

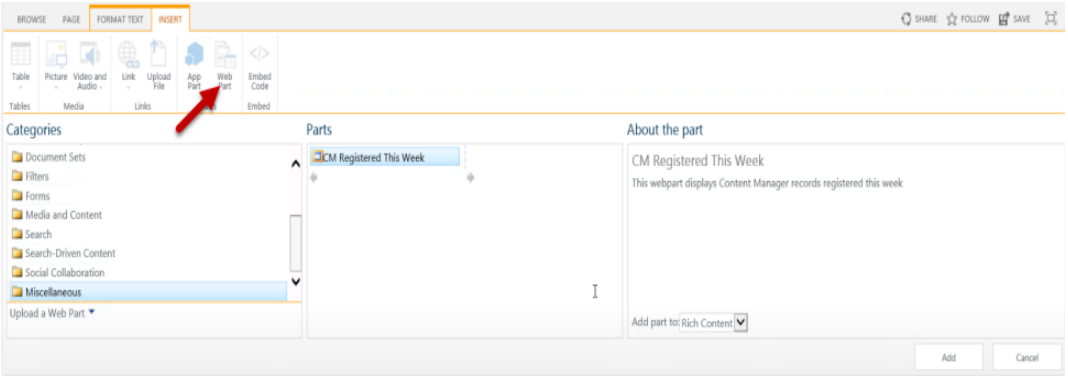


8. Now navigate to the root of the site collection you wish this web part to be available on, and go to **Site Settings > Web Designer Galleries > Web Parts**.

9. Upload your saved webpart file into the gallery, modify the description to reflect your search parameters before saving into the gallery.

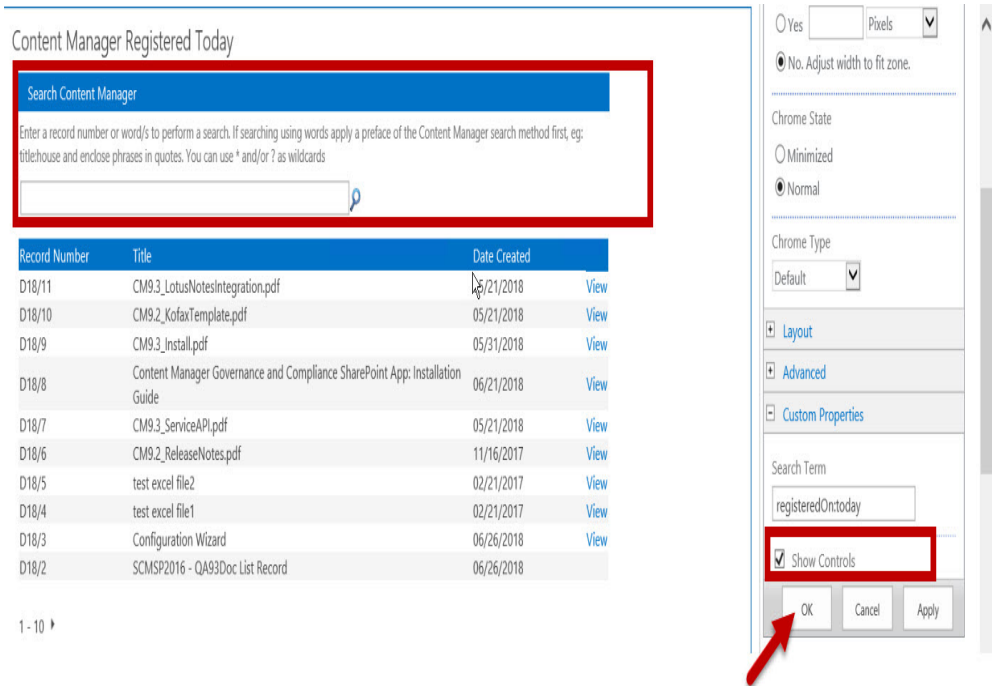


10. You can now add this customized search to any site as a web part, from the Miscellaneous section.



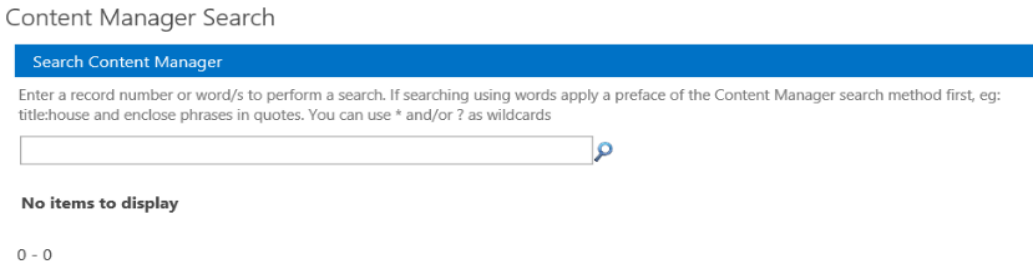
18.2.1 Including the search controls in custom app parts

You can include the search controls in a custom app part if you want users to have the ability to specify a different search term. Under the **Custom Properties** section of the app part configuration, check the **Show Controls** check box.



18.3 Using the Content Manager Search app part

This search app part is different, in that it allows users to perform on-demand searches of content stored in Content Manager. You can add this app part in the same way as the pre-defined app parts (See 18.1 Adding pre-configured app parts, on page 255 above), just select **Content Manager Search** from the **Parts** list.



> **NOTE:** The default chrome for the search app part shows the title. It is recommended to edit the app part and set the chrome to **None**.

There are two distinct types of searches that can be performed:

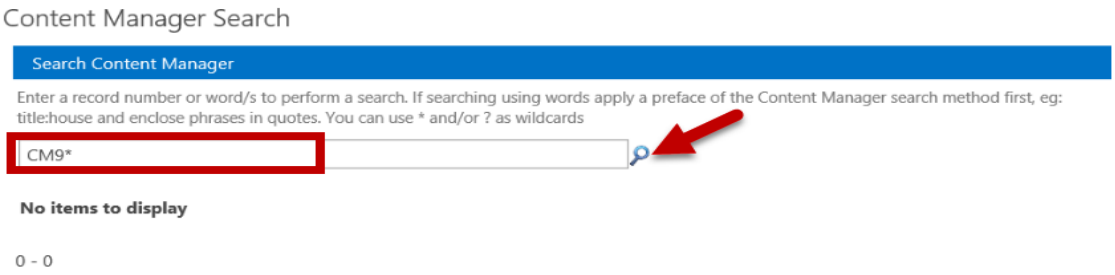
- Keyword searches – These are simple Boolean word searches against three key Content Manager fields (and optionally document content, see 18.4 Including content indexes in search results, on page 263 below).
  - Title
  - Notes

- Record Number

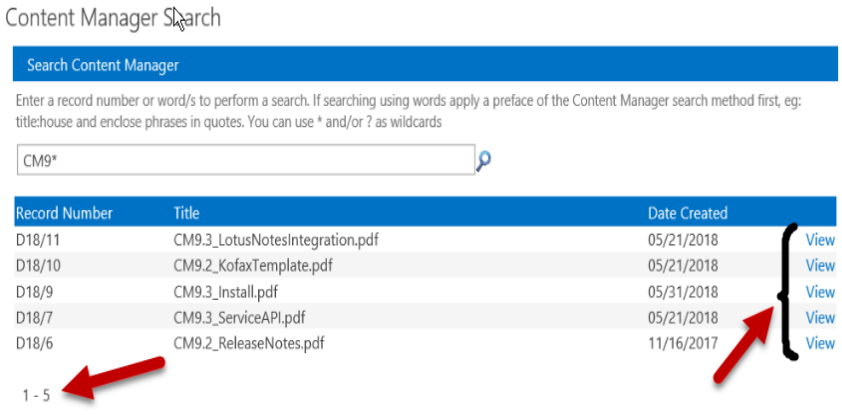
- Content Manager string searches – These can be used to perform relatively complex searches against specific Content Manager fields and criteria using a **METHOD:PARAMETER** format (e.g. **Title:report –** searches for records with the word **report** in the **title**)

To perform a keyword search:

1. Enter the required term/s into the search box and press the enter key, or click on the search icon to perform the search.



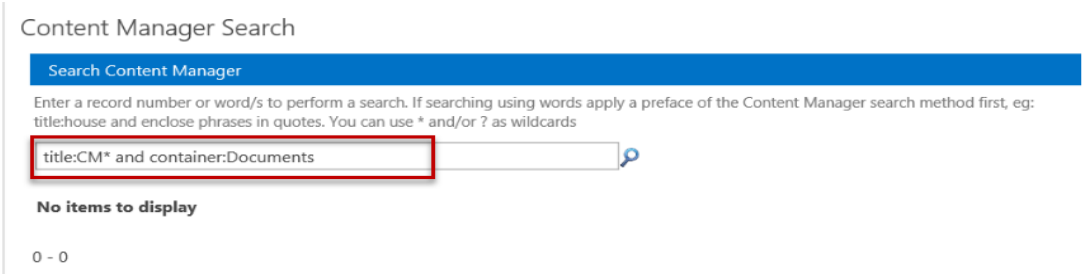
2. Once results are returned, you can click on the View link to view the associated document or, where still stored in SharePoint, the list item. Click on the paging arrow to go to the next page of results.



