

Gimmel Records

Gimmel Records

Exported on 07/20/2023

Table of Contents

1	Featured Pages.....	18
2	Recently Updated	19
3	User Guide	20
3.1	Signing In and Out.....	20
3.2	Inbox	20
3.3	Physical Assets	20
3.4	Signing In and Out.....	20
3.4.1	Sign In	20
3.4.2	Sign Out	20
3.5	Inbox	21
3.5.1	Overview	21
3.5.2	Accessing the Inbox.....	21
3.5.3	Adding and Removing Columns	22
3.5.4	Filtering the Inbox	22
3.5.5	Sorting the Inbox.....	23
3.5.6	Saving and Using Views	24
3.5.6.1	Using a View	24
3.5.6.2	Saving existing View.....	24
3.5.6.3	Deleting a View	25
3.5.6.4	Changing the Default View	25
3.5.7	Disposition Actions	26
3.5.7.1	Selecting Records.....	26
3.5.8	Approving Records.....	27
3.5.9	Unapprove.....	29
3.5.10	Pause	30
3.5.11	Reject	32
3.5.12	Submitting Approvals	33
3.5.12.1	Approving and Submitting together	34
3.5.13	Adding Columns to Your Inbox Views	35
3.6	Physical Assets	36
3.6.1	Requesting an Asset.....	36
3.6.1.1	Creating a Request.....	37

3.6.1.2	Adding and Removing Assets from a Request	37
3.6.1.3	Submitting a Request	37
3.6.1.4	Request an Extension for a Charged Out Asset	37
3.6.1.5	Canceling and Deleting a Request	37
3.6.1.6	Creating a Request	38
3.6.1.7	Adding and Removing Assets from a Request	41
3.6.1.8	Submitting a Request	45
3.6.1.9	Request an Extension for a Charged Out Asset	50
3.6.1.10	Canceling and Deleting a Request	53
3.6.2	Returning an Asset	56
3.6.2.1	Creating a Return	56
3.6.2.2	Adding and Removing Assets from a Return	56
3.6.2.3	Submitting a Return.....	56
3.6.2.4	Canceling and Deleting a Return.....	56
3.6.2.5	Creating a Return	57
3.6.2.6	Adding and Removing Assets from a Return	59
3.6.2.7	Submitting a Return.....	64
3.6.2.8	Canceling and Deleting a Return.....	68
3.6.3	Managing Charge-Outs	69
3.6.3.1	Viewing Asset's Properties.....	69
3.6.3.2	Returning an Asset	70
3.6.4	Taking Custody of an Asset.....	71
4	Record Manager Guide.....	73
4.1	Building Your File Plan	73
4.2	Manage	73
4.3	Disposition.....	73
4.4	Monitor	73
4.5	Rule Builder	73
4.6	Physical Records	73
4.7	Creating and Managing Legal Cases and Legal Holds.....	73
4.8	Filtering Records by Rules and Metadata	73
4.9	Record Class Permissions	73
4.10	Building Your File Plan	73
4.10.1	Triggers.....	75

4.10.2	Retentions	75
4.10.3	Lifecycles	75
4.10.4	Rule Sets	75
4.10.5	Editing the File Plan	75
4.10.6	Record Classes	75
4.10.7	Triggers.....	75
4.10.7.1	Editing Triggers	76
4.10.7.2	Date Property Triggers.....	76
4.10.7.3	Event Triggers.....	77
4.10.7.4	Rule Triggers.....	79
4.10.7.5	Special Triggers.....	80
4.10.8	Retentions	81
4.10.8.1	Retention Properties.....	81
4.10.8.2	Creating a Retention	82
4.10.9	Lifecycles	82
4.10.10	Rule Sets	85
4.10.10.1	Building Rules.....	85
4.10.10.2	Creating Rule Sets.....	86
4.10.10.3	Adding Rule Sets	86
4.10.11	Editing the File Plan	87
4.10.11.1	Editing the File Plan for existing records	87
4.10.11.2	Editing the File Plan for new records	88
4.10.12	Record Classes	91
4.10.12.1	Creating a Record Class	91
4.10.12.2	Case-Based Record Class.....	93
4.10.12.3	Classification	95
4.10.12.4	Lifecycles and Record Classes	97
4.10.12.5	Approvers	98
4.10.12.6	Inbox View	100
4.11	Manage	102
4.11.1	Manage Records 1	102
4.11.2	Manage Record Classes	102
4.11.3	Manage Records 1	102
4.11.3.1	Viewing Record Details	103
4.11.3.2	Manually Classifying a Record	104

4.11.3.3	Declaring & Undeclaring Different Types of Records	104
4.11.3.4	Creating a Legal Hold Manually.....	105
4.11.3.5	Viewing the Record Audit.....	105
4.11.3.6	Viewing the Record Properties	105
4.11.4	Manage Record Classes	105
4.12	Disposition.....	106
4.12.1	Disposing Physical Assets	107
4.12.1.1	Approving Physical Records	107
4.12.1.2	Confirming Physical Disposition	108
4.12.2	Expired Records	109
4.12.3	Rejected Records	110
4.12.3.1	Hold and Classify.....	111
4.12.3.2	Reinstating Records	111
4.12.4	Legal Holds and Reclassification During Disposition	112
4.12.4.1	Legal Hold.....	113
4.12.4.2	Reclassify	114
4.12.5	Exceptions	114
4.12.5.1	Retry Automation.....	114
4.12.5.2	Complete	115
4.12.6	Disposed Records.....	115
4.13	Monitor	116
4.13.1	Dashboard	116
4.13.2	Reports	116
4.13.3	Destruction Certificates	116
4.13.4	Audit.....	116
4.13.5	Event Occurrences	116
4.13.6	Pending Automation.....	116
4.13.7	Dashboard	116
4.13.8	Reports	117
4.13.9	Destruction Certificates	119
4.13.10	Audit.....	120
4.13.11	Event Occurrences	121
4.13.11.1	Manual Events vs. Recurring Events.....	122
4.13.11.2	Creating an Event Occurrence for a Manual Event.....	122
4.13.12	Pending Automation.....	123

4.14	Rule Builder	125
4.14.1	Rule Components.....	126
4.14.2	Rules for SharePoint and SharePoint Online.....	127
4.14.3	Rules for File Shares.....	127
4.14.4	SharePoint Property Value Formatting.....	128
4.14.4.1	SharePoint and SharePoint Online	128
4.14.5	Understanding the Classification Rule Operators.....	129
4.14.5.1	Like Operator.....	129
4.14.5.2	Matches Operator	129
4.14.6	Rule Tokens	129
4.14.6.1	System Tokens	130
4.14.6.2	Altitude Tokens	130
4.14.6.3	Documentum Tokens	131
4.14.6.4	Exchange Tokens	131
4.14.6.5	File Share Tokens.....	132
4.14.6.6	Physical Records Management Tokens	132
4.14.6.7	SharePoint and SharePoint Online Tokens.....	133
4.15	Physical Records	134
4.15.1	Locations	134
4.15.2	Containers	134
4.15.3	Assets.....	134
4.15.4	Barcode Schemes.....	134
4.15.5	Request and Returns.....	134
4.15.6	Custom Metadata and Templates.....	134
4.15.7	Locations	134
4.15.7.1	Creating a New Location.....	134
4.15.7.2	Creating a Child Location	135
4.15.7.3	Editing and Deleting a Location	135
4.15.7.4	Moving a Location	135
4.15.7.5	Searching for a Location.....	136
4.15.8	Containers	137
4.15.8.1	Managing Container Permissions	137
4.15.8.2	Container Properties.....	137
4.15.8.3	Creating a Container.....	137
4.15.8.4	Searching for a Container.....	137

4.15.8.5	Making changes to containers.....	137
4.15.8.6	Record Classes and Containers	137
4.15.8.7	Legal Cases and Holds on Containers	137
4.15.8.8	Managing Container Permissions	137
4.15.8.9	Container Properties.....	140
4.15.8.10	Creating a Container	142
4.15.8.11	Searching for a Container	144
4.15.8.12	Making changes to containers.....	145
4.15.8.13	Record Classes and Containers	148
4.15.8.14	Legal Cases and Holds on Containers	150
4.15.9	Assets	153
4.15.9.1	Asset Properties	153
4.15.9.2	Associating Assets to a Record Class.....	153
4.15.9.3	Creating Physical Assets	153
4.15.9.4	Modifying Existing Assets.....	153
4.15.9.5	Copying Assets	153
4.15.9.6	Searching for Assets.....	153
4.15.9.7	Viewing Asset Properties and Record Details	153
4.15.9.8	Asset Properties	153
4.15.9.9	Associating Assets to a Record Class.....	156
4.15.9.10	Creating Physical Assets	161
4.15.9.11	Modifying Existing Assets.....	166
4.15.9.12	Copying Assets	169
4.15.9.13	Searching for Assets.....	170
4.15.9.14	Viewing Asset Properties and Record Details	171
4.15.10	Barcode Schemes.....	176
4.15.10.1	Barcode Properties	176
4.15.10.2	Barcode Uniqueness	176
4.15.10.3	Creating a New Barcode Scheme	176
4.15.10.4	Editing or Deleting Barcode Scheme	178
4.15.11	Request and Returns.....	178
4.15.11.1	Processing Request.....	178
4.15.11.2	Processing Return	179
4.15.11.3	Managing All Charge-Outs	179
4.15.11.4	Processing a Request.....	180

4.15.11.5	Processing a Request Extension.....	183
4.15.11.6	Processing a Return	186
4.15.12	Custom Metadata and Templates.....	189
4.15.12.1	Custom Metadata.....	189
4.15.12.2	Templates.....	189
4.15.12.3	Adding Custom Metadata to Containers and Assets.....	190
4.16	Creating and Managing Legal Cases and Legal Holds.....	191
4.16.1	Legal Case Properties	191
4.16.2	Creating a Legal Case.....	191
4.16.3	Managing Legal Holds.....	192
4.16.4	Viewing Legal Holds for a Legal Case	193
4.17	Filtering Records by Rules and Metadata	193
4.17.1	Intro to Record Filters	194
4.17.1.1	Record Filters in Practice.....	194
4.17.2	Creating Record Filters	198
4.17.2.1	Group Membership	199
4.17.2.2	Record Filter Rules	199
4.17.3	Adding Filters to Record Classes	200
4.18	Record Class Permissions.....	201
4.18.1	Granting Permissions.....	201
4.18.2	Revoking Permissions.....	201
4.18.2.1	Revoking from Record Class.....	201
4.18.2.2	From User Profile	202
4.18.3	Permission Inheritance.....	202
5	Getting started	203
5.1	1. Deployment	203
5.1.1	Connector Deployment	203
5.1.2	Physical Records Management Deployment.....	203
5.2	2. First time setup.....	203
5.3	3. Creating the File Plan	204
5.4	4. Add classification rules	204
5.5	5. Adding policies to Record Classes.....	204
5.6	6. Using the inbox.....	204
5.7	7. Setting up Crawl Overrides in SPOC.....	204

5.8	Terminology	204
5.8.1	Physical Records Management Terminology	208
5.9	First time setup	210
5.9.1	Admin.....	211
5.9.2	Users and Record Managers	211
5.9.3	Admin.....	211
5.9.3.1	Creating the Master Account	211
5.9.3.2	Assign System Admin Users.....	211
5.9.3.3	Global Preferences and Theme	211
5.9.3.4	Email Settings	211
5.9.3.5	Creating the Master Account	211
5.9.3.6	Assign System Admin Users.....	212
5.9.3.7	Global Preferences and Theme	213
5.9.3.8	Email Settings	214
5.9.4	Users and Record Managers	217
5.9.4.1	Requirements.....	217
5.9.4.2	Signing In.....	217
5.9.4.3	User Preferences	218
6	Administrator Guide.....	221
6.1	Plan Your Deployment	221
6.2	Deploying On-Premise	221
6.3	Records Management Core Deployment.....	221
6.4	Managing Security.....	221
6.5	Connector Deployment	221
6.6	Physical Records Management Deployment.....	221
6.7	Monitoring Services	221
6.8	Migration Utility	221
6.9	Setting Up Crawl Library Overrides.....	221
6.10	Plan Your Deployment	221
6.11	Deploying On-Premise	222
6.11.1	Plan Your Deployment	223
6.11.2	Install Records Management Core	223
6.11.3	Configure Records Management Core	223

6.11.4	Administrators first time setup	223
6.12	Records Management Core Deployment	223
6.12.1	Records Management Core Planning (On-Premises)	223
6.12.2	Records Management Core Installation (On-Premises)	223
6.12.3	Records Management Core Configuration (On-Premises)	223
6.12.4	Uninstalling the Core Platform	223
6.12.5	Records Management Core Planning (On-Premises)	223
6.12.5.1	Topology and Architecture	224
6.12.5.2	System Requirements and Considerations	224
6.12.5.3	Scalability	224
6.12.5.4	Disaster Recovery	224
6.12.5.5	High Availability	224
6.12.5.6	Load Balancing	224
6.12.5.7	Authentication	224
6.12.5.8	Topology and Architecture	224
6.12.5.9	System Requirements and Considerations	226
6.12.5.10	Scalability	229
6.12.5.11	Disaster Recovery	230
6.12.5.12	High Availability	233
6.12.5.13	Load Balancing	235
6.12.5.14	Authentication	236
6.12.6	Records Management Core Installation (On-Premises)	237
6.12.6.1	Setup Screen	237
6.12.6.2	Manager Web Pre-Installation	238
6.12.6.3	Installing Manager Web	239
6.12.6.4	Installing Lifecycle Services	241
6.12.6.5	Installing the Migration Utility	242
6.12.7	Records Management Core Configuration (On-Premises)	243
6.12.7.1	Ensuring Successful Authentication with NTLM	243
6.12.7.2	Configuring Fully Qualified Domain Name (FQDN)	243
6.12.7.3	Supporting FQDN from Browser on Localhost	243
6.12.7.4	IIS Configuration	243
6.12.7.5	Ensuring Successful Authentication with NTLM	243
6.12.7.6	Configuring Fully Qualified Domain Name (FQDN)	243
6.12.7.7	Supporting FQDN from Browser on Localhost	244

6.12.7.8	IIS Configuration	244
6.12.8	Uninstalling the Core Platform.....	247
6.13	Managing Security.....	248
6.13.1	Account Types	248
6.13.2	Security Roles.....	248
6.13.3	Security Role Privilege Overview.....	248
6.13.4	Permission Overview	248
6.13.5	File Plan Editor Permissions.....	248
6.13.6	Creating a Service Account.....	248
6.13.7	Granting and Revoking User Access.....	248
6.13.8	Creating Local Groups	248
6.13.9	Changing the Master Account Password	248
6.13.10	Account Types	248
6.13.10.1	Master Account.....	249
6.13.10.2	User Account	249
6.13.10.3	Service Account.....	249
6.13.11	Security Roles.....	249
6.13.11.1	System Admin	249
6.13.11.2	Global Record Manager	250
6.13.11.3	Record Manager	250
6.13.11.4	Users	250
6.13.11.5	Physical Administrator.....	250
6.13.11.6	Physical User	251
6.13.12	Security Role Privilege Overview.....	251
6.13.13	Permission Overview	253
6.13.13.1	Record Classes	253
6.13.13.2	Physical Records	254
6.13.14	File Plan Editor Permissions.....	255
6.13.14.1	Accessing and Using the File Plan Editors Feature.....	255
6.13.14.2	Limitations	258
6.13.15	Creating a Service Account.....	258
6.13.16	Granting and Revoking User Access.....	260
6.13.16.1	Granting Access.....	260
6.13.16.2	Revoking User Access.....	261
6.13.17	Creating Local Groups	262

6.13.17.1	User Profile Properties.....	262
6.13.17.2	Local Groups.....	262
6.13.18	Changing the Master Account Password	263
6.14	Connector Deployment	264
6.14.1	Box Connector.....	264
6.14.2	Documentum Connector	264
6.14.3	FileNet Connector	264
6.14.4	(5.2.4) Microsoft 365 SharePoint Connector https://gimmel.atlassian.net/wiki/spaces/GR/pages/178159684/%285.2.4%29++Microsoft+365+SharePoint+Connector	0
6.14.5	SharePoint Online Connector	264
6.14.6	SharePoint Server Connector.....	264
6.14.7	Universal File Share Connector.....	264
6.14.8	Box Connector.....	264
6.14.8.1	Box Connector Planning and Requirements	265
6.14.8.2	Box Connector On-Premise Installation	265
6.14.8.3	Box Connector Configuration.....	265
6.14.8.4	Removing the On-Premise Box Connector	265
6.14.8.5	Configuring Box.....	265
6.14.8.6	Box Connector Jobs.....	265
6.14.8.7	Box Connector Planning and Requirements	265
6.14.8.8	Box Connector On-Premise Installation	266
6.14.8.9	Box Connector Configuration.....	267
6.14.8.10	Removing the On-Premise Box Connector	269
6.14.8.11	Configuring Box.....	269
6.14.8.12	Box Connector Jobs.....	276
6.14.9	Documentum Connector	278
6.14.9.1	Documentum Connector Architecture.....	278
6.14.9.2	Documentum Connector Upgrade from 5.0 to 5.1	279
6.14.9.3	Documentum Connector System Requirements	288
6.14.9.4	Documentum Connector Installation	289
6.14.9.5	Applying Documentum Foundation Class Properties.....	294
6.14.9.6	Enable Documentum Audit Events	295
6.14.9.7	Documentum Connector Configuration	298
6.14.9.8	Uninstall Documentum Connector	304
6.14.9.9	Documentum Connector Upgrade 5.1 to 5.1.1	305

6.14.9.10	Documentum Services Installation	323
6.14.10	FileNet Connector	325
6.14.10.1	FileNet Connector System Requirements.....	325
6.14.10.2	FileNet Connector Installation	325
6.14.10.3	FileNet Services Installation	325
6.14.10.4	Applying FileNet Property Settings	325
6.14.10.5	FileNet Connector Configuration	325
6.14.10.6	Uninstall FileNet Connector	325
6.14.10.7	FileNet Connector System Requirements.....	325
6.14.10.8	FileNet Connector Installation	326
6.14.10.9	FileNet Services Installation	332
6.14.10.10	Applying FileNet Property Settings	334
6.14.10.11	FileNet Connector Configuration	334
6.14.10.12	Uninstall FileNet Connector	338
6.14.11	SharePoint Online Connector	339
6.14.11.1	SharePoint Online Requirements	339
6.14.11.2	Prepare to use the SharePoint Online Connector	341
6.14.11.3	SharePoint Online Connector On-Premise Only	344
6.14.11.4	Uploading SharePoint Online Connector App Package.....	355
6.14.11.5	SharePoint Online Connector Configuration.....	356
6.14.11.6	Renewing a Client Secret.....	362
6.14.11.7	Unregistering a SharePoint App from an Individual Web	363
6.14.12	SharePoint Server Connector.....	364
6.14.12.1	Architecture.....	365
6.14.12.2	Scalability.....	365
6.14.12.3	Additional Topics	366
6.14.12.4	SharePoint Server Connector Installation	366
6.14.12.5	Configure SharePoint Server	368
6.14.12.6	SharePoint Server Connector Configuration.....	371
6.14.12.7	SharePoint Server Connector Requirements	382
6.14.13	Universal File Share Connector	382
6.14.13.1	Universal File Share Connector Architecture	383
6.14.13.2	Scalability	383
6.14.13.3	Universal File Share System Requirements.....	384
6.14.13.4	Universal File Share Connector Installation	385

6.14.13.5	Universal File Share Connector Configuration	388
6.14.13.6	Uninstall Universal File Share Connector	391
6.15	Physical Records Management Deployment	392
6.15.1	Physical Records Management Server Deployment	392
6.15.2	Physical Records Management Configuration	392
6.15.3	Physical Records Management Server Deployment	392
6.15.3.1	Physical Records Management Requirements	392
6.15.3.2	Physical Records Management Installation	392
6.15.3.3	Starting Gimmel Records Management Service	392
6.15.3.4	Physical Records Management Plugin Configuration	392
6.15.3.5	Uninstall Physical Records Management	392
6.15.3.6	Physical Records Management Requirements	392
6.15.3.7	Physical Records Management Installation	392
6.15.3.8	Starting Gimmel Records Management Service	399
6.15.3.9	Physical Records Management Plugin Configuration	399
6.15.3.10	Uninstall Physical Records Management	403
6.15.4	Physical Records Management Configuration	404
6.16	Monitoring Services	405
6.16.1	Heartbeat Icon Legend	406
6.16.2	Lifecycle Processing Service	406
6.16.3	Deleting services no longer in use	407
6.17	Migration Utility	407
6.17.1	Running the Migration Utility	408
6.17.1.1	Open the Migration Utility	408
6.17.1.2	Welcome Screen	408
6.17.2	Import	409
6.17.2.1	Import Configuration	409
6.17.2.2	Destination Connection	409
6.17.2.3	Executing Import	410
6.17.2.4	Import Mapping File	411
6.17.2.5	Object Schema for Import Mapping	415
6.17.3	Migrate	417
6.17.3.1	Source Connection	417
6.17.3.2	Destination Connection	418
6.17.3.3	Record Class Selection	419

6.17.3.4	Legal Case Selection	420
6.17.3.5	Ready to Migrate	421
6.17.3.6	Executing Migration	422
6.17.3.7	Migration Complete	423
6.18	Setting Up Crawl Library Overrides.....	424
6.18.1	Background	424
6.18.2	Creating a New Library Override	424
6.18.2.1	Managing Existing Library Overrides	428
6.18.2.2	Editing Existing Library Overrides	429
6.18.2.3	Deleting Existing Library Overrides.....	430
7	Developer Guide.....	432
7.1	SDK.....	432
7.2	PowerShell CmdLets.....	432
7.3	Reporting Tool.....	432
7.4	PowerShell CmdLets.....	432
7.4.1	File Share Connector Web Cmdlets.....	432
7.4.2	File Share Connector Service Cmdlets	432
7.4.3	Lifecycle Services Cmdlets	432
7.4.4	SharePoint Connector Cmdlets.....	432
7.4.5	SharePoint Online Connector Web Cmdlets.....	432
7.4.6	SharePoint Online Connector Service Cmdlets.....	432
7.4.7	Manager Web Cmdlets	432
7.4.8	File Share Connector Web Cmdlets.....	432
7.4.8.1	Cmdlets.....	433
7.4.9	File Share Connector Service Cmdlets.....	433
7.4.9.1	Cmdlets.....	434
7.4.10	Lifecycle Services Cmdlets	435
7.4.10.1	Cmdlets.....	436
7.4.11	SharePoint Connector Cmdlets.....	436
7.4.11.1	Cmdlets.....	437
7.4.12	SharePoint Online Connector Web Cmdlets.....	438
7.4.12.1	Set-SPOConnectorWeb.....	438
7.4.13	SharePoint Online Connector Service Cmdlets.....	438
7.4.13.1	Cmdlets.....	439

7.4.14	Manager Web Cmdlets	440
7.4.14.1	Cmdlets.....	441
7.5	Reporting Tool.....	442
7.5.1	Overview	442
7.5.2	Reporting Licensing	443
7.5.3	Report Life Cycle	443
7.5.4	Report Deployment.....	443
7.5.5	Database Schema for Reporting	444
7.5.6	Creating Custom Reports	444
7.5.7	Telerik Report Designer	448
7.5.8	Creating Report Parameters.....	451
8	Release Notes.....	456
8.1	Release Date	456
8.2	Resolved Bugs and Issues.....	456
8.3	Known Issues.....	456
8.4	End-of-Life Update.....	457
8.5	Upgrading.....	457
8.5.1	Core Service.....	457
9	Certified Records Management.....	458
9.1	Compliance Suite	458
9.2	Classified Records	458
9.3	Enterprise Events	459

[Download Gimmel Records 5.2.2 Server Documentation \(One PDF\)](#)¹

Create policies for the retention and disposition of content in multiple sources.

¹https://gimmel.atlassian.net/wiki/download/attachments/178159620/Gimmel%20Records-v1-20221106_014931.pdf?api=v2&cacheVersion=1&modificationDate=1684799064108&version=1






1 Featured Pages

Content by label

There is no content with the specified labels



2 Recently Updated

-  [Getting started](#)(see page 203)
2 minutes ago • contributed by Jake Adams²
-  [Record Locking with Microsoft 365 Retention Labels](#)³
Jul 11, 2023 • contributed by Jake Adams⁴
-  [Quick Start Guide](#)⁵
Jul 11, 2023 • contributed by Jake Adams⁶
-  [Create Microsoft Graph API Connection Settings](#)⁷
Jun 26, 2023 • contributed by Jake Adams⁸
-  [\(4.7\) Manager Web Cmdlets](#)⁹
Jun 13, 2023 • contributed by Jake Adams¹⁰

2 <https://gimmel.atlassian.net/wiki/display/~63593084c97f5473af70413f>

3 <https://gimmel.atlassian.net/wiki/spaces/GR/pages/18776274/Record+Locking+with+Microsoft+365+Retention+Labels>

4 <https://gimmel.atlassian.net/wiki/display/~63593084c97f5473af70413f>

5 <https://gimmel.atlassian.net/wiki/spaces/GR/pages/18776212/Quick+Start+Guide>

6 <https://gimmel.atlassian.net/wiki/display/~63593084c97f5473af70413f>

7 <https://gimmel.atlassian.net/wiki/spaces/GR/pages/18776194/Create+Microsoft+Graph+API+Connection+Settings>

8 <https://gimmel.atlassian.net/wiki/display/~63593084c97f5473af70413f>

9 <https://gimmel.atlassian.net/wiki/spaces/GR/pages/18776945/%284.7%29+Manager+Web+Cmdlets>

10 <https://gimmel.atlassian.net/wiki/display/~63593084c97f5473af70413f>

3 User Guide

The topics under this guide are for users primarily using Gimmel Records Management to approve items for disposition.

3.1 Signing In and Out

3.2 Inbox

3.3 Physical Assets

3.4 Signing In and Out

3.4.1 Sign In

To access Records Management, use a web browser to navigate to ([https://\[yourURL\]](https://[yourURL])). You must use the fully qualified domain name (FQDN) of your server (e.g., <https://demo.recordsmanagement.com:8080>.) Because Records Management is a secure system, the first thing you must do is sign in using your credentials. Your administrator will provide you with the necessary credentials, however, since the system uses Single Sign-On technology, they should be the same as the credentials used to access your other corporate systems.



3.4.2 Sign Out

To sign out of the system, click on your user name in the upper right of the page, and then select Sign Out.



3.5 Inbox

3.5.1 Overview

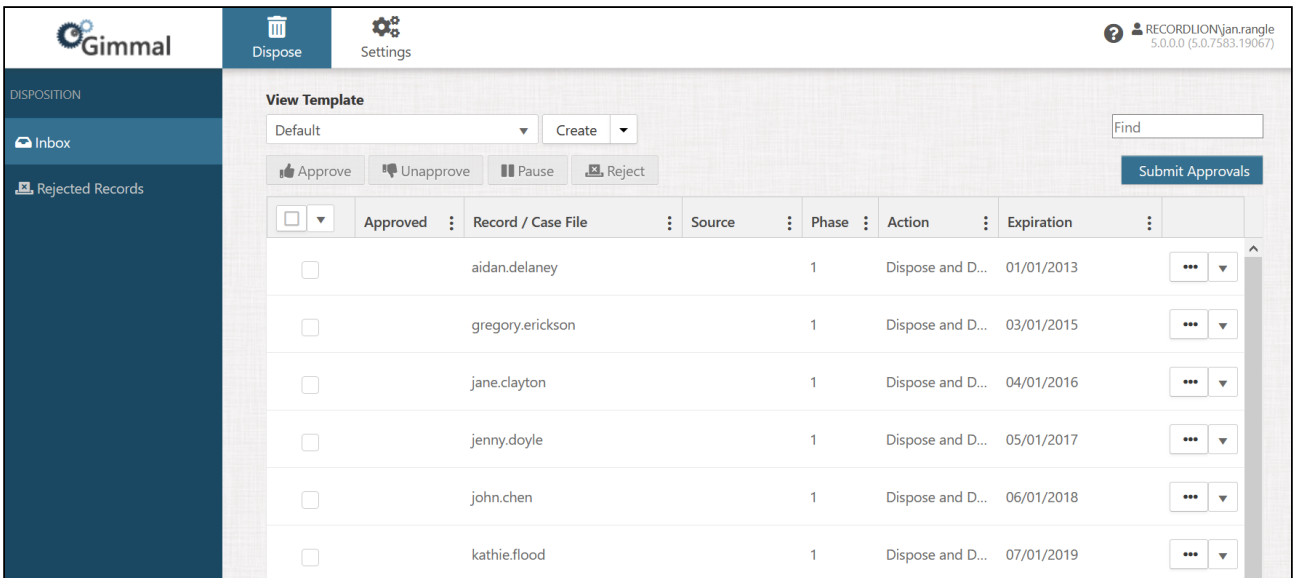
You have created Lifecycles, associated them with Record Classes, and created Event Occurrences. Now, you are ready to approve items that are waiting at the end of the retention period of a specific Lifecycle Phase, typically known as disposition. The Inbox is where you approve and submit items to either move to the next phase or go through final disposition.

3.5.2 Accessing the Inbox

Items in the Inbox are available if there are records specifically for you to approve:

- You have been added to one of the [Approval Groups](#)(see page 98) for the Record Class of a record.
- There are no Approval Groups for the Record Class of the records, and you are either a Global Records Manager or you are a Record Manager and you are not prevented from seeing the record due to a filter.

To access this section of the application, goto **Dispose** → **Inbox**.



3.5.3 Adding and Removing Columns

The visible columns can be changed by selecting the ellipsis to the right of any column in the header of the Inbox list.

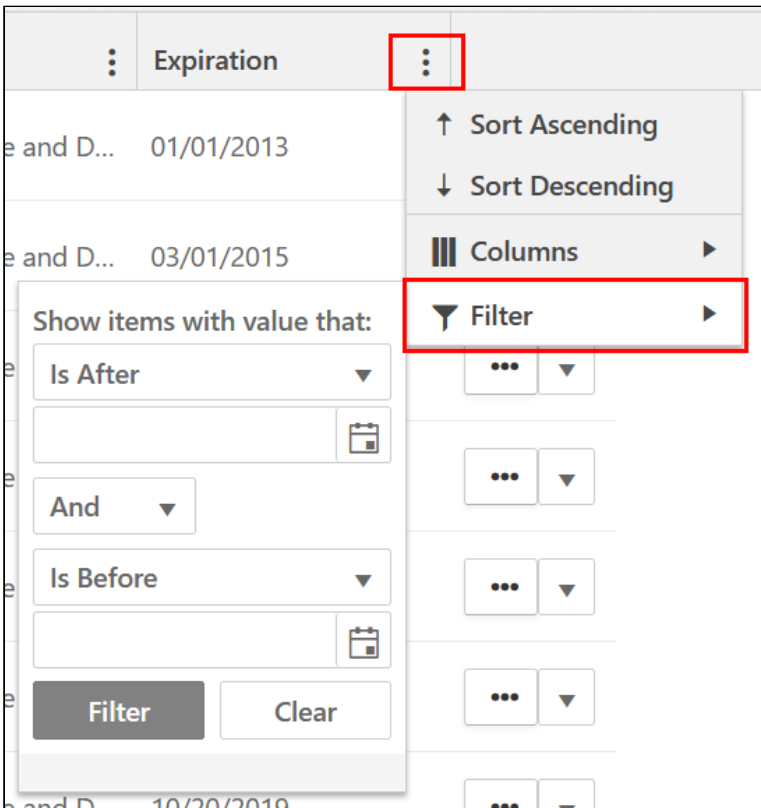
Turn the checkboxes on and off to make a column visible or to hide it.

Record Class	Record / Case File	Source
Personnel Files HR01	↑ Sort Ascending ↓ Sort Descending	
Personnel Files HR01	Columns	<input checked="" type="checkbox"/> Approved <input checked="" type="checkbox"/> Record Class <input checked="" type="checkbox"/> Record / Case File <input checked="" type="checkbox"/> Source <input type="checkbox"/> Phase <input checked="" type="checkbox"/> Action <input checked="" type="checkbox"/> Expiration
Personnel Files HR01	Filter jane.clayton	
Personnel Files HR01	jenny.doyle	
Personnel Files HR01	john.chen	

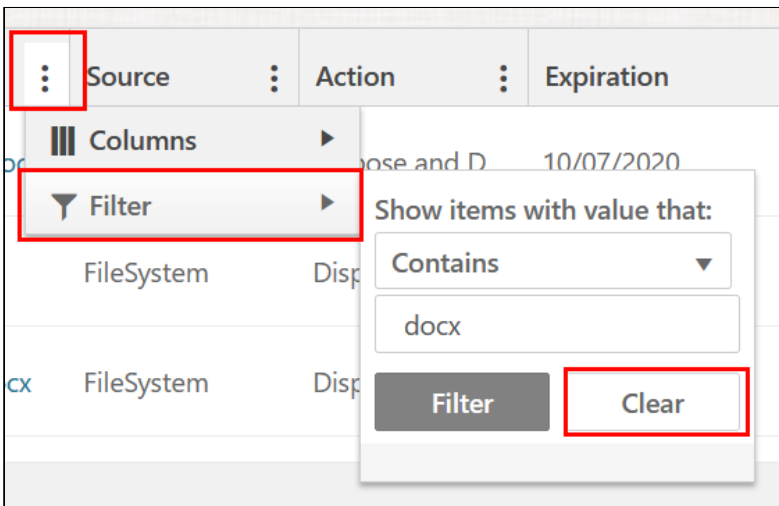
For information on how to make a new column available, view the [\(5.2.3\) Adding Columns to Your Inbox Views](#)(see [page 35](#)) topic.

3.5.4 Filtering the Inbox

The Inbox can be filtered by any of the visible columns in the header of the list. To set a filter select the ellipsis to the right of any column. The filter options will be different depending on the data type of the specific column. Enter the necessary values and select the **Filter** button to save it.



Filters can be added to more than one column at a time, and in order to clear filters, you will need to remove them from each individual column.

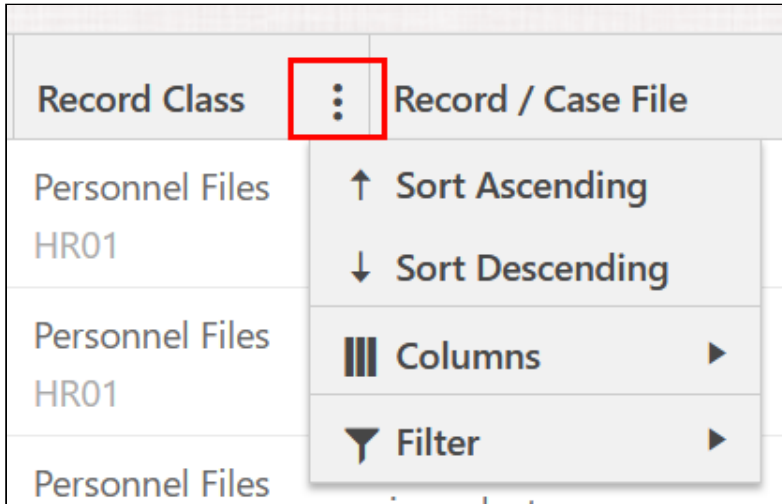


3.5.5 Sorting the Inbox

The Inbox can only be sorted on specific columns and it cannot be sorted on properties you add to the Inbox. To sort the Inbox select the ellipsis to the right of one of the following column headers:

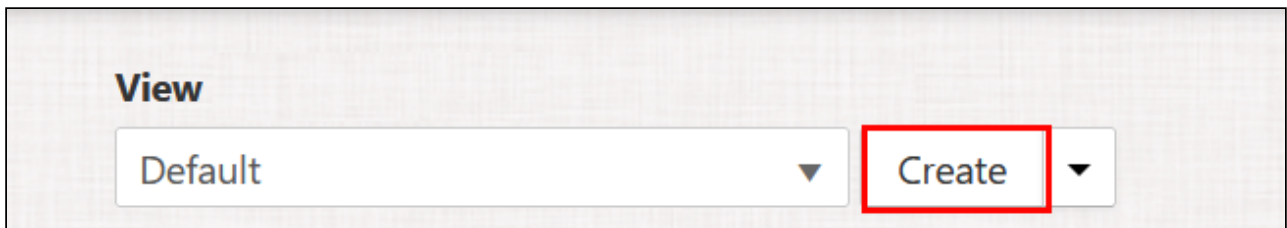
- Record Class
- Expiration Date

Select whether you want to sort in ascending or descending order for that column.