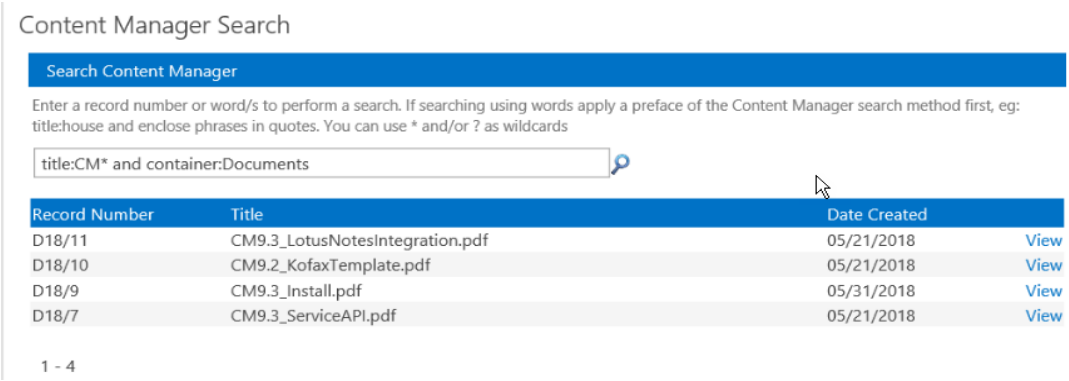
> **NOTE:** If the Content Manager web client is installed and configured, for results that are not in SharePoint, the view link will show the record in the Content Manager web client.

To perform a string search:

1. Enter the required string search into the search box and press the enter key, or click on the search icon to perform the search. In this example, the search is for records with **report** in the **title**, located in a container with **project** in the **title**.



2. You can see the results are somewhat different from just the keyword search on ***report***, as now the record container is a parameter too.



String searches allow you to perform much more sophisticated searching. There are many different parameters that can be searched against. Here are a few examples (For more details, see the Content Manager help documentation):

- ***Title:reef or editedOn:17/04/2009*** - returns all records with ***reef*** in the title or that have a ***Date Modified*** of ***17/04/2009***.
- ***Title:reef and not (Assignee:Fred and class:Top Secret)*** - returns all records with ***reef*** in the title that neither have the ***Assignee*** value ***Fred*** nor the ***Record Class*** value ***Top Secret***.
- ***container:[none]*** - returns all records that do not have a container

18.4 Including content indexes in search results

When entering keywords in the search input field, as described in 18.3 Using the Content Manager Search app part, on page 261 section above, it is possible to include a search against the Content Manager content index.

To enable this, perform the following steps:

1. Navigate to the default site collection, and go to the **Content Manager Governance and Compliance** app start page.
2. From the **Management options** section, click on **Default Integration Settings**.
3. On the **Default Integration Settings** page, from the **Search options** section, enable the **Include document content in searches** checkbox. Click **OK** at the bottom of the page to save the configuration.

4. Keyword searches using the search app part will now search against the content index as well as the metadata fields.

> **NOTE:** You must ensure Content Manager has an active, configured content index. If there is no content index in place, no search results will be returned.

19 Exposing existing Content Manager records into SharePoint

Organizations often have significant amounts of corporate information stored in Content Manager. Although and an organization may have elected to use SharePoint as the primary platform for collaboration and content management, it is reasonable to expect that from time to time, historical, or even current data located in Content Manager will be required by staff. Ideally this information can be accessed without having to leave SharePoint. This prevents users from having to work across systems and context and also removes the requirement for them to be trained in multiple systems.

Although search is a good tool for locating Content Manager records, this requires the user to actually make the effort to search for content. In doing so, they need to leverage the search tools in SharePoint.

In many cases, it would be preferable to simply “surface” the relevant Content Manager records in SharePoint as just another item in a library or list. This allows users to access all relevant content in a single location without the need to:

1. Remember to search for other relevant information.
2. Switch context in order to retrieve this information.

The Content Manager Governance and Compliance App includes a feature called ***Exposure***. Exposure allows surfacing records in Content Manager as native SharePoint list items, providing use of SharePoint functionality with that exposed content.

Exposure allows a single record to be surfaced in multiple locations across the SharePoint farm. For example, an authoritative policy document could be surfaced in many departmental sites across the SharePoint farm. If that policy is updated, that change is immediately available in all locations that the document is exposed.

The benefits of exposure include:

- Providing the ability to salvage information that has been previously **Relocated** or **Archived** to Content Manager, enabling an implementation to be more confident in turning over content in the “live” operating environment more readily;
- Enhancing accessibility of SharePoint content throughout a farm by providing the ability to surface ‘working’ instances of authoritative information across lists, sites, site collections and potentially even web applications; all the while maintaining version synchronicity between all exposed instances;
- Establishing ‘real’ content rollup lists (i.e. not just queries of external sources)thus enabling use of all of SharePoint’s View and Metadata Filtering/Navigation capabilities; and
- For any records that have been registered in Content Manager though use of integrations with other systems or line of business applications, pushing that content into SharePoint to standardize the end user interface.

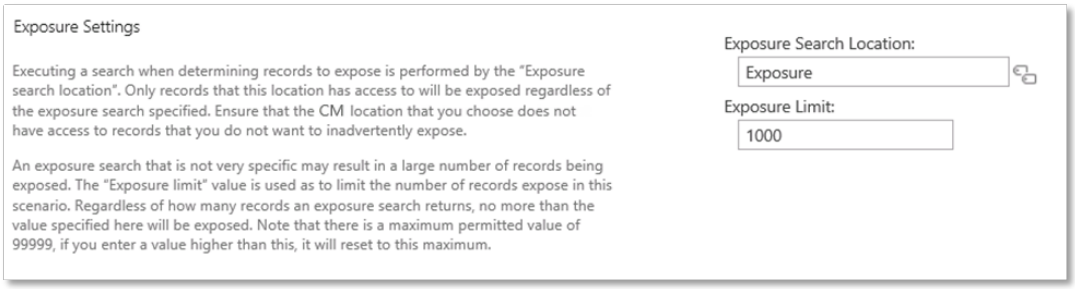
19.1 Configuring exposure

The process of configuring exposure can be divided into two tasks:

1. Configuring the common configuration.
2. Configuring on a list by list basis which records should be exposed.

19.1.1 Common configuration

There are two configuration values that must be provided to enable exposure. These can be accessed on the Default Integration Settings page. At the bottom of this page is the ***Exposure Settings*** section:



Exposure Search Location

Exposing records involves executing a search in Content Manager and surfacing the records that were found by that search. The results of a search can vary depending on who executes the search due to security and access controls.

The **Exposure Search Location** allows you to specify a location in your Content Manager dataset to use whenever this search is executed. When determining which account to use, consider what types of records you want exposed. For example, if it is not acceptable in your organization for any records to be exposed that have a security level other than unclassified, make sure that the location you choose does not have a security level higher than this. This ensures that any search that account performs will not return these types of records and therefore they will not be inadvertently exposed.

The location chosen should:

- Have a login specified on the profile tab in Content Manager.
- Be an Inquiry User (the intention is that they can perform searches with the minimum of permissions).
- Not be an administrator (as this will override any security and access control specified).
- Not have a security level higher than the level that is acceptable to expose.
- Not have any caveats that are used to control access to records that are not acceptable to expose.
- Not be a member of any Content Manager groups that are used control access to records that are not acceptable to expose.

You should bear in mind that changing the ***Exposure Search Location*** may result in significant changes to the records that are already exposed. If the location being changed to has access to significantly more or less records, this may result in a large number of exposure changes occurring the next time exposure maintenance is performed.

Exposure Limit

A search entered in exposure configuration could inadvertently result in a very large number of records being returned and therefore exposed. As exposure can be a performance intensive process, accidental exposure of large numbers of records may have an impact on the performance of your system.

To prevent users accidentally instigating large exposure tasks, the **Exposure Limit** value is used as a limit on the number of records to expose in any one list, regardless of how many results are returned by the search. The default value for this is 1000 but may be changed to any value if this does not suit the requirements of your implementation.

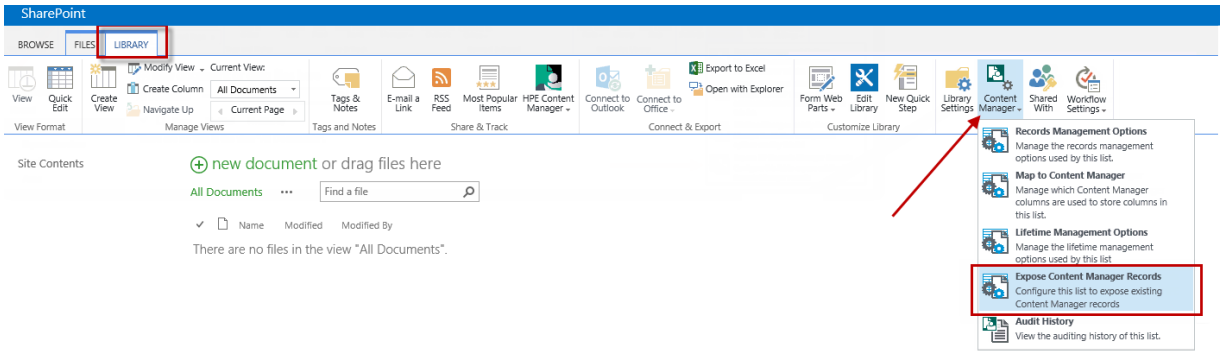
Setting this to a value of 0 will cause no records to be exposed. This can be used to in effect, disable exposure if required.

19.1.2 List/library specific configuration

You must specifically configure any list or library that records should be exposed to. This configuration is performed using the **Exposure Settings Page**.

Accessing the exposure settings page

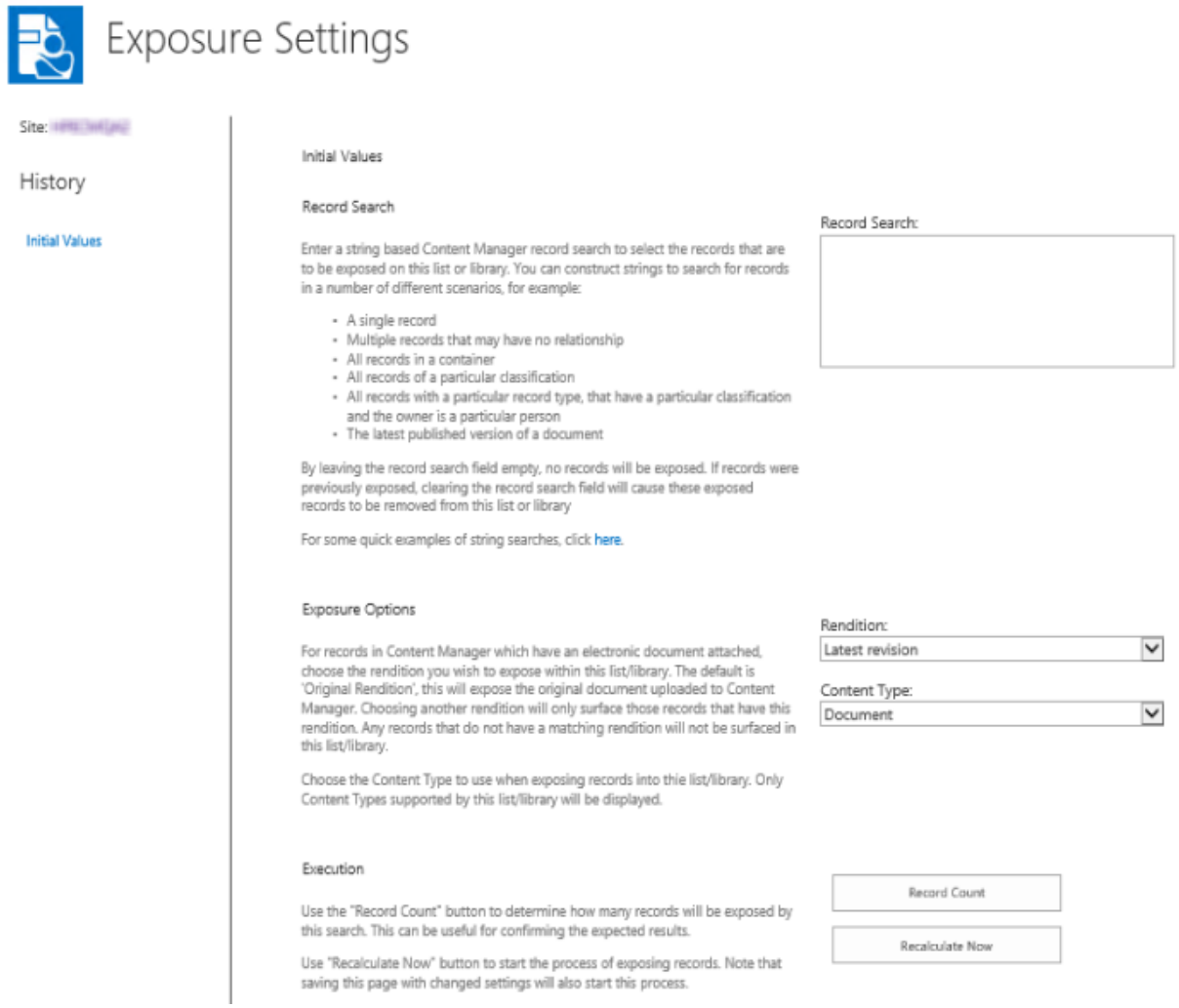
To access the **Exposure Settings Page** for a particular list or library, navigate to the that list/library then from the **Library**ribbon, select **Settings > Content Manager > Expose Content Manager Records**.



> **NOTE:** To access this page you must be the owner of the list.

Record Search

The **Record Search** text box allows entry of the Content Manager search to execute in order to determine the records to expose.



This is a Content Manager string based search. Examples of string based searches can be found by clicking the link in the description column of this section.

> **NOTE:** The Content Manager documentation provides comprehensive cover regarding how to author string based searches.

The following are some examples of searches that could be used:

Records to expose	Record search
A single record	number:D12/123
Multiple records that may have no relationship	number:D15/56 or number:D15/57
All records in a container	container:D10/4
All records of a particular classification	classification:Health-Policies

Records to expose	Record search
All records of a particular classification and below	classification:Health-Policies+
All records with a particular record type, that have a particular classification and the owner is a particular person	type:Policy and classification:Health-Policies and assignee:Smith
The latest published version of a document	currentVersion:D12/123

Exposure Options

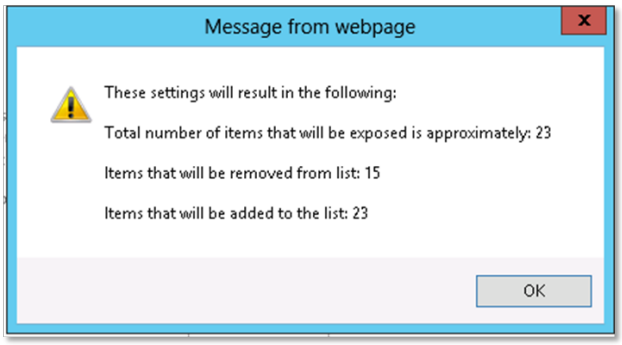
A record may have multiple renditions of the attached document. For example, although the document on the record is a Microsoft Word document, there may be a PDF rendition of the document available on the record. During exposure, the default is to expose the document associated with the record. Using the Rendition dropdown, it is possible to specify to expose a particular type of rendition instead.

If a particular rendition is selected, and a record does not have that rendition, then regardless of the fact that the record was returned by the record search, it will not be exposed. This feature can be used to ensure that you only expose for example, read only or redacted renditions of a record.

When exposing a record to a list or library, the list item created must use a content type. The ***Content Type*** drop down allows selecting the content type to use when creating these items. Only the content types supported by the list/library are shown in this dropdown.

Execution

The **Count** in the execution section of the **Exposure Settings** page allows you to test the settings you have entered. When clicked, the number of records that will be exposed is calculated. In addition, statistics regarding how many new items will be added and how many will be removed are shown.



> **NOTE:** The text on this dialog uses the term “approximately” to indicate the number of records exposed. This is because in some scenarios there may be inaccuracies that cannot be determined until the exposure has been completed.

Un-exposing content

To remove records that have been exposed there are two options.

To remove an individual item from the list/library, relocating the item will un-expose it.

To remove all items that have been exposed, setting the record search to empty will cause this to occur.

19.2 Updating exposed records

The records that are exposed are based on a search of Content Manager. There are many things that can change the results of this search therefore which records should be exposed. These include:

- A new record has been added
- A record has been deleted
- A property of a record has been modified such that it no longer matches the search
- A property of a record has been modified such that it now matches the search when it didn't previously
- The security of a record previously exposed has been increased so that the exposure search account cannot see it
- The security of a record has been decreased so that the exposure search account can see it when it previously couldn't
- A new rendition has been created such that a record now satisfies the exposure settings
- The Exposure Search Account is changed to a location with different security and access controls

Any of these events could happen at any time. The ***ExposureMaintenance*** recurring job in the job queue is responsible for periodically checking that the exposed records are correct. This job executes every 1 hour.

It is possible to force exposure maintenance for a particular list at any time though. Whenever exposure settings are modified and saved, exposure is recalculated. Additionally, the **Recalculate Now** on the **Exposure Settings** page for a list will start recalculation even if no change to exposure settings has been made.

19.3 Editing exposed items

As of version 8.3, exposed items can be edited in SharePoint.

Documents

In order to allow editing, an exposed document must be first checked out in SharePoint. This means that the library that a document is exposed must have ***require check out*** configured in the library versioning settings.

If a document is exposed in multiple places, each library that it is exposed to must also have this setting. If one of the libraries does not have this configured, when you attempt to edit the document an error will state that this setting has not been configured on all libraries.

Non documents

Meta data only exposed list items can be edited without the need to check the item out.

19.4 Known limitations

In this version, there are some limitations to exposure that should be considered:

- Records that have documents can be exposed to non document library lists, however, the document will not be surfaced as an attachment to that list item.

20 Understanding the job queue

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.

20.1 Defining 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.).

1. **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.

2. **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. See the 20.4 Jobs – Reference List, on page 280 chapter for details on all jobs, including recurring jobs.

   When accessing the job queue, members of the job administrators group will see all jobs including recurring jobs, for the current Content Manager Farm, all other users will only see their own jobs.

Job states

A job has a state associated with it, an individual job can only ever be in one of those states. The following table describes the meaning of each state:

State	Description
Pending	The job has not started yet, and is scheduled to be executed. The job is visible in the ***Scheduled*** view.
In Progress	The job is currently running, and is being processed. The job is visible in the ***In Progress*** view.
Failed pending retry	The job has failed for some reason. Viewing the job details will show the reason for the failure. The job is scheduled to be retried. The job is visible in the ***Scheduled*** view.
Failed	The job has failed three times, and has entered a permanent failed state. Manual intervention is required to fix the issue, before the job should be retried. The job is visible in the ***Failed*** view. See the 20.5 Troubleshooting jobs, on page 283 section below for more details.
Complete	The job has successfully completed all tasks. The job is visible in the ***History*** view.