3.5.6 Saving and Using Views

There are two types of possible views on the Inbox. Record Class views and personal views. Setting up Record Class views are covered in the [\(5.2.3\) Inbox View](#) (see page 100) topic. Personal views are created by clicking the Create button next to the Inbox views list.



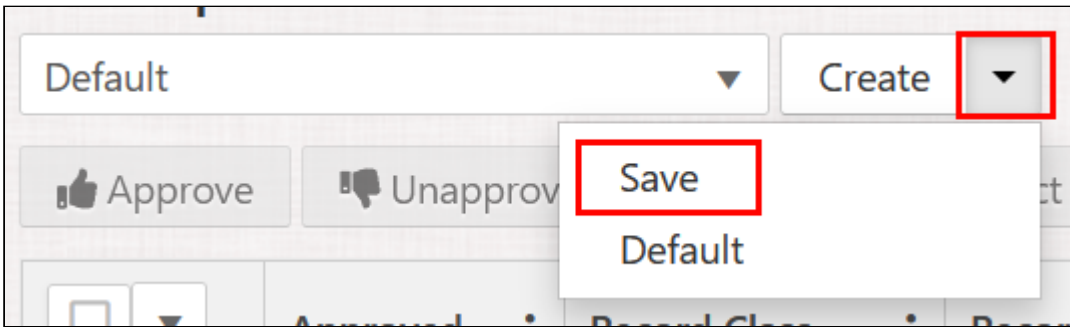
All your settings related to the current layout of the Inbox are saved including visible columns, column order, column width, filters, and any sorting.

3.5.6.1 Using a View

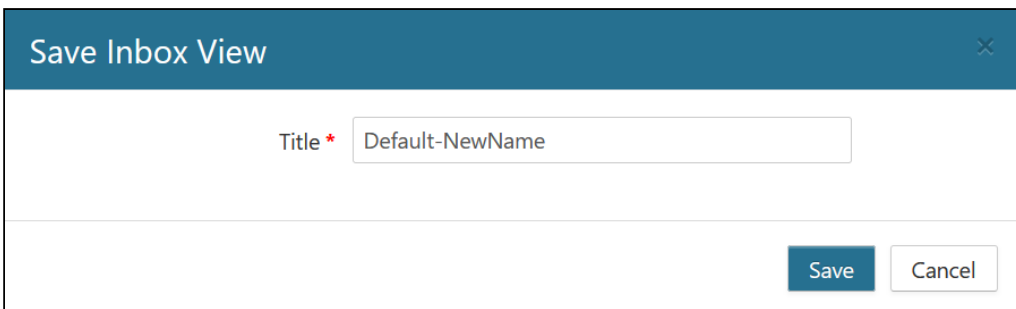
To use a saved view, simply select it from the list of views.

3.5.6.2 Saving existing View

Existing views, including the Default view, can be overwritten by selecting the Save menu item on the dropdown next to Create.

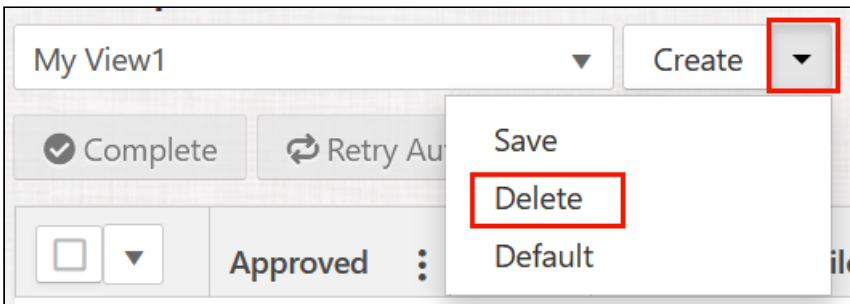


After selecting Save a window will be displayed allowing you to change the name of the view before saving it.



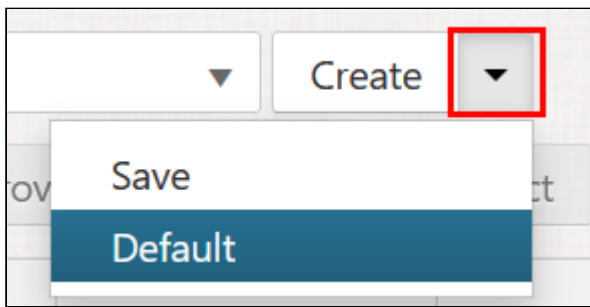
3.5.6.3 Deleting a View

Only personal views can be deleted. To delete a view, ensure a personal view is currently selected, click the dropdown menu on the right of the Create button, and select Delete.

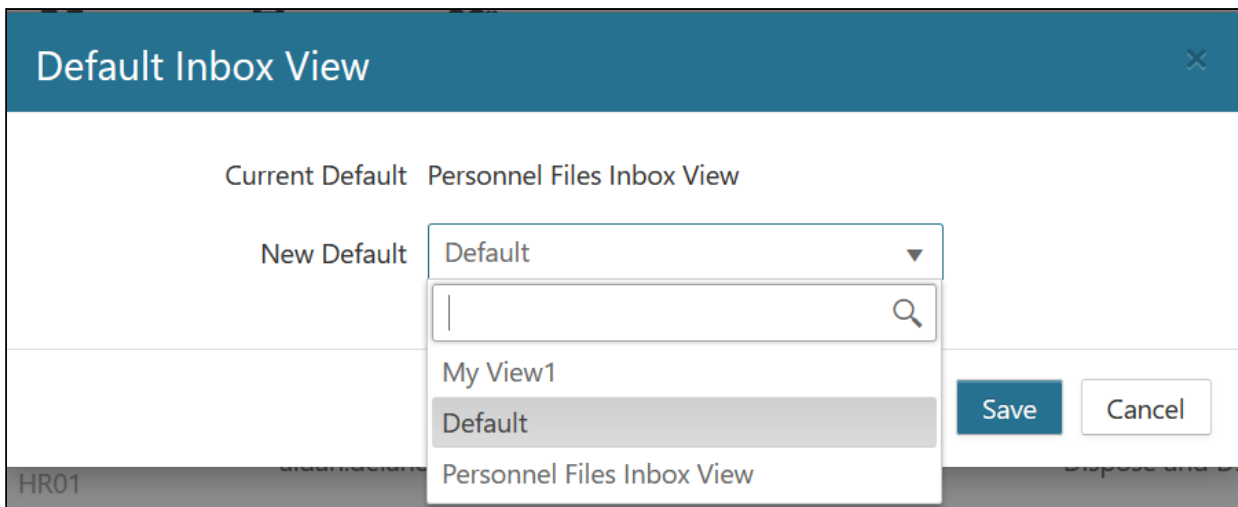


3.5.6.4 Changing the Default View

The first time you use the Inbox, a view called Default will be the only view (not including the Inbox Views setup for Record Classes) available. If more than one view exists you can change the view that is displayed when you open the Inbox. To do this select the dropdown next to Create, and then select Default.



Select the view you would like to use as default and then click Save.



3.5.7 Disposition Actions

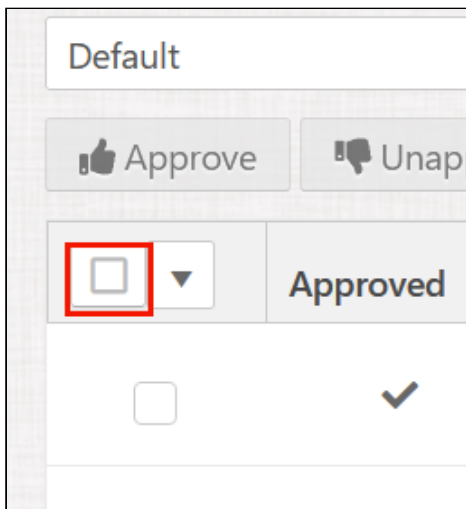
There are several actions that can be taken on records in the Inbox. These actions can be executed on one record at a time, or on any number of selected records. Each action is detailed in the following topics:

- [Approving Records](#)(see page 27)
- [Unapprove](#)(see page 29)
- [Pause](#)(see page 30)
- [Reject](#)(see page 32)
- [Submitting Approvals](#)(see page 33)
- [Adding Columns to Your Inbox Views](#)(see page 35)

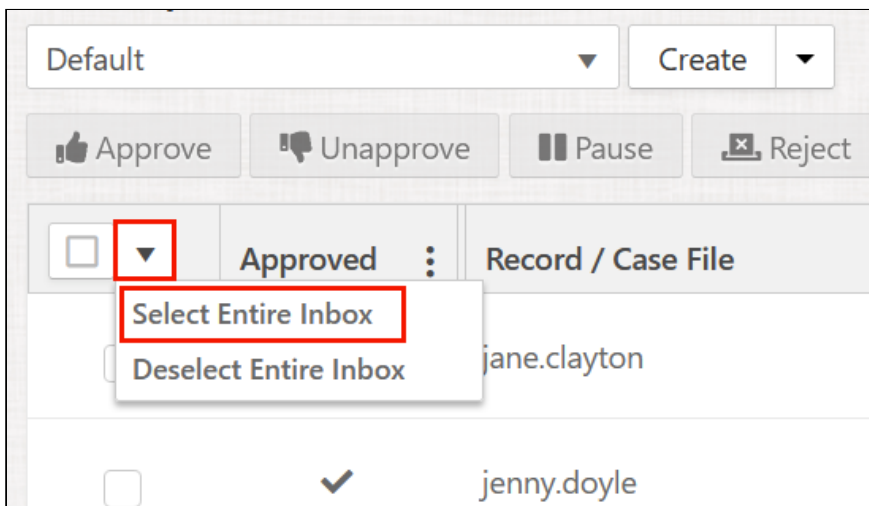
3.5.7.1 Selecting Records

To select multiple records, you can turn on the checkbox in the leftmost column, select records just on the current page, or the entire set of records on all pages.

To select records on the current page, select the checkbox on the leftmost column header.



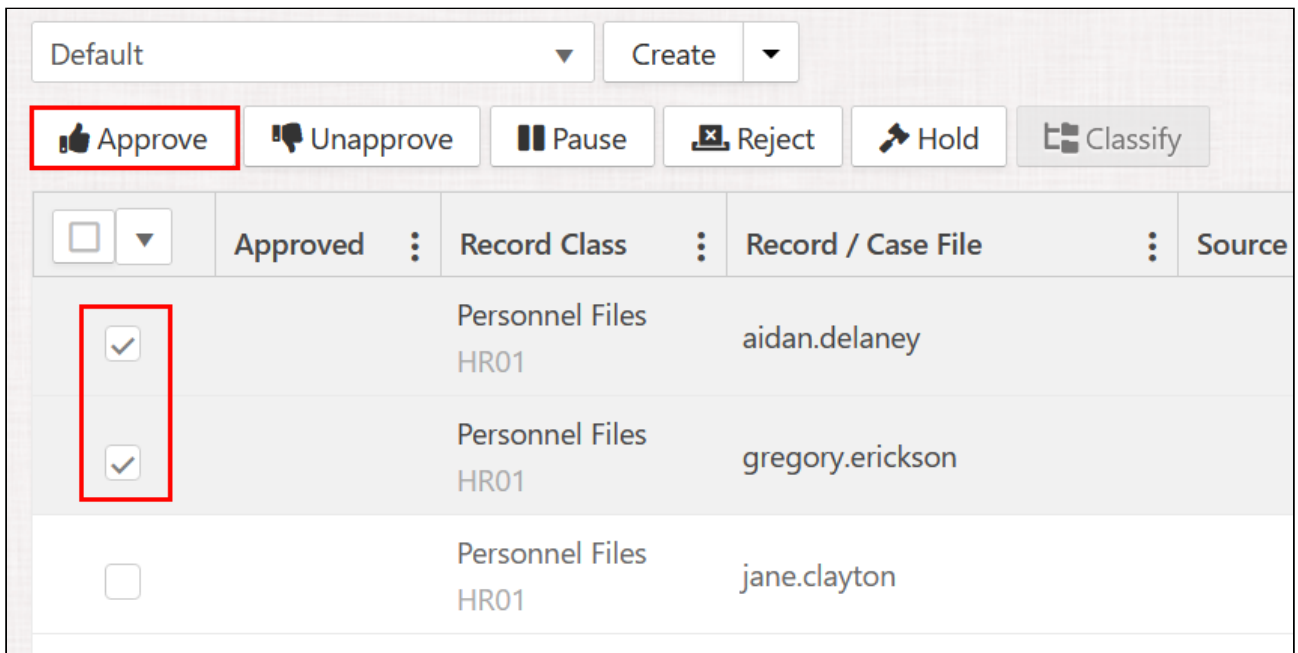
To select records on all pages, select the pulldown on the leftmost column header, and then Select Entire Inbox. You can also deselect the entire Inbox. Records on all pages except the current page will also get deselected if you deselect any one item after selecting the entire Inbox.



3.5.8 Approving Records

When records have expired and are ready to be approved, they will appear in the Inbox of the user who is set to approve those items.

To approve records, select one or more items, and then select the approve button.



The screenshot shows the Gimmel Records interface. At the top, there is a 'Default' dropdown menu and a 'Create' button. Below these are several action buttons: 'Approve' (highlighted with a red box), 'Unapprove', 'Pause', 'Reject', 'Hold', and 'Classify'. The main area is a table with columns: 'Approved', 'Record Class', 'Record / Case File', and 'Source'. The table contains three rows of data, all with 'Personnel Files' as the Record Class and 'HR01' as the Record / Case File. The first two rows have checkmarks in the 'Approved' column, which are also highlighted with a red box. The third row has an empty checkbox in the 'Approved' column.

Approved	Record Class	Record / Case File	Source
<input checked="" type="checkbox"/>	Personnel Files HR01	aidan.delaney	
<input checked="" type="checkbox"/>	Personnel Files HR01	gregory.erickson	
<input type="checkbox"/>	Personnel Files HR01	jane.clayton	

A window will be displayed asking for confirmation to approve these records.



The screenshot shows a 'Confirm Approval' dialog box. The title bar is dark blue with the text 'Confirm Approval' and a close button (X). The main content area is white and contains the text 'Confirm approval of 2 item(s)'. At the bottom right, there are two buttons: 'Confirm' (dark blue) and 'Cancel' (white).

Once the records are approved a check will show up in the Approved column for that item.

Default		Create			
Approve	Unapprove	Pause	Reject	Hold	Classify
<input type="checkbox"/>	Approved	Record Class	Record / Case File	Source	
<input type="checkbox"/>	✓	Personnel Files HR01	aidan.delaney		
<input type="checkbox"/>	✓	Personnel Files HR01	gregory.erickson		
<input type="checkbox"/>		Personnel Files HR01	jane.clayton		

3.5.9 Unapprove

If records were approved by mistake, they can be unapproved. To unapprove records, select those items, followed by the Unapprove button.

Default		Create			
Approve	Unapprove	Pause	Reject	Hold	Classify
<input type="checkbox"/>	Approved	Record Class	Record / Case File	Source	
<input checked="" type="checkbox"/>	✓	Personnel Files HR01	aidan.delaney		
<input checked="" type="checkbox"/>	✓	Personnel Files HR01	gregory.erickson		
<input type="checkbox"/>		Personnel Files HR01	jane.clayton		

You will be asked to confirm the unapproval action.

Confirm Unapprove ✕

Confirm remove approval for 2 item(s).

Confirm
Cancel

3.5.10 Pause

Often times, you may want to delay a decision on whether to approve an item and no longer want to see it in the Inbox. The **Pause** action allows records disposition to be paused for a set period of time.

The time period is determined by the Lifecycle of the record as shown below:

Edit Lifecycle ✕

Title *

Description

Notes

Phase	Retention	Action	Automation Level
1	Hired + 3 Years	None	Automatic
Require Approval <input type="checkbox"/> Employee Hired + 3 Year(s) >> Automatic None			
2	Terminated + 1 Year	Dispose and Delete	Automatic
Require Approval <input checked="" type="checkbox"/> <div style="border: 2px solid red; padding: 5px; display: inline-block;"> Pause Duration <input type="text" value="30"/> Day(s) </div>			
Employee Terminated + 1 Year(s) >> Automatic Dispose and Delete (Approval)			

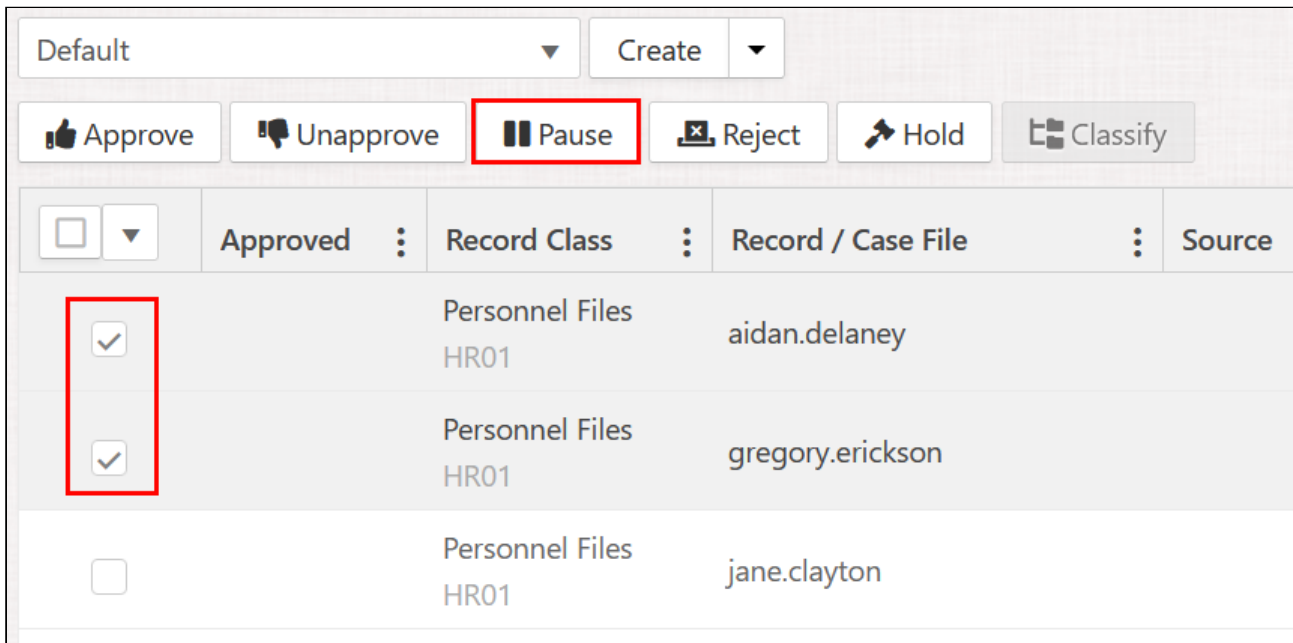
+ Add Phase
+ Add Alternate Phase

Save
Cancel

In the example above, the Pause Duration is set to 30 days, therefore removing the record from your Inbox for that period of time. You can Pause a record as many times as you like, with each duration using the same time period.

Your records manager will still be able to see Paused records when they are looking at all the records that have expired.

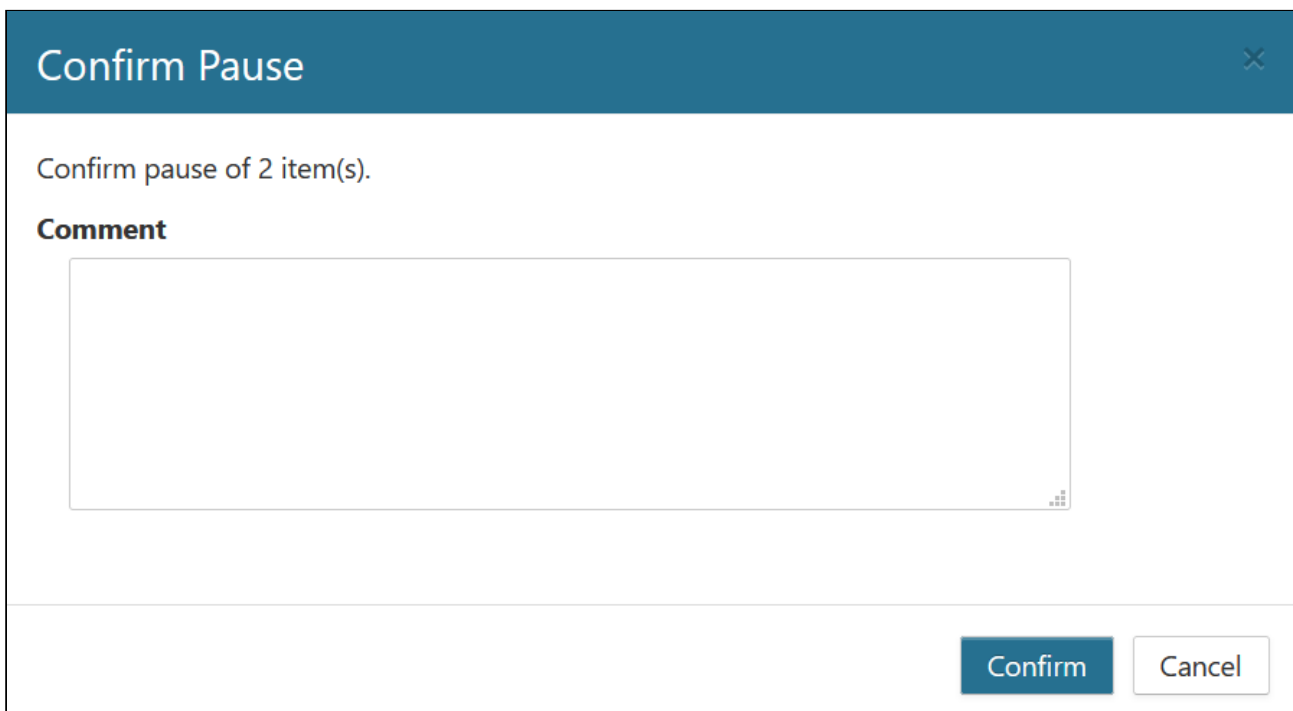
To pause a record, select one more records from the Inbox and select the Pause button.



The screenshot shows the Gimmel Records interface. At the top, there is a 'Default' dropdown menu and a 'Create' dropdown menu. Below these are several action buttons: 'Approve', 'Unapprove', 'Pause' (highlighted with a red box), 'Reject', 'Hold', and 'Classify'. The main area displays a table of records with columns for 'Approved', 'Record Class', 'Record / Case File', and 'Source'. The 'Approved' column contains checkboxes, with the first two checked (also highlighted with a red box). The records are:

Approved	Record Class	Record / Case File	Source
<input checked="" type="checkbox"/>	Personnel Files HR01	aidan.delaney	
<input checked="" type="checkbox"/>	Personnel Files HR01	gregory.erickson	
<input type="checkbox"/>	Personnel Files HR01	jane.clayton	

You will be asked to confirm the Pause and enter a reason. It is recommended to explain each time you are pausing a record so your records manager can understand why those items are not being approved.



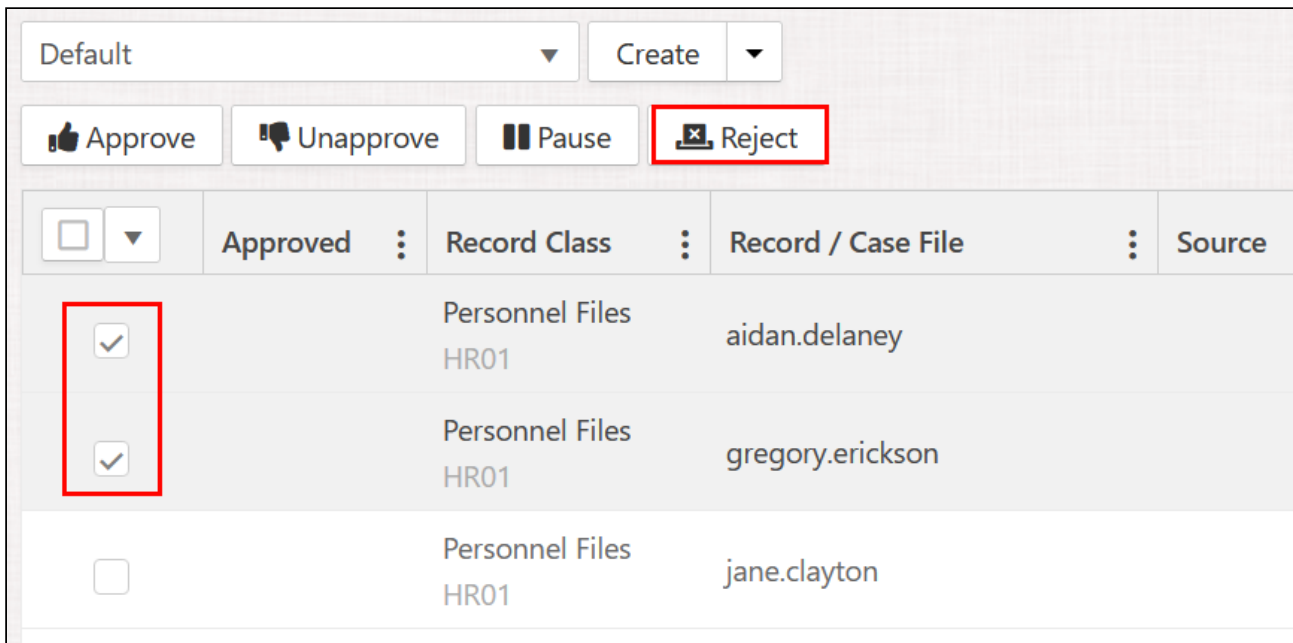
The screenshot shows a 'Confirm Pause' dialog box. The title bar is dark blue with the text 'Confirm Pause' and a close button. The main content area is white and contains the text 'Confirm pause of 2 item(s).' followed by a 'Comment' label and a large text input field. At the bottom right, there are two buttons: 'Confirm' (dark blue) and 'Cancel' (white).

3.5.11 Reject

Rejecting records should be used sparingly and only in cases where you would like the record to be moved out of the Inbox and into the Rejected Records area indefinitely. If you would only like to temporarily pause the disposition of a record, the Pause option will use the preset period of time to hide the record from your Inbox.

One advantage of using Reject is that the record will become visible to your records manager where they can make a decision to place it on legal hold, reclassify it, or perhaps reinstate it for you to approve again.

To reject a record, select one or more items and then click the Reject button.



The screenshot shows the Gimmel Records interface. At the top, there is a 'Default' dropdown menu and a 'Create' dropdown menu. Below these are four buttons: 'Approve', 'Unapprove', 'Pause', and 'Reject'. The 'Reject' button is highlighted with a red box. Below the buttons is a table with the following columns: 'Approved', 'Record Class', 'Record / Case File', and 'Source'. The table contains three rows of records, all of which are 'Personnel Files' with 'HR01' as the Record Class. The first two rows have their 'Approved' checkboxes checked, and these two rows are also highlighted with a red box. The third row has its 'Approved' checkbox unchecked.

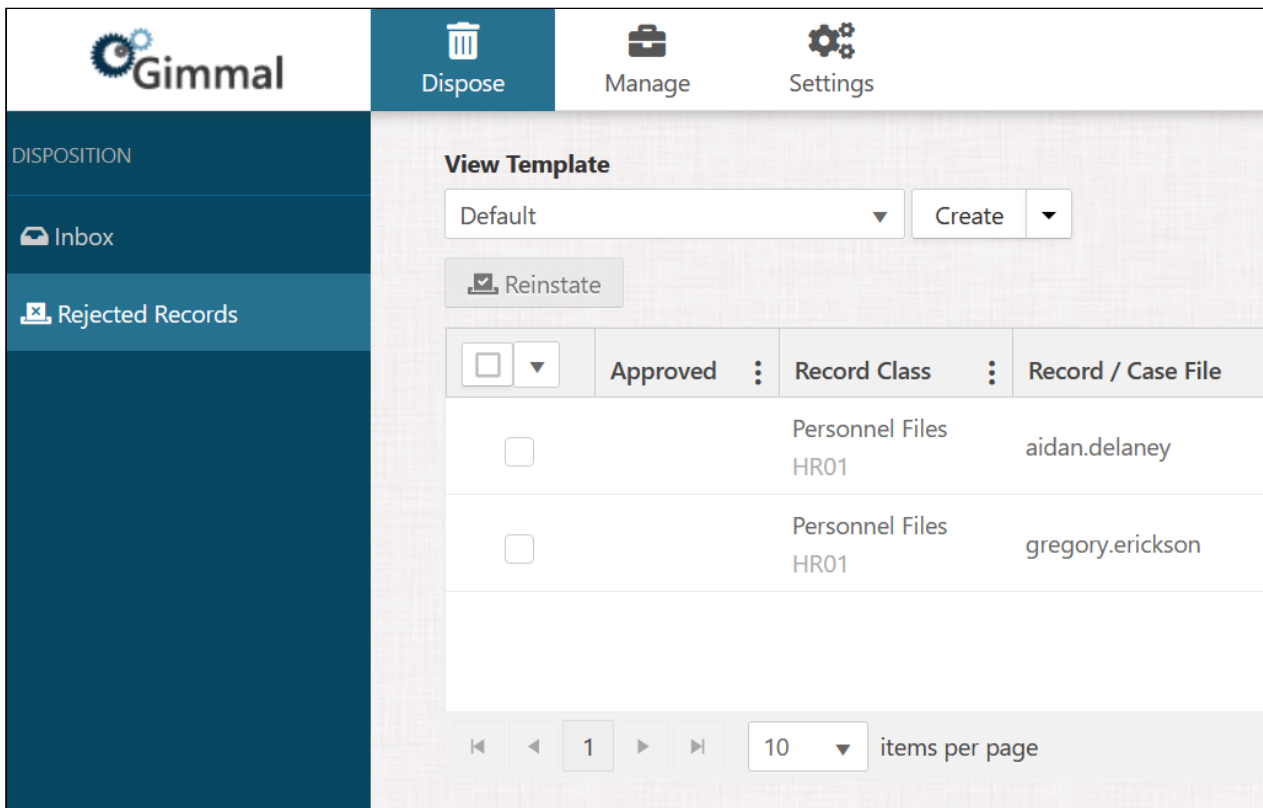
Approved	Record Class	Record / Case File	Source
<input checked="" type="checkbox"/>	Personnel Files HR01	aidan.delaney	
<input checked="" type="checkbox"/>	Personnel Files HR01	gregory.erickson	
<input type="checkbox"/>	Personnel Files HR01	jane.clayton	

You will be asked to confirm and give a reason for rejecting the record. It is recommended that you explain in the Comment section why the record was rejected in order for you records manager to understand the reasoning.



The screenshot shows a dialog box titled 'Confirm Rejection of'. The dialog box contains the text 'Confirm rejection of 2 item(s)'. Below this text is a section labeled 'Comment' with a large text input area. At the bottom right of the dialog box are two buttons: 'Confirm' and 'Cancel'.

Once a record is rejected it will be moved to the Rejected Record area where it will remain indefinitely until it is reinstated. When a user with the Record Manager role or higher views Rejected Records, they will have the option to place the record on legal hold or reclassify it.



3.5.12 Submitting Approvals

In order for the disposition process to start, approved records will need to be submitted. Approval and Submittal are typically two separate actions, the former allowing users to work on a group of records over a period of time, and the latter to submit all those records for disposition together.

The primary reason to use to group many records into one submittal is to produce a single Destruction Certificate. When the final disposition action is taking place, all the records that had that action (typically delete) taken on the same day for their particular Record Class will be grouped into a single Destruction Certificate. If you worked on approving over a period of several days, submitting each time, you will produce multiple Destruction Certificates and that may not be desirable for your records manager.

Use the Submit Approval button to submit all approved items in your Inbox.

Default		Create		Find					
Approve		Unapprove		Pause		Reject		Submit Approvals	
<input type="checkbox"/>	Approved	Record / Case File	Source	Phase	Action	Expiration			
<input type="checkbox"/>	✓	jane.clayton		1	Dispose and D...	04/01/2016			
<input type="checkbox"/>	✓	jenny.doyle		1	Dispose and D...	05/01/2017			
<input type="checkbox"/>		john.chen		1	Dispose and D...	06/01/2018			

You will be asked to confirm the submittal and enter any comments necessary.

Submit Approvals ✕

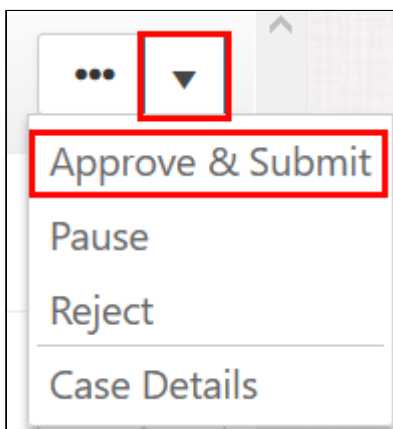
Confirm submission of approvals for the **Entire Inbox**

Comment

Confirm
Cancel

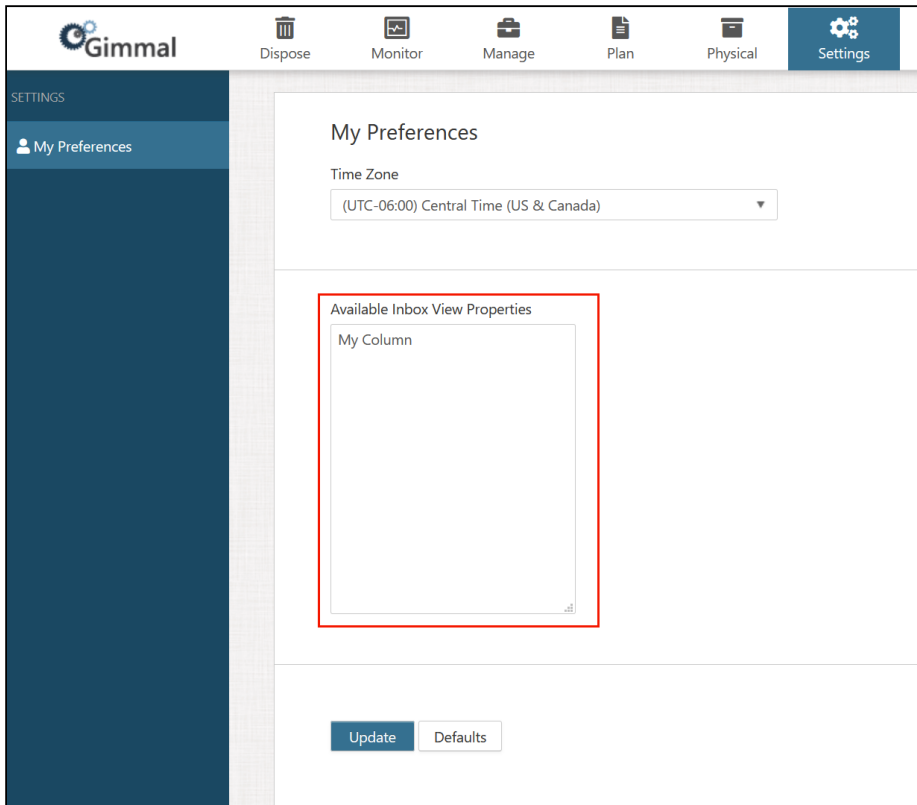
3.5.12.1 Approving and Submitting together

It is possible to approve and submit in a single step, but only on individual records. Use the dropdown menu on the right side of any record and the select Submit and Approve.



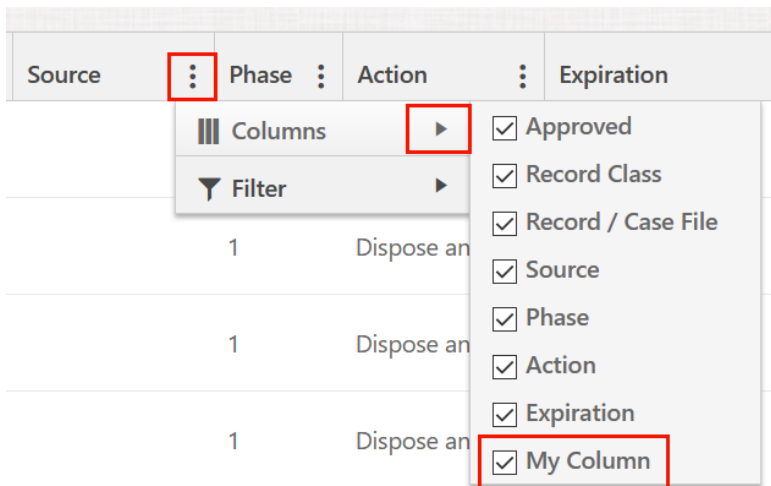
3.5.13 Adding Columns to Your Inbox Views

The Inbox, as well as the Rejected Records area (and Expired Records if you are a Record Manager), can contain different views that you can create yourself. One of the options on each view is to modify the columns that are available for viewing and filtering. The columns that are available for your user are either configured by your system administrator or added in the My Preferences settings.



In the **Available Inbox View Properties** text box, enter each column you'd like to have an option for using on a separate line, and then click the Update button.

Now each of these columns will be available to use within the different areas of Disposition.



3.6 Physical Assets

Physical Records Management allows you to request a physical asset (for example, a box, a folder, etc.) so that you can take possession of it. Then, when you are done with the asset, you can return it so that it's available for other users.

This process is done by creating a request for a physical asset, which must be approved by the Processor/Administrator before the item is shipped to you. You can compare this to requesting a book from a library. The book may be available or not. Other users may have requested it for the same or an overlapping time frame. It is up to the Administrator to honor or refuse your request. If the request is honored, the physical asset is circulated to you, the availability status is set to "Out", and the Current location is updated to show the location/address of where the item is currently residing.

When you are ready to return the physical asset to its home location, you will submit a return. Again, the Administrator will process this request, return the physical asset to its proper location, the availability status changes to "In" and the Current location will list the home location of the item.

In order for physical assets to be requested, the following settings must be configured:

- **Allow Requests** must be set to **Yes** on the Container.
- **Allow Requests** must be set to **Yes** on the parent Asset, if there is one.

3.6.1 Requesting an Asset

The following topics cover how to request an asset.

3.6.1.1 Creating a Request

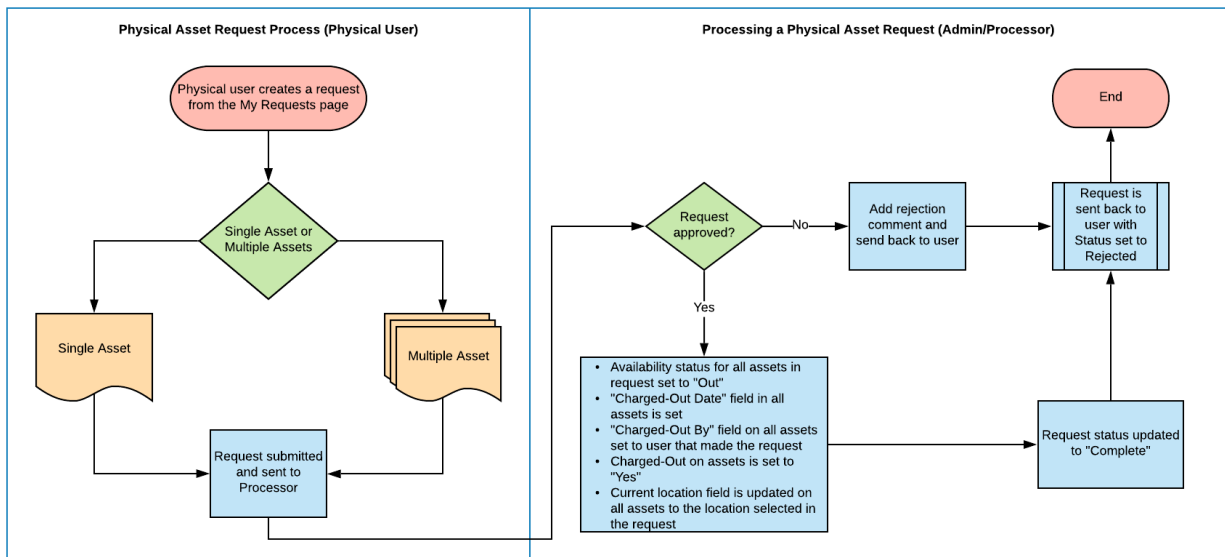
3.6.1.2 Adding and Removing Assets from a Request

3.6.1.3 Submitting a Request

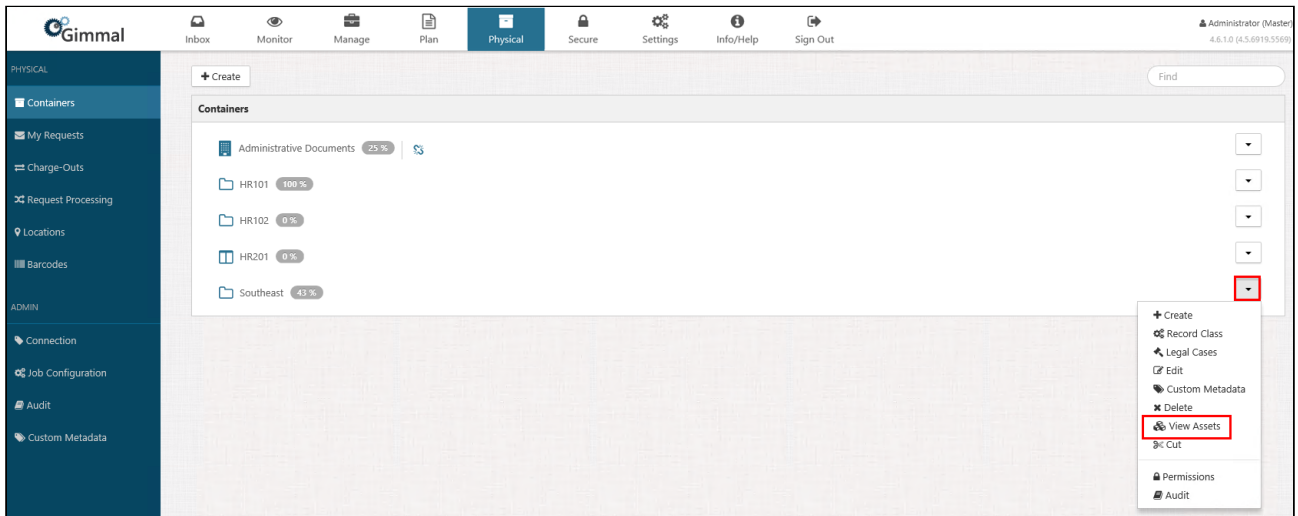
3.6.1.4 Request an Extension for a Charged Out Asset

3.6.1.5 Canceling and Deleting a Request

The following flowchart illustrates the request process.



3.6.1.6 Creating a Request



There are two methods in which you can request an asset, from the My Requests page or from the View Assets Window.

Creating a Request from the My Requests Page

1. Select **Physical** from the Main Menu, and then **My Requests** from the left navigation menu. The My Requests page displays.
2. Click **+Create Return**. The Create Return dialog opens.

Create Request ✕

Name

Reason

Request Date

Due Date

Urgent

Ship To Location

Notes

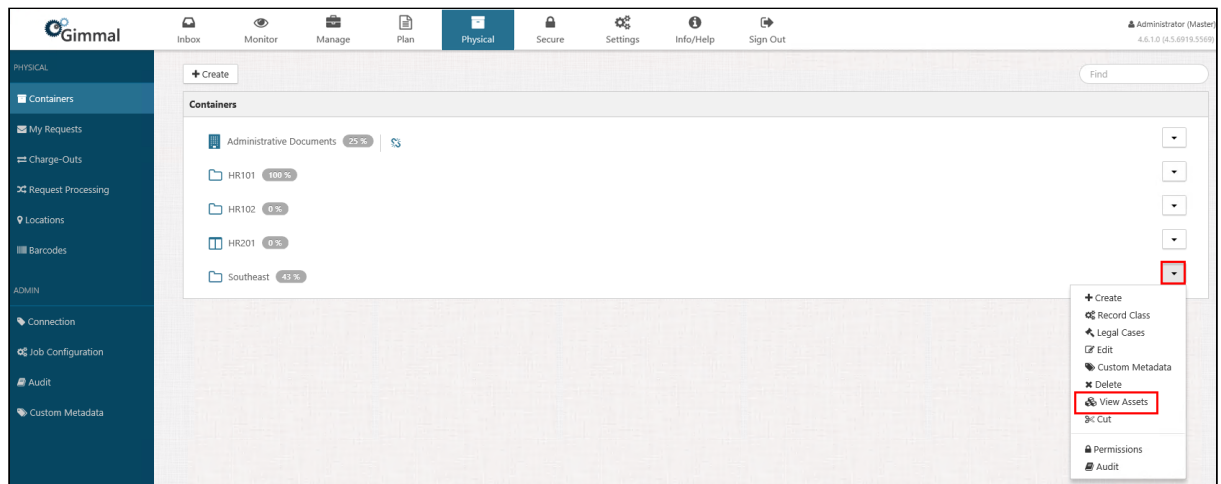
3. Enter the following information.
 - **Name** – Enter a name/title for the request. Does not have to be unique, but it is required.
 - **Reason** – Enter an optional reason for requesting the asset.
 - **Pickup Date** – Enter the pickup date for the return.
 - **Due Date** – Enter the date when you expect to return the physical asset by.
 - **Urgent** – Indicate if this request is urgent or not.
 - **Ship To Location** – Specify the pickup location by clicking the Location Picker icon and selecting from the [Locations](#)¹¹
 - **Notes** – Optionally enter any additional notes about the return.
4. Click **Create**. The new request displays on the My Requests page. Notice that "New" displays under the Status column for that return.
5. Before your return is processed, you must associate one or more assets with the return. This will ensure that the asset is circulated to you once the return is processed. See [Adding a Physical Asset to a Request](#)¹².

Creating a Return from the View Assets Dialog

1. Select **Physical** on the Main Menu, and then **Containers** on the left navigation menu. The Containers page displays.

¹¹ <http://docs.gimmel.com/en/5905-managing-locations.html>

¹² <http://docs.gimmel.com/en/6709-adding---removing-physical-asset-from-a-return.html>



2. Locate the container whose physical asset(s) you want to return, and click the drop-down arrow on the right side. The container context menu displays. (The drop-down options you see may vary, depending on your permissions.)
3. Click **View Assets**.
The Physical Assets window displays, showing a list of all the physical assets in that container.

Physical Assets

/ Southeast

+ Create + Create Request + Create Return

Name	Title	Owner	Availability Status
▶ Box of Admin Files	Box of Admin Files	Administrator	In
▶ Field Laptop	Field Laptop	Administrator	In
▶ Legal Contracts Folder	Legal Contracts Folder	Administrator	In

1 - 3 of 3 items

Close

4. Click **+Create Return**. The Create Return dialog opens.
5. Perform steps 3 through 5, listed in the section above.
6. Click **Close** to close the Physical Assets dialog.

3.6.1.7 Adding and Removing Assets from a Request

Adding a Physical Asset to a Request

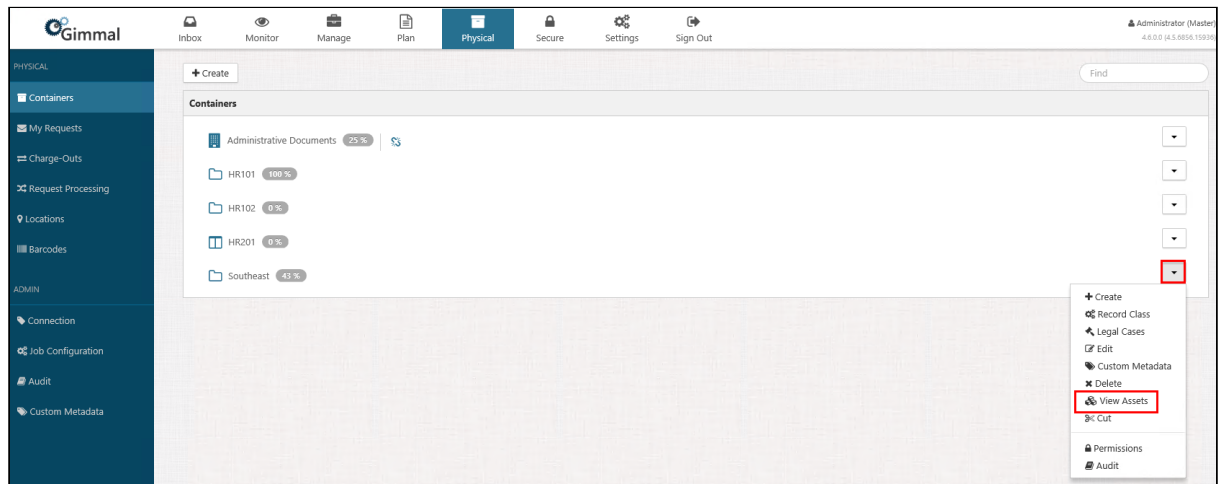
You can add one or more physical asset(s) to an existing request (one that has not yet been submitted) or you can create a new request and add it then. You must add an asset(s) to a request before you can submit it. If you do not, you an error message displays.

Child Assets

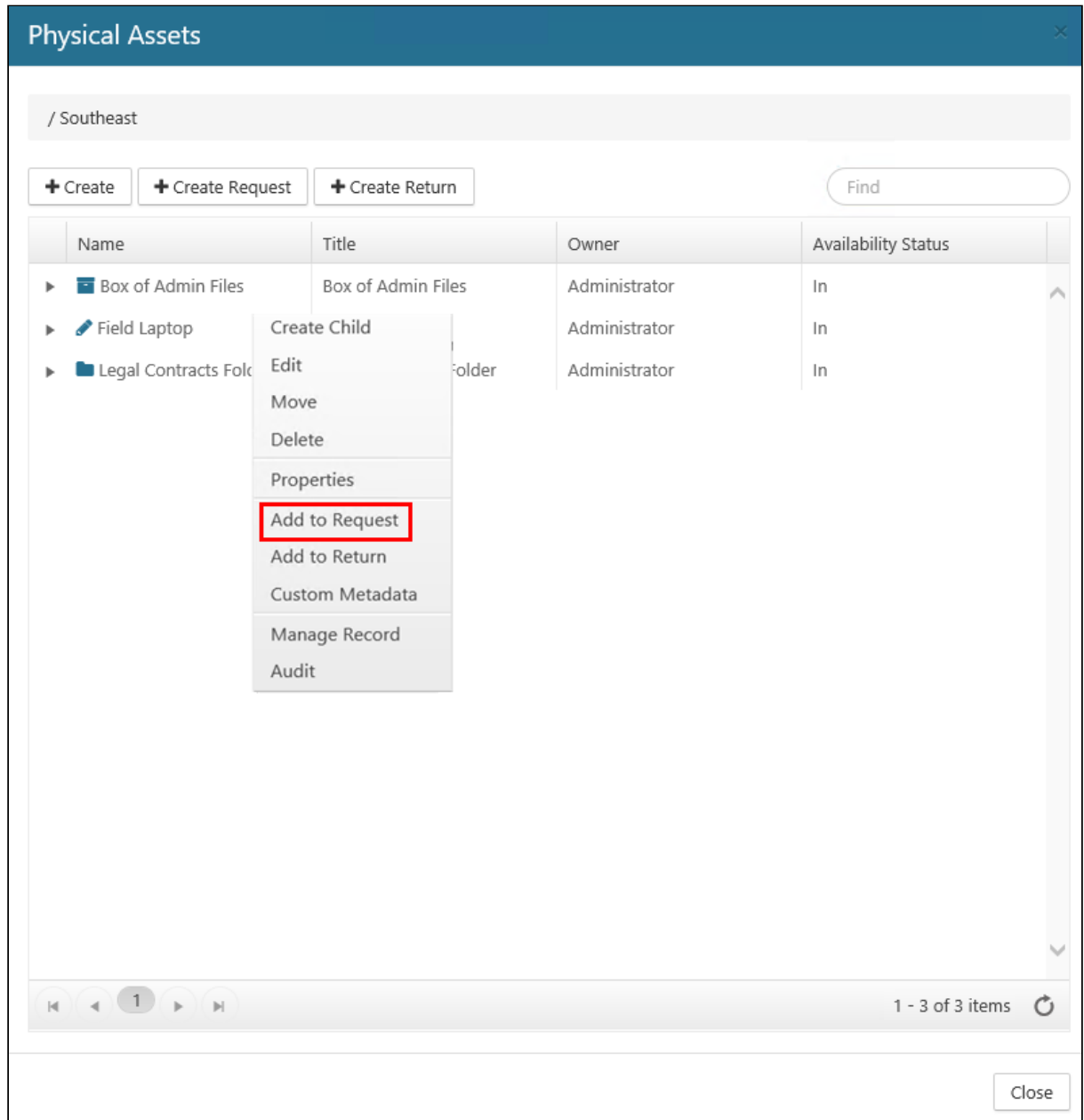
If you request a parent physical asset, all child assets will be included with the request. Conversely, you can request a child asset without requesting its parent asset.

To add a physical asset to a request, perform the following steps:

1. Click **Physical** on the Main Menu, and then click **Containers** on the left navigation menu. The Containers page displays.
2. Locate the container whose physical asset(s) you want to request, and click the drop-down arrow on the right side. The container context menu displays. (The drop-down options you see may vary, depending on your permissions.)



3. Click **View Assets**. The Physical Assets dialog displays, showing a list of all the physical assets in that container.
4. On the Physical Assets dialog, right-click the asset you want to add to your request and select **Add to Request**. (The drop-down options you see may vary, depending on your permissions.)

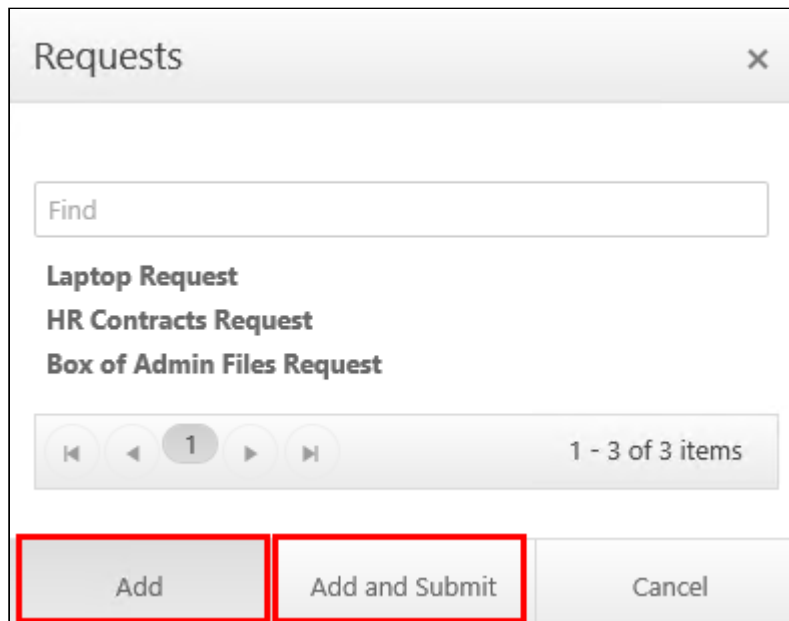


The screenshot displays the 'Physical Assets' interface. At the top, there is a header bar with the title 'Physical Assets' and a close button. Below the header, the breadcrumb path is '/ Southeast'. The main area contains three buttons: '+ Create', '+ Create Request', and '+ Create Return', along with a search box labeled 'Find'. A table lists three assets:

Name	Title	Owner	Availability Status
▶ Box of Admin Files	Box of Admin Files	Administrator	In
▶ Field Laptop		Administrator	In
▶ Legal Contracts Folder	Legal Contracts Folder	Administrator	In

A context menu is open over the 'Legal Contracts Folder' row, listing the following actions: Create Child, Edit, Move, Delete, Properties, **Add to Request** (highlighted with a red box), Add to Return, Custom Metadata, Manage Record, and Audit. At the bottom of the table, there are navigation controls (back, forward, refresh) and a status indicator '1 - 3 of 3 items'. A 'Close' button is located at the bottom right of the interface.

The Requests dialog opens, which provides a list of all of your open requests.



5. Perform either of the following steps:

- Select the request you want to add the asset to, and then click **Add**. A green confirmation message displays in the upper right corner, indicating that the request was added. (You can verify the asset was added to the request by returning to the My Requests page, clicking the drop-down next to the request name, and selecting **Edit**. On the Edit Request dialog, the added asset displays in the Assets list in the middle of the dialog. Note that the Status column still indicates that the request is "New", since it hasn't been submitted yet.)
- Select the request you want to add the asset to, and then click **Add and Submit**. Two green confirmation messages display in the upper right corner, indicating that the request was added and submitted. (You can verify the asset was added to the request by returning to the My Requests page, clicking the drop-down next to the request name, and selecting **Edit**. On the Edit Request dialog, the added asset displays in the Assets list in the middle of the dialog. Note that the Status column now indicates that the request is "Submitted", since you added the asset and submitted the request in one step.)

Removing a Physical Asset from a Request

If you no longer wish to request the asset, you can remove the asset from a request provided that the request has not been processed by the Processor/Administrator (i.e. the Status column on the My Requests page is listed as **New** or **Submitted** for the request.) If a request is in the Processing stage, you cannot delete the asset from the request.

To remove a physical asset from a request, perform the following steps:

1. Select Physical from the Main Menu, and then select My Requests from the left navigation menu. The My Requests page displays.
2. Locate the request you want to remove the asset from, click the drop-down arrow on the right side, and then click **Edit**. (The drop-down options you see may vary, depending on your permissions.) The Edit Request dialog opens.
3. Under the Assets section of the dialog, locate the asset you want to remove, right-click its name, and select **Remove**.

The screenshot shows the 'Edit Request' dialog box. The 'Assets' section contains the following table:

Name	Title	Owner	Availability Status
Field Laptop	Field Laptop	Administrator	In

A context menu is open over the 'Field Laptop' row, with the 'Remove' option highlighted in red.

A Remove confirmation dialog opens, asking you to confirm the removal of this asset.

4. Click **Confirm**. The Edit Request dialog refreshes, and the asset you removed no longer displays under the Assets list on the Edit Request dialog.

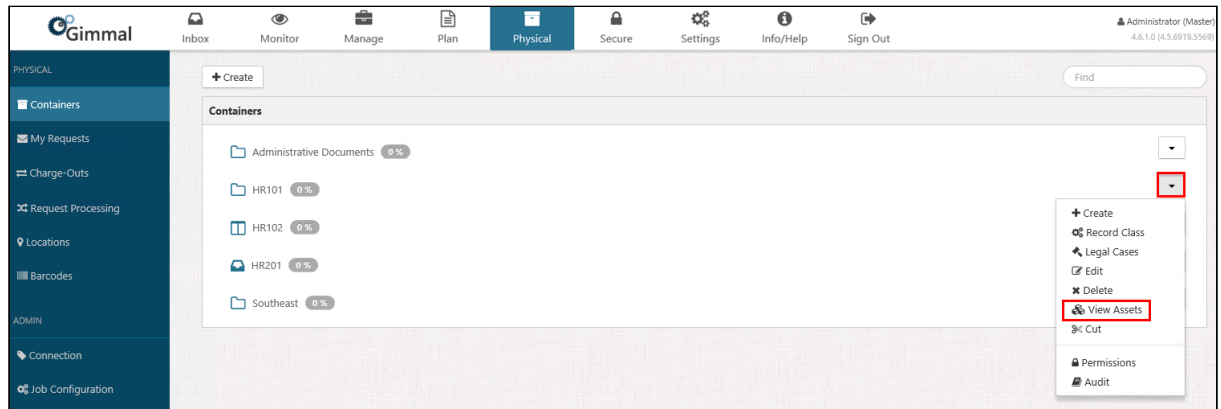
3.6.1.8 Submitting a Request

After you create a request for a physical asset, you must submit the request so that it will be processed by the Processor/Administrator. There are two ways to submit a request:

- Submitting it from an asset
- Submitting it from the My Requests page

Submitting from an Asset

1. Select **Physical** on the Main Menu, and then **Containers** on the left navigation menu. The Containers page displays.
2. Locate the container whose physical asset(s) you want to request and click the drop-down arrow on the right side. The container context menu displays. (The drop-down options you see may vary, depending on your permissions.)

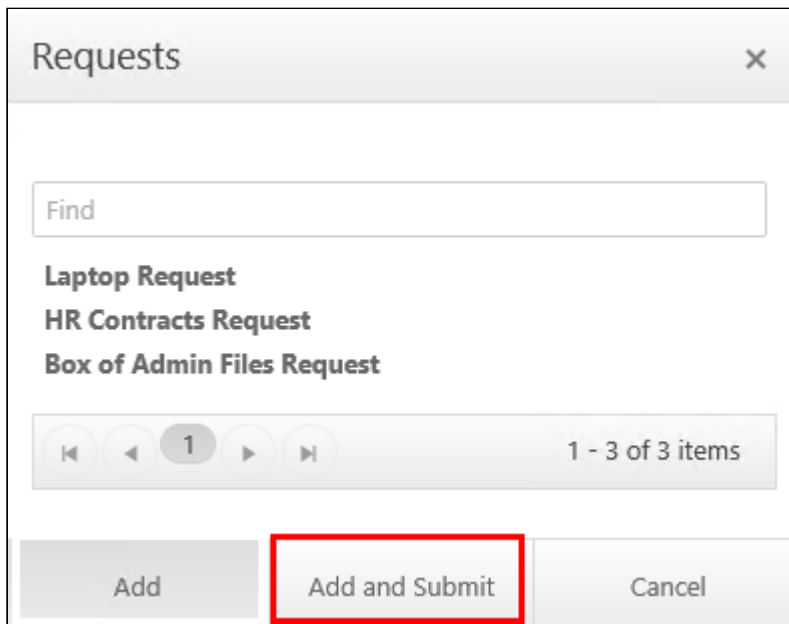


3. Click **View Assets**. The Physical Assets dialog displays, showing a list of all the physical assets in that container.
4. On the Physical Assets dialog, right-click the asset you want to add to your request and select Add to Request. (The drop-down options you see may vary, depending on your permissions.)

The screenshot shows the 'Physical Assets' interface. At the top, there is a header 'Physical Assets' with a close button. Below the header, the breadcrumb path is '/ Southeast'. There are three buttons: '+ Create', '+ Create Request', and '+ Create Return', along with a 'Find' search box. The main content is a table with columns: Name, Title, Owner, and Availability Status. The table contains three rows of assets. A context menu is open over the 'Legal Contracts Folder' asset, listing actions: Create Child, Edit, Move, Delete, Properties, Add to Request (highlighted with a red box), Add to Return, Custom Metadata, Manage Record, and Audit. At the bottom of the table, there are navigation controls (back, forward, refresh) and a status indicator '1 - 3 of 3 items'. A 'Close' button is located at the bottom right of the interface.

Name	Title	Owner	Availability Status
▶ Box of Admin Files	Box of Admin Files	Administrator	In
▶ Field Laptop		Administrator	In
▶ Legal Contracts Folder	Legal Contracts Folder	Administrator	In

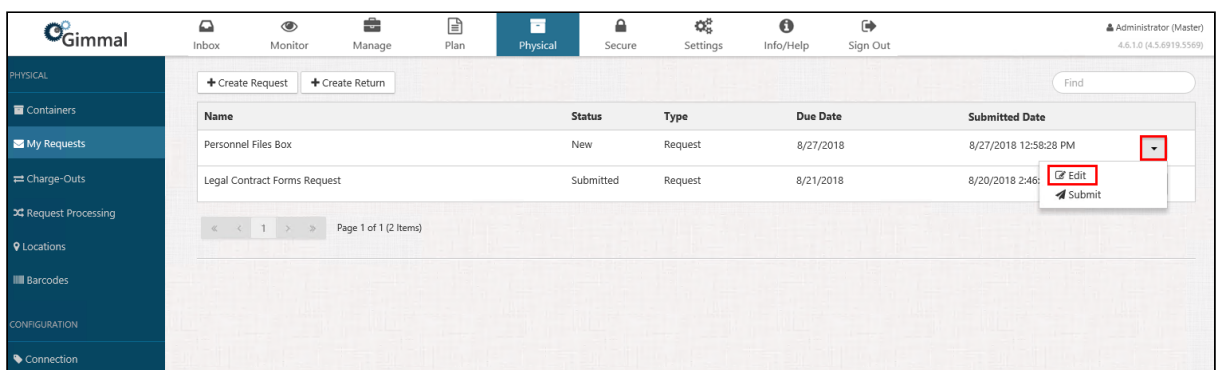
The Requests dialog opens, which lists all of your open requests



5. Select the request you want to add the asset to, and then click **Add and Submit**. This step performs two actions: it adds your request to the My Requests page and it submits the request to be processed. Two green confirmation messages display in the upper right corner of your screen. The return's Status changes from **New** to **Submitted**. After the Request Processor job has finished running (defaults to every 5 minutes), the Status will change to **Processing**. This indicates that the request is now ready to be processed by the Processor/Administrator.

Submitting a Request from the My Requests Page

1. Select **Physical** from the Main Menu, and then select **My Requests** from the left navigation menu. The My Requests page displays
2. Locate the request you want to cancel or edit. The request must have a Status of **Submitted** if you want to cancel. Click the drop-down list on the right side, and select the action you want to take



The Edit Request dialog opens. Make the desired changes to the properties and then click **Save**. The request updates on the My Requests page. If you chose to cancel, go to step 3.

Edit Request ✕

Name

Reason

Request Date

Due Date

Urgent

Charged-Out User --

Charged-Out Date --

Ship To Location

Notes

Assets

Name	Title	Owner	Availability Status
Field Laptop	Field Laptop	Administrator	In ⬆️⬇️⬆️⬇️

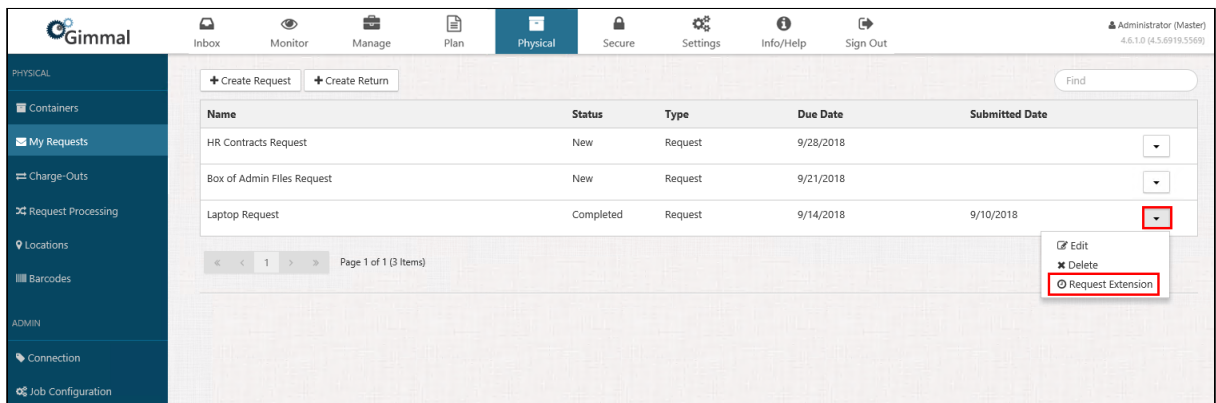
⏪ ⏩ 1 ⏪ ⏩
1 - 1 of 1 items 🔄

3.6.1.9 Request an Extension for a Charged Out Asset

You may request an extension for your charged-out physical assets (those that display on the [Charge-Outs page](#)¹³). This enables you to set a new due date for the request. The Processor will then either approve the extension request with the new requested date, approve the request but change the date, or reject the request.

To request an extension, perform the following steps:

1. Select **Physical** from the Main Menu, and then select **My Requests** from the left navigation menu. The My Requests page displays.
2. Locate the request whose due date you want to request an extension for, click the drop-down arrow to the right of the request name, and click **Request Extension**.



¹³ <http://docs.gimmal.com/en/6467-managing-charge-out-list.html>

The Request Extension window opens.


Request Extension

Name Laptop Request

Reason Request for laptop to be used by contractor in the field

Request Date 9/25/2018

Due Date 9/28/2018

Extension Date 

Urgent No


Charged-Out User Administrator


Charged-Out Date 9/25/2018

Ship To Location Houston Warehouse

Notes

Assets

Name	Title	Owner	Availability Status
 Field Laptop	Field Laptop	Administrator	Out

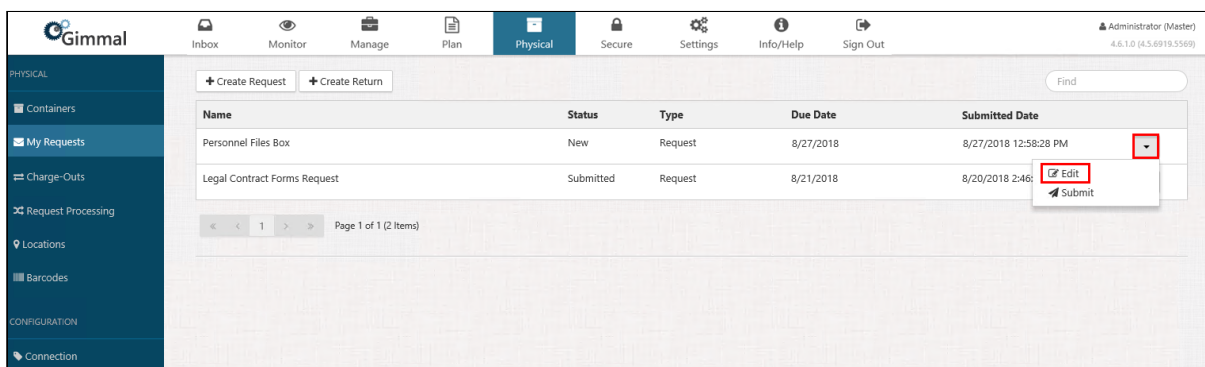
1 - 1 of 1 items 

3. Enter or select a new due date in the Extension Date field, and then click **Submit**.
The extension request's Status changes from **Completed** to **Submitted**. After the Request Processor job has finished running (defaults to every 5 minutes), the Status will change to **Processing**. This indicates that the request is now ready to be processed by the Processor/Administrator.