Job queue

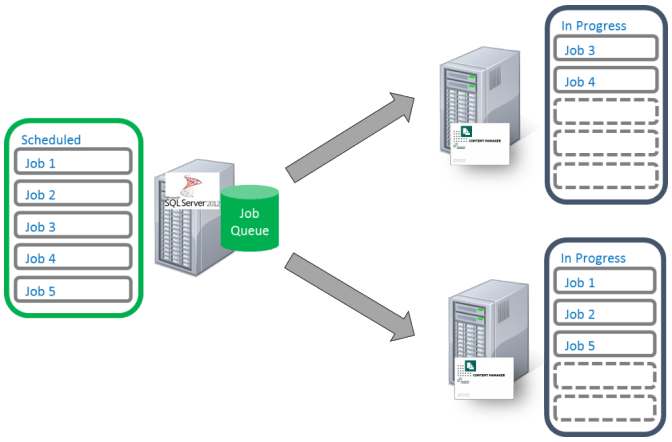
The job queue is a centralized list of all jobs in the Content Manager Farm, it includes all jobs that are due to be processed, are currently running, have completed or have failed. The queue is also a useful area to identify any issues with the ***Content Manager Governance and Compliance*** app, information from the queue can help administrators and OpenText 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.

Distributing jobs 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 (see the installation guide for details). 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 of concurrent running jobs equal to the sum of the ***Maximum job count*** for all servers you have configured in the Content Manager farm.

Depending on the type of job being processed, the job either runs as the configured job service account, or as the interactive user performing the action.

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.

Automatic removal of jobs

The job queue is stored in the configuration database. To prevent this from growing indefinitely, the job queue is automatically maintained. Jobs older than 30 days are removed from the queue.

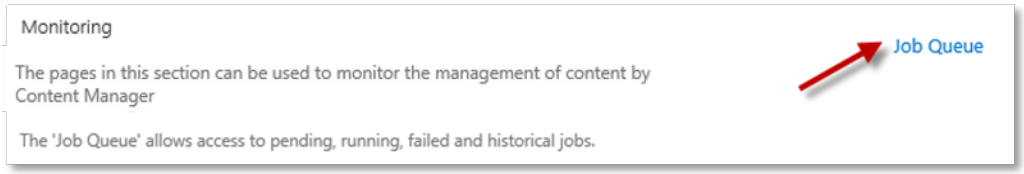
To perform retrospective analysis on older jobs, you would need to restore the relevant configuration database backup into a temporary SQL database (NOT overwriting the production configuration database), and use SQL tools to retrieve information from the job queue table.

20.2 Working with the job queue

Accessing the job queue

The job queue can be accessed from 4.1 The app start page, on page 27 on any site where the ***Content Manager Governance and Compliance*** app has been added:

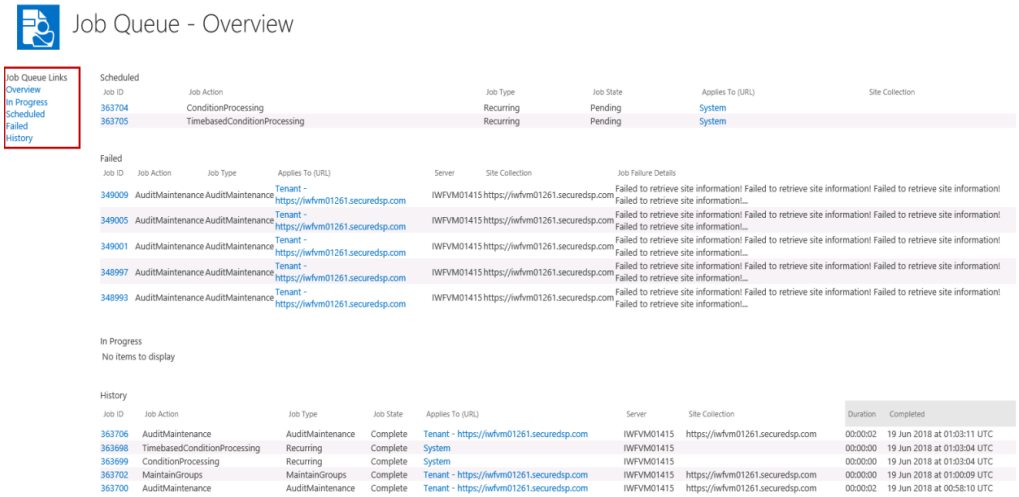
From the **Monitoring** section, click on the **Job Queue** link.



When accessing the job queue, members of the job administrators group will see all jobs for the current Content Manager Farm, all other users will only see their own jobs.

The different views

When first opening the **Job Queue**, *the* **Overview** *page is displayed, along with links to other available views:*

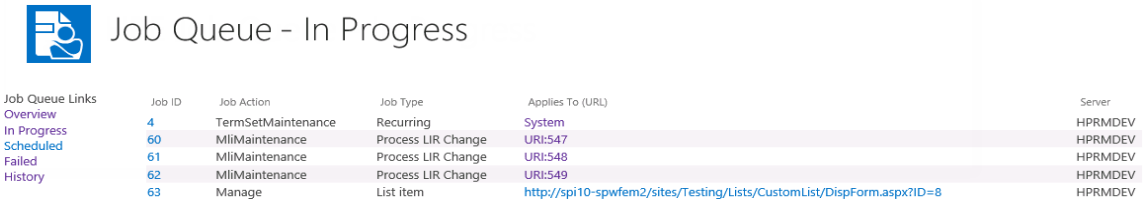


The **Overview** page displays a dashboard view of the job queue, showing a subset of jobs in various states. It is useful to get an initial picture of the queue, and its health.

Click the links in the **Quick-Launch** section to display dedicated views filtered by state.

In progress jobs

Shows all the jobs that are currently running in the Content Manager farm, along with a progress percentage indicator - ***Job Progress***.



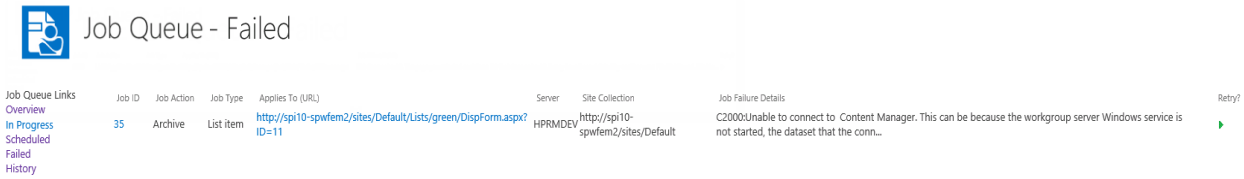
Scheduled jobs

Shows a list of all jobs that are scheduled to be processed, non-recurring jobs will largely be processed in the order seen in the list. Recurring jobs are processed on a pre-defined schedule. This view includes jobs that are in the ***Pending*** and ***Failed pending retry*** state.

Job ID	Job Action	Job Type	Job State	Applies To (URL)
1	Cleanup	Recurring	Pending	System
4	TermSetMaintenance	Recurring	Pending	System
5	MaintainGroups	Recurring	Pending	System
8	TimebasedConditionProcessing	Recurring	Pending	System
9	ConditionProcessing	Recurring	Pending	System
10	AuditMaintenance	Recurring	Pending	System

Failed jobs

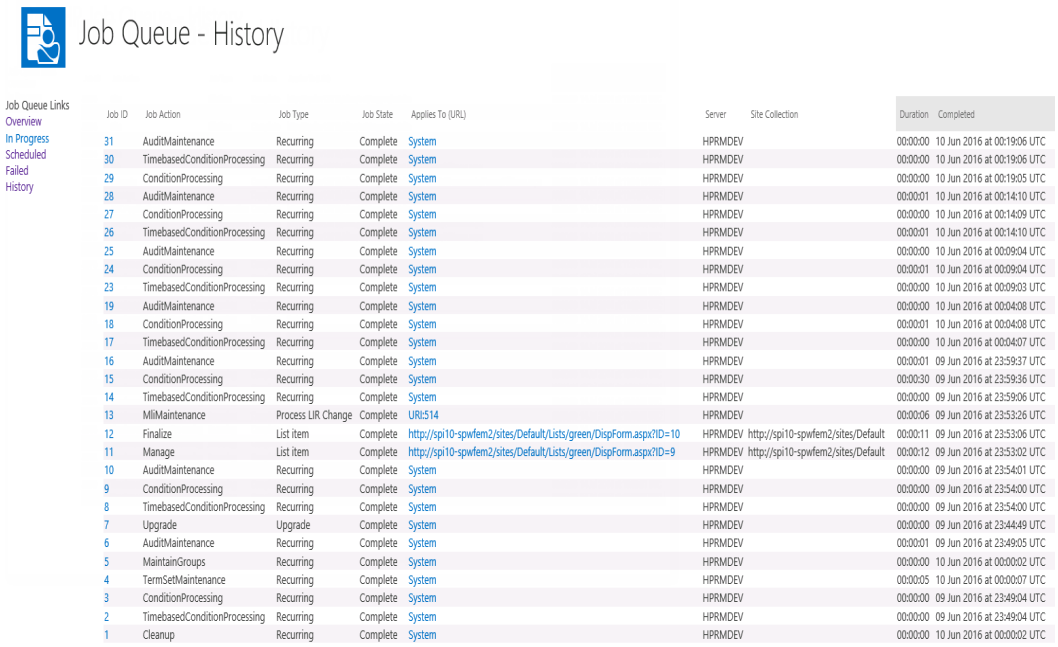
Jobs that have failed and are no longer scheduled for retry are shown here. This view includes a ***Retry*** button, to retry failed jobs once the underlying issue has been resolved. Refer to the 20.5 Troubleshooting jobs, on page 283 section below for more details on resolving and retrying failed jobs.