3.6.1.10 Canceling and Deleting a Request

Canceling a Request

1. Select **Physical** from the Main Menu, and then select **My Requests** from the left navigation menu. The My Requests page displays
2. Locate the request you want to cancel or edit. The request must have a Status of **Submitted** if you want to cancel. Click the drop-down list on the right side, and select the action you want to take



The Edit Request dialog opens.

Edit Request ✕

Name

Reason

Request Date

Due Date

Urgent

Charged-Out User --

Charged-Out Date --

Ship To Location

Notes

Assets

Name	Title	Owner	Availability Status
Field Laptop	Field Laptop	Administrator	In

⏪ ⏩ 1
1 - 1 of 1 items

3. Select **Cancel**, a confirmation window will open. Click **Cancel Request**. On the My Requests page, the request still displays, but the Status for the request changes to **Canceled**.

Cancel Request ✕

Name	Notes
Laptop Request	--
Reason	ProcessingUser
Contractor needs laptop to work in the field	--
Request Date	Created Date
10/2/2018 12:00:00 AM	10/2/2018 8:56:49 AM
Due Date	Submitted Date
10/12/2018 12:00:00 AM	10/2/2018 9:08:37 AM
Urgent	ProcessedDate
No	--
Ship To Location;	
Houston Warehouse	

Cancel Request
Cancel

Deleting a Request

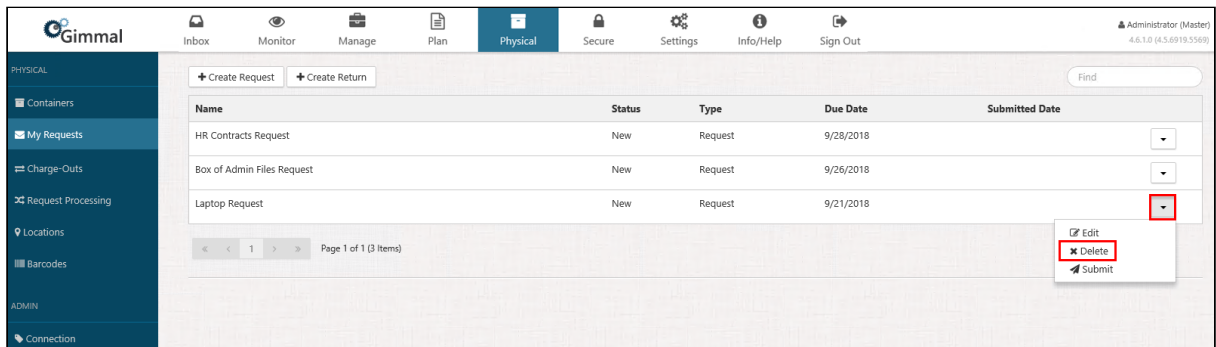
You can delete a request under the following conditions:

- The request has a Status of New.
- The request has been rejected or canceled.

To delete a request, perform the following steps:

1. Select **Physical** from the Main Menu, and then select **My Requests** from the left navigation menu. The My Requests page displays.

2. Locate the request you want to delete, click the drop-down list on the right side, and select **Delete**.



A confirmation window displays, showing you the properties of this request.

3. Click **Delete**. The request is deleted and no longer displays on the My Requests page.

3.6.2 Returning an Asset

The following topics cover how to return an asset.

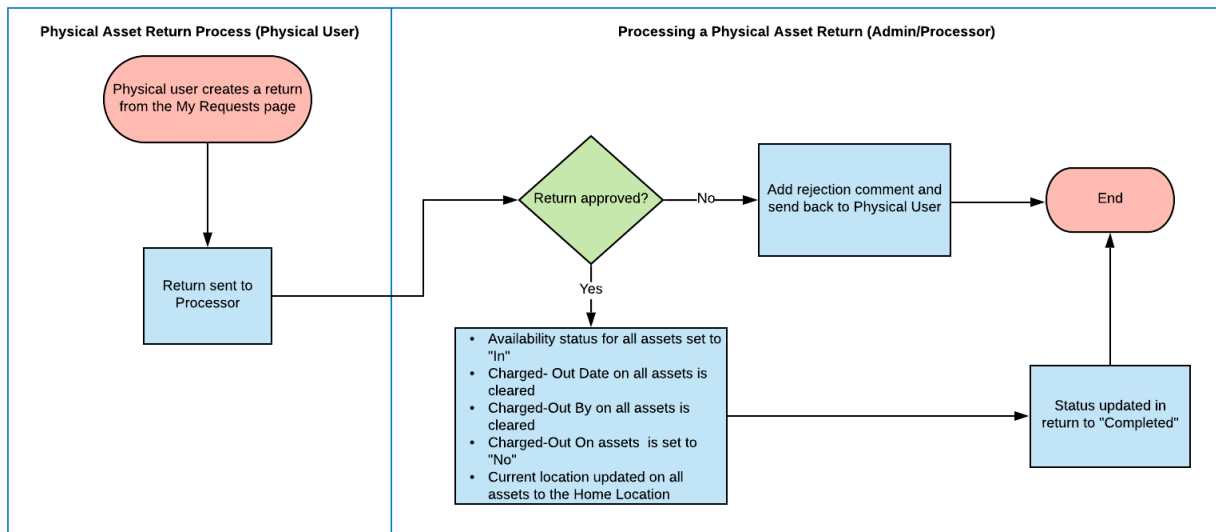
3.6.2.1 Creating a Return

3.6.2.2 Adding and Removing Assets from a Return

3.6.2.3 Submitting a Return

3.6.2.4 Canceling and Deleting a Return

The following flowchart illustrates the return process.



3.6.2.5 Creating a Return

There are two methods you can use to create a request for a physical asset:

- Create a request from the **My Requests** page
- Create a request from the **Physical Assets** window, accessed from the Containers page

Creating a Return from the My Requests Page

1. Select **Physical** from the Main Menu, and then **My Requests** from the left navigation menu. The My Requests page displays.
2. Click **+Create Return**. The Create Return window opens.
3. Enter the following information. An asterisk (*) indicates a required field.
 - **Name** – Enter a name/title for the request. Does not have to be unique, but it is required.
 - **Reason** – Enter an optional reason for requesting the asset.
 - **Pickup Date** – Enter the pickup date for the return.
 - **Due Date** – Enter the date when you expect to return the physical asset by.
 - **Urgent** – Indicate if this request is urgent or not.
 - **Pickup Location** – Specify the pickup location by clicking the Location Picker icon and selecting from the [Locations](#)¹⁴
 - **Notes** – Optionally enter any additional notes about the return.
4. Click **Create**. The new request displays on the My Requests page. Notice that "New" displays under the Status column for that return.
5. Before your return is processed, you must associate one or more assets with the return. This will ensure that the asset is circulated to you once the return is processed. See [Adding a Physical Asset to a Request](#)¹⁵.

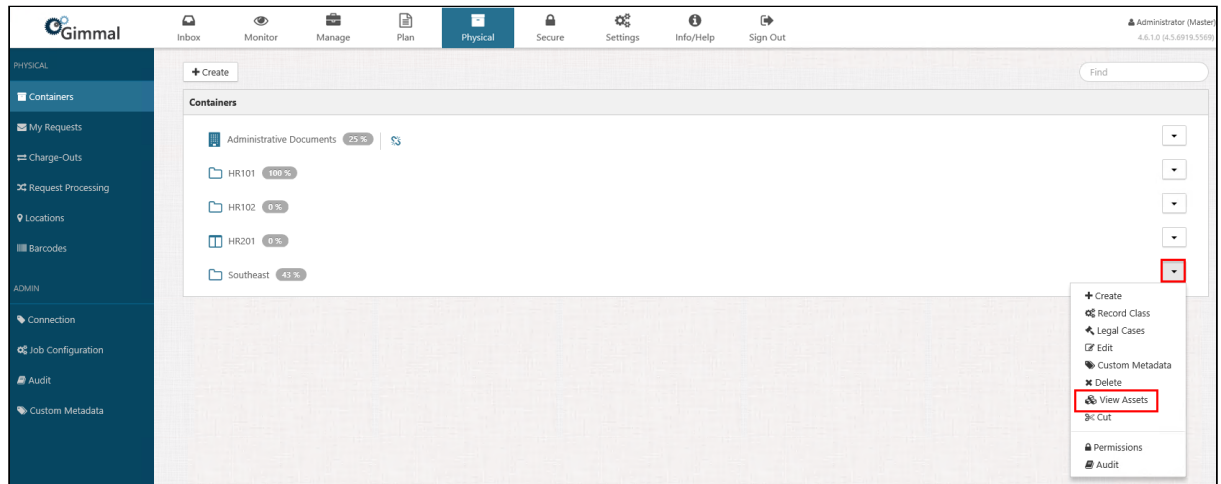
Creating a Return from the View Assets Dialog

1. Select **Physical** on the Main Menu, and then **Containers** on the left navigation menu. The Containers page displays.

¹⁴ <http://docs.gimmel.com/en/5905-managing-locations.html>

¹⁵ <http://docs.gimmel.com/en/6709-adding---removing-physical-asset-from-a-return.html>

2. Locate the container whose physical asset(s) you want to return, and click the drop-down arrow on the right side. The container context menu displays. (The drop-down options you see may vary, depending on your permissions.)
3. Click **View Assets**.



The Physical Assets window displays, showing a list of all the physical assets in that container.

The screenshot shows a window titled "Physical Assets" with a close button in the top right corner. Below the title bar is a breadcrumb path "/ Southeast". There are three buttons: "+ Create", "+ Create Request", and "+ Create Return" (which is highlighted with a red box). To the right of these buttons is a "Find" search input field. Below the buttons is a table with the following data:

Name	Title	Owner	Availability Status
▶ Field Laptop	Field Laptop	Administrator	In
▶ Legal Contracts	Legal Contracts	Administrator	Out

At the bottom of the window, there is a pagination bar showing "1 - 2 of 2 items" and a "Close" button.

4. Click **+Create Return**. The Create Return dialog opens.
5. Perform steps 3 through 5, listed in the section at the top.

3.6.2.6 Adding and Removing Assets from a Return

Adding an Asset to a Return

You can add a physical asset to an existing return (one that has not yet been submitted) or you can [create a new return](#)(see page 57) and add it then. You must add an asset(s) to a return before you can submit it. If you do not, you an error message displays. There are two methods you can use to add a physical asset to a return:

- Add the asset from the **Charge-Outs** page
- Add the asset from the **Physical Assets** window, accessed from the Containers page

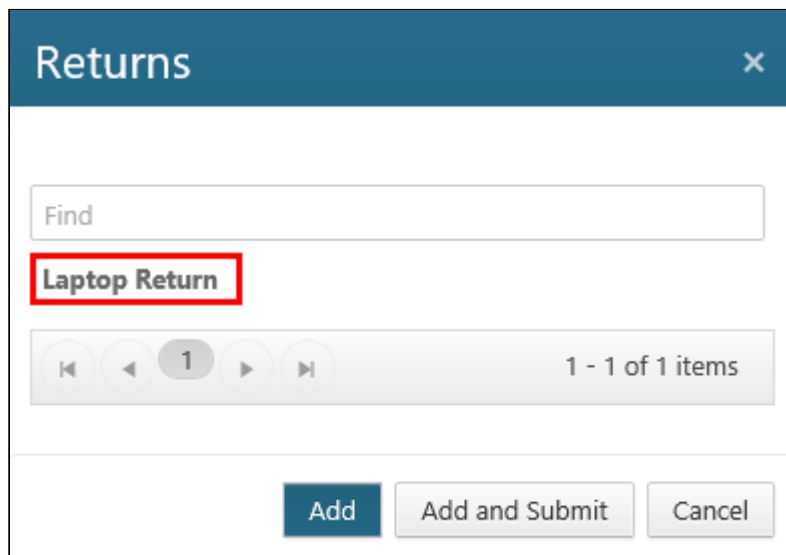


- You can only add a physical asset to a return if the asset is currently charged-out to you.
- If you return a parent physical asset, all child assets will be included with the return. However, you can return a child asset without returning its parent asset.

Adding a Physical Asset to a Return from the Charge-Outs Page

Physical Records Management provides a convenient way to return assets from one central location via the Charge-Outs page. The Charge-Outs page provides a list of all of your charged-out assets, and enables you to add each asset to a previously-existing return, and submit the return for processing.

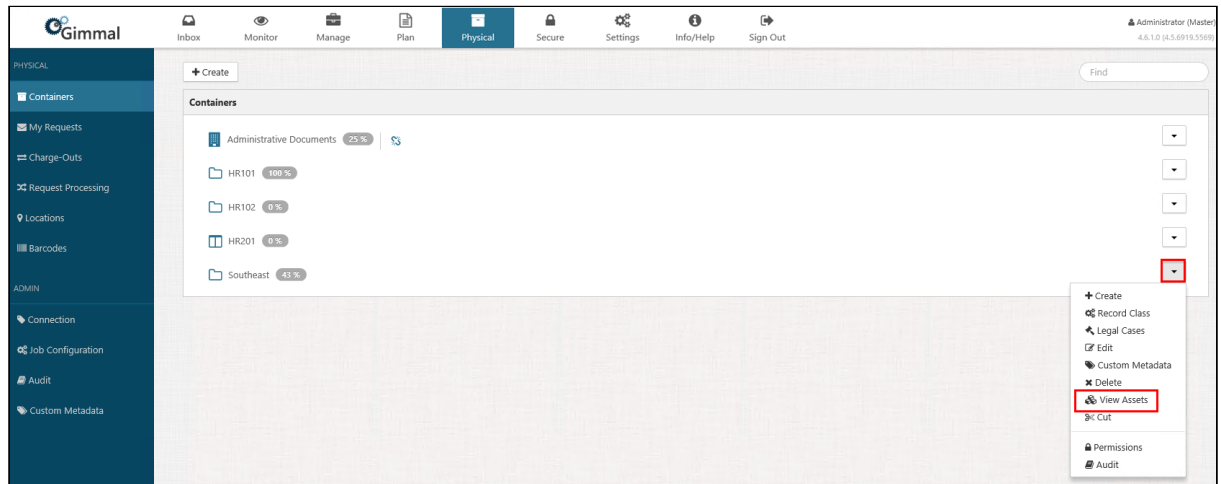
1. Select **Physical** from the Main Menu, and then **Charge-Outs** from the left navigation menu. The Charge-Outs page opens, displaying a list of your charged-out assets.
2. Locate the asset you want to return, click the drop-down arrow on the right, and select **+Add to Return**. The Returns window opens.



3. Perform either of the following steps:
 - Select the return you want to add the asset to, and then click **Add**. A green confirmation message displays in the upper right corner, indicating that the return was added. (You can verify the asset was added to the return by returning to the My Requests page, clicking the drop-down next to the return name, and selecting **Edit**. On the Edit Return window, the added asset displays in the Assets list in the middle of the window. Note that the Status column still indicates that the return is **New**, since it hasn't been submitted yet.)
 - Select the return you want to add the asset to, and then click **Add and Submit**. Two green confirmation messages display in the upper right corner, indicating that the return was added and submitted. (You can verify the asset was added to the return by returning to the My Requests page, clicking the drop-down next to the return name, and selecting **Edit**. On the Edit Return window, the added asset displays in the Assets list in the middle of the window. Note that the Status column now indicates that the return is **Submitted**, since you added the asset and submitted the return in one step.)

Adding an Asset to a Return from the Physical Assets Window

1. Select **Physical** on the Main Menu, and then **Containers** on the left navigation menu. The Containers page displays.
2. Locate the container whose physical asset(s) you want to return, and click the drop-down arrow on the right side. The container context menu displays. (The drop-down options you see may vary, depending on your permissions.)



3. Click **View Assets**. The Physical Assets window displays, showing a list of all the physical assets in that container.
4. On the Physical Assets window, right-click the asset you want to add to your return and select **Add to Return**. (The drop-down options you see may vary, depending on your permissions.)

Physical Assets

/ Southeast

[+ Create](#) [+ Create Request](#) [+ Create Return](#)

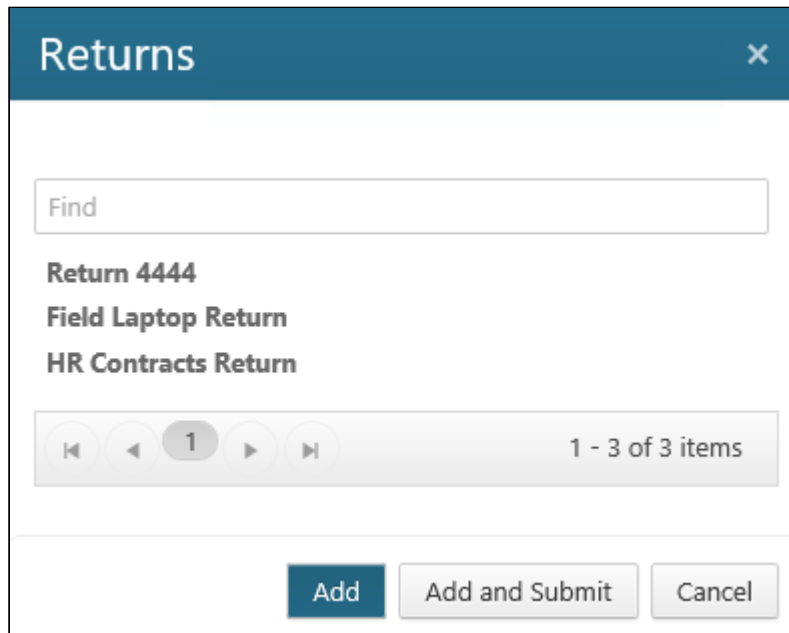
Name	Title	Owner	Availability Status
▶ Box of Admin Files	Box of Admin Files	Administrator	In
▶ Field Laptop		Administrator	In
▶ Legal Contracts	Folder	Administrator	In

- Create Child
- Edit
- Move
- Delete
- Properties
- Add to Request
- Add to Return**
- Custom Metadata
- Manage Record
- Audit

1 - 3 of 3 items

Close

The Returns window opens, which provides a list of all of your open returns.



5. Perform either of the following steps:
 - Select the return you want to add the asset to, and then click **Add**. A green confirmation message displays in the upper right corner, indicating that the return was added. (You can verify the asset was added to the return by returning to the My Requests page, clicking the drop-down next to the return name, and selecting **Edit**. On the Edit Return window, the added asset displays in the Assets list in the middle of the window. Note that the Status column still indicates that the return is **New**, since it hasn't been submitted yet.)
 - Select the return you want to add the asset to, and then click **Add and Submit**. Two green confirmation messages display in the upper right corner, indicating that the return was added and submitted. (You can verify the asset was added to the return by returning to the My Requests page, clicking the drop-down next to the return name, and selecting **Edit**. On the Edit Return window, the added asset displays in the Assets list in the middle of the window. Note that the Status column now indicates that the return is **Submitted**, since you added the asset and submitted the return in one step.)

Removing an Asset from a Return

You can remove the asset from a return provided that the return has not been processed (i.e. the Status column on the My Requests page is listed as **New** or **Submitted** for the return.) If a return is in the Processing stage, you cannot delete the asset from the return.

1. Select **Physical** from the Main Menu, and then **My Requests** from the left navigation menu. The My Requests page displays.
2. Locate the request you want to remove the asset from, click the drop-down arrow on the right side, and then click **Edit**. (The drop-down options you see may vary, depending on your permissions.) The Edit Request window opens.
3. Under the Assets section of the window, locate the asset you want to remove, right-click its name, and select **Remove**.

The screenshot shows the 'Edit Request' window with the following details:

- Name:** Laptop Request
- Reason:** Request for laptop to be used by contractor in the field
- Request Date:** 9/25/2018
- Due Date:** 9/28/2018
- Urgent:** No
- Charged-Out User:** --
- Charged-Out Date:** --
- Ship To Location:** Houston Warehouse
- Notes:** (Empty text area)

Assets Table:

Name	Title	Owner	Availability Status
Field Laptop	Field Laptop	Administrator	In

A context menu is open over the 'Field Laptop' row, with the 'Remove' option highlighted in red.

A confirmation window opens, asking you to confirm the removal of this asset.

4. Click **Confirm**. The Edit Request window refreshes, and the asset you removed no longer displays under the Assets list on the Edit Request window.

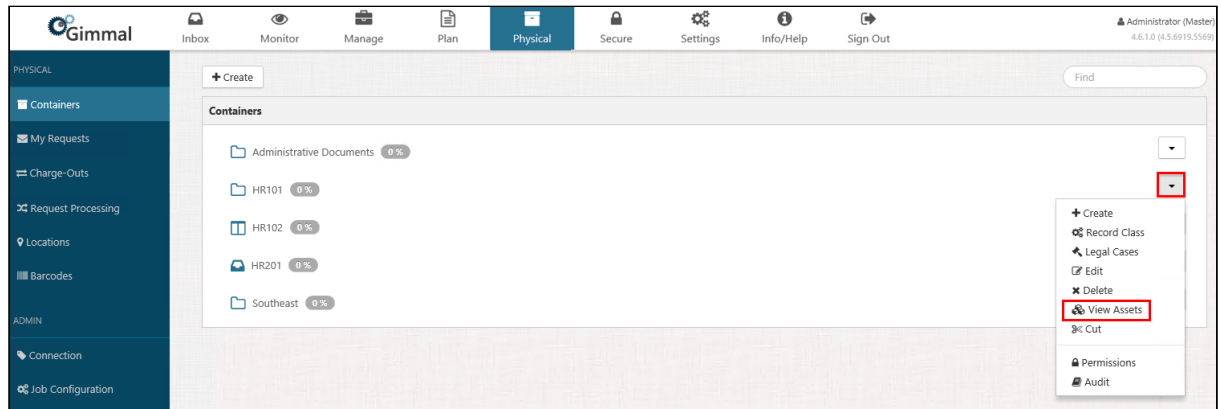
3.6.2.7 Submitting a Return

After you create a return for a physical asset, you must submit the return so that it will be processed. There are two ways to submit a return:

- Submitting it from the Returns window
- Submitting it from the My Requests page

Submitting from the Returns Window

1. Select **Physical** on the Main Menu, and then **Containers** on the left navigation menu. The Containers page displays.
2. Locate the container whose physical asset(s) you want to return and click the drop-down arrow on the right side. The container context menu displays. (The drop-down options you see may vary, depending on your permissions.)



3. Click **View Assets**. The Physical Assets dialog displays, showing a list of all the physical assets in that container.
4. On the Physical Assets dialog, right-click the asset you want to add to your return and select **Add to Request**. (The drop-down options you see may vary, depending on your permissions.)

Physical Assets

/ Southeast

[+ Create](#) [+ Create Request](#) [+ Create Return](#)

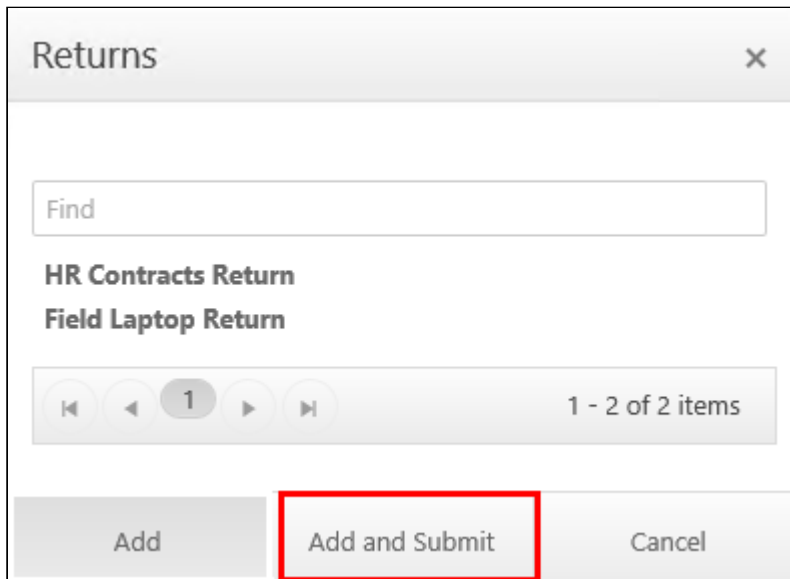
Name	Title	Owner	Availability Status
▶ Box of Admin Files	Box of Admin Files	Administrator	In
▶ Field Laptop		Administrator	In
▶ Legal Contracts	Folder	Administrator	In

- Create Child
- Edit
- Move
- Delete
- Properties
- Add to Request
- Add to Return**
- Custom Metadata
- Manage Record
- Audit

1 - 3 of 3 items

Close

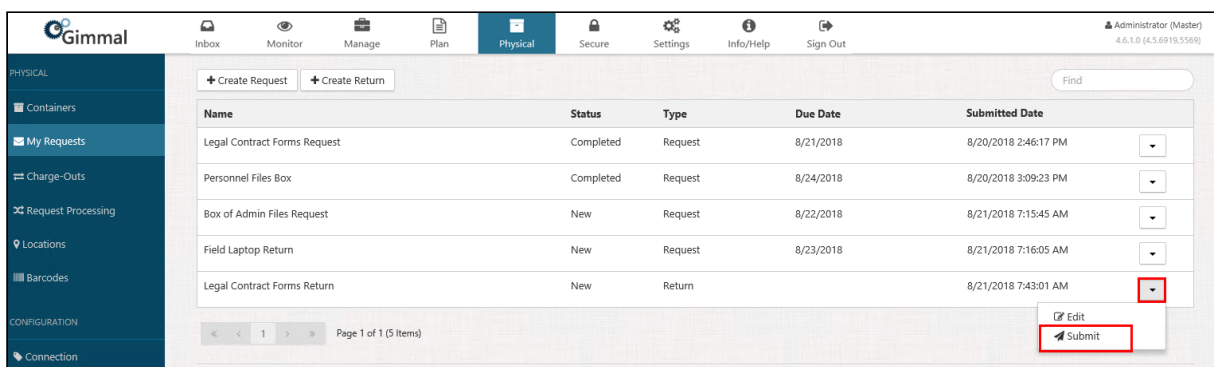
The Returns dialog opens, which lists all of your open request



5. Select the return you want to add the asset to, and then click **Add and Submit**. This step performs two actions: it adds your return to the My Requests page and it submits the return to be processed. Two green confirmation messages display in the upper right corner of your screen. The return's Status changes from **New** to **Submitted**. After the Request Processor job has finished running (defaults to every 5 minutes), the Status will change to **Processing**. This indicates that the return is now ready to be processed by the Processor/Administrator.

Submitting a Return from the My Requests Page

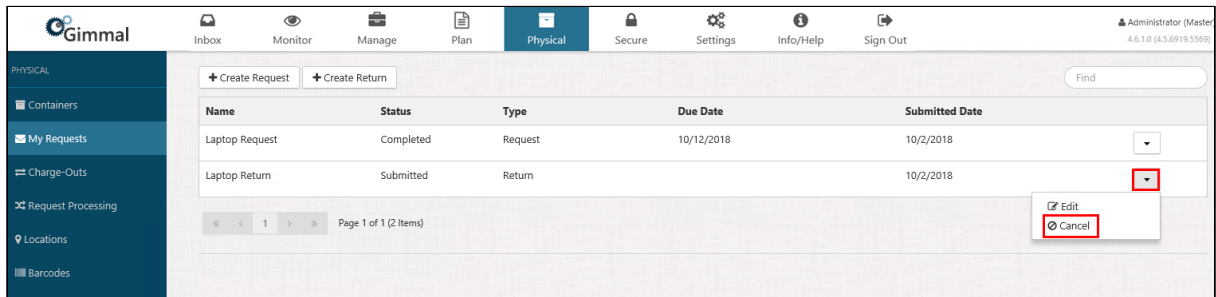
1. Select **Physical** from the Main Menu, and then select My **Requests** from the left navigation menu. The requests page displays.
2. Locate the return you want to submit, click the drop-down arrow on the right side, and then click **Submit**. (The drop-down options you see may vary, depending on your permissions.)



The request's Status changes from **New** to **Submitted**. After the Request Processor job has finished running (defaults to every 5 minutes), the Status will change to **Processing**. This indicates that the return is now ready to be processed.

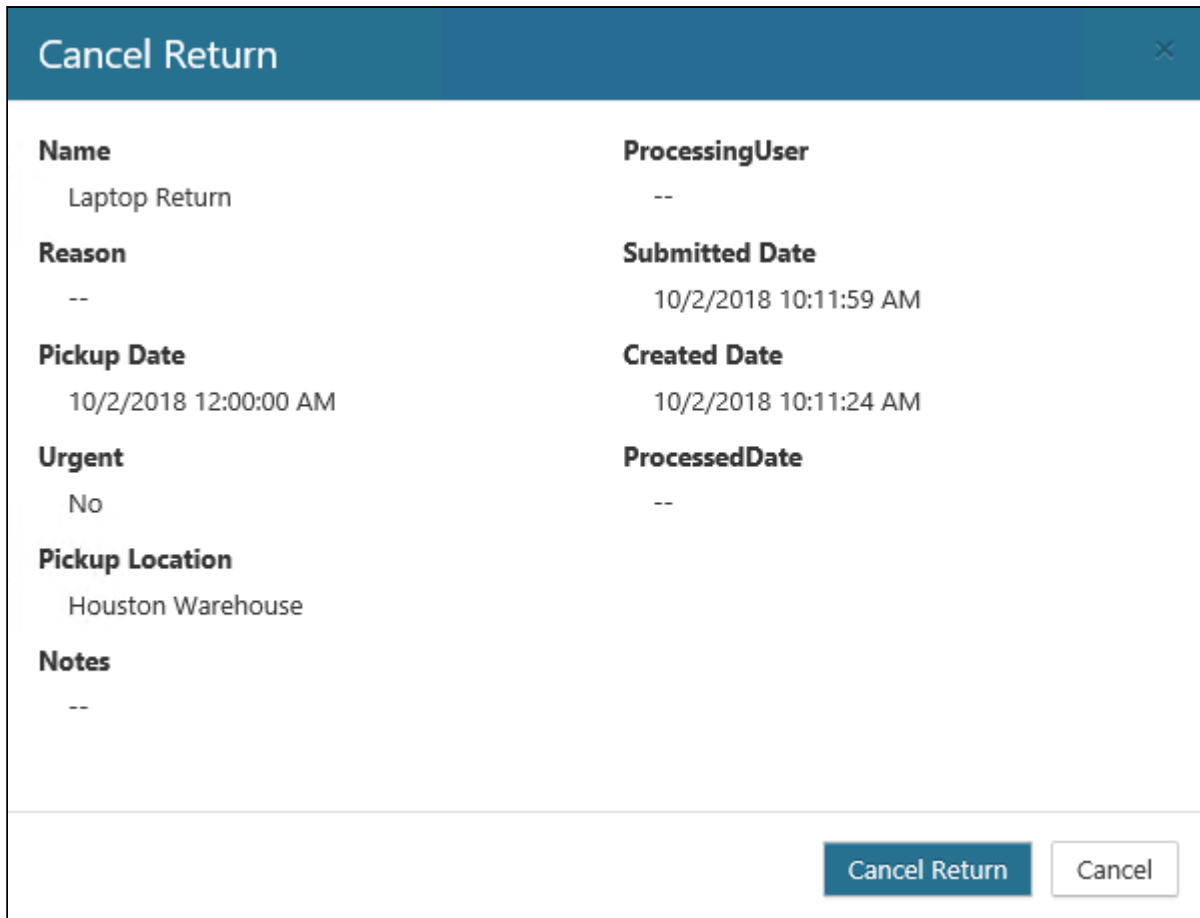
3.6.2.8 Canceling and Deleting a Return

1. Select **Physical** from the Main Menu, and then select **My Requests** from the left navigation menu. The My Requests page displays
2. Locate the return you want to cancel or edit. The return must have a Status of **Submitted** if you want to cancel. Click the drop-down list on the right side, and select Cancel



The Edit the Return dialog opens. Make the desired changes to the properties and then click **Save**. The return updates on the My Requests page. If you chose to cancel, go to step 4.

3. If you chose to **Cancel**, a confirmation window will open. Click **Cancel Return**. On the My Requests page, the request still displays, but the Status for the return changes to **Canceled**.



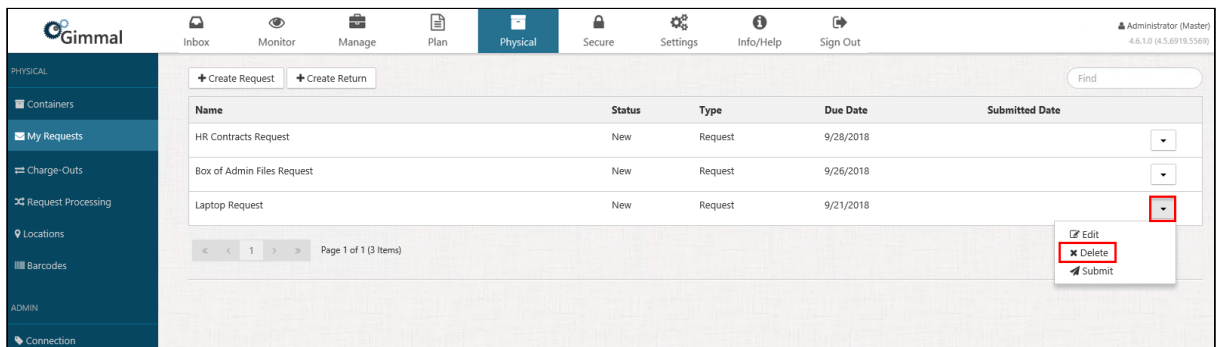
Deleting a Return

You can delete a return under one of the following conditions:

- The return has a Status of **New**.
- The return has been rejected or canceled.

To delete a return, perform the following steps:

1. Select **Physical** from the Main Menu, and then select **My Requests** from the left navigation menu. The My Requests page displays
2. Locate the return you want to delete, click the drop-down list on the right side, and select **Delete**.

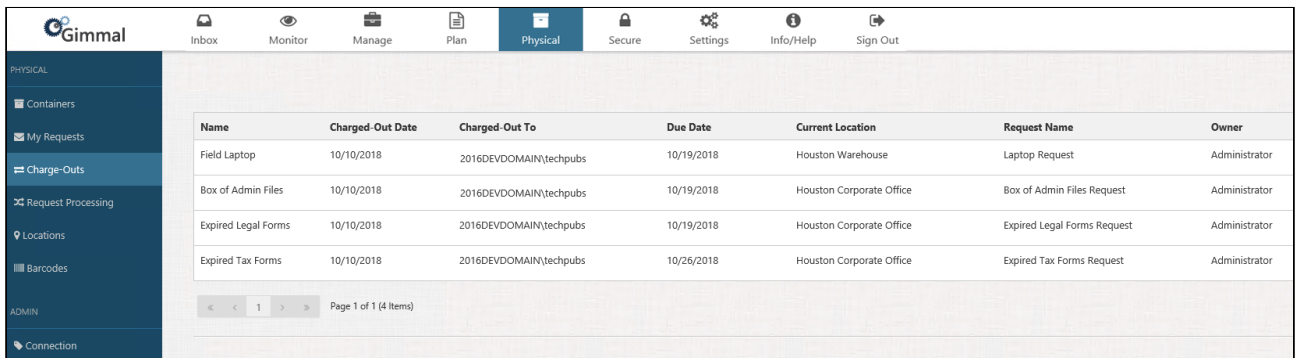


A confirmation window displays, showing you the properties of this return.

3. Click **Delete**. The return is deleted and no longer displays on the My Requests page

3.6.3 Managing Charge-Outs

Users can see a list of their charged-out assets by browsing to the Charge-Outs page in Physical Records Management. Select **Physical** from the Main Menu, then **Charge-Outs** from the navigation bar on the right side.



3.6.3.1 Viewing Asset's Properties

You can view the Properties of any charge-out by clicking the drop-down arrow on the right, and selecting **Properties**.

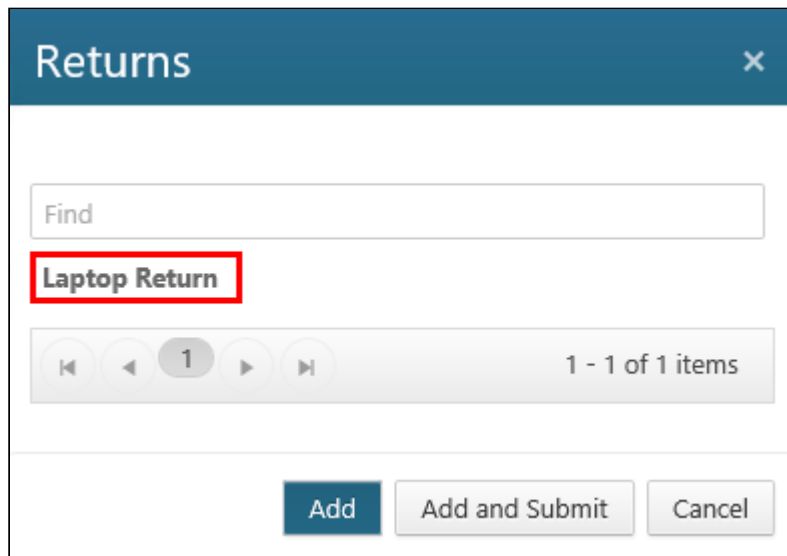
The screenshot displays the 'Properties' dialog box for a 'Field Laptop' asset. The dialog box is overlaid on a table of charged-out assets. The table has columns for Name, Charged-Out Date, and Charged-Out To. The 'Field Laptop' row is highlighted. The 'Properties' dialog box contains the following information:

Name	Field Laptop
Title	Field Laptop
Subject	--
Keywords	--
Home Location	/ Southeast
Temporary Location	--
Current Location	Houston Warehouse
Asset Type	Other
Other Asset Type	Hardware
Format	Other
Other Format	Laptop
Owner	Administrator
Allow Requests	Yes
Charged-Out	Yes
Charged-Out To	Administrator
Charged-Out Date	10/10/2018
Is Child Asset	No
Barcode	--
Barcode Symbology	Code39
Barcode Alternate	--
Barcode Symbology Alternate	Code39

3.6.3.2 Returning an Asset

The system provides a convenient way to return assets from one central location via the Charge-Outs page. The Charge-Outs page provides a list of all of your charged-out assets and enables you to add each asset to a previously-created return, and submit the return for processing.

1. Locate the asset you want to return, click the drop-down arrow on the right, and select **+Add to Return**. The Returns dialog opens.



2. Perform either of the following steps:

- Select the return you want to add the asset to, and then click **Add**. A green confirmation message displays in the upper right corner, indicating that the return was added. (You can verify the asset was added to the return by returning to the My Requests page, clicking the drop-down next to the return name, and selecting **Edit**. On the Edit Return dialog, the added asset displays in the Assets list in the middle of the dialog. Note that the Status column still indicates that the return is **New**, since it hasn't been submitted yet.)
- Select the return you want to add the asset to, and then click **Add and Submit**. Two green confirmation messages display in the upper right corner, indicating that the return was added and submitted. (You can verify the asset was added to the return by returning to the My Requests page, clicking the drop-down next to the return name, and selecting **Edit**. On the Edit Return dialog, the added asset displays in the Assets list in the middle of the dialog. Note that the Status column now indicates that the return is **Submitted**, since you added the asset and submitted the return in one step.)

3.6.4 Taking Custody of an Asset

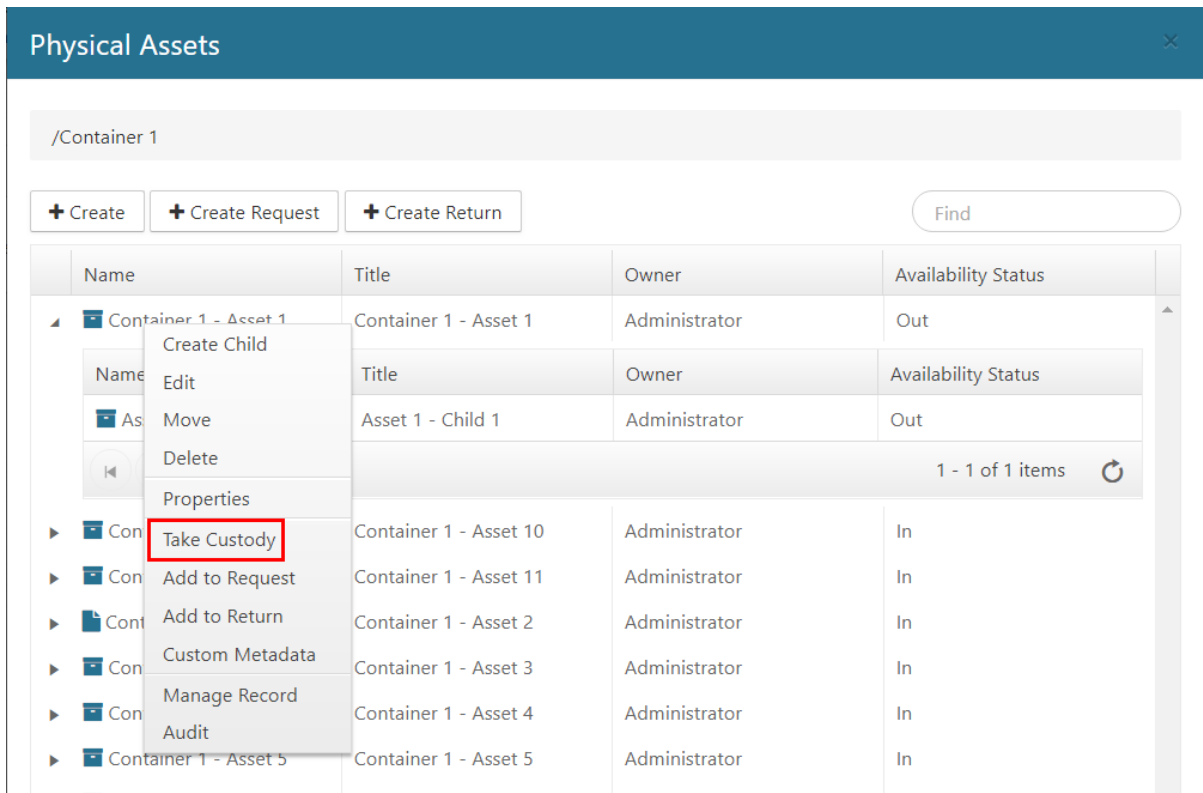
You can take custody of an asset in Physical Records Management that is charged out to someone else if you are a Physical Administrator or a Physical User with at least View permissions on the asset. Once you take custody it will be up to you to return the asset.

If the physical asset you are taking custody of has child assets that are charged-out to the same user, those child assets will be included with the parent. If the child asset is not charged out, or if a child asset is charged out to another user, they custody of those assets will not be given to you.

To take custody of a physical asset, perform the following steps:

1. Select **Physical** on the Main Menu, and then **Containers** on the left navigation menu. The Containers page displays.
2. Locate the container whose physical asset you want to take custody of, and click the drop-down arrow on the right side. The container context menu displays. (The drop-down options you see may vary, depending on your permissions.)
3. Click **View Assets**. The Physical Assets window displays, showing a list of all the physical assets in that container

- Right-click on the desired asset and select **Take Custody**. The **Charged-Out To** field (located on the Properties window for an asset) displays the new user name.



4 Record Manager Guide

Gimmel Records Management has two levels of record manager roles:

- **Global Record Manager** - Assign this role to record managers who have responsibility for ensuring compliance on all records regardless of country, sensitivity, or department. It is possible to not have an account assigned **Global Record Manager**, in which case the System Admin role would be responsible for the configuration of Record Filters and securing the File Plan.
- **Record Manager** - Assign this role to record managers who have limitations on their scope of records they are responsible for. The **Record Manager** role is bound by Record Filters, and will not be able to configure Record Class permissions for end users.

Topics in this guide are for the **Record Manager** role, including setting up the file plan, classifying content, and monitoring the records program. The Global Record Manager role also has these capabilities.

4.1 Building Your File Plan

4.2 Manage

4.3 Disposition

4.4 Monitor

4.5 Rule Builder

4.6 Physical Records

4.7 Creating and Managing Legal Cases and Legal Holds

4.8 Filtering Records by Rules and Metadata

4.9 Record Class Permissions

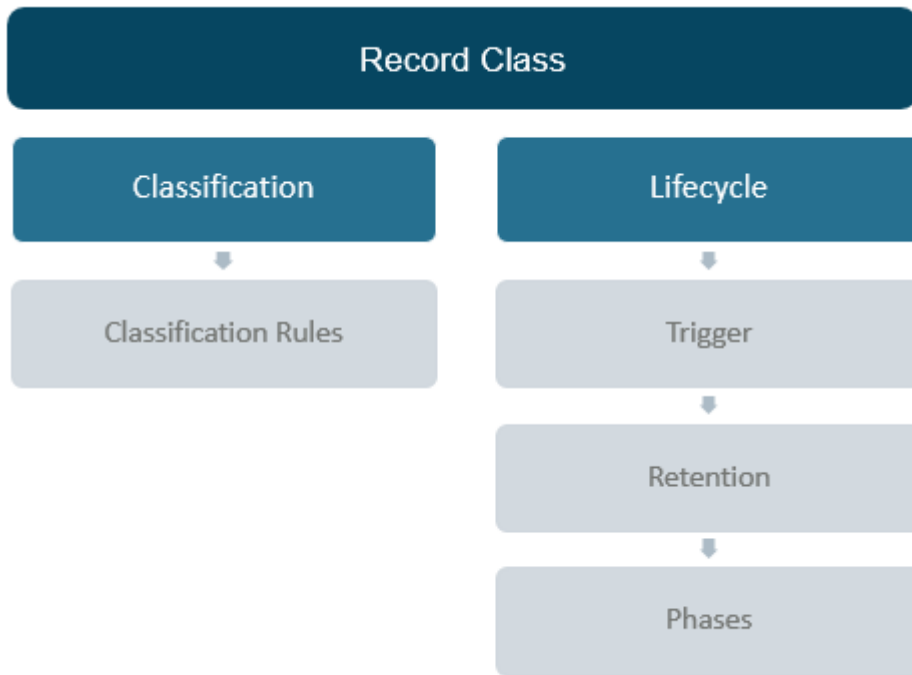
4.10 Building Your File Plan

The first task that is required to effectively use Records Management is to create a file plan. Often in Records Management, the terms "file plan" and "retention schedule" are used synonymously, however, the latter is really a subset of the file plan as a whole. You will need the Record Manager, Global Record Manager, or System Admin role in order to see the file plan.

A retention schedule typically lists all the record classes (also known as a record series or record category), the length of time each document or record will be retained, the reason for retention, and the disposition of the item.

A file plan is much more detailed. It not only contains the retention schedule, but it also shows where the information resides, specifies the type of record (case or administrative), indicates the rules to determine when a record is declared, and identifies the type of trigger that will start the retention.

The file plan consists of multiple key entities that will be created, each of which plays its own role in a document’s lifecycle. The following illustration shows each of these entities and their relationship with each other.



4.10.1 Triggers

4.10.2 Retentions

4.10.3 Lifecycles

4.10.4 Rule Sets

4.10.5 Editing the File Plan

4.10.6 Record Classes

4.10.7 Triggers

A Trigger represents a reusable entity that defines the structure of how a retention period begins. You use a Trigger as a building block for defining another type of entity called Retentions. The Trigger does NOT contain the Retention Duration. The Trigger is used by the Retention Entity to determine the Retention Rule. The Trigger, together with the Retention and Lifecycle Action, make up the Lifecycle Phase.



See the following table for each trigger type:


Trigger Type	Description
Special	Predefined triggers for dates that can be assigned to items dynamically according to user interaction
Event	There are two types of Event Triggers: <ul style="list-style-type: none"> • Recurring - These are typically for Case Records and are created by a recurring date. For example: <ul style="list-style-type: none"> • End of Fiscal Year (EFY) • End of Calendar Year (ECY), also known as End of Current Year • Manual - These are typically for Case Records and are created manually by a user or can be generated by the API. For example <ul style="list-style-type: none"> • Employee Termination & Contract Expiration

Trigger Type	Description
Date Property	Starts retention when a date property is met. For example: <ul style="list-style-type: none"> • Date Created (@Created) • Date Modified (@Modified) • Custom date column (e.g. True Document Date, Contract Date)
Rule	Starts retention on when a rule evaluates to true. For example: <ul style="list-style-type: none"> • Status = Completed • Flag = Yes

Event Triggers result in one or more occurrences that specify the date and time that particular event happened and the specific record(s) that should be targeted. Events are typically used for Case Records. Date and Rule Triggers define how the date and time will be determined based on the properties of the record itself.

4.10.7.1 Editing Triggers

You may edit the Title or Description of a Trigger, and the property will simply be changed throughout the software.

 Changing properties other than Title or Description may cause the lifecycle or all items using the trigger to be reset.

4.10.7.2 Date Property Triggers

A Date Property Trigger represents a date derived from an item's metadata properties. For example, suppose a document contains the property of Created Date. To use this property as a Trigger, you must define a new Date Property Trigger.

Date Property Triggers are typically used to compare a "True Document Date" with the current date to determine if retention should begin. A "True Document Date" can be any date property stored with a record. For example:

1. Start retention on the date a record's content was modified:
 - Set Property Name to "@modified"
2. Start retention on a custom date column in SharePoint
 - Set Property Name to the SharePoint column name
 - For SharePoint, use the Display Name, not the internal name

Date Property Trigger Properties

The properties for the Date Property Trigger are described in the following table:

Property	Description
Title	Defines the unique name of the Date Property Trigger

Property	Description
Description	Defines the description of the Date Property Trigger for informational purposes
Property Name	Defines the name of the Repository Item's property which will contain a date

Creating a Date Property Trigger

1. To create a Date Property Trigger, perform the following steps:
2. Select **Plan** from the Main Menu.
3. Select **Triggers** from the left navigation menu.
4. Select **Date Property Trigger**. The Create Date Property Trigger dialog opens.
5. Enter the desired Date Property Trigger Properties.
6. Select **Create**.

4.10.7.3 Event Triggers

An Event Trigger is a re-usable entity that represents an event that will occur at some point in the future, which is not driven by the Repository Item's properties. An example of an Event Trigger may be a one-time event such as the Termination of an employee or a recurring event such as Tax Year.

Event Triggers allow the generation of Event Occurrences, each containing an event date, which specifies a retention start date. Event Triggers are especially important when working with Case Based Records, since individual items do not drive retention of case records.

A few key terms to understand before creating Event Triggers are:

Term	Description
Event Occurrence	One instance of the Trigger.
Target Records	The records that each individual Event Occurrence will look for in order to see if a record should be assigned, therefore starting retention.
Trigger Assignment Position	Determines which Event Occurrence will be used for each record.
Event Date	The date an Event Occurrence actually took place. (ex. Hired Date).

Term	Description
Originated Date	The date associated with the record that will be used to compare against the event date in order to determine if a specific Event Occurrence should be used. This is also known as the Record Origin.
Target Date	A date property that can be used instead of the default Originated Date to compare against the event date.

Event Trigger Properties

Property	Description
Title	Defines the unique name of the Event Trigger.
Description	Defines the description of the Event Trigger for informational purposes.
Starting Event Date	Defines the date in which the first Event Occurrence of a trigger should be created. Note: Creating an event in the past will generate an occurrence at the specified interval up to the current date.
Recurrence	Defines the interval in which an Event Occurrence should be created beginning on Next Event Date. This is a drop-down, and the available options are: <ul style="list-style-type: none"> • Manual • Once • Daily • Monthly • Yearly
Assignment Position	Defines how (Link) event occurrences are selected for a Record. This is a drop-down, and the available options are: <ul style="list-style-type: none"> • Nearest Occurrence After Target Date • Nearest Occurrence Before Target Date • Nearest Occurrence To Target Date
Target Date Property Name	Defines a different date to use, instead of the records' Originated Date, to use to compare against the event date, to determine if retention should begin. If this property is left blank, Originated Date is used.

Creating an Event Trigger

1. Select **Plan** from the Main Menu.
2. Select **Triggers** from the left navigation menu.
3. Click **Event Trigger**. The Create Event Trigger dialog opens.
4. Enter the desired Event Trigger Properties.
5. Click **Create**.

4.10.7.4 Rule Triggers

Rule Triggers enable you to define a Trigger based on Property values. This enables you to create more robust rules beyond just dates, events based on dates, or manual events. For example, the Record may have a property (e.g. met-data field) called "Status". You can trigger an event based on the value of the "Status" field matching a specific value.

Rule Triggers are similar to an Event Trigger, but Rule Triggers are targeted towards individual items and do not target Case Record Classes. A common example would be to have a Rule Trigger based on the "Status" property being changed to "Complete". See the illustration below.

The screenshot shows a dialog box titled "Edit Rule Trigger". At the top, there is a "Title" field containing the text "Complete". Below this is a "Clear" button and a dropdown menu. To the right of the dropdown is an "Add Rule Set" button. Below these elements is a table with the following structure:

Property	Operator	Value	Data Type	Join
Status	=	Complete	Text	None

At the bottom right of the dialog, there are "Save" and "Cancel" buttons.

Rule Trigger Properties

The only property for a rule trigger is the Title, which must be unique to other Trigger Titles.

Building rules for Triggers is the same as building rules for other elements. Besides adding individual rules on each line, you can also add Rules Sets.

Component	Description
Property	Represents the property of the Repository Item to compare against. *The property can be any public property that exists for an item or a special token that is defined (see Classification Rule Tokens appendix for details).

Component	Description
Operator	Represents the operator to use when comparing against the item. Possible values are: <ol style="list-style-type: none"> 1. < (less than) 2. <= (less than or equal to) 3. = (equal to) 4. > (greater than) 5. >= (greater than or equal to) 6. Like 7. Not = (not equal to) 8. Starts With 9. Matches
Value	Represents the value of the expression that will be used when comparing against the item
Data Type	Represents the data type of the Repository Item to compare against. Using a more specific data type will result in a more accurate expression result. Possible values are: <ol style="list-style-type: none"> 1. Date 2. Date and Time 3. Text 4. Number
Join	Represents how individual Classification Rules are combined within the list of rules defined for Record Class

Creating a Rule Trigger

To create Rule Triggers, perform the following steps:

1. Select **Plan** from the Main Menu.
2. Select **Triggers** from the left navigation menu.
3. Click **Rule Trigger**.
4. Enter the unique Title for the Rule Trigger.
5. You can create the rules for the Rule Trigger in two different ways. Refer to Understanding Rule Sets & Rule Groups for more information.
 - Select **Create** to manually define the rules.
 - Specify the Properties for this Rule Trigger. The Rule Trigger Properties are identical to the Classification Rule Properties. Refer to Classification Rule Properties for a detailed description of the properties.
 - Select **Add Rule Set** to add a Rule Set that has been pre-defined.
6. Click **Save**

4.10.7.5 Special Triggers

Special Triggers are predefined system triggers for dates that can be assigned to items dynamically according to user interaction. The following Special Triggers are available.

Trigger	Description
Obsolete	The Obsolete trigger allows Retentions to be driven based on the date that an item is marked Obsolete.
Supersede	The Supersede trigger allows Retentions to be driven based on the date that an item is marked Superseded.
Declare	The Declare trigger allows Retentions to be driven based on the date that an item is marked Declared.
Undeclare	The Undeclare trigger allows Retentions to be driven based on the date that an item is marked as Undeclared.
Record Class Closed	The Record Class Closed trigger allows Retentions to be driven based on the date that an item's Record Class is marked as Closed.

4.10.8 Retentions

A Retention represents a reusable entity that defines a time period from an associated Trigger. It is used to represent regulation or policy that refers to some duration. One or more Retentions are used to build a Lifecycle.

4.10.8.1 Retention Properties

Property	Description
Title	Defines the unique name of the Retention
Description	Defines the description of the Retention for informational purposes
Authority	Defines the Authority for which the Retention has been defined. For example, this may be the Policy Number or the Tax Code.
Trigger	Defines the associated Trigger, which defines what triggers the retention timer
Interval	Defines the numeric value, which represents how long the Time Period of the Retention lasts

Property	Description
Time Period	<p>Defines how the Interval is to be interpreted</p> <p>Supported values are:</p> <ul style="list-style-type: none"> • Day(s) • Month(s) • Year(s)

4.10.8.2 Creating a Retention

1. Select **Plan** from the Main Menu.
2. Select **Retentions** from the left navigation menu.
3. Click **Create**. The Create Retention dialog opens.
4. Enter the desired Retention Properties.
5. Click **Create**.

4.10.9 Lifecycles

A Lifecycle brings together the existing Triggers and Retentions to define which action should happen to an item at specific points in time. Each of these points in time is represented within a Lifecycle by a Phase. Lifecycles can be assigned to any number of Record Classes which will ultimately determine the retention of records, and how it goes through disposition.

Lifecycle Properties

Property	Description
Title	Defines the unique name of the Lifecycle
Description	Defines the description of the Lifecycle for informational purposes
Notes	Defines a free form field that can be used to provide detailed notes for the Lifecycle
Phases	Defines the lifecycle of the managed item

Phase Properties

Property	Description
Phase	Numeric value indicating Phase order. This property is automatically populated.
Retention	Defines the associate Retention for the Phase. A drop-down list of Retentions is provided.

Property	Description
Action	Defines the Action that is performed on the item once the Retention has expired. See Supported Phase Actions for a description of the supported Actions.
Automation Level	<p>Defines whether the Action is conducted automatically by the system or performed manually by the user.</p> <ol style="list-style-type: none"> Automatic – Action will be performed automatically if supported by the Connector; otherwise it will revert to Manual. Manual – Action will be displayed in the Inbox once Retention has expired, and must be manually executed and marked complete. Performing a manual action for a Physical Record is an example of when this setting is useful.
Require Approval	Indicates whether Action must be approved before being executed. Items requiring Approval will appear in the Inbox.
Pause Duration	<p>This property is only available if the Require Approval checkbox is marked and takes effect when a record is Paused during disposition. This property indicates the time period for how long the item will wait before reappearing in disposition when paused.</p> <p>This property is not required, and if it is left blank, the item will appear back in the Inbox immediately after paused.</p> <p>There is no limit to the number of times a record can be paused.</p>

Supported Phase Actions

Action	Description
Declare Record	<p>Flags the item as a Declared Record and locks the item in the Repository from modification and deletion.</p> <p>Cannot be assigned to the final phase in a lifecycle.</p>
Dispose and Delete	<p>Deletes the item from the Repository and removes any information about the item.</p> <p>Can only be assigned to the final phase in a lifecycle.</p>
Dispose and Recycle	<p>Deletes the item from the Repository and removes any information about the item. The Recycle part of the Action is dependent upon the Repository Connector.</p>
Dispose and Transfer	<p>Moves the item to a specified location within the Repository and removes any information about the item.</p> <p>Can only be assigned to the final phase in a lifecycle.</p>
None	No action is performed.*Cannot be assigned to the final phase in a lifecycle

Action	Description
Permanent	Marks the item as Permanent and locks the item in the Repository from modification and deletion. Can only be assigned to the final phase in a lifecycle.
Transfer	Moves the item to a specified location within the Repository. Cannot be assigned to the final phase in a lifecycle.
Undeclare Record	Removes the Declared Record flag and removes any lock on the item in the Repository. Cannot be assigned to the final phase in a lifecycle.
Workflow (*SharePoint on-premises only; not supported in SharePoint Online)	Starts a specified Workflow in the Repository. Cannot be assigned to the final phase in a lifecycle.

Creating a Lifecycle

1. Select **Plan** from the Main Menu.
2. Select **Lifecycles** from the left navigation menu.
3. Click **Create**. The Create Lifecycle dialog opens.
4. Enter the desired Lifecycle Properties.
5. Add/Remove Phases as desired.
6. Click **Create**.

Edit Lifecycle
✕

Title *

Notes

Description

Phase	Retention	Action	Automation Level
1	Modified + 10 Years	Dispose and Delete	Automatic
<p>Require Approval <input checked="" type="checkbox"/></p> <p>Pause Duration <input type="text" value="0"/> Day(s)</p> <p>Modified + 5 Year(s) >> Automatic Dispose and Delete (Approval)</p>			
1	Supersede + 1 year	Dispose and Delete	Automatic
<p>Require Approval <input checked="" type="checkbox"/></p> <p>Pause Duration <input type="text" value="0"/> Day(s)</p> <p>Supersede + 1 Year(s) >> Automatic Dispose and Delete (Approval)</p>			

+ Add Phase
+ Add Alternate Phase

Save Cancel

4.10.10 Rule Sets

Rule Sets provide the ability to create pre-defined rules that can be used when creating Classification Rules, Triggers, and Legal Hold Rules. This enables a set of rules to be re-used across Classification Rules, Rule Triggers, and Legal Hold Rules.

4.10.10.1 Building Rules

Building rules are similar across the software. Refer to the [Rule Builder](#)(see page 125) for more information.

4.10.10.2 Creating Rule Sets

To create a Rule Set, perform the following steps:

1. Select **Plan** from the Main Menu.
2. Select **Rule Sets** from the left navigation menu.
3. Click **Create**. The Create Rule Set dialog opens.
4. Enter a **Title** for the Rule Set.
5. Click the **Create** button under the Title field.
6. Enter the remaining rules.
7. Click the **Create** button at the bottom of the window.

×
Create Rule Set

Title

Human Resource File Share

Clear

Property	Operator	Value	Data Type	Join	
@uri	Like ▼	\\rldemo\managed shared\	Text ▼	And ▼	✖
@repo	= ▼	FileSystem	Text ▼	None ▼	✖

Create
Cancel

4.10.10.3 Adding Rule Sets

Rules Sets can be used anytime rules are being created. In lieu of creating new rule elements, you may add a Rule Set instead by selecting the dropdown arrow for Add Rules Set and selecting the desired Rule Set and clicking **Add Rule Set**.

×
Classification Rules

Create

▼

Add Rule Set

Box Folder

Human Resource File Share

Human Resource SharePoint

Is Demo

PDF Files

PST Files

SharePoint Site Collection

Status Complete

Save
Cancel

Rule Sets may be combined together or used in conjunction with other rules elements.

Classification Rules
✕

Clear

▼

Add Rule Set

Property	Operator	Value	Data Type	Join	
Human Resource File Share					
@uri	Like	\\rldemo\managed sha...	Text	And	+
@repo	=	FileSystem	Text	Or	+
Human Resource SharePoint					
@sp.web	=	Human Resources	Text	None	+

Save
Cancel

4.10.11 Editing the File Plan

Gimmel Records Management has a unique ability to allow the lifecycle of a record to be changed assuming it has not yet been disposed of. You may want to consider if you really want to modify the course of existing records, versus creating a path for newly classified records.

4.10.11.1 Editing the File Plan for existing records

When editing Triggers, Retentions, or Lifecycles there may be an impact on the records that are currently classified and following the lifecycle impacted.

Upon saving the Lifecycle, the following behavior occurs:










- All expired items (Inbox or Pending) associated with the Lifecycle will be reset and regenerated based on the updated Lifecycle, if necessary
- If the Record has already completed a Phase, the Phase (and the Action that was completed for the Phase) will remain completed (the current phase always remains the same)
- If the Record's current Phase was updated, the Effective Phase and Retention Expiration Date will be reset and the Effective Phase will be reevaluated
- If the Record's current Phase is greater than the Lifecycle's range of Phases, the Record's current Phase will be reset to the last Phase to ensure that the Record is finalized. This is the only time that a Record may technically move backward in a Lifecycle and would only be caused by deleting Phases from a Lifecycle resulting in a Record's current Phase being beyond the number of Phases in the updated Lifecycle.

4.10.11.2 Editing the File Plan for new records

Often it may make sense to only allow new records to follow an update to your File Plan. Perhaps a regulation or law was changed that impacts records created day forward. Follow the following steps to ensure that new records follow a new lifecycle.

1. Close the existing Record Class. This will prevent any new records from being classified to it.


Edit Record Class ✕

Title *	<input type="text" value="Accounting and finance"/>	
Code *	<input type="text" value="ACC"/>	
Priority *	<input type="text" value="100"/>	
Description	<input type="text"/>	
Organization	<input type="text"/>	
Notes	<input type="text"/>	
Archive Records *	<input type="text" value="No"/>	
Destruction Certificates *	<input type="text" value="No"/>	
Record Declaration Rule *	<input type="text" value="Possible"/>	
Vital Rule *	<input type="text" value="Never"/>	
Expected Monthly Volume	<input type="text"/>	
Originated Date	<input type="text" value="9/3/2019"/>	
Closed Date	<input type="text"/>	
Case Based *	<input type="text" value="No"/>	
Case File Rule	<input type="text"/>	

2. Create a new Lifecycle to meet the new regulation, which may include a new Trigger and Retention as well.
3. Create a new Record Class.
4. Add the new Lifecycle to the Record Class.
5. Give the Record Class the same Priority as the Record Class just closed.
6. Create the same Classification Rules as the Record Class just closed.

4.10.12 Record Classes

The central entity that makes up the File Plan is called a Record Class. A Record Class defines a named grouping in which records can be assigned. Associated with this grouping, or Record Class is a number of properties that define more detailed information about the grouping, as well as the Lifecycle that is assigned to this Record Class.

 A Record Class named "Undefined" is created and available by default. You can't perform the typical tasks on this Record Class that you can on others (e.g., edit, delete, set lifecycles, etc.)

4.10.12.1 Creating a Record Class

To create a Record Class, perform the following steps:

1. Select **Plan** from the Main Menu.
2. Select **Record Classes** from the left navigation menu. The Record Classes page displays.
3. Click **Create**. The Create Record Class dialog opens.
4. Enter the desired Record Class Properties.

Property	Description
Title	Defines the unique name of the Record Class
Code	Defines a unique code for the Record Class
Priority	Defines the priority of this Record Class in relation to other Record Classes when Classification Rules overlap amongst multiple Record Classes (see Classification section)
Description	Defines the description of the Record Class for informational purposes
Organization	Defines the organization that owns this Record Class (i.e. Department, Region, etc)
Notes	Defines a free form field that can be used to provide detailed notes for the Record Class

Property	Description
Preserve	<p>Defines how Preservation Copies will be created. Possible values are:</p> <ul style="list-style-type: none"> a. New Versions – retain all new versions of a document, as well as the current version. b. All Versions – retain all previous versions and all new versions of a document. c. Never – retain no versions of a document. <p>NOTE – Enabling Preserve only works for items managed by the Microsoft 365 SharePoint Connector.</p>
Archive Records	<p>Defines whether the primary record data will be archived during disposition <i>Note: Version 4.0 and above</i></p>
Archive Record Properties	<p>Defines whether the record properties will be archived. This is only available if Archive Records property is set to "Yes". <i>Note: Version 4.0 and above</i></p>
Archive Record Audits	<p>Defines whether the audit trail will be archived. This is only available if the Archive Records property is set to "Yes". <i>Note: Version 4.0 and above</i></p>
Destruction Certificates	<p>Defines whether a Destruction Certificate will be generated during disposition <i>Note: Version 4.0 and above</i></p>
Record Declaration Rule	<p>Defines how items become Declared Records in the system. Possible values are:</p> <ul style="list-style-type: none"> a. Always – Items are always automatically Declared Records and cannot be Undeclared Records. b. Possible – Items are not automatically Declared Records but can be Declared either Manually or as defined by Lifecycle. c. Never – Items cannot be Declared Records. <p>It is important to understand the difference between a Record and Declared Record to understand how this property works.</p>

Property	Description
Vital Rule	Defines how items become Vital Records in the system. Possible values are: <ol style="list-style-type: none"> a. Always – Items are always automatically Declared Vital and cannot be Undeclared Vital. b. Possible – Items are not automatically Declared Vital but can be Declared either Manually or as defined by Lifecycle. c. Never – Items cannot be Declared Vital.
Expected Monthly Volume	Defines the expected monthly volume of new records into this Record Class. This property is optional.
Originated Date	Defines when the Record Class was first defined. If not provided, the creation date will be automatically used when you click Save . This can be a date in the future and will prevent classification from starting until this date
Close Date	Defines when items can no longer be associated with this Record Class. The Record Class will continue to exist and items assigned to the class will continue to be associated, but new items cannot be added. This property can also be used as a trigger for retention rules.
Case-Based	Specifies if this Record Class is Case-Based (see Case-Based Record Classes ¹⁶)
Case File Rule	Specifies how Case File titles should be automatically generated (see Case-Based Record Classes ¹⁷)

5. Click the **Create** button at the bottom of the window. The new Record Class displays on the page.

4.10.12.2 Case-Based Record Class

The Case-Based Record Class allows you to combine content together associated with a common "case" together into one record. The biggest advantage of using Case-Based Record Classes is so records associated with the case show up for disposition as a single entity, eliminating the need to approve every single file.

A Case-Based Record Class is created by changing the **Case Based** setting on a Record Class to Yes.

¹⁶ <http://docs.gimmel.com/en/2948-case-based-record-classes.html>

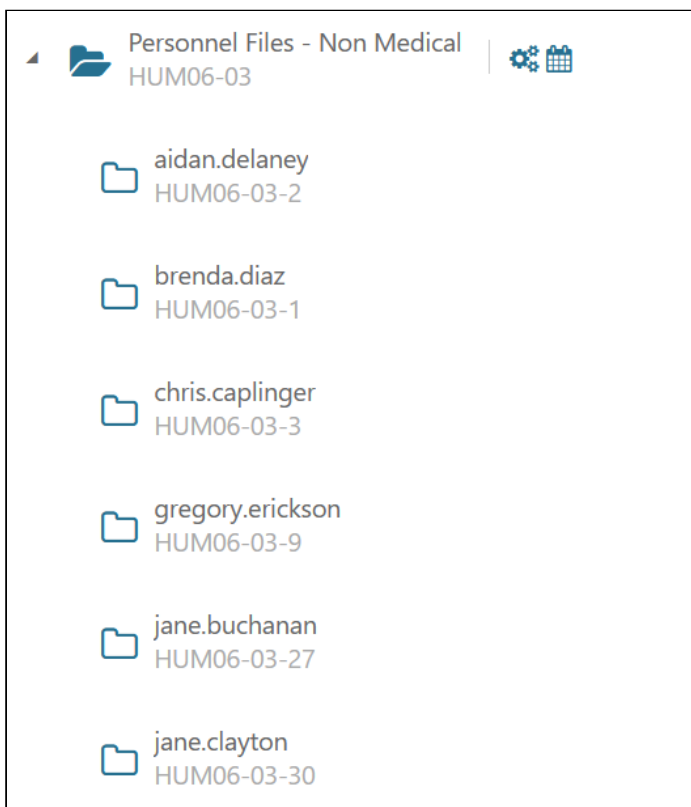
¹⁷ <http://docs.gimmel.com/en/2948-case-based-record-classes.html>

Case Based *	No
Case File Rule	Yes
	No

Case File

Case Files can be created manually or automatically (see Case File Rules) and are essentially a special type of child Record Classes. There should be a Case File for each case, which often relates back to business processes such as personnel files, projects, accounts. For example, for each employee of an organization, a Case File could be created.