Job ID	Job Action	Job Type	Applies To (URL)	Server	Site Collection	Job Failure Details	Retry?
35	Archive	List item	http://spi10-spwfem2/sites/Default/Lists/green/DispForm.aspx?ID=11	HPRMDEV	http://spi10-spwfem2/sites/Default	C2000:Unable to connect to Content Manager. This can be because the workgroup server Windows service is not started, the dataset that the conn...	

Job history

All completed and failed jobs are shown in the ***history*** view. The ***history*** view includes information on the date and time the job completed and its duration. This can be useful in determining areas of app usage that are taking a long while to complete, and can aid in designing server architecture to ensure consistent job performance.



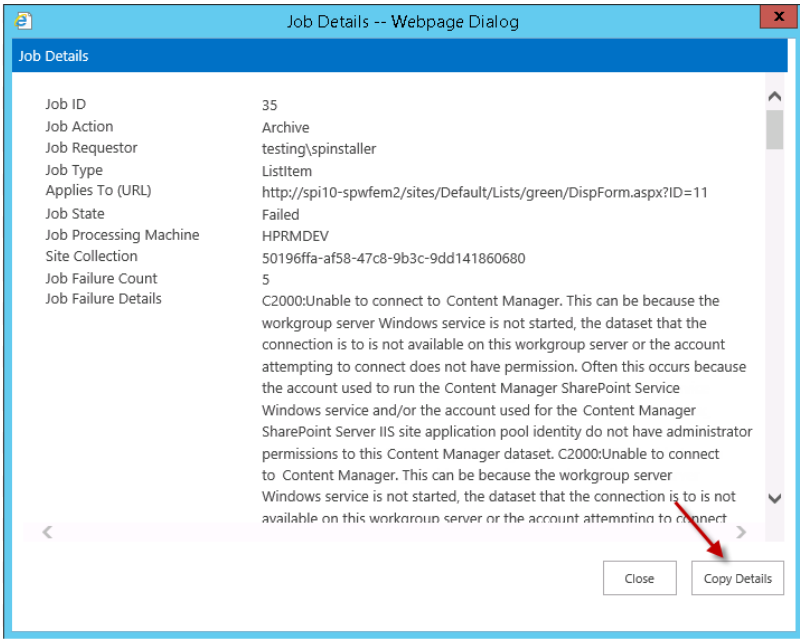
Job ID	Job Action	Job Type	Job State	Applies To (URL)	Server	Site Collection	Duration	Completed
31	AuditMaintenance	Recurring	Complete	System	HPRMDEV		00:00:00	10 Jun 2016 at 00:19:06 UTC
30	TimebasedConditionProcessing	Recurring	Complete	System	HPRMDEV		00:00:00	10 Jun 2016 at 00:19:06 UTC
29	ConditionProcessing	Recurring	Complete	System	HPRMDEV		00:00:00	10 Jun 2016 at 00:19:05 UTC
28	AuditMaintenance	Recurring	Complete	System	HPRMDEV		00:00:01	10 Jun 2016 at 00:14:10 UTC
27	ConditionProcessing	Recurring	Complete	System	HPRMDEV		00:00:00	10 Jun 2016 at 00:14:09 UTC
26	TimebasedConditionProcessing	Recurring	Complete	System	HPRMDEV		00:00:01	10 Jun 2016 at 00:14:10 UTC
25	AuditMaintenance	Recurring	Complete	System	HPRMDEV		00:00:00	10 Jun 2016 at 00:09:04 UTC
24	ConditionProcessing	Recurring	Complete	System	HPRMDEV		00:00:01	10 Jun 2016 at 00:09:04 UTC
23	TimebasedConditionProcessing	Recurring	Complete	System	HPRMDEV		00:00:00	10 Jun 2016 at 00:09:03 UTC
19	AuditMaintenance	Recurring	Complete	System	HPRMDEV		00:00:00	10 Jun 2016 at 00:04:08 UTC
18	ConditionProcessing	Recurring	Complete	System	HPRMDEV		00:00:01	10 Jun 2016 at 00:04:08 UTC
17	TimebasedConditionProcessing	Recurring	Complete	System	HPRMDEV		00:00:00	10 Jun 2016 at 00:04:07 UTC
16	AuditMaintenance	Recurring	Complete	System	HPRMDEV		00:00:01	09 Jun 2016 at 23:59:37 UTC
15	ConditionProcessing	Recurring	Complete	System	HPRMDEV		00:00:30	09 Jun 2016 at 23:59:36 UTC
14	TimebasedConditionProcessing	Recurring	Complete	System	HPRMDEV		00:00:00	09 Jun 2016 at 23:59:06 UTC
13	MliMaintenance	Process LIR Change	Complete	URI:514	HPRMDEV		00:00:06	09 Jun 2016 at 23:53:26 UTC
12	Finalize	List item	Complete	http://spi10-spwfem2/sites/Default/Lists/green/DispForm.aspx?ID=10	HPRMDEV	http://spi10-spwfem2/sites/Default	00:00:11	09 Jun 2016 at 23:53:06 UTC
11	Manage	List item	Complete	http://spi10-spwfem2/sites/Default/Lists/green/DispForm.aspx?ID=9	HPRMDEV	http://spi10-spwfem2/sites/Default	00:00:12	09 Jun 2016 at 23:53:02 UTC
10	AuditMaintenance	Recurring	Complete	System	HPRMDEV		00:00:00	09 Jun 2016 at 23:54:01 UTC
9	ConditionProcessing	Recurring	Complete	System	HPRMDEV		00:00:00	09 Jun 2016 at 23:54:00 UTC
8	TimebasedConditionProcessing	Recurring	Complete	System	HPRMDEV		00:00:00	09 Jun 2016 at 23:54:00 UTC
7	Upgrade	Upgrade	Complete	System	HPRMDEV		00:00:00	09 Jun 2016 at 23:44:49 UTC
6	AuditMaintenance	Recurring	Complete	System	HPRMDEV		00:00:01	09 Jun 2016 at 23:49:05 UTC
5	MaintainGroups	Recurring	Complete	System	HPRMDEV		00:00:00	10 Jun 2016 at 00:00:02 UTC
4	TermSetMaintenance	Recurring	Complete	System	HPRMDEV		00:00:05	10 Jun 2016 at 00:00:07 UTC
3	ConditionProcessing	Recurring	Complete	System	HPRMDEV		00:00:00	09 Jun 2016 at 23:49:04 UTC
2	TimebasedConditionProcessing	Recurring	Complete	System	HPRMDEV		00:00:00	09 Jun 2016 at 23:49:04 UTC
1	Cleanup	Recurring	Complete	System	HPRMDEV		00:00:00	10 Jun 2016 at 00:00:02 UTC

> **NOTE:** Jobs are only stored up to 30 days, after this time they are automatically purged from the queue. See the Automatic removal of jobs, on page 274 section above for more details.

Viewing the details of a job

You can access the details for any job by clicking on the ***Job ID*** link. This would typically only need to be accessed as part of troubleshooting or analysis. Clicking the link opens the job details page, the most relevant information is presented at the top of the page:

Click ***Copy Details*** will copy all of the job details to the clipboard as text. You can paste this text into an email or document, to share job details with internal or OpenText Support teams.



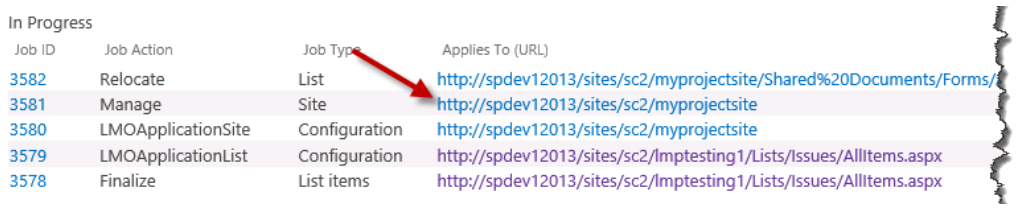
The contents of the job details fields are described in the following table:

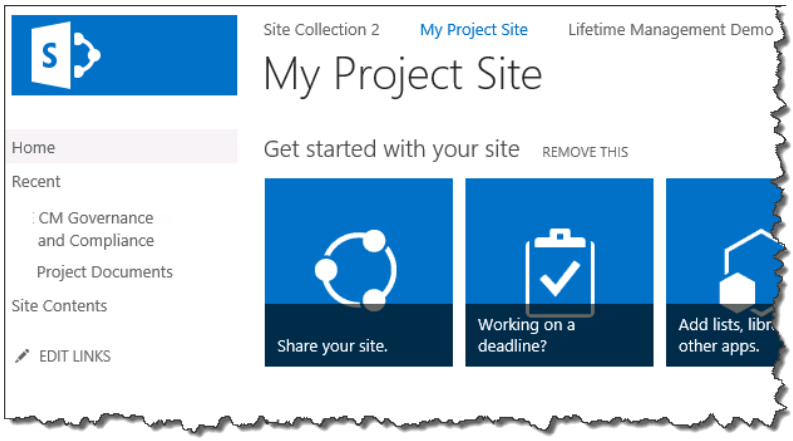
Job Field Name	Description
Job ID	The unique identifier for the job. The IDs are automatically allocated as a sequential number on job creation (e.g. ***3255***).
Job Action	The name of the job itself (e.g. ***ListItems, LMOApplicationSite***).
Job Requestor	The security identifier for the requesting user. Can be the job service account or an individual user, depending on the job type.
Job Type	Describes what type of job this is, and what it relates to (e.g. ***Lifetime, Configuration, and List***).
Applies To (URL)	Certain jobs perform actions against SharePoint content. This field displays a hyperlink to the relevant location.
Job State	Describes what state the job is currently in (e.g. ***Pending, In Progress,***