The Case File is both a Record Class and a Record and contains any number of items. The Case File will be visible primarily in three places; the File Plan, Managing the records on a Record Class, and during disposition.



Case Files themselves cannot contain other Case Files. All Case Files will possess the Lifecycle of the parent Case-Based Record Class and cannot be overridden. All items that are assigned to a Case File will move concurrently through their lifecycle as a single unit, as opposed to a regular Record Class where each item moves independently through its lifecycle.

- ⚠ While Case Files are designed to work as a cohesive unit, moving them through the Lifecycle and the disposition process as a whole, it is possible that the items in the Case File move from phase to phase separately. While it would be unusual, because of the design of the software this is possible. To ensure that all items move together it is important to design a trigger that will work with all the items for a Case File in the same manner.
- Event Triggers - this is the preferred Trigger for working with a Case File. However, if the Event is based on the value of a property and items have different values, the items may not move through the lifecycle together.
 - Date Property Triggers - be very careful when using date properties as the triggers as it is likely that none of the items will have consistent dates causing the records to move through the lifecycle separately.
 - Rule Triggers - If a Rule Trigger is used, we recommend using a rule that uses a similar rule as the Case File Rule in order to ensure the items move through the lifecycle together.

Case File Rule

When configuring Case-Based Record Classes, it is possible to specify a Case File Rule that enables Case Files to be automatically generated and for items to be automatically assigned to a Case File. If a Case Files Rule is not specified, items will need to be manually assigned to their appropriate Case File and the Case Files themselves will need to be created manually or generated using the API.

A Case File Rule is an expression - that will be evaluated against an item's properties to determine how to assign an item to a Case File and if the Case File does not exist, automatically create it.

To specify a Case File Rule, simply enter a string into the Case File Rules using brackets to specify where the value of an item's metadata should be substituted. It is possible to use any number of substitution expressions in a single Case File Rule.

- Single expression example: "Employee [EmployeeID]"
- Dual expression example: "Employee [firstname].[lastname]"

The output of the Case File Rule evaluation will determine the name of the Case File to be generated and all items that produce the same resulting output will be assigned to the same Case File. In the single expression example above, if the EmployeeID was "1234", then the name of the Case File would be "EmployeeID 1234". In the dual expression example, if the employees name was "John Doe", and both the firstname and lastname where represented properties, then the name of the Case File would be "Employee John.Doe".

4.10.12.3 Classification

Classification is the process by which content in a Repository gets associated to a Record Class. Classification can be performed both manually and automatically.

Manual Classification

Manual Classification is accomplished by a user selecting an item within a Repository and manually choosing a Record Class in which the document should be assigned.

Automatic Classification

Automatic Classification is accomplished by specifying a set of Classification Rules, which are simple expressions that define to which Record Class an item within a repository should be assigned.

When an item is added or updated within a Repository, the Connector notifies Information Lifecycle, which in turn evaluates the properties of an item against the Classification Rules and assigns the item to the appropriate Record Class. If multiple matches are found due to overlapping Classification Rules, the Record Class with the highest priority is assigned.

i A higher priority is indicated by a lower numeric value (ex. 1 > 10). Think of this priority as a ranking system, where number 1 would be the highest-ranking (i.e. highest priority), followed by number 2, number 3, and so on.

Creating Classification Rules

1. Select **Plan** from the Main Menu.
2. Select **Record Classes** from the left Navigation Menu.
3. Click the drop-down for the desired Record Class.
4. Select the **Classification Rules** option to open the Classification Rules dialog.
5. Click **Create** to create the Classification Rules. The [Rule Builder page](#)(see page 125) describes the process of creating rules.
6. Click **Save**.

Unclassified Items and the Undefined Record Class

As items are recordized into the system, not all items will be assigned a Record Class. This occurs because no Record Class was assigned through manual classification or it did not match any rules specified for automatic classification. When this happens, the system automatically assigns these items to a built-in Record Class called the Undefined Record Class which represents the absence of a Record Class.

The Undefined Record cannot be assigned a Lifecycle, so items that are assigned to this Record Class will never be disposed. The benefit of items being assigned to the Undefined Record Class is that it allows reports to be generated which help to visualize and identify those items which are essentially not being managed and improves a Records Manager's ability to discover areas where they must broaden the scope of their management efforts.

About Rule Evaluations

When Classification Rules are evaluated for a repository item, if the result of the evaluation is True, then the item will be assigned to the Record Class. If the result is False, then the Record Class is not assigned. The following example demonstrates this.

Classification Rules ✕

Clear

▼

Add Rule Set

Property	Operator	Value	Data Type	Join	
<input type="text" value="@sp.contenttype"/>	= ▼	<input type="text" value="Invoice"/>	Text ▼	Or ▼	✕
<input type="text" value="@sp.contenttype"/>	= ▼	<input type="text" value="PO"/>	Text ▼	None ▼	✕

Save
Cancel

If an item in the Repository has the following properties:

- Title: PO 12345
- Content Type: PO

When the Classification Rules are evaluated, the following expression result will look like the following, since this results in a value of True, the item will be assigned to the Record Class.:

- “Content Type = Invoice” = FALSE Or “Content Type = PO” = TRUE

4.10.12.4 Lifecycles and Record Classes

Assigning a Lifecycle to a Record Class

To assign or remove a Lifecycle to a Record Class, perform the following steps:

1. Select **Plan** from the Main Menu.
2. Select **Record Classes** from the left Navigation Menu.
3. Click the drop-down for the desired Record Class.
4. Click **Lifecycle**.
5. Choose the desired Lifecycle from the drop-down list to assign.
6. Click **Save**.

The screenshot shows a modal window titled "Lifecycle" with a close button (X) in the top right corner. Below the title bar is a breadcrumb path: "/ Accounting / Accounts Payable". The main content area displays "Record Class" as "Accounts Payable ACC-10". Below this, the "Lifecycle" field is a dropdown menu currently showing "Accounts Payable" with a downward arrow. Underneath the dropdown is the text "* Unique Lifecycle". At the bottom of the configuration area is a button labeled "Revert To Parent" with a circular arrow icon. At the bottom right of the modal are two buttons: "Save" (in a dark blue box) and "Cancel" (in a light grey box).

Lifecycle Inheritance

Record Classes support Lifecycle inheritance. When a Lifecycle is assigned to a Record Class, the Lifecycle is propagated to all child Record Classes. However, once a Lifecycle is changed for a specific Record Class, the inheritance chain is broken and the Lifecycle will no longer be propagated to that child if the parent’s Lifecycle is changed.

In order to re-enable Lifecycle inheritance, you must open the Lifecycle Selection dialog for a specific Record Class and click the **Revert to Parent** button, which will propagate the parent’s Lifecycle back down.

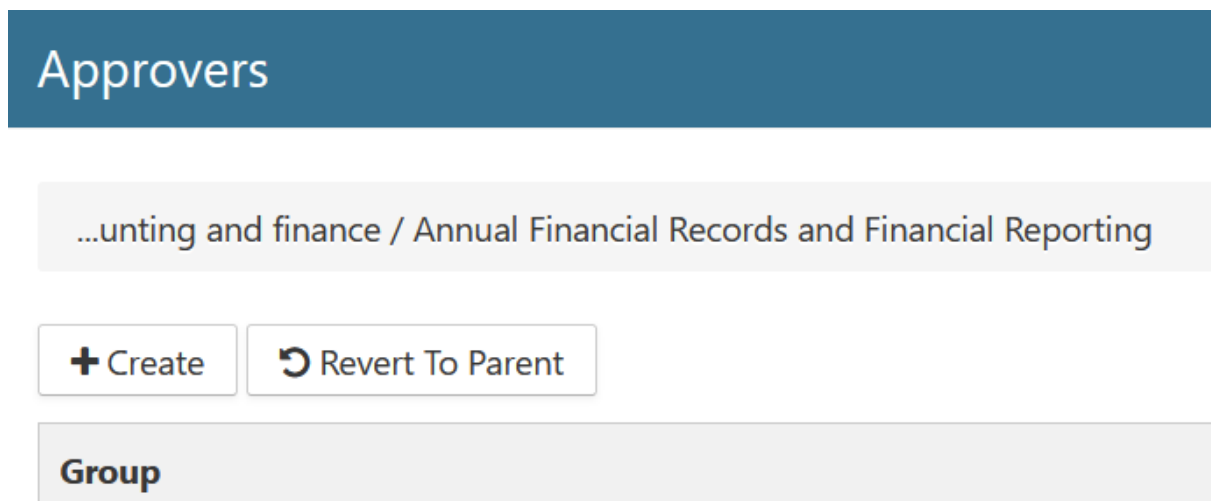
4.10.12.5 Approvers

Records Classes can be assigned groups of approvers that represent the users that are required to approve retention action in the Action Items Inbox. A Record Class can define multiple approver groups, and each group can be assigned multiple users. For a retention action to be approved for an item, all groups must approve the retention action. However, only a single user in each group is necessary to approve the item for that group.

Approver Inheritance

Record Classes support Approver inheritance. When Approvers are assigned to a Record Class, the Approvers are propagated to all child Record Classes. However, once Approvers are changed for a specific Record Class, the inheritance chain is broken and the Approvers will no longer be propagated to that child if the parent’s Approvers are changed.

To re-enable Approver inheritance, you must open the Approvers selection dialog for a specific Record Class and click the **Revert to Parent** button, which will propagate the parent’s Approval Groups back down.

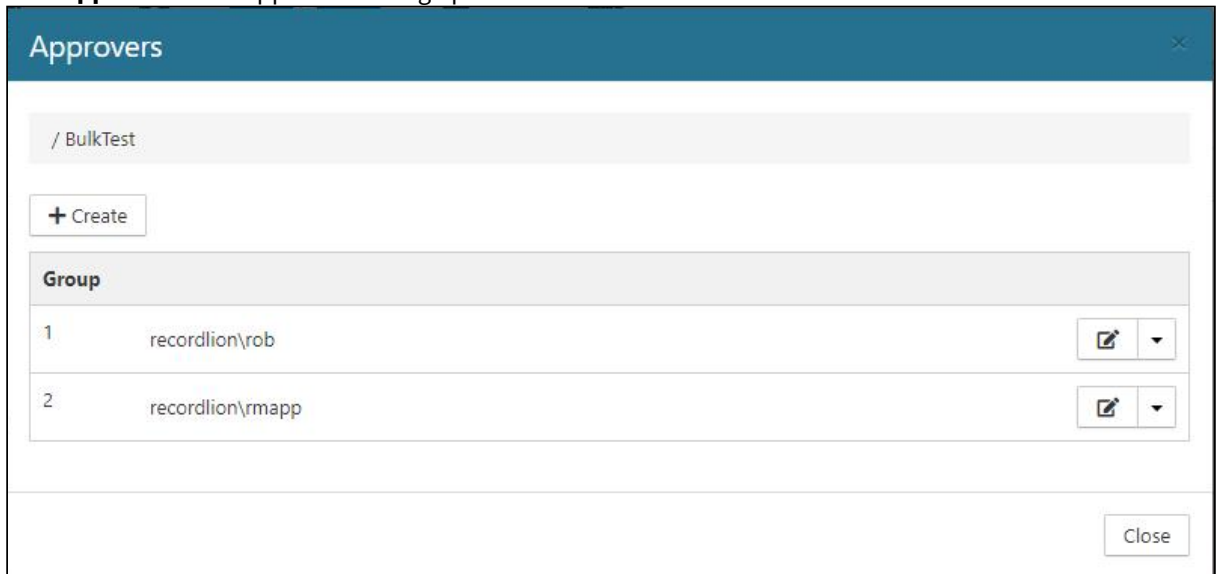


Defining Approver groups

To define groups, perform the following steps:

1. Select **Plan** from the Main Menu.
2. Select **Record Classes** from the left Navigation Menu.
3. Click the drop-down for the desired Record Class.

4. Click **Approvers**. The Approvers dialog opens.

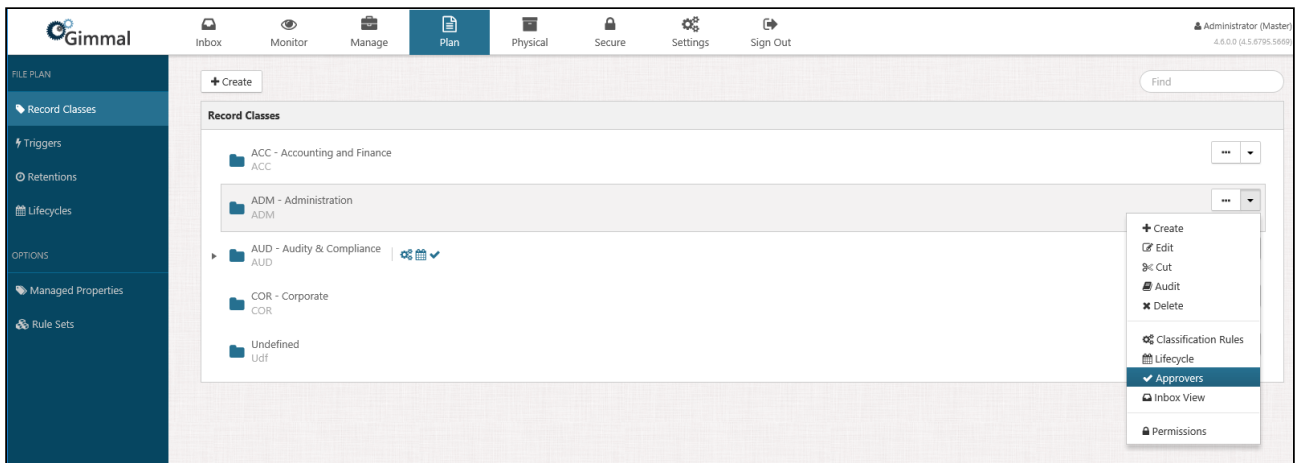


5. Click **Create**.
6. Select a User or Group, and then click **Add** (Repeat for each user in the group).
7. Click **Close**.
8. Repeat Steps 6 and 7 to define more groups.

Viewing an Item's Approvals

After an item has been approved, it is possible to view the users who have already approved the item and how many approvals are required. In the example below, two approvals are required and one has already been completed.

1. Select **Inbox** from Main Menu.
2. Select **Action Items** from the left Navigation Menu.
3. Select the drop-down for the desired Action Item.
4. Select **Approvals**.



Approvals		
Group	Approval Date	User
1	9/28/2021 4:17:41 PM	RECORDLION\rob
2		

Close

4.10.12.6 Inbox View

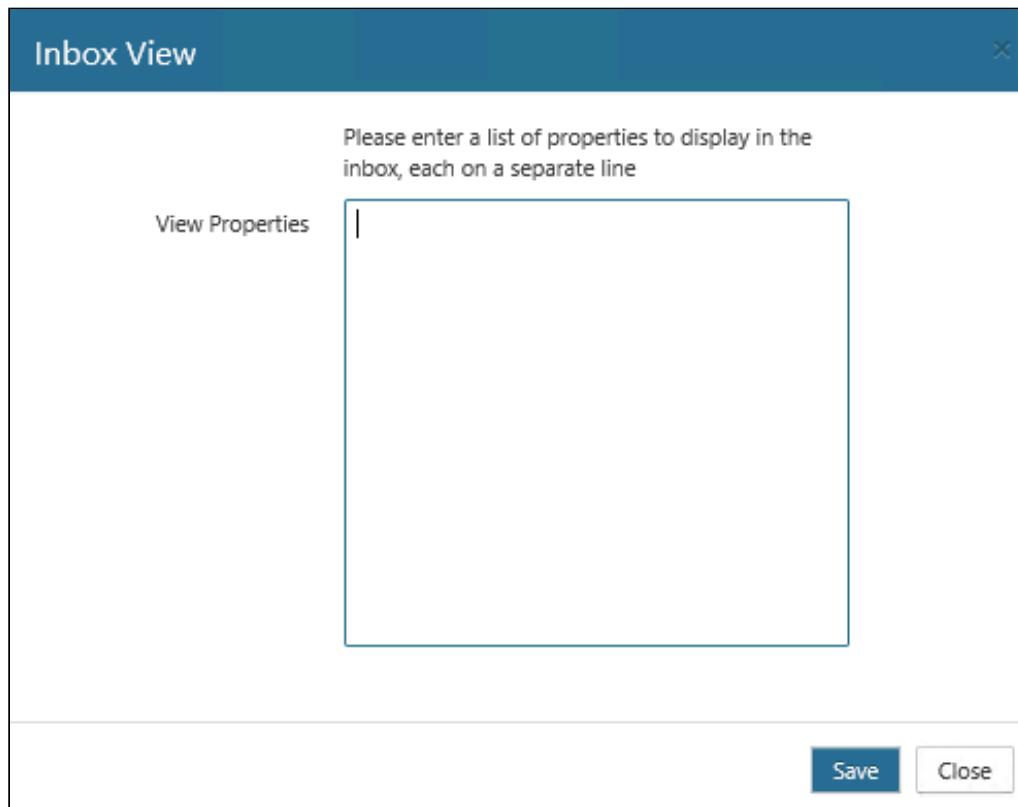
- ⚠ It is no longer recommended to use the Inbox View on a Record Class and may be deprecated in the future. The system now has the ability for users to create their own views using either global or user configured properties. See the following topics for using personal views and configuring properties:
- [User Preferences](#)(see page 218)
 - [Global Preferences](#)(see page 213)
 - [Inbox](#)(see page 21)

The Inbox View enables you to create a customized view that can be used in the Inbox. The view is specific to a Record Class. This enables you to view all Action Items for a specific Record Class, and to specify which properties should be shown in the view.

The view is accessible from the Action Items Inbox. See the (Link) Views topic for more information.

To create an Inbox View, perform the following steps:

1. Select **Plan** from the Main Menu.
2. Select **Record Classes** from the left Navigation Menu.
3. Click the drop-down for the desired Record Class.
4. Click **Inbox View**. The Inbox View dialog opens.



Inbox View

Please enter a list of properties to display in the inbox, each on a separate line

View Properties

Save Close

5. Enter the Properties that should be shown in the view. The following example shows three properties that will be included in the view. To see the available properties for a Record, perform these steps:
 - Click **Manage** from the main menu
 - Click **Records** from the left Navigation Menu.
 - Click the drop-down for the desired Record.
 - Select **Properties**.
6. Click **Save**

Inbox View ✕

Please enter a list of properties to display in the inbox, each on a separate line

View Properties

```
ContractNumber  
DeliverOrder  
ProposalNumber
```

4.11 Manage

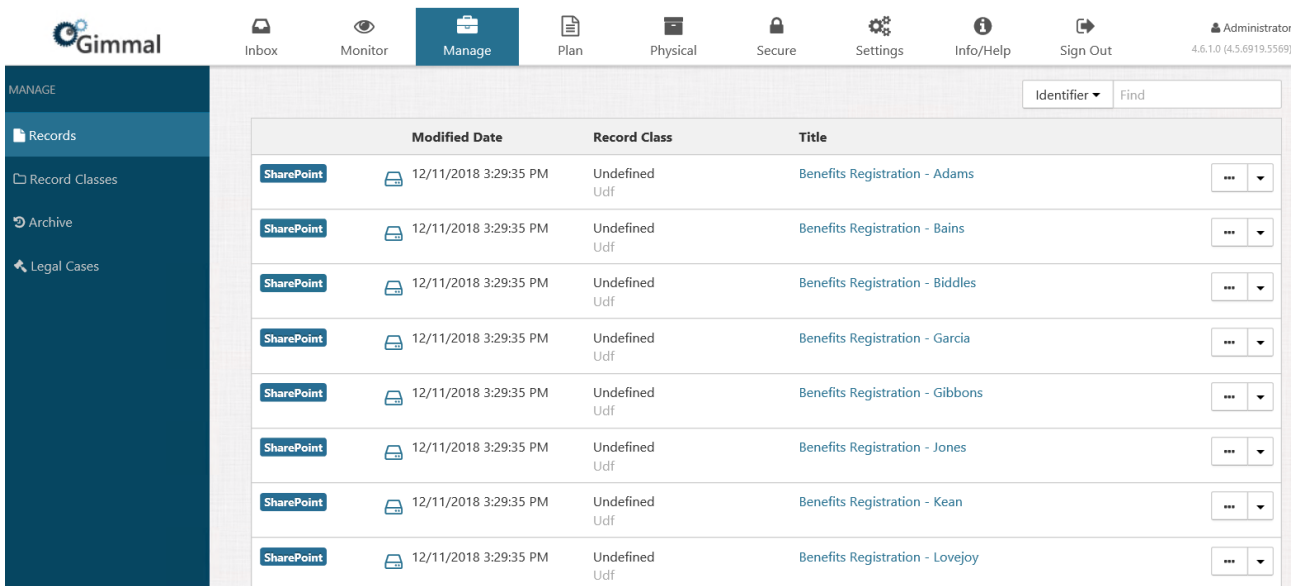
4.11.1 [Manage Records 1](#)

4.11.2 [Manage Record Classes](#)

4.11.3 Manage Records 1

The **Records** option, available under **Manage** on the Main Menu, provides access to all Records that are being managed by Records Management.

From this section, you can view the Record Details, perform declaration functions, manually place an item on Legal Hold, and manually classify an item as a particular Record Class.



4.11.3.1 Viewing Record Details

The Record Details screen provides detailed information pertaining to an Individual Record. From this screen, you can see what Record Class an item has been assigned, where the item is in its Lifecycle, its declaration status, as well as any Legal Holds that may exist on the item.

To view the details of a Record, perform the following steps:

1. Select Manage from the Main Menu.
2. Select Records from the left Navigation Menu.
3. Click the ellipsis (...) for the desired Record. The Record Details screen displays, as shown below.

Record Details ×

Title	Record Class
test1	Accounting and finance ACC
Identifier	
ee61b86b-d578-420f-8858-a8ccfe3c5385	
Type	
Physical	
URI	
https://dev.recordlion.net:443/pam/6b2a45bb-841b-ea11-add2-501ac5124850	

Lifecycle
Accidents and Injuries Lifecycle

Current Phase

1. Declare + 6 Year(s) >> Automatic Dispose and Delete (Approval)

Registered Date 12/10/2019 7:41:02 PM
Updated Date 12/10/2019 7:41:02 PM

Close

4.11.3.2 Manually Classifying a Record

To manually assign a Record to a specific Record Class, perform the following steps:

1. Select **Manage** from the Main Menu.
2. Select **Records** from the left Navigation Menu.
3. Click the drop-down for the desired Record.
4. Select **Classify**.
5. Choose the desired Record Class.
6. Click **Save**.


4.11.3.3 Declaring & Undeclaring Different Types of Records

1. Select **Manage** from the Main Menu.
2. Select **Records** from the left Navigation Menu.
3. Click the drop-down for the desired Record.
4. Select one of the following:
 - Declare Record
 - Undeclare Record
 - Declare Vital
 - Undeclare Vital
 - Declare Obsolete
 - Declare Superseded
5. Click **Confirm**.

4.11.3.4 Creating a Legal Hold Manually

To create a Legal Hold on an item manually, perform the following steps:


1. Select **Manage** from the Main Menu.
2. Select **Records** from the left navigation menu.
3. Click the drop-down for the desired Record. (The drop-down options you see may vary, depending on your permissions.)
4. Select **Legal Hold**.
5. Select the appropriate Legal Case from the drop-down.
6. Click **Confirm**.

 Only legal cases that are created and open are available for holding new items.

4.11.3.5 Viewing the Record Audit

To view the Audit Log for an individual item, perform the following steps:

1. Select **Manage** from the Main Menu.
2. Select **Records** from the left navigation menu. A list of records displays on the page.
3. Click the drop-down to the right of the desired Record. (The drop-down options you see may vary, depending on your permissions.)
4. Select **Audit**. The Audit window opens for the selected Record, showing a time-stamped list of all of the operations performed on that Record.

 To search for a specific audit log entry, enter a keyword(s) in the **Find** field in the upper right corner.



4.11.3.6 Viewing the Record Properties

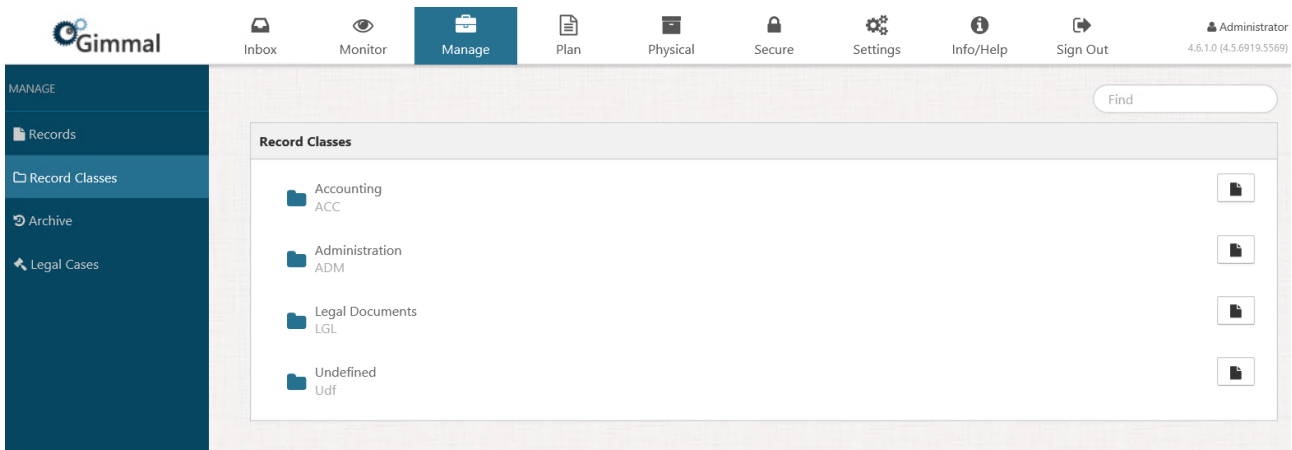
To view the Properties for an individual item, perform the following steps:

1. Select **Manage** from the Main Menu.
2. Select **Records** from the left Navigation Menu.
3. Click the drop-down for the desired Record.
4. Select **Properties**. The Record Properties dialog opens, enabling you to view all of the properties for that record.
5. Click **Close** to close the dialog.

4.11.4 Manage Record Classes

The Record Classes option in the left Navigation menu provides a list of the records being managed. The list is organized by Record Class, and the Record icon to the right of the Record Class name enables you to view all of the records associated with a Record Class.

To view the Records associated with a Record Class, click the **Record** icon to the right of the Record Class name.



Record Class Records

Find

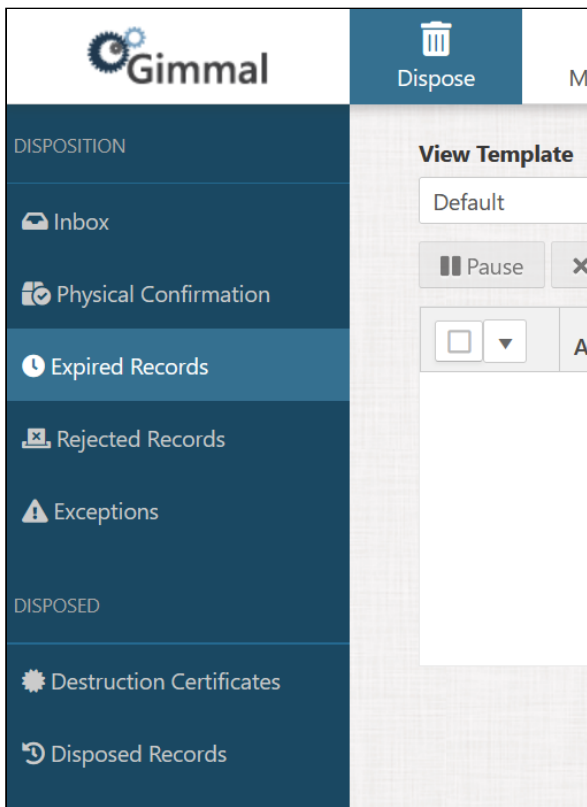
	Modified Date	Record Class	Title	
SharePoint	5/11/2016 4:38:19 PM	Accounts Payable ACC-10	\$PC210C1001_103114_10038	...
SharePoint	5/11/2016 4:38:19 PM	Accounts Payable ACC-10	\$PC210R1002_110314_10020	...
SharePoint	5/11/2016 4:38:19 PM	Accounts Payable ACC-10	\$PC210R1002_112414_10006	...
SharePoint	5/11/2016 4:38:19 PM	Accounts Payable ACC-10	\$PC210R1002_121814_10003	...
SharePoint	5/4/2016 10:59:05 AM	Accounts Payable ACC-10	\$PC210R1002_121914_10006	...

Page 1 of 59 (294 Items)

Close

4.12 Disposition

Disposition is an area of the system where you go for anything related to disposing of records that have expired in their lifecycle. As a Record Manager you will be able to see all items that have expired, as well as rejected records, destruction certificates, and information about the records that have previously been disposed of. To access this section, click on Dispose from the Main Menu.



The following topics are available on disposition.

- [Disposing Physical Assets](#)(see page 107)
- [Expired Records](#)(see page 109)
- [Rejected Records](#)(see page 110)
- [Legal Holds and Reclassification During Disposition](#)(see page 112)
- [Exceptions](#)(see page 114)
- [Disposed Records](#)(see page 115)

4.12.1 Disposing Physical Assets

A physical record, like electronic records, need to be disposed at the end of their lifecycle. Unlike electronic records, physical records need to be destroyed by a manual act, regardless of whether that is done by your organization or a third party storage/shredding service.

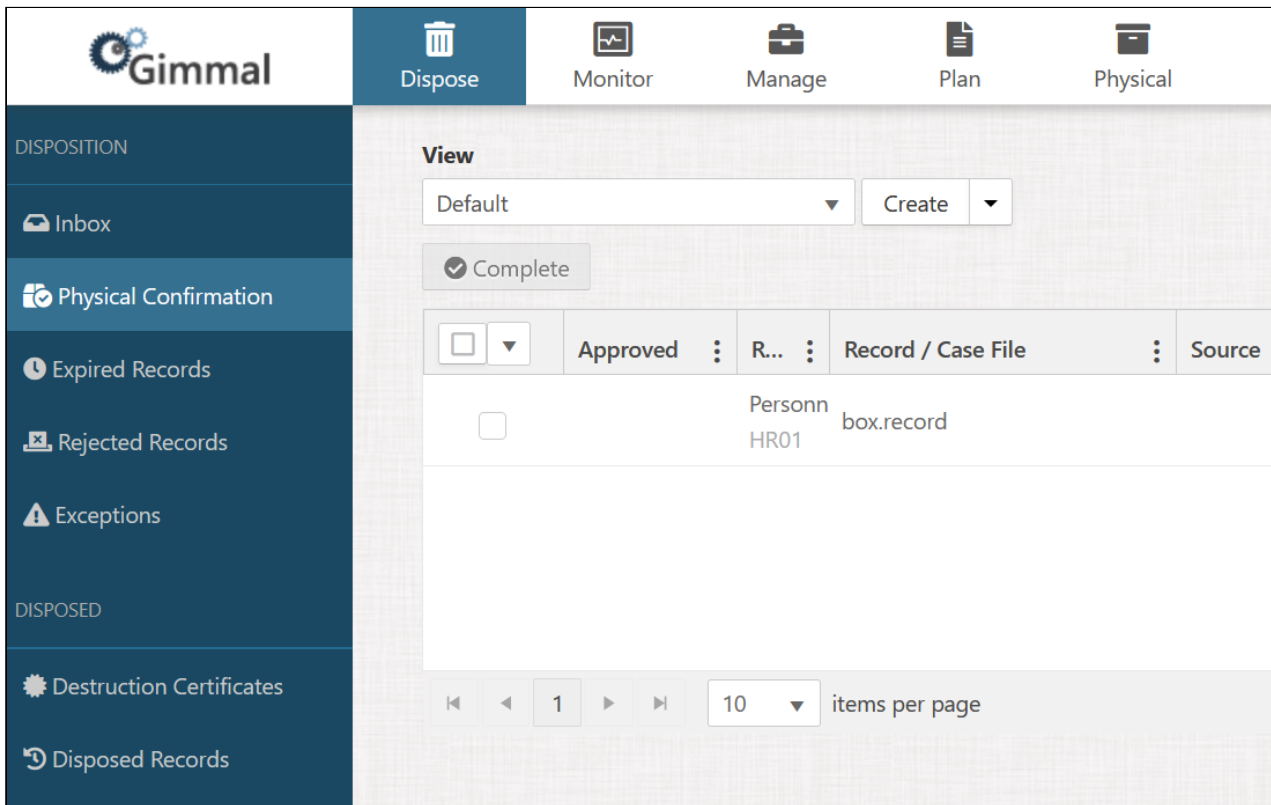
4.12.1.1 Approving Physical Records

If the final phase of a physical record is configured to be approved, then the asset will go through the same process as an electronic record. The same rules apply, from record filters to approval groups. Once a physical record is approved and submitted, it will still require manual intervention to complete its disposition process.

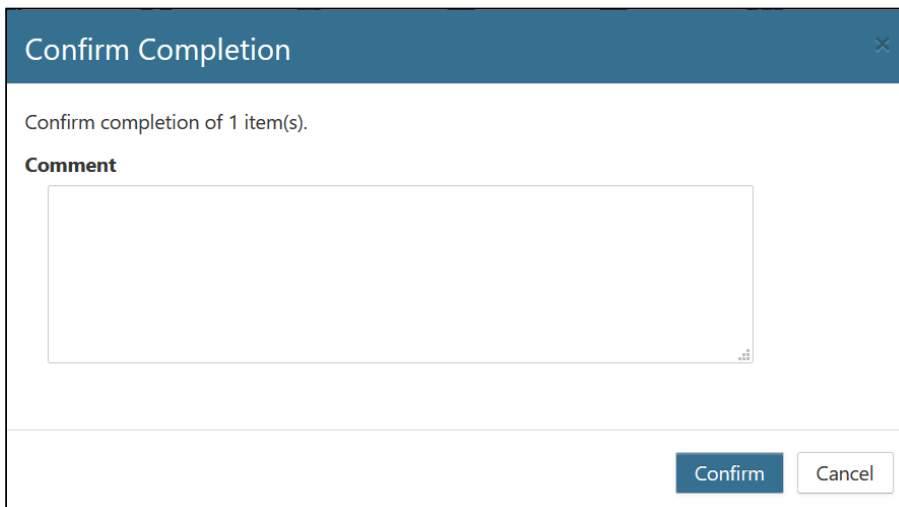
4.12.1.2 Confirming Physical Disposition

Once the asset has been submitted for disposition, it will create a task in the Physical Confirmation area to be manually completed by a records manager. Goto **Dispose** → **Physical Confirmation** to see the Physical Confirmation area.

The Physical Confirmation area is only available for the System Admin, Global Record Manager, and Record Manager roles.



Once there is proof that the asset has been properly disposed of, your organization's record manager will need to confirm it's completion. One or more confirmations can be completed at one time by selecting the checkboxes in the leftmost column of each record. Clicking Complete will display a confirmation window in which you can comment and confirm that the physical record has been destroyed.

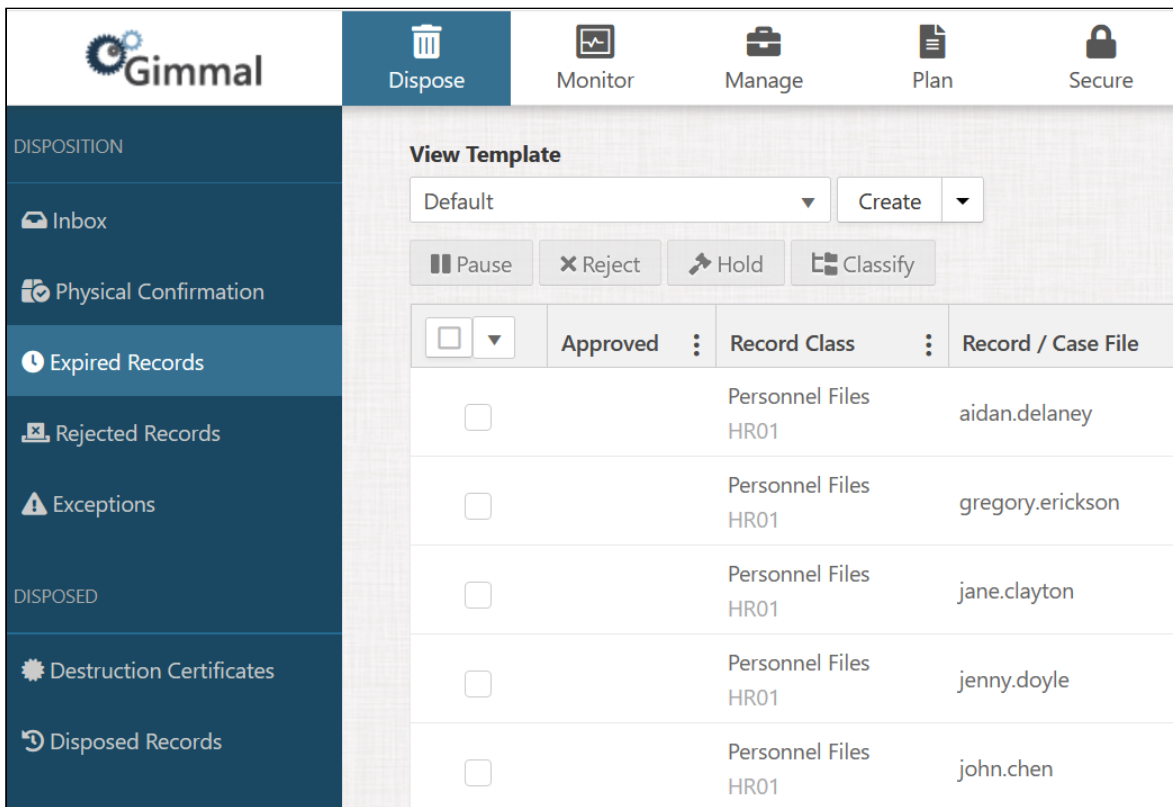


The image shows a 'Confirm Completion' dialog box. It has a dark blue header with the title 'Confirm Completion' and a close button (X) in the top right corner. Below the header, the text reads 'Confirm completion of 1 item(s)'. Underneath, there is a section labeled 'Comment' with a large, empty text input area. At the bottom of the dialog, there are two buttons: 'Confirm' (a dark blue button) and 'Cancel' (a light gray button).

4.12.2 Expired Records

As a Record Manager (or higher role), you may have times when you want to see every item in the system that has reached the end of its lifecycle and is ready for the disposition process. **Expired Records** from **Dispose** allows you to view all Expired Records that have not been filtered from you. Several actions are available from **Expired Records**.

- You can pause records so they are removed from disposition approval for the length of time configured in the Lifecycle.
- You can reject records so they are removed from disposition for an indefinite period of time.
- You can place records on Legal hold.
- You can reclassify records if they were initially classified to the wrong Record Class.
- You can view approvals that have already been submitted.

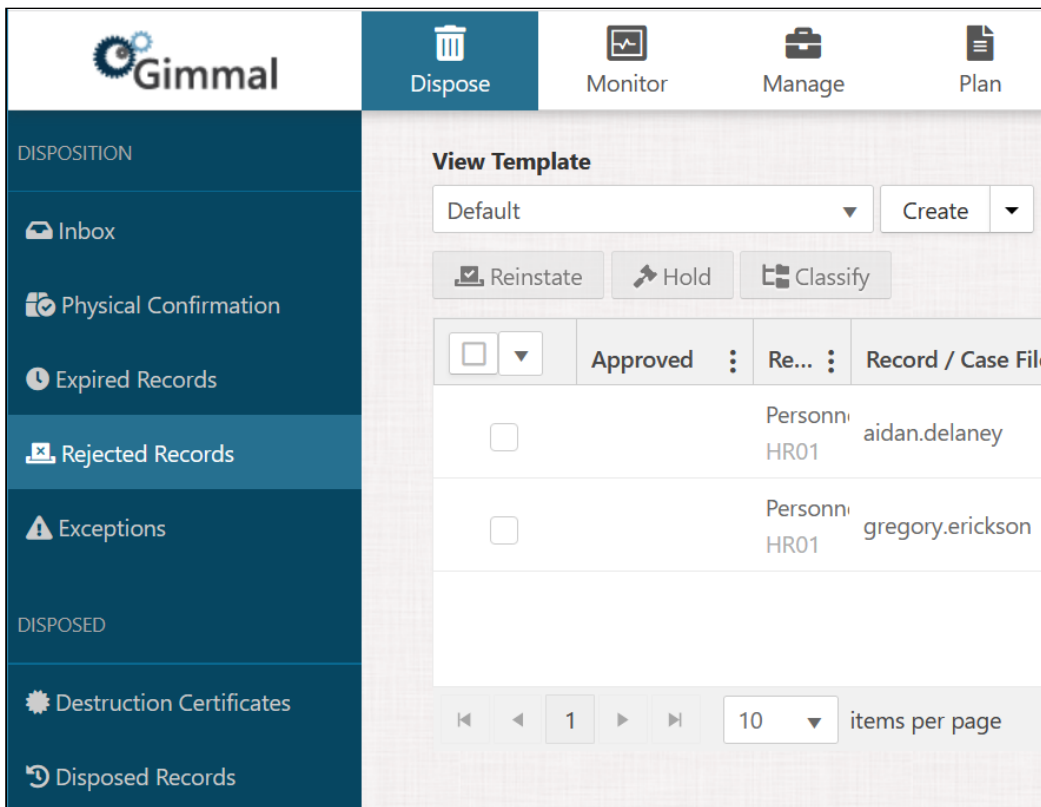


4.12.3 Rejected Records

Rejected Records are the area that records that have been rejected are viewed. You will be able to see a rejected record if any of the following are true:

- You have the System Admin or Global Record Manager role
- You have the Record Manager role and the record is not filtered from you
- You have the User role and are part of the approval group that rejected the record

To access Rejected Records, goto Dispose → Rejected Records.

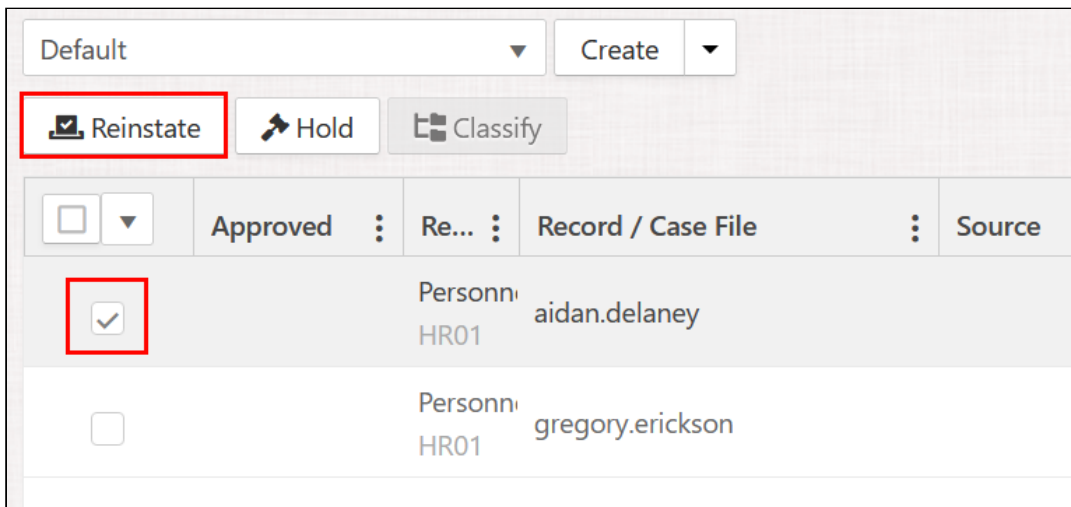


4.12.3.1 Hold and Classify

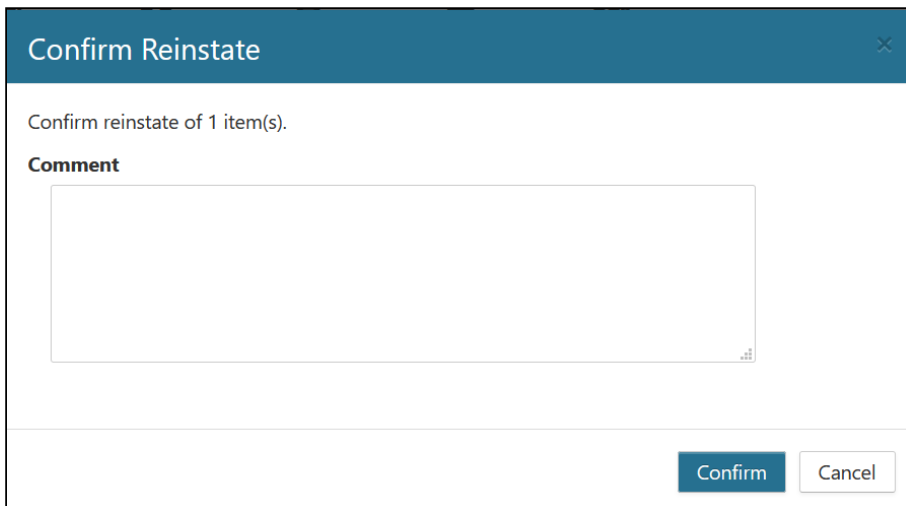
If you have the System Admin, Global Record Manager, or Record Manager role, you can place a record on legal hold or reclassify it.

4.12.3.2 Reinstating Records

In order to submit records for disposition, they must be first reinstated. Anyone with access to the record in Rejected Records will be able to reinstate it. To reinstate, select the necessary records and click the Reinstate button.



You will be prompted to confirm the reinstatement and give a reason.



4.12.4 Legal Holds and Reclassification During Disposition

Users with the Record Manager role or higher can place items on hold or reclassify during the disposition process. These options are available in the Inbox, Expired Records, and Rejected Records.

The screenshot shows a software interface with a top navigation bar containing a dropdown menu set to 'Default' and a 'Create' button. Below this is a row of action buttons: 'Pause', 'Reject', 'Hold', and 'Classify'. The 'Hold' button is highlighted with a red rectangular box. Below the buttons is a table with three columns: 'Approved', 'Record / Case File', and 'Source'. The table contains three rows of data:

<input type="checkbox"/>	Approved	Record / Case File	Source
<input type="checkbox"/>	✓	jane.clayton	
<input type="checkbox"/>	✓	jenny.doyle	
<input type="checkbox"/>		john.chen	

4.12.4.1 Legal Hold

When the **Hold** button is selected, a list of available open legal cases are displayed.

The screenshot shows a dialog box titled 'Create Legal Holds' with a close button (X) in the top right corner. The text inside the dialog reads 'Create Legal Holds for 1 item(s)'. Below this is a section labeled 'Legal Case' with a dropdown menu showing 'Kramer vs Kramer'. At the bottom right of the dialog are two buttons: 'Confirm' and 'Cancel'.

Select a legal case and click the Confirm button.

4.12.4.2 Reclassify

Only individual records are available to be classified. If a case record is selected, the **Classify** button will be disabled. If both individual and case records are selected, the **Classify** button will also be disabled.

When the **Classify** button is selected, a list of Record Classes will be displayed.



The screenshot shows a dialog box titled "Classify" with a close button in the top right corner. The main content area contains the text "Reclassify 1 item(s)." followed by a label "Record Class *" and a dropdown menu. The dropdown menu currently displays "Automatic". At the bottom right of the dialog, there are two buttons: "Confirm" and "Cancel".

The first item in the list is Automatic, and while not a Record Class, if selected the records will revert back to the Classification rules to determine which Record Class should be assigned to them.

The other special Record Class in the list is called Undefined. If selected, the records will become unassigned to any particular class and will no longer have a lifecycle, thus they will no longer be managed, and will never expire.

Selecting a Record Class defined by your organization will start the records at the beginning of the lifecycle associated with the Record Class. These records could still meet the requirements for being expired, and therefore be eligible for disposition again. However, if a rejected record is reclassified, it will no longer be considered rejected.

4.12.5 Exceptions

The Exceptions area is used to show a list of anomalies that may happen during the disposition process. If for some reason the connectors are not able to reconcile a disposition action, an exception will be shown in this area. These reasons could be:

- A connector did not have the appropriate permission to take the necessary action. This is often the case when a connector was not configured with permission to move or delete a file.
- The file could not be found by the connector. While the connectors are designed to reconcile when records may exist in the system, but the associated content is no longer available, it is possible for this to happen given the right circumstances.

4.12.5.1 Retry Automation


There are two options available when an exception happens; retry or complete. Retry Automation will remove the exception and inform the connector to try the action again.

Before retrying, you should work with the owner or administrator of the content to try and understand why the connector failed to complete the action. Typically this is a permission issue of some type, however, some data sources may have the ability to lock the content in a way that blocks a connector from taking action

4.12.5.2 Complete

Complete will remove the exception and take no further action.

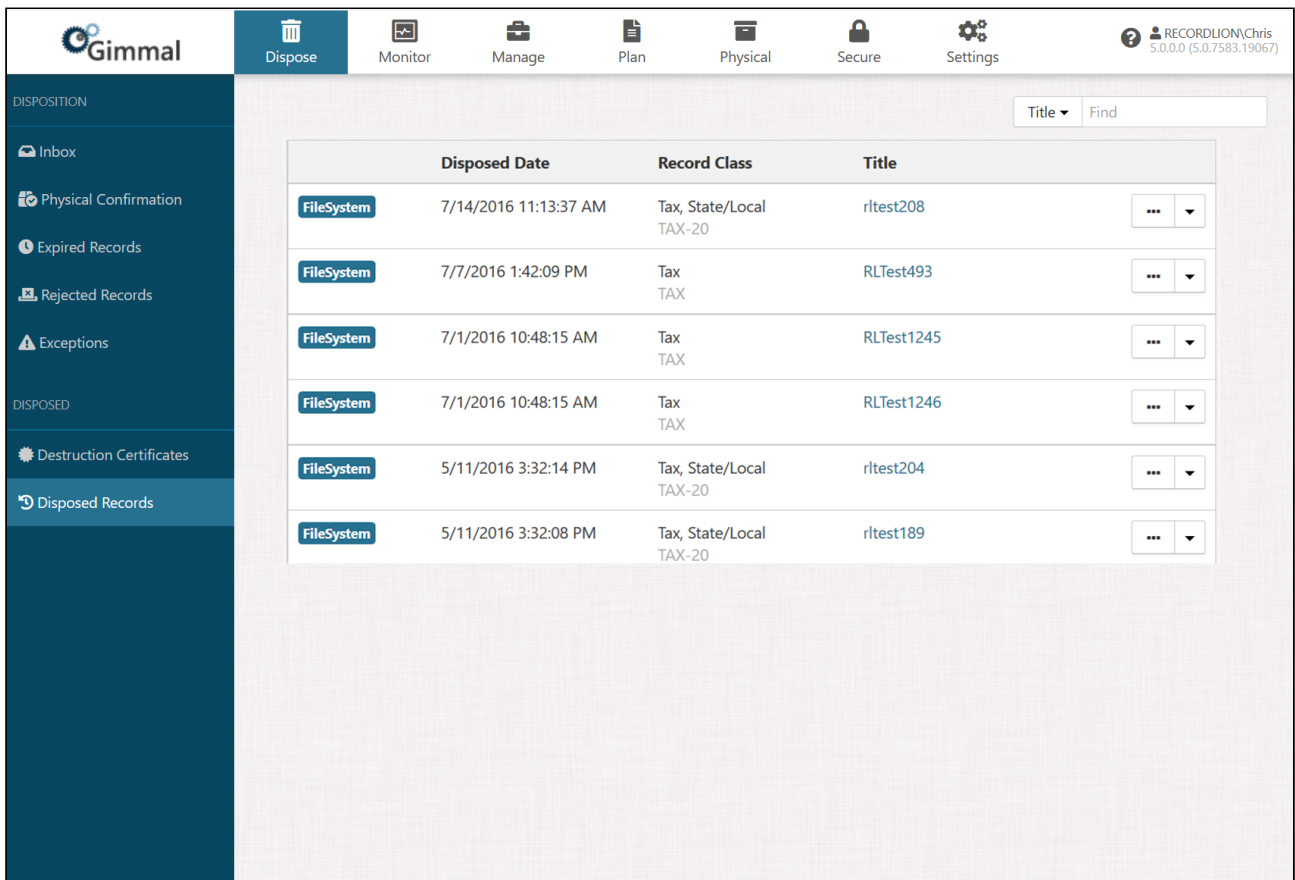
4.12.6 Disposed Records

 In previous versions, this feature was known as Archived Records.

Disposed Records is a location that contains information about all records specified to be archived according to their Record Class. Record data (details) will be present for every item, while the Properties and Audit Trail are optional, again determined by the setting on their Record Class. Disposed Records does not store the content of the record, just potentially the properties and audit trail.

Items in the Archive are still counted against the total record count for the purposes of your license. The Archive does not currently have a separate retention period. To start keeping information about records that have been disposed of, use the Archive settings on the Record Class itself by editing the Record Class.

To view **Disposed Records**, goto **Dispose** → **Disposed Records**.



	Disposed Date	Record Class	Title	
FileSystem	7/14/2016 11:13:37 AM	Tax, State/Local TAX-20	rltest208	...
FileSystem	7/7/2016 1:42:09 PM	Tax TAX	RLTest493	...
FileSystem	7/1/2016 10:48:15 AM	Tax TAX	RLTest1245	...
FileSystem	7/1/2016 10:48:15 AM	Tax TAX	RLTest1246	...
FileSystem	5/11/2016 3:32:14 PM	Tax, State/Local TAX-20	rltest204	...
FileSystem	5/11/2016 3:32:08 PM	Tax, State/Local TAX-20	rltest189	...

To see the details about an item, perform the following steps:

1. Select the ellipsis (...) to the right of an item to view Record data (details).
2. Click the drop-down menu to see the Audit Trail and Properties at the time of disposition and the Destruction Certificate, if one exists.

4.13 Monitor

4.13.1 Dashboard

4.13.2 Reports

4.13.3 Destruction Certificates

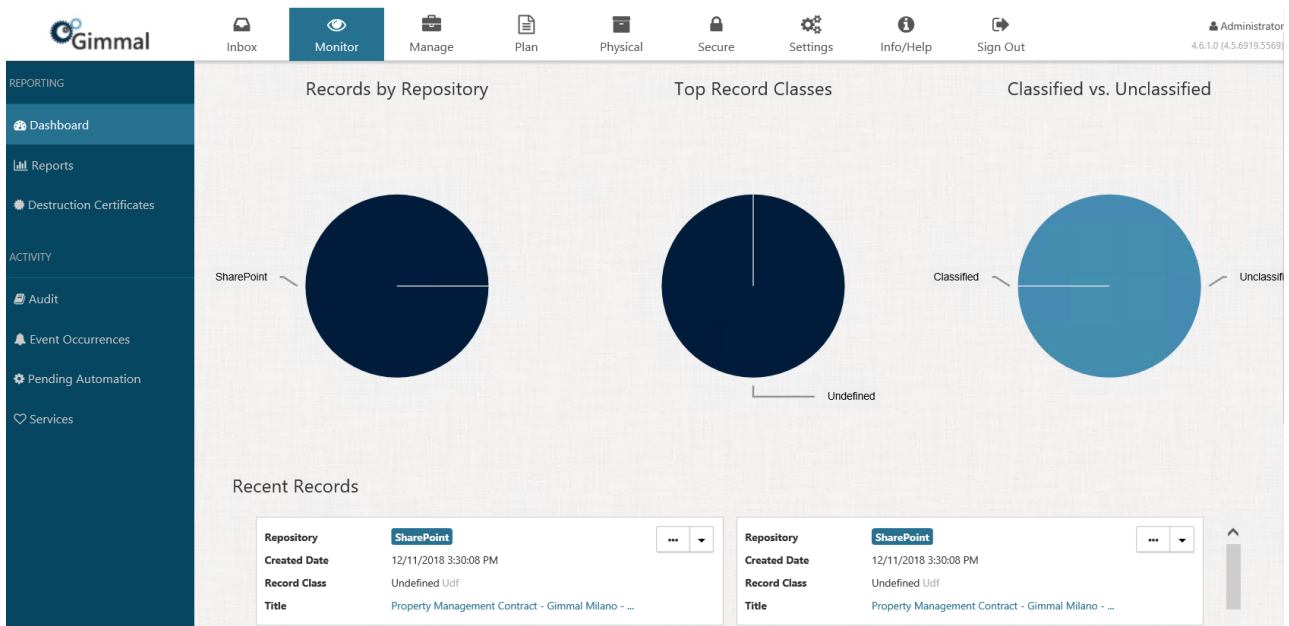
4.13.4 Audit

4.13.5 Event Occurrences

4.13.6 Pending Automation

4.13.7 Dashboard

The Dashboard option, available from the left Navigation Menu, provides a set of Key Performance Indicators (KPI). As shown below, these KPIs provide detailed information and statistics about your Information Lifecycle records.

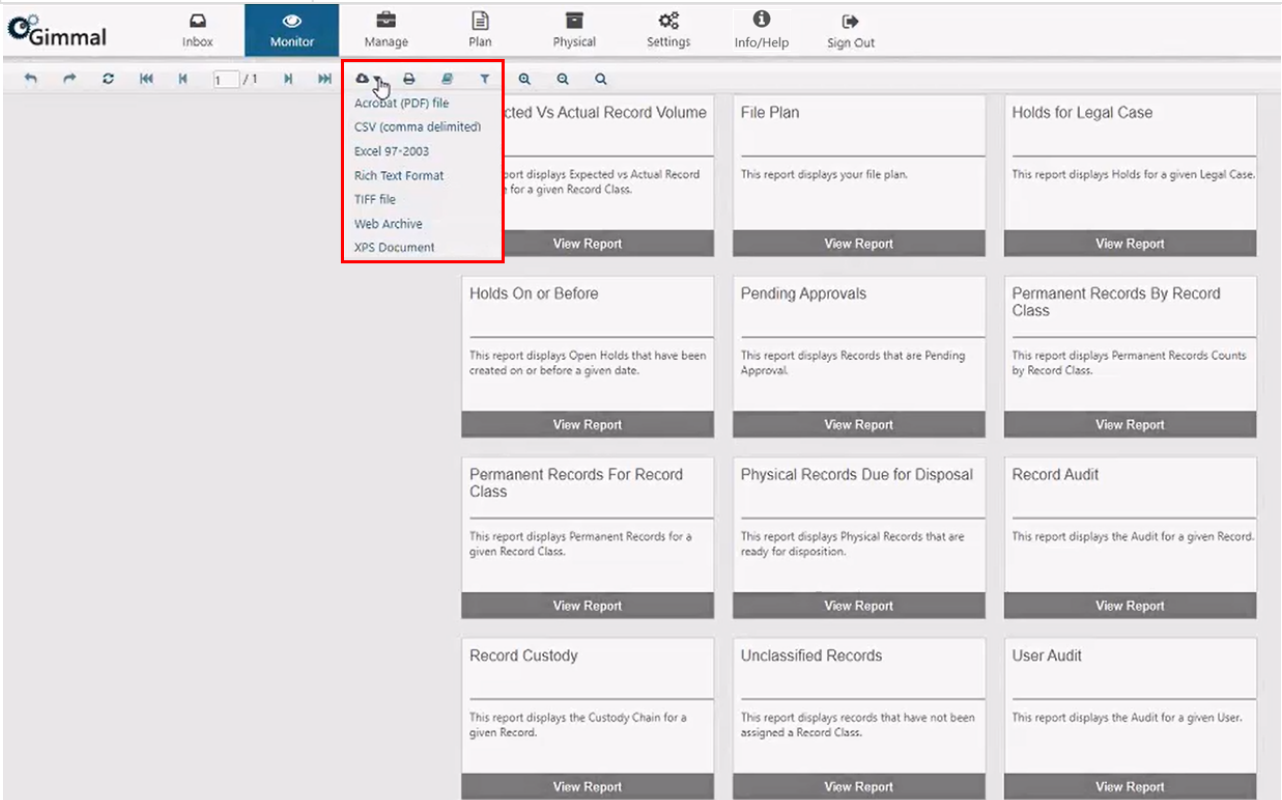


4.13.8 Reports

The Reports option, available from the left Navigation menu, provides a set of Reports that provide a picture of overall compliance and system activity. The following pre-configured reports are available:

Report	Description
Approaching Phase Expiration	Displays Phases that are approaching expiration for a given date organized by Record Class and Action
Approaching Phase Expiration for Record Class	Displays records approaching expiration for a given date and Record Class
Case Discrepancies	Displays Records that are assigned a Case-Based Record Class but have not been placed into a Case Record
Classification Rules	Organized view of the rules that classify content into record classes
Destruction Certificate	Shows archived records for a selected Destruction Certificate
Expected Vs Actual Record Volume	Displays Expected vs Actual Record Volume for a given Record Class
File Plan	Organized view of your file plan
Holds for Legal Case	Displays Holds for a given Legal Case
Holds On or Before	Displays Open Holds that have been created on or before a given date
Pending Approvals	Displays records that are pending approval
Permanent Records by Record Class	Displays Permanent Records Counts grouped by Record Class
Permanent Records for Record Class	Displays Permanent Records for a given Record Class
Physical Records due for Disposal	Displays Physical Records that are ready for disposition
Record Audit	Displays the Audit for a given Record

Report	Description
Record Custody	Displays the Custody Chain for a given Record
Unclassified Records	Displays items that are registered but have not been assigned a Record Class
User Audit	Displays the Audit for a given User
Vital Records by Record Class	Displays Vital Records Counts grouped by Record Class
Vital Records for Record Class	Displays Vital Records for a given Record Class
Volume by Record Class	Displays Record Volume by Record Class
Volume by Record Class and File Type	Displays Record Volume by Record Class and File Type
Volume by Record Class and Repository	Displays Record Volume by Record Class and Repository



4.13.9 Destruction Certificates

The Destruction Certificates option, in the left navigation menu, displays a list of the Destruction Certificates that have been generated. A Destruction Certificate is evidence that information has been securely destroyed. Destruction Certificates are generated for Record Classes that have the Destruction Certificate property enabled. The Destruction Certificate report lists all certificates by default. The report can be filtered by Record Class, Approver, or Date.



To generate a Destruction Certificate, ensure the following:

- You must enable the Destruction Certificate property on the Create/Edit Record Class dialog. For more information, see Record Class Properties.
- The disposition action of the lifecycle must require approval.

Disposed Date	Record Class	Record Count	
5/10/2016	Tax, State/Local TAX-20	2	...
5/10/2016	Tax Year 2002 TAX-10-2	10	...
5/10/2016	Tax Year 2001 TAX-10-19	44	...
5/4/2016	_Test 000-000	4	...

Page 1 of 1 (4 Items)

If you click on the ellipsis (...) for a certificate, you will see the Destruction Certificate Details as shown below. The **View as Report** option launches the Destruction Certificate Details Report in the Reporting section and allows exporting of the certificate in a variety of formats.


Destruction Certificate Details ×

Record Class
Tax, State/Local TAX-20

Disposed Date
5/10/2016

Retention Expiration Range	Record Count	Medium	Method
3/14/2009 - 3/14/2009	2	Electronic	Deleted

Approval Group	Approval Date	Approver
1	5/11/2016 3:32:05 PM	RECORDLION\Chris

 View as Report

Close

4.13.10 Audit

Almost every component of the software has an audit trail that tracks every change made to the system for that particular components. The Audit option under the Manage main menu item is an interface to find all audit items in the system that can only be filtered by date, but not by component.

		5/1/2019	6/1/2019	Filter	Clear
5/22/2019 10:04:07 PM	Updated Record: '____conduent_approvers_query.dql (785fce6d-fc11-43e8-85b9-5576f34c4418)'				
	Source System			Target Record	
	Event Update			Target Id 114	
	User mpalmer-BoxSvc@gimmel.com				
5/22/2019 10:04:07 PM	Updated Record: '____5_cim_oil_contract_jacket.dql (69d4f7ff-52fa-4134-bc70-299a556544f6)'				
	Source System			Target Record	
	Event Update			Target Id 130	
	User mpalmer-BoxSvc@gimmel.com				
5/22/2019 10:01:08 PM	Action System LockItem was Completed for Record ____conduent_approvers_query.dql (785fce6d-fc11-43e8-85b9-5576f34c4418)				
	Source System			Target Record	
	Event Action			Target Id 114	
	User mpalmer-BoxSvc@gimmel.com				
5/22/2019 10:01:07 PM	Action DeclareRecord Success Message: Record at https://gimmalmike.app.box.com/file/462312230246 was locked.				
	Source External			Target Record	
	Event Action			Target Id 114	
	User mpalmer-BoxSvc@gimmel.com				
5/22/2019 10:00:46 PM	Updated Record: '____conduent_approvers_query.dql (785fce6d-fc11-43e8-85b9-5576f34c4418)' Record marked as Declared				
	Source System			Target Record	
	Event Update			Target Id 114	
	User mike.palmer@gimmel.com				

« < 1 2 3 4 ... > » Page 1 of 223 (1111 Items)

4.13.11 Event Occurrences

The Event Occurrences option provides a history of all of the occurrences that have been generated through the API, or created manually. It also enables you to create a new Event Occurrence. Event Occurrences are generated or created based on the Event Triggers that have been defined. When an Event Occurrence is generated or created, any Retention that is assigned to the associated Event Trigger will begin tracking its interval from the Event Occurrence date.

Multiple Event Occurrences may be generated for a single Event Trigger. For example:

- Each loan that is closed
- Each contract that expires
- Each employee that is hired

The same event may happen more than once:

- An employee leaves a company, but is rehired
- A customer closes an account, but reopens it a short time later

To avoid issues with targeting the same records more than once, understand and use the assignment positions on the Event Trigger. In summary, Triggers are the entity, and Occurrences are the instances of the entity. For example:

- Employee Hired is the Event Trigger (entity)
- John Doe hired on 7/1/2016 is the Event Occurrence (instance)

4.13.11.1 Manual Events vs. Recurring Events

When you define an Event Trigger, you must specify the Recurrence type. If the Recurrence type is set to Once, Daily, Monthly, or Yearly, the Event Occurrence for this Event Trigger will be generated automatically and cannot be generated any other way.

If the Recurrence type is set to Manual, the Event Occurrence for this Trigger will not generate automatically. Event Occurrences for this Event Trigger must be manually created from the Event Occurrences or using the API.

4.13.11.2 Creating an Event Occurrence for a Manual Event

To create an Event Occurrence for a Manual Event Trigger, perform the following steps:

1. Select Monitor from the Main Menu.
2. Select Event Occurrences from the left navigation menu.
3. Click Create.
4. Click the Event drop-down to see a list of Triggers that have been defined as Manual Events.
5. Provide the Event Occurrence Properties. (See below)
6. If Event Occurrence should target specific items, specify the appropriate targeting conditions.
7. Click Create.

Event Occurrent Properties

Property	Description
Event	Defines the associated manual Trigger for the Event Occurrence
Event Date	Defines the date of the Event Occurrence.
What should this event occurrence target?	<p>Defines if this Event Occurrence should target specific items. Options include:</p> <ul style="list-style-type: none"> • Specific Case File - The Event Occurrence targets only records that belong to a specific case file. If you select this option, a drop-down for the Case File displays. • Records with Property Value - The Event Occurrence targets records that have a specific property value. If you select this option, two additional fields display to specify the Target Property and Target Value. • Any Record - The Event Occurrence will target any record.
Case File	Defines the Case File that should be targeted; only displays if you select "Specific Case File".

Property	Description
Target Property	Defines the Target Property that should be targeted; only displays if you select "Records with Property Value".
Target Value	<p>Defines the Target Value that should be targeted based on the Target Property selected; only displays if you select "Records with Property Value".</p> <p>When using this condition, it is possible to specify fuzzy matching logic using the wildcard characters. See the table below for the permitted Characters.</p>

Target Value Properties

Character	Description
%	Any string of zero or more characters
_ (underscore)	Any single character
[]	Any single character within the specified range ([a-f]) or set ([abcdef])
[^]	Any single character not within the specified range ([^a-f]) or set ([^abcdef])

4.13.12 Pending Automation

Pending Automation provides a view into tasks that have been queued up by the system based on processing and evaluation of a given record's lifecycle status. These tasks define the actions to be taken with respect to a given record to meet the requirements to initiate and/or complete the next step in the record's retention lifecycle.

The screenshot shows the Gimmal Records Management interface. The top navigation bar includes the Gimmal logo and tabs for Inbox, Monitor (selected), Manage, Plan, Physical, Secure, and Settings. A left sidebar menu is divided into 'REPORTING' and 'ACTIVITY' sections. The 'REPORTING' section includes Dashboard, Reports, and Destruction Certificates. The 'ACTIVITY' section includes Audit, Event Occurrences, and Pending Automation (with a notification badge showing '3'). The main content area displays a table of tasks with the following data:

Record Class	Record	Phase	Action
Accounts Payable ACC-10	TEST2	System Action	Lock Item
Government Contracts CO.GOV	E4770 Final Pricing	System Action	Unlock Item
Government Contracts CO.GOV	E4770 CLC Price Proposal	System Action	Unlock Item

Below the table is a pagination control showing 'Page 1 of 1 (3 Items)' with navigation arrows.

Gimmal Records Management connectors will query this list of tasks, looking for any tasks associated with any of the repositories for which the connector is responsible, and then execute the actions defined by the task. Once the connector has completed the actions associated with the task, it flags the task as completed, and then the system will update the status of the corresponding record entry in Gimmal Records Management, and then remove the completed task from the queue.

For example, if a record stored in SharePoint has reached the end of its retention period and was approved for disposition by a record manager, a task to “Dispose and Delete” will be queued when the record manager submits his approval. In this scenario, the SharePoint connector then pulls the task from the queue, locates the document record in SharePoint, deletes it, and then updates the task as complete. The system then locates and deletes the corresponding record entry in Gimmal Records Management.

Similarly, if a record has been classified from Documentum to a record class that has an associated 2-Step lifecycle (e.g. “Record Declaration” and a subsequent “Retain for 5 Years then Dispose” step), when the entry criteria for the initial step is met, a task is queued to “Lock Item”. The Documentum connector will pull this task, locate the document in the repository, lock it down, then flag the task as completed. The system will then locate the record entry in Gimmal Record Management, update its status to declared/locked, and update the lifecycle settings as needed to allow the retention clock to begin ticking.