Job Field Name	Description
	Complete).
Job Processing Machine	The name of the machine in the Content Manager farm that processed (or is processing) the job.
Site Collection	The identifier of the site collection that the job is for.
Job Failure Count	In the case of jobs in the ***Failed pending retry***, or ***Failed*** state, this shows how many times the job has failed, up to a maximum of 3.
Job Failure Details	Very useful for troubleshooting purposes, this field displays the details of the error encountered when trying to process the job.
Job Details	System parameter used for the job.
Completed	The number of items that have been processed (if the job requires processing of multiple items).
Job Progress	Shows the percentage completed for the displayed job.
Start Time	Displays the time & date that the job entered ***the In progress*** state, in UTC. (e.g. ***14 Jul 2014 at 13:04:01 UTC***)
Completed	Displays the time and date that the job successfully completed, in UTC. (e.g. ***14 Jul 2014 at 12:59:01 UTC***)
Duration	Shows the time the job took to complete, from ***Start time*** to ***Completed***. Displayed in ***hh:mm:ss.***

Viewing the SharePoint location that a job applies to

> **NOTE:** Some jobs are applying directly to SharePoint sites/lists/items. Where relevant, the SharePoint URL is shown in the ***Applies to (URL)*** column. Clicking the URL takes you directly to the affected location. This can be very useful during troubleshooting or analysis, e.g. checking that a Lifetime Management Policy was applied to the correct location, or checking the context of content on a site where some content has been managed.





20.3 Job queue settings

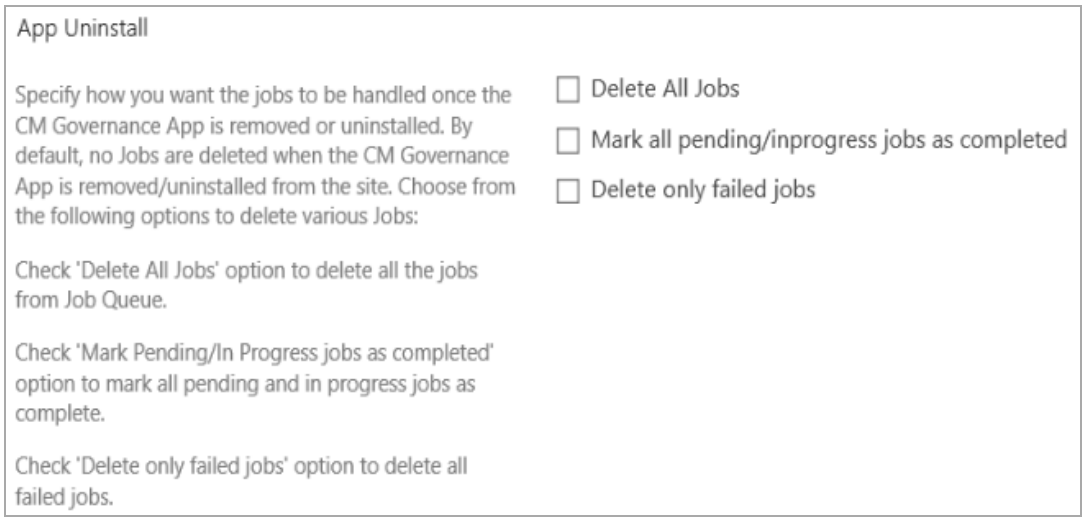
The Job Queue Settings page provides options to SharePoint administrators to configure job queue related operations based on the requirement.

Similar to job queue, the job queue settings can be accessed from 4.1 The app start page, on page 27 on any site where the ***Content Manager Governance and Compliance*** app has been added:

From the **Monitoring** section, click on the **Job Queue Settings** link.

20.3.1 App Uninstall

The App Uninstall section allows you to handle jobs once the CM Governance App***Content Manager Governance and Compliance*** app is removed or uninstalled.



The **Delete All Jobs** check box deletes all the jobs from the job queue.

> **NOTE:** Even after running **Delete All Jobs** option, there may be few system jobs left over in the Job Queue Table. This is because, when you upgrade from 9.4 or earlier versions, the jobs created in those versions will not have the site ID field. Therefore, it is not possible to determine

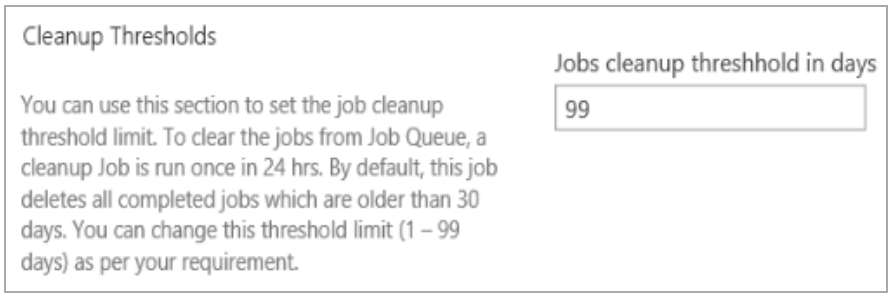
> which site or subsite a job belongs to and hence, some of the jobs may remain in the Job Queue Table.

The **Mark all pending/in progress jobs as completed** check box marks all the pending and in progress jobs as completed.

The **Delete only failed jobs** check box deletes all failed jobs.

20.3.2 Cleanup Thresholds

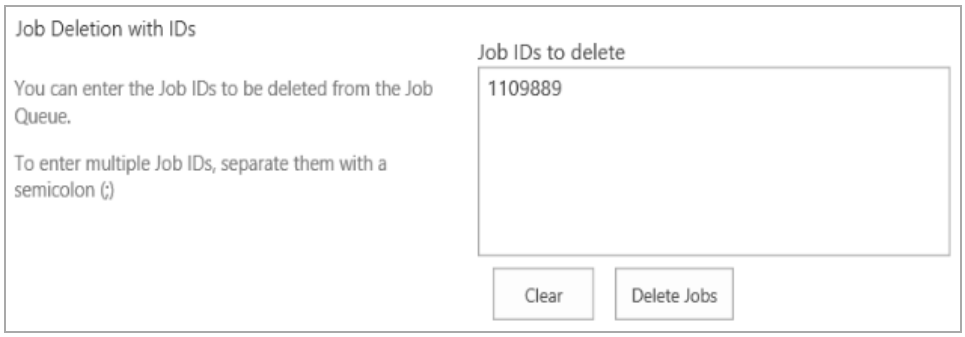
The Cleanup Thresholds section helps you to set the cleanup threshold limit.



A cleanup job is run once every 24 hours. This job deletes all completed jobs that are older than 30 days. You can set the cleanup threshold limit between 1 and 99 as per your requirement.

20.3.3 Job Deletions with IDs

This section allows you to delete a specific job(s) using the job ID(s).



To delete jobs using the job ID, enter the job ID in the **Job IDs to delete** box and click **Delete Jobs**. If you have more jobs to be deleted, separate each job ID with a semicolon (;).

Click **Clear** to clear the box.

20.4 Jobs – Reference List

This table lists many of the common jobs used by the Content Manager Governance and Compliance app, with a short description of each:

Job Name	Job Type	Description
Manage	List items	Raised when a user manually manages individual items on a list.
Finalize	List items	Raised when a user manually finalizes individual items on a list.
Relocate	List items	Raised when a user manually relocates individual items on a list.
Archive	List items	Raised when a user manually archives individual items on a list.
Manage	List	Raised when a user manually manages an entire list.
Finalize	List	Raised when a user manually finalizes an entire list.
Relocate	List	Raised when a user manually relocates an entire list.
Archive	List	Raised when a user manually archives an entire list.
Manage	Site	Raised when a user manually manages an entire site.
Finalize	Site	Raised when a user manually finalizes an entire site.
Relocate	Site	Raised when a user manually relocates an entire site.
Archive	Site	Raised when a user manually archives an entire site.
ListItem	Lifetime	Raised when an item is added or changes, which is subject to a LMP. May result in a management action being performed, if a rule is met.
List	Lifetime	Raised when a list property changes (Number of items, modified date etc.), which is subject to a LMP. May result in a management action being performed, if a rule is met.
Site	Lifetime	Raised when a site property changes (Number of items, modified date etc.), which is subject to a LMP. May result in a management action being performed, if

Job Name	Job Type	Description
		a rule is met.
LMOApplicationSite	Configuration	Raised when LMOs for a site change. For example this could be because a LMP was added directly to/from a site or parent site, Re-apply policies is instigated, active policies are edited or policies are removed.
LMOApplicationList	Configuration	Raised when LMOs for a list change. For example this could be because a LMP was added directly to/from a list or parent site, Re-apply policies is instigated, active policies are edited or policies are removed.
MliMaintenance	Process LIR Change	Raised when a managed item changes in Content Manager. This job makes sure the metadata stays in sync between the two platforms. Note the metadata change could either be instigated by a user, or automatically through workflow or third-party add-on.
TimeBasedConditionProcessing		This recurring job supports ***Lifetime Management Policies*** that include time/date-based conditions. It periodically checks the ***Job Diary*** to ascertain if any Lifetime jobs need to be raised to initiate actions for content that might meet a defined time or date based rule.
TermSetMaintenance		Term Sets are used throughout the app, providing access to Content Manager constructs (Classifications, Record Types, and Security Levels etc.) through standard SharePoint metadata functionality. This recurring job ensures that any information that is changed or added in Content Manager, is properly synchronized into the appropriate SharePoint term set.
Cleanup		This recurring job is used to remove jobs that are older than 30 days from the job

Job Name	Job Type	Description
		queue
ExposureMaintenance	Recurring	Periodically checks that exposed records are correct and performs updates to if changes have occurred.
MaintainGroups	Recurring	Periodically checks Content Manager's security groups and performs updates if changes have occurred.

20.5 Troubleshooting jobs

20.5.1 Stalled jobs

Sometimes, problematic jobs may get stuck in an ***In Progress*** state. This could be for any number of reasons. Fortunately, the job queue has a mechanism to deal with stalled jobs. If the job doesn't progress within 60 minutes from the ***Start time***, then the state is automatically set to ***Failed pending retry***. This will force the job to be retried. If the failure repeats, the job will eventually (after 3 retries) go to a ***Failed*** state, at which point the issue should be investigated.

This prevents problematic jobs from getting stuck in an ***In Progress*** state, and preventing other jobs from being processed.

20.5.2 Jobs stay in pending state and don't get processed

If jobs are all staying in a ***Pending*** state, and never move to ***In Progress***, check the following:

1. Confirm that the ***Content Manager SharePoint Service*** is running on each server in the Content Manager farm
2. Check that the Workgroup Server name/s are correct in the configuration tool, and republish if necessary

The Content Manager Governance and Compliance App log (Located under *<Install Path>\Logs* – e.g. *C:\Program Files\Micro Focus\Content Manager\Content Manager SharePoint Integration\Logs*) will likely show errors similar to:

Unable to locate the job processing settings to use for this machine Content Manager**1. This could be because the machine name for this workgroup server was entered incorrectly in the configuration tool. Use the configuration tool to confirm that this server has the machine name entered correctly. If it hasn't, correct the name and republish the settings.**

20.5.3 Deleting a job

On some occasions a problematic job may not be able to be resolved. In these cases it may be necessary to delete a job. Note that this is considered to be a very rare occurrence, as most problematic jobs should end up in a failed state, and will not need to be removed.

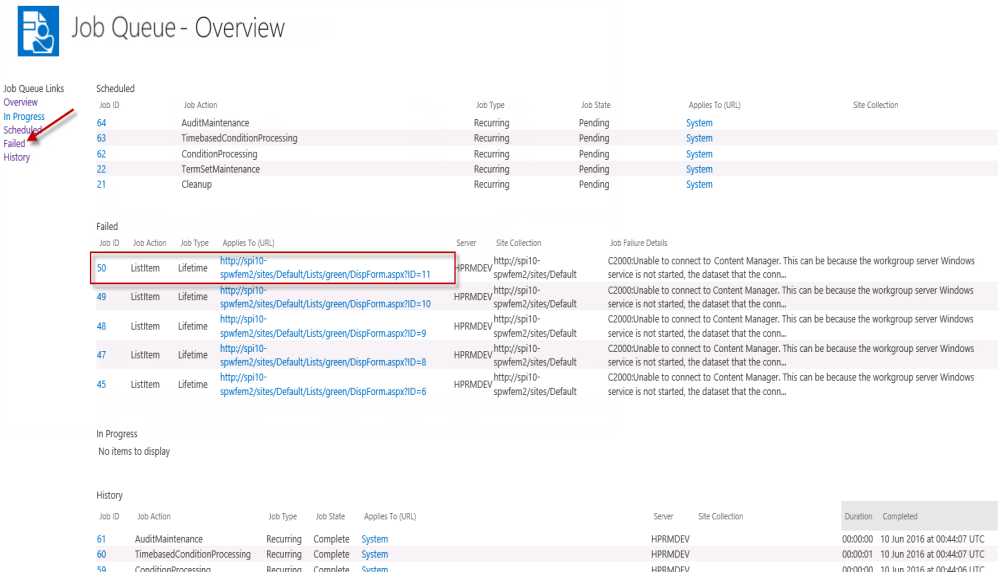
However, if the requirement does arise, you can navigate to **Jobs Queue Settings** page and remove or delete the job(s). For details, see 20.3 Job queue settings.

20.5.4 Restarting a failed job

When a job enters the failed state, it will not rerun without manual intervention. Troubleshoot and fix the underlying issues first, then rerun the job if required.

To restart a failed job:

1. Go to the job queue and click **Failed** link in the left-hand navigation.



2. On the ***Job Queue – Failed*** page, locate the relevant job in the list and click the green arrow in the ***Retry*** column. The job will automatically be changed into a ***Pending*** state, and will be retried.

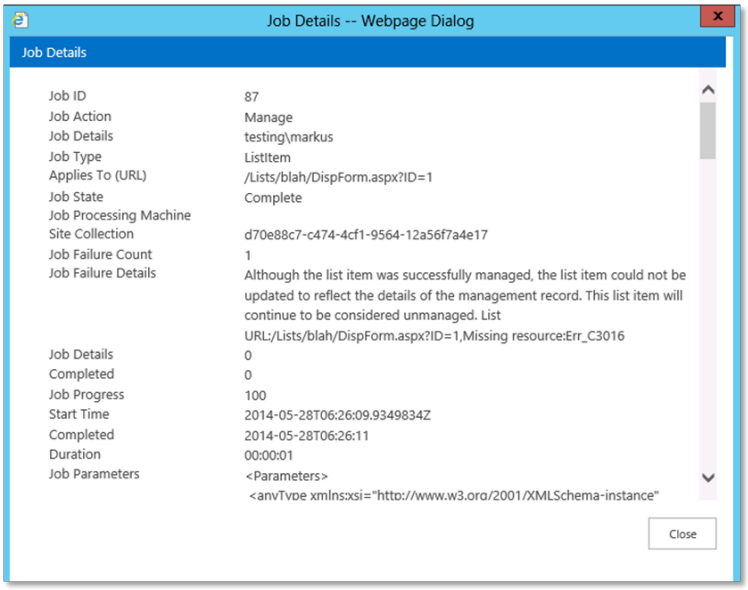
20.5.5 Management job fails

If a management job fails, with the following text in the Job Failure Details:

Although the list item was successfully managed, the list item could not be updated to reflect the details of the management record. This list item will continue to be considered unmanaged. List <URL>

This indicates that the application pool account, for the Content Manager SharePoint site in IIS, does not have the required permissions in the Content Manager content database.

Refer to the Identify and configure accounts section in the *Content Manager Governance and Compliance SharePoint App: Installations Guide* for details on the required permissions.



20.6 Notifications

Notifications have been enhanced to permit the ability for users to specify which job notifications they are interested in. The configurable notifications are available for the following:

Core Process

Core Process can be configured for when notifications should be sent for jobs. Options can be set individually for when jobs complete, fail, or fail pending retry.

The specific options on the Job Notifications Page are:

• Manual Core process (on any item) success

• Manual Core process (on any item) failure pending retry

• Manual Core process (on any item) failure

Exposure

Exposure Notification Settings can be configured for when notifications should be sent for jobs. Options can be set individually for when the following occurs in relation to exposure jobs:

• Exposure success

• Exposure failure

Lifetime Management

Lifetime Management notifications can be configured to be sent when a lifetime management job fails. When enabled, this will allow users the ability to define who these notifications should be sent to by entering one or more email addresses into the appropriate form field.

The specific option on the Job Notifications Page is:

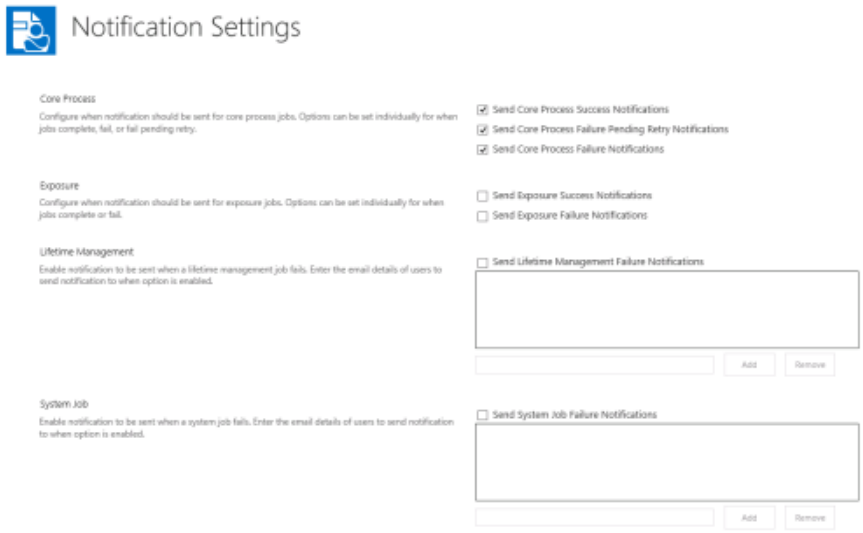
• Lifetime management failures - provide a way to define recipients

System Job

The specific option on the Job Notifications Page is:

• System job failures

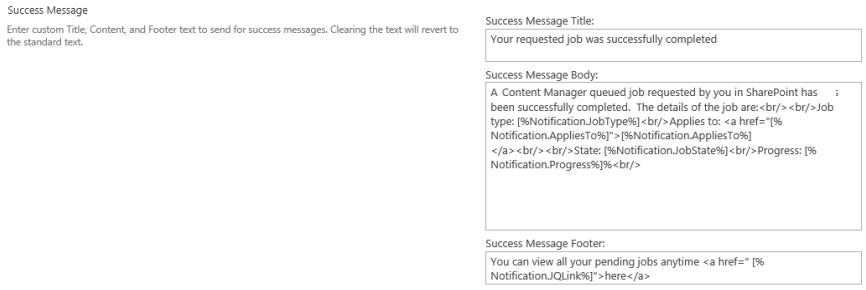
To access the Notifications page navigate to the "App Start page" and select "Notifications".



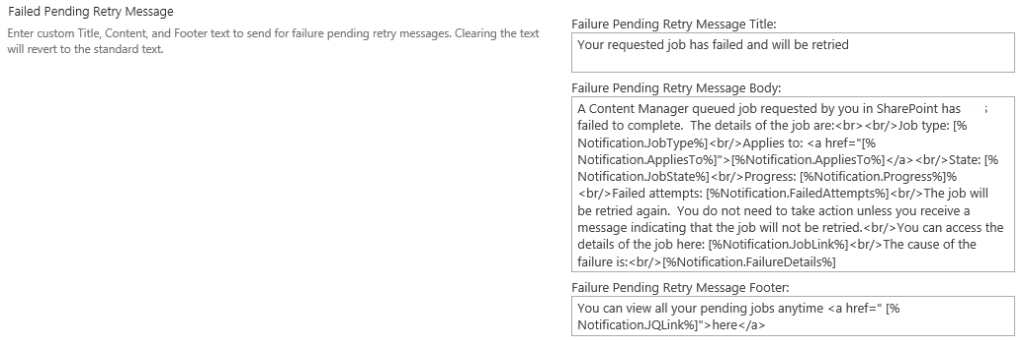
Customizable Job Notifications

The ability to customize a Job Notification message title, message body and the message footer are available for all three types of notification messages. Job Notifications can be customized from the Job Notifications page on the App Start page. The different Job Notifications that can be customized are:

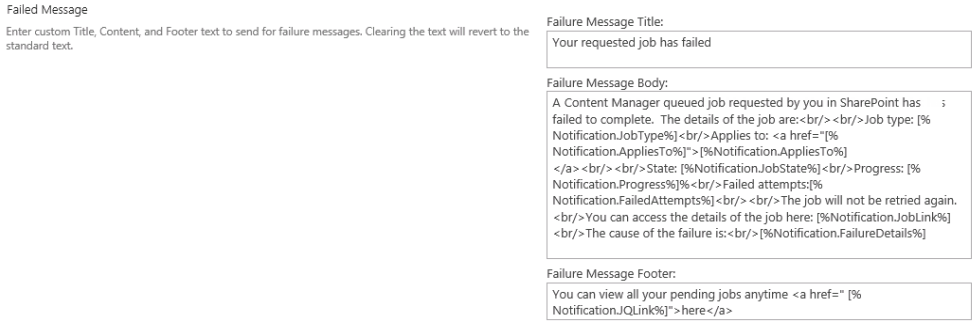
Success Message



Failed Pending Retry Message



Fail Message



The Job Notification messages can be reverted back to the original notification message by clearing all of the fields for the specific job notification message and selecting OK on the Job Notifications Page.

Use of Substitution Strings

In order to customize the notifications, users are given access to SharePoint data by means of substitution strings. These allow exposure of SharePoint data items by means of special "tags". The available data and associated tags are outlined below.

Substitution String	Description
[%Notification.JobType%]	The type of job which is being run. Those include: • List Item or List Items • List • Site • Exposure • Configuration • Lifetime

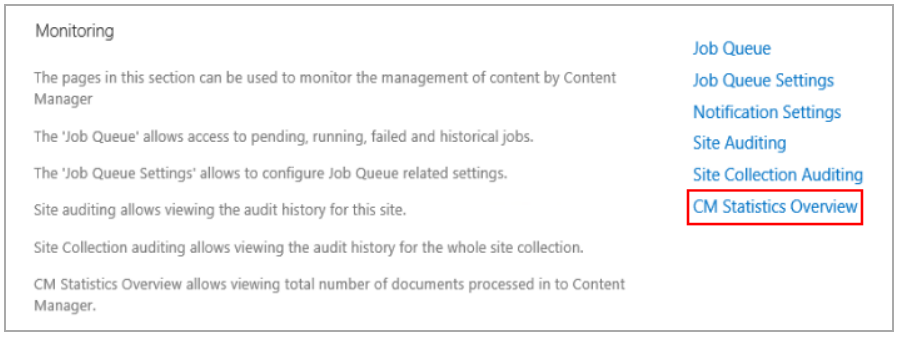
Substitution String	Description
	• Calculate User Claims • Invalidate Claims Cache • Security Refresh • Populate TRIM group • Process LIR Change • Recurring • Populate Security Group • Refresh Security Groups • Upgrade • Content Manager Security Refresh • Administration • Not Set
[%Notification.AppliesTo%]	The particular artifact which the notification applies to.
[%Notification.JobState%]	The state of the current job. • Pending • Failed Pending Retry • Failed • Complete
[%Notification.Progress%]	The progress of the current job, as a percentage of completeness (0 - 100).
[%Notification.JQLink%]	Job Queue Link, the link to the job queue in which this artifact resides.
[%Notification.FailedAttempts%]	The total amount of failed attempts.
[%Notification.JobLink%]	The direct link to the job in SharePoint
[%Notification.FailureDetails%]	The associated details as to why a particular job has failed.

21 Content Manager statistics

The Content Manager app start page provides statistics of the SharePoint items for sites and sub-sites.

21.1 Accessing Content Manager statistics

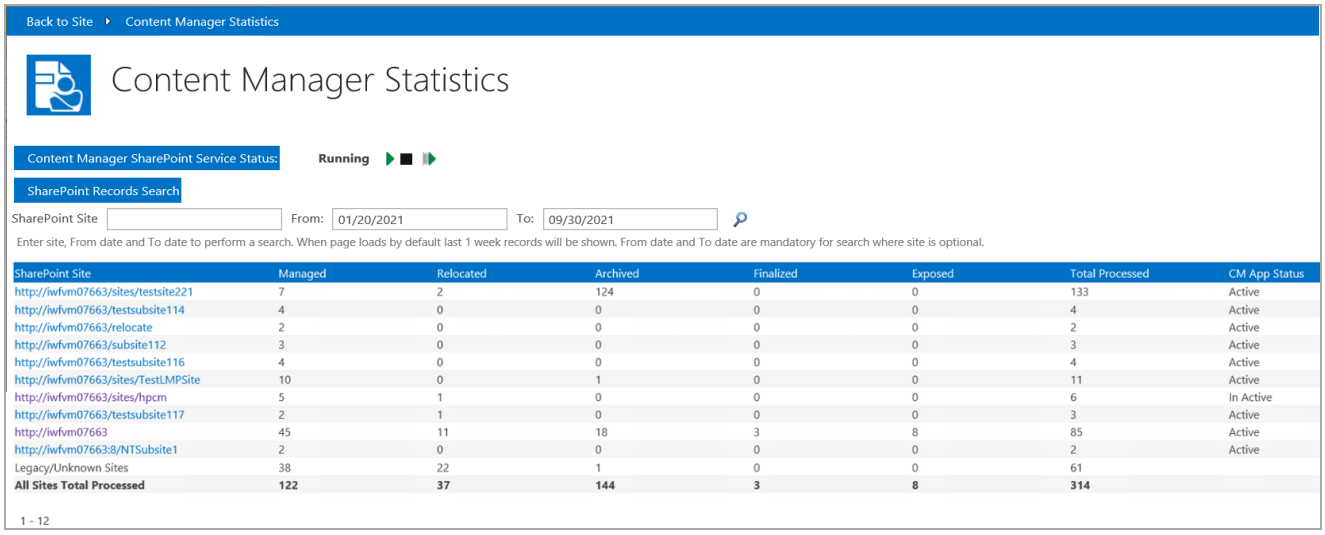
You can access the Content Manager statistics from the app start page. In the app start page, scroll down to **Monitoring** section and click **CM Statistics Overview**.



21.2 Inclusions in Content Manager statistics overview

Viewing the Content Manager statistics overview page will display the following information:

- Start, stop or restart the Content Manager SharePoint service
- Status of the Content Manager SharePoint service
- Number of SharePoint items managed, relocated, archived, finalized, and exposed for each site and sub-site
- Status of Content Manager app



SharePoint Site	Managed	Relocated	Archived	Finalized	Exposed	Total Processed	CM App Status
http://iwfvm07663/sites/testsite221	7	2	124	0	0	133	Active
http://iwfvm07663/testsubsite114	4	0	0	0	0	4	Active
http://iwfvm07663/relocate	2	0	0	0	0	2	Active
http://iwfvm07663/subsite112	3	0	0	0	0	3	Active
http://iwfvm07663/testsubsite116	4	0	0	0	0	4	Active
http://iwfvm07663/sites/TestLMPSite	10	0	1	0	0	11	Active
http://iwfvm07663/sites/hpcm	5	1	0	0	0	6	In Active
http://iwfvm07663/testsubsite117	2	1	0	0	0	3	Active
http://iwfvm07663	45	11	18	3	8	85	Active
http://iwfvm07663:8/NTSubsite1	2	0	0	0	0	2	Active
Legacy/Unknown Sites	38	22	1	0	0	61	
All Sites Total Processed	**122**	**37**	**144**	**3**	**8**	**314**	

By default, the statistics are displayed for the last one week. You can get the details as per your requirement by entering the SharePoint site, the duration (from and to dates) for which you need the statistics, and then click the search icon.

> **NOTE:** When you upgrade from prior version of Content Manager to 25.1 and if some of the sites or sub-sites were deleted, the statistics for such sites will be listed under **Legacy/Unknown Sites**.