Users are able to see additional retention-related details for the record to which the task applies by clicking the ellipsis (...) button for a given task.

Action Item Details

Record Class COSD Test With Approval Category COSD-Test-2 --	Phase 1 Require Approval Yes
Record Contract_3_1 -- a8ed08bd-bdb0-4111-bc49-fc9672f81cdb	Phase Approved Yes Retention Created + 5 Day(s) Retention Expiration 9/9/2020 Expired Action Dispose and Delete Automation Level Automatic

In addition, for records that require approval for disposition, there will also be a drop-down menu button that users can click to access the details associated with the approval, such as when approval was granted and who granted it.

Approvals

Group	Approval Date	User
1	9/24/2020 10:34:33 PM	Administrator

4.14 Rule Builder

Rules are used throughout Gimmal Records Management for many purposes. This page documents how to build rules and the specifics of the different options.

4.14.1 Rule Components

Component	Description
Property	<p>Represents the property of the Repository Item to compare against.</p> <p>*The property can be any public property that exists for an item or a special token that is defined. All possible tokens are available on the (5.2.2) Rule Tokens(see page 129) page.</p>
Operator	<p>Represents the operator to use when comparing against the item. Possible values are:</p> <ul style="list-style-type: none"> • < (less than) • <= (less than or equal to) • = (equal to) • > (greater than) • >= (greater than or equal to) • Like(see page 129) • Not = (not equal to) • Starts With • Matches(see page 129)
Value	Represents the value of the expression that will be used when comparing against the item
Data Type	<p>Represents the data type of the Repository Item to compare against. Using a more specific data type will result in a more accurate expression result. Possible values are:</p> <ul style="list-style-type: none"> • Date • Date and Time • Text • Number
Join	<p>Represents how individual rules are combined within the list.</p> <ul style="list-style-type: none"> • <i>AND</i> - All rules using subsequent AND joins are nested together • <i>OR</i> - Does not nest, instead it separates groups of ANDed rules, for example (Exp1 AND Exp2) OR (Exp3) NOTE: Each Rule Group (indicated with parentheses) is evaluated individually and independently of any others. In this example expression, there are two Rule Groups. <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>Example</p> <p>If Expr1 is TRUE and Expr2 is TRUE then the whole expression is TRUE. Also: If only Expr3 is TRUE, then the whole expression is TRUE. Also: If Expr3 is FALSE and either Expr1 is FALSE or Expr2 is FALSE, then the whole expression is FALSE.</p> </div>

4.14.2 Rules for SharePoint and SharePoint Online

To create rules for SharePoint, you can either use SharePoint column properties or you can use tokens. See [System Tokens](#)(see page 0) and [SharePoint Tokens](#) (see page 0)for a complete list.


To create broad rules, use the Site or Site Collection. In the example below, @sp.web matches the Site of a document and @sp.siteurl matches the URL of the HR site.

Property	Operator	Value	Data Type	Join	
@sp.web	=	Human Resources	Text	Or	✕
@sp.siteurl	=	https://server/sites/hr	Text	None	✕

 Rule Groups are visually indicated by a dotted blue line. This is accomplished by using the "Or" join.

Another example would be to use the Content-Type or Library. Using the Content-Type is recommended, if possible because then the rule will apply to records across any Site.

- @sp.contenttype = Hiring Record
- @sp.library = Human Resources

 SharePoint has some atypical formats in order for values to work correctly. See the [\(5.2.2\) SharePoint Property Value Formatting](#)(see page 128) page for specific usage.

4.14.3 Rules for File Shares

To create rules for a File Share, you can use System Tokens or File Share Tokens.

Here are a few examples of how to use tokens to create rules for a File Share:

1. Rules for a Directory Path or Shared Folder
 - @folder = parentfolder
 - @folder LIKE *parentfolder*
 - @uri LIKE \\server\folder1\folder2*
 - @uir MATCHES [Regular Expression]
2. Rule for a Folder and all Sub-Folders that contain a specific name
 - @uril LIKE *\folder*
3. Rule for a Folder that begins with a specific name
 - @folder LIKE name*

4.14.4 SharePoint Property Value Formatting

Creating Rules is straight forward for most situations because you are usually just comparing the rule value to the item being classified's property value. This key-value formatting is referred to as Standard Formatting.

However, some Connectors support different types of properties that may provide atypical value formats or multiple values for a single property. Handling these scenarios requires that you understand how the Connector will format Repository-specific property values for atypical property types. This type of formatting is referred to as Special Formatting.

4.14.4.1 SharePoint and SharePoint Online

Property Type	Property Value Formatting	Notes
Single line of text	Text Value	
Multiple lines of text	Text Value	
Choice	Choice1	
Choice (Multiple)	Choice1 Choice2 Choice2	
Number	7	
Currency	\$7.00	
Date and Time	2014-02-24T23:35:50.0000000Z	UTC
Date Only	2014-02-24T00:00:00.0000000Z	UTC
Lookup	Value1	
Lookup (Multiple)	Value1 Value2 Value3	
Yes/No	Yes	Yes or no
Person Group	Login Name1	
Person or Group (Multiple)	Login Name1 Login Name2	
Hyperlink or Picture	http://url , Description	

Property Type	Property Value Formatting	Notes
Managed Metadata	Term1 Term2 Term3	

4.14.5 Understanding the Classification Rule Operators

When creating rules, there are two operators that appear to be somewhat similar by name, but behave drastically different. These are the Like and Matches operators.

4.14.5.1 Like Operator

The Like Operator is used for fuzzy matching against a value by using simple pattern expressions. The most common character used in a Like-based pattern expression is an asterisk which represents a wild card character.

For example, “Property Like *Value*” will match if the property contains the word “Value” anywhere within its value. The full pattern expression syntax is as follows:

Characters in Pattern	Matches in String
?	Any single character
*	Zero or more characters
#	Any single digit (0-9)
[charlist]	Any single character in charlist
[! charlist]	Any single character not in charlist

4.14.5.2 Matches Operator

The Matches Operator is used for matching against patterns specified by a regular expression.

For example, “Property Matches \b4[0-9]{12}(?:[0-9]{3})?\b” will match if the property contains a credit card number in its value. Regular Expression Language Quick Reference: [http://msdn.microsoft.com/en-us/library/az24scfc\(v=vs.110\).aspx](http://msdn.microsoft.com/en-us/library/az24scfc(v=vs.110).aspx)

4.14.6 Rule Tokens


This section contains a list of valid tokens that can be used anywhere the rule builder is available, including:

- Classification Rules
- Legal Hold Rules
- Triggers
- Rule Sets

The tokens are separated by Connector/Extension type, with the System Tokens being available regardless of Connector type.

4.14.6.1 System Tokens

Token	Description
@repo	The repository of the connector. For SharePoint, this value will be SharePoint. If you use the File Share Connector, this value would be FileSystem, for example.
@folder	The name of the item's parent folder
@file	The name of the item, including file extension
@record.isRecord	A Record's Declared status.
@filesize	The size of the file in bytes
@created	The date and time the item was created
@modified	The date and time the item was last modified
@uri	The full URI of the item
@uri_level#	One property for each level of the @uri value. For example, on SharePoint, if @uri started with "https://servername", @uri_level0 would be "servername". The last of these properties will represent filename and file extension, such as "test.docx".

 System tokens are case-sensitive and will not display values correctly unless you enter the token in all lowercase format.
Example: **@created** not @Created

4.14.6.2 Altitude Tokens

Token	Description
@altitude.label	The label given to a file.

4.14.6.3 Documentum Tokens

Token	Description
@dctm.docbase	The DocBase where the document resides
@dctm.docbroker	The DocBroker for the document
@dctm.cabinetid	A list of cabinet IDs where the document can be found
@dctm.cabinetname	A list of the cabinet names where the document can be found
@dctm.objecttype	The documents object type
@dctm.folderid	A list of folder IDs where the document can be found
@dctm.foldername	A list of folder names where the document can be found
@dctm.applicationid	The id of the application for the document
@dctm.objectid	The version specific ID of the document
@dctm.chronicleid	The id for tracking all versions of the document

4.14.6.4 Exchange Tokens

Token	Description
@ex.from	Sender

Token	Description
@ex.owner	Owner of the mailbox the item is in
@ex.to ¹⁸	Recipients
@ex.cc ¹⁹	CC'd recipients

4.14.6.5 File Share Tokens

Token	Description
@fs.owner	The owner of the file from the File System; for example, "Gimmel\Susan"

4.14.6.6 Physical Records Management Tokens

Token	Description
@prm.containername	The name of the container that holds the physical asset
@prm.assetname	The name of the physical asset
@prm.assetbarcode	The Barcode value of the physical asset
@prm.assetbarcodealternate	The "Alternate Barcode" value of the physical asset
@prm.assetkeywords	The keywords of the physical asset
@prm.assethome location	The "Home Location" value attached to the asset
@prm.assetcurrent location	The "Current Location" value attached to the asset
@prm.owner	The owner listed for the asset

¹⁸ <http://ex.to>

¹⁹ <http://ex.cc>

Token	Description
@prm.containerkeywords	The keywords of a container that holds the physical asset
@prm.assettemplocation	The "Temporary Location" value attached to the asset
@prm.assetchargedout	Status of the asset charged-out/in
@prm.assetchargedoutto	The user that an asset is charged-out to
@prm.assettype	The "Type" value attached to the asset
@prm.locationtype	The "Location Type" value attached to a location asset
Asset metadata	<p>The following asset metadata can be used:</p> <ul style="list-style-type: none"> • Any Custom field (if configured) • Title • Subject • Asset Type • Format <p>For specificity, use @repo = physical to only affect physical assets</p>

4.14.6.7 SharePoint and SharePoint Online Tokens

Token	Description
@sp.library	The title of the SharePoint List that contains the document
@sp.siteurl	The full URL of the root web site in the site collection; for example " https://servername/ "
@sp.web	The title of the item's web/site
@sp.weburl	The server relative URL of the item's web/site, for example <code>"/accounting"</code>
@sp.folderurl	The server relative URL of the item's parent folder, for example, <code>"/accounting/ap"</code>
@sp.contenttype	The name of the item's content type

Token	Description
@sp.title	The Title property from SharePoint
SharePoint Column Display Name	Any SharePoint Column Display Name can be used in Classification Rules

4.15 Physical Records

4.15.1 [Locations](#)

4.15.2 [Containers](#)

4.15.3 [Assets](#)

4.15.4 [Barcode Schemes](#)

4.15.5 [Request and Returns](#)

4.15.6 [Custom Metadata and Templates](#)

4.15.7 [Locations](#)

Locations are physical places where assets can be stored, such as an office, a warehouse, a box, etc. A location can also represent a person (as long as there is an address associated with that person). The locations functionality enables you to create locations, associate locations with a parent, update a location, and delete a location. The locations list "Address" value is used for the Home Location, the Current Location, and the Temporary Location entries on a physical asset.

4.15.7.1 [Creating a New Location](#)

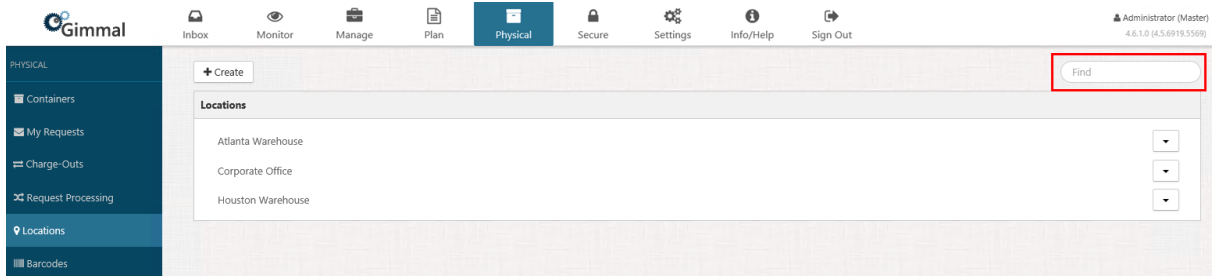
To create a new location, perform the following steps:

1. Select **Physical** on the Main Menu, and then **Locations** on the left navigation menu. The Locations page displays.
2. Click **+Create**. The Create Location dialog opens.
3. Enter the following information:
 - Name of the location
 - Description of the location
 - Address of the location
4. Click **Create**. The new location is added to the Locations page.

4.15.7.2 Creating a Child Location

You can create a child location under the parent location. The Location list can support a hierarchy up to six levels deep. An example of a child location is if the parent location is an office, the child location would be a file cabinet or a box located in that office. To create a child location, perform the following steps:

1. Click the drop-down arrow for the parent location, click **+Create**, and enter a name, description, and address.



2. Click **Create**. The new child location is added to the Locations page, under the parent location. Click the expand arrow to the left of the parent location's name to see the child location(s) under it.

4.15.7.3 Editing and Deleting a Location

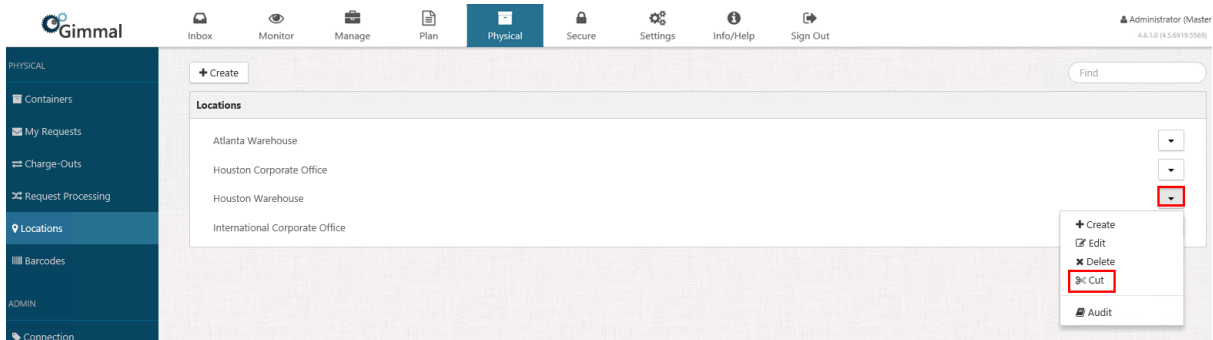
Take the same steps as creating a location, but select Edit or Delete instead.

4.15.7.4 Moving a Location

The only purpose for moving a location is to move it to a different parent or to/from the root. It may appear that you can reorder the Location, but the page will refresh and place them back in alphabetical order.

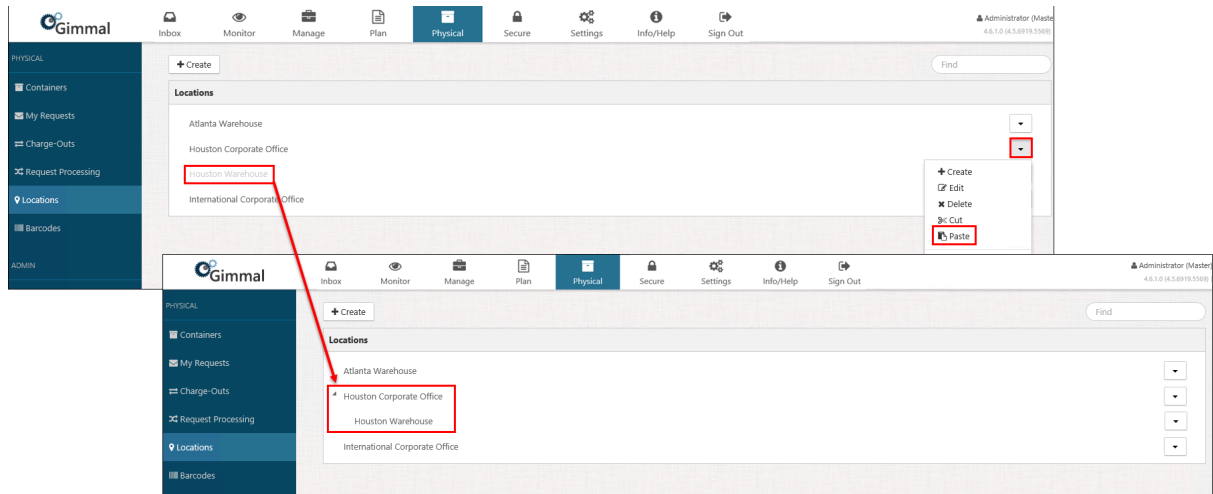
Cut and Paste

1. Find the location you want to move, and click the drop-down arrow on the right side. The location context menu displays.



2. Click **Cut**. The location "grays out" on the page, indicating that it's been selected for cutting.
3. Locate the target/parent location you want to move the selected location to, and click the drop-down arrow on the right side. The target location context menu displays.

4. Click **Paste**. The selected (cut) location moves under the target location.



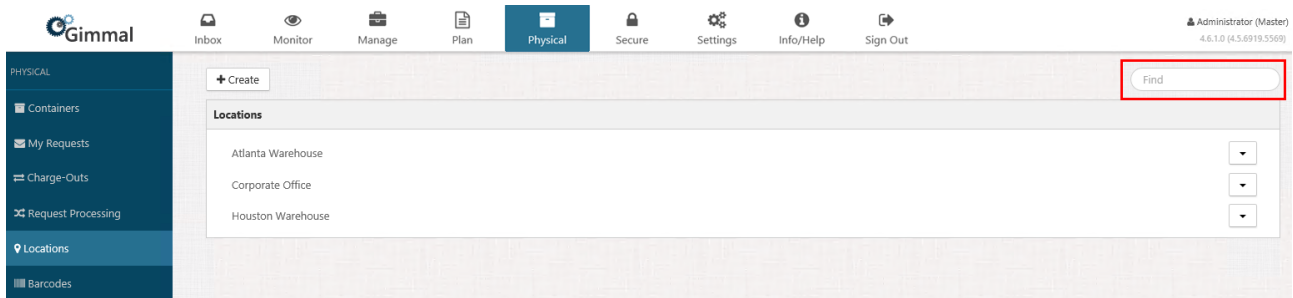
Drag and Drop

Find the location you want to move, click and hold the pointer on the location row, and drag the location over to the target location. The location is moved under the target location. When dragging and dropping one of several icons displays at the top of the popup, which indicates the dragging status.

	Dragging the container to this location is permitted
	Dragging the container to this location is not permitted
	Drag the container below this row
	Drag the container above this row (Note: Parent/root containers display on this page in alphabetical order. If you drag a container whose name is lower in alphabetical order above a container whose name is higher in alphabetical order, the page will refresh, and place the dragged container back in proper alphabetical order on the page.)

4.15.7.5 Searching for a Location

Your Locations list can potentially have thousands of entries. As a result, Physical Records Management enables you to search the Locations list by **name** or **address** to easily find a specific location. To find a specific location, place your cursor in the **Find** field in the upper right corner, enter the first few letters of the location name (e.g. "hou" for Houston) or the first few letters of the location's street (e.g. "smi" for Smith St.) or the first few numbers of the location's address (e.g. "120" for 1200). The Locations list is filtered to only show the location that has that name, that street number, or that street name.



4.15.8 Containers

A container is a logical or location-based structure used for organizing and managing physical assets. For example, you can create a container to represent a real-world folder, and that folder can contain physical documents (i.e., physical assets). Containers enable the physical container structure of an organization to be modeled electronically. As references to physical assets are created, they will be associated with one of these configured containers.

This hierarchical view of containers also makes it possible to see which physical assets exist in a specific container. Physical containers will never be considered records, but instead act as an organizational hierarchy only.

4.15.8.1 Managing Container Permissions

4.15.8.2 Container Properties

4.15.8.3 Creating a Container

4.15.8.4 Searching for a Container

4.15.8.5 Making changes to containers

4.15.8.6 Record Classes and Containers

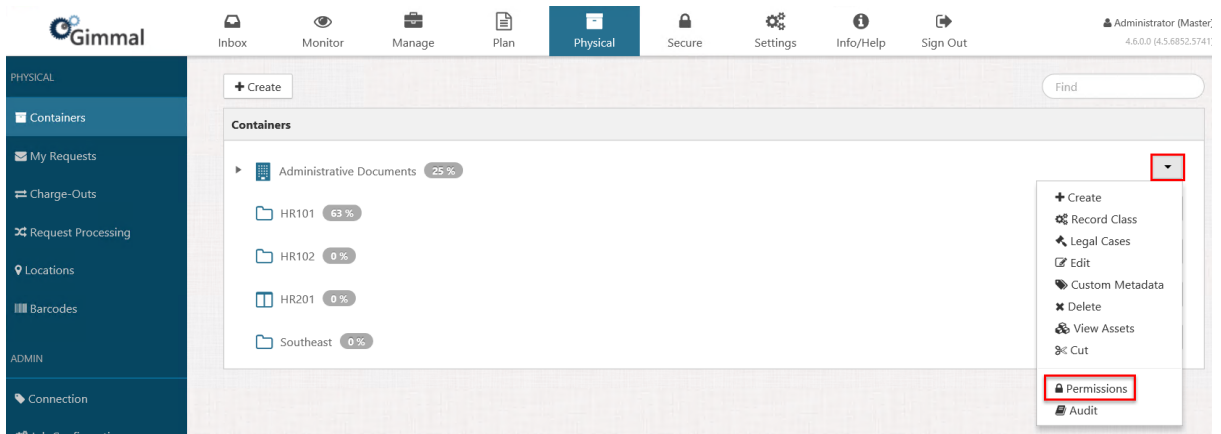
4.15.8.7 Legal Cases and Holds on Containers

4.15.8.8 Managing Container Permissions

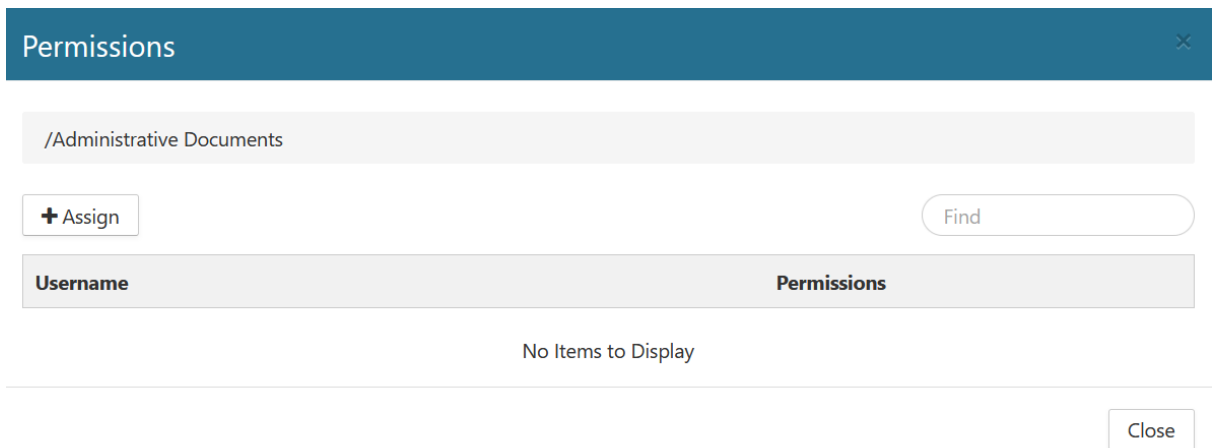
Containers have their own set of permissions, which are required in order for the Physical User to perform certain tasks involving parent containers and child containers. This topic describes how to set, edit, and remove permissions. It also describes permission inheritance, with respect to parent and child containers. An overview of container permissions can be found in the [Physical Records Permission Overview](#)(see page 253) topic.

Setting Permissions for a Container

1. Login to Records Management with either of the following roles/permissions:
 - A user with the **Physical Administrator** role, or
 - A Physical User with container permissions set to **Edit Container Permission**
2. Click **Physical** on the Main Menu, and then click **Containers** on the left navigation menu. The Containers page displays.
3. Click the drop-down arrow to the right of the desired container, and then select **Permissions**. (The drop-down options you see may vary, depending on your permissions.)



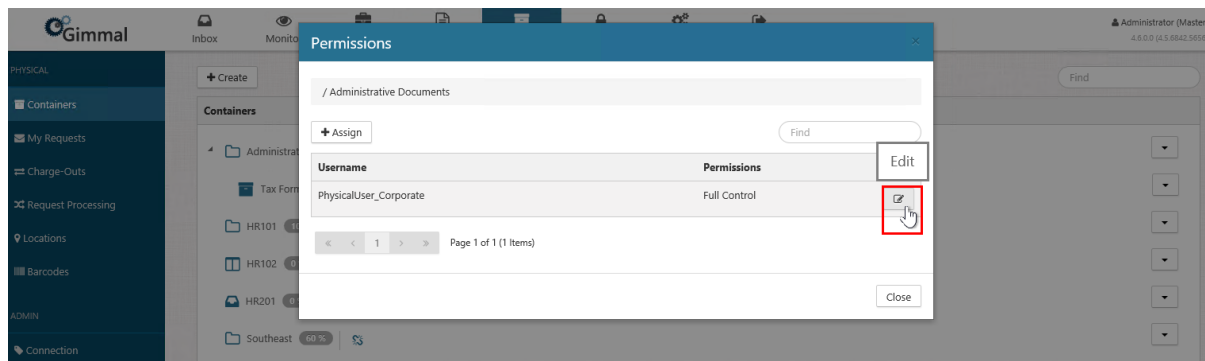
4. On the Permissions window, click **+Assign**.



5. On the Assign Permissions window, select a user from the drop-down list, or enter a valid user name. This can be a user or a group, however, the only users who display in this list are those who are Physical Administrators or Physical Users.
6. Apply the desired permission(s) to the user, and then click **Save**.
7. The new user and associated permission(s) displays on the Permissions window.
8. Click **Close**.

Editing Permissions for a Container

1. From the Permissions window, referenced in step 4 above, click the Edit icon for the user whose permissions you wish to edit.



2. The Edit Permissions window opens. Make the desired changes to the user's permissions, and then click **Save**. The permissions are updated for that user.

Removing Permissions for a Container

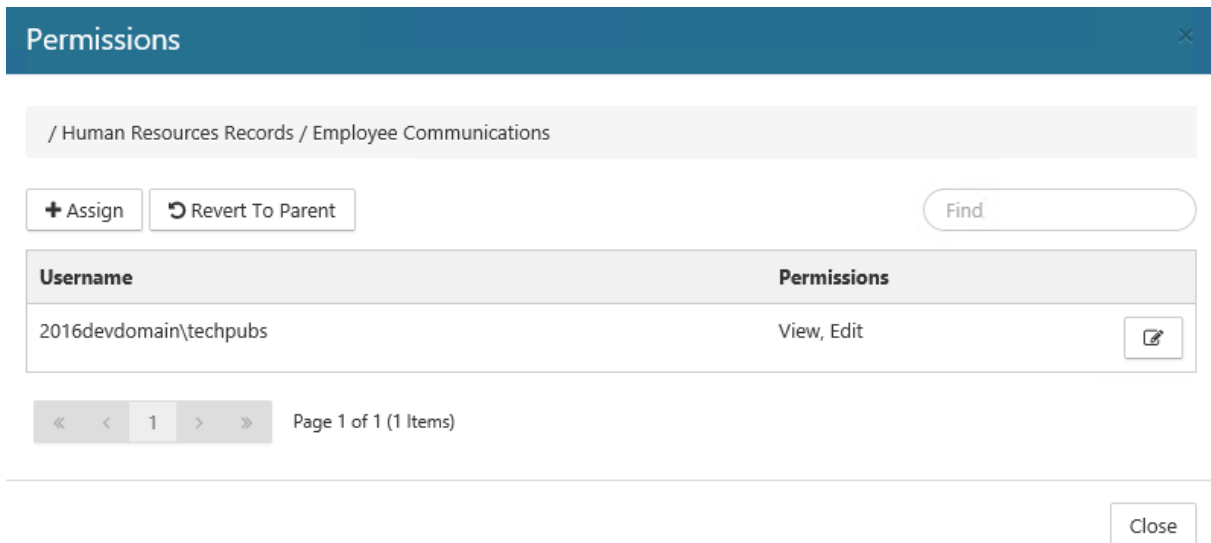
1. From the Permissions window, referenced in step 4 above, click the **Edit** icon for the user whose permissions you wish to remove. The Edit Permissions window opens.
2. Deselect all of the permissions for the user, and then click **Save**. The user no longer displays in the list on the Permissions window.

Permission Inheritance

By default, a child container inherits the permission of its parent. However, you can specify unique permissions for a child container (thus breaking the inherited permissions), as well as the ability to revert back to the original parental permissions if desired.

1. Login to Records Management with either of the following roles/permissions:
 - A user with the **Physical Administrator** role, or
 - A Physical User with container permissions set to **Edit Container Permission**.
2. If you haven't done so already, create a parent and child container hierarchy by performing the steps in [Creating a New Container](#)²⁰.
3. Click **Physical** on the Main Menu, and then click **Containers** on the left navigation menu. The Containers page displays.
4. Set permissions for the parent container using the steps in the previous section.
5. On the Containers page, select the drop-down arrow for the child container you want to break permissions for and select **Permissions**. (The drop-down options you see may vary, depending on your permissions.)
6. Break the inheritance by adding additional user permissions or by deleting permissions.
7. Click **Save** to close the Edit Permissions window and return to the Permissions window. On the Permissions window, the revised permission(s) will display, as well as a **Revert to Parent** button located above the permissions table. This button indicates that permission inheritance has been broken.

²⁰ <http://docs.gimmel.com/en/6109-creating---searching-for-new-container.html>



8. To revert back to the original permissions of the parent container, click **Revert to Parent**. The Confirm Revert window opens, asking you to confirm the reversion.
9. Click **Confirm**. The child container permission listed on the child Permissions window reverts back to the parent container permissions.
10. Click **Close** to close the Permissions window.

4.15.8.9 Container Properties

The following table contains a list and description of the container properties found on the **Create** and **Edit Container** dialogs. An asterisk (*) indicates that the property is mandatory.


Property	Required	Default	Description
Name	Yes		The unique name for the parent container.
Title	No		An optional title.
Subject	No		An optional subject/description of the container.
Keywords	No		Optional keyword(s) about the container.

Property	Required	Default	Description
Node Type	Location	Yes	<p>Defines the node type: Location or Logical (Only permissible for the root (parent) container. Child containers inherit this value from the parent container, so it cannot be changed. If you want to change the node type, you must create a new root container of the appropriate type.)</p> <p>A Location node refers to an actual physical location where physical assets can be located, such as an office, a warehouse, a filing cabinet, etc.</p> <p>A Logical node can be any representation to organize and catalog physical assets. It does not have to mirror any structure or organization in the "real world". You can create and use both location-based and logical-based containers.</p> <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>✔ The Home location for a Location node is automatically calculated and provides the full path to the asset (i.e., all assets in the same container share the same Home location). This is not the same with a Logical node, as assets in the same container may have different locations.</p> </div>
Location Type	Yes	Folder	<p>The location type that only displays if you select Location as your node type. Options are:</p> <ul style="list-style-type: none"> • Aisle • Bin • Box • Cabinet • Drawer • Folder • Shelf • Warehouse
Capacity	No		<p>The maximum number of physical assets in a container. Does not include assets in any child containers.</p> <p>If you enter a capacity, it displays as a percentage. This percentage is calculated from the number of a parent container's assets divided by the capacity value entered on the properties dialog. For example:</p> <p><input type="checkbox"/></p> <p>If capacity is not entered, a numerical count of the parent container's assets will display. For example:</p> <p><input type="checkbox"/></p> <div style="border: 1px solid blue; padding: 5px; margin-top: 10px;"> <p>ℹ If capacity reaches 100% for a container, you can still add additional child containers, but you cannot add additional physical assets.</p> </div>

Property	Required	Default	Description
Can Contain Assets	Yes	No	Defines if physical assets can be added to this container. If you select No, then this container can only contain a child container.
Allow Requests	Yes	No	Defines if you want any physical assets that were created in this container to be able to be requested or not.
Barcode	No		Allows manual entry of a barcode to apply to a container or displays the barcode schemes to allow selection from there (if configured). These values appear from the drop-down menu and the next available barcode number according to the scheme is entered automatically.
Barcode Symbology	Yes	Code 39	The type of barcode symbology to use.
Barcode Alternate	No		A Barcode Alternate is useful when you have assets that may have need separate barcodes for internal and external usage. This property works the same way as Barcode Symbology.
Barcode Symbology Alternate			The type of barcode symbology to use for the Barcode Alternate.

4.15.8.10 Creating a Container

A container is a logical or location-based structure used for organizing and managing physical assets. For example, a location-based container could be a shelf, and the boxes that are stored on the shelf (which represent the physical assets). For logical-based, the container can be anything, a charge-code, a taxonomy value, etc. and the assets contained therein are those that are being managed (boxes/folders/microfiche) etc. You can create parent (root) containers and a child container, depending on your permissions. The following sections describe how to create each type of container.

 While it is possible to so create many levels of child containers, only six levels deep is supported.

By default, a child container inherits the Node Type (Location or Logical) of its parent container, so the parent container Node Type cannot be changed. If you want to change the node type, you must create a new root container and select the appropriate type. By default, a child container inherits the Record Class of its parent container. If the parent container does not have a Record Class, the child container will not have one either.

Creating a Parent (Root) Container

1. Login to Records Management as a user with the **Physical Administrator** role.
2. Click **Physical** on the Main Menu, and then click **Containers** on the left navigation menu. The Containers page displays.

3. Click **+Create**. The Create Container dialog opens.

Create Container
✕

Name *

Title

Subject

Keywords

Node Type *

Location Type

Capacity

Can Contain Assets *

Allow Requests *

Barcode

Barcode Symbology *

Barcode Alternate

Barcode Symbology Alternate *

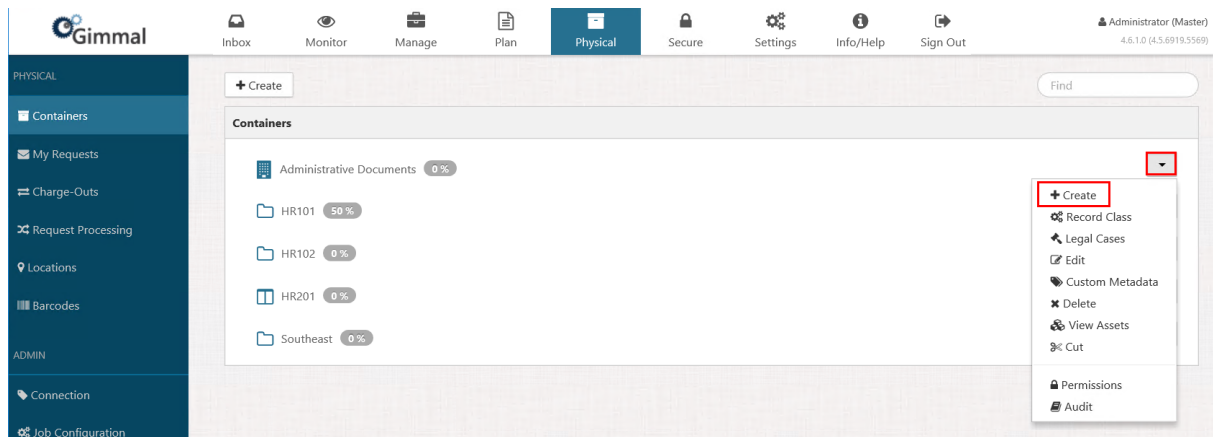
Custom Metadata Template

4. Enter the required and optional fields as described in [Container Properties](#)(see page 140).
5. Click **Create**. The new container displays on the Containers page.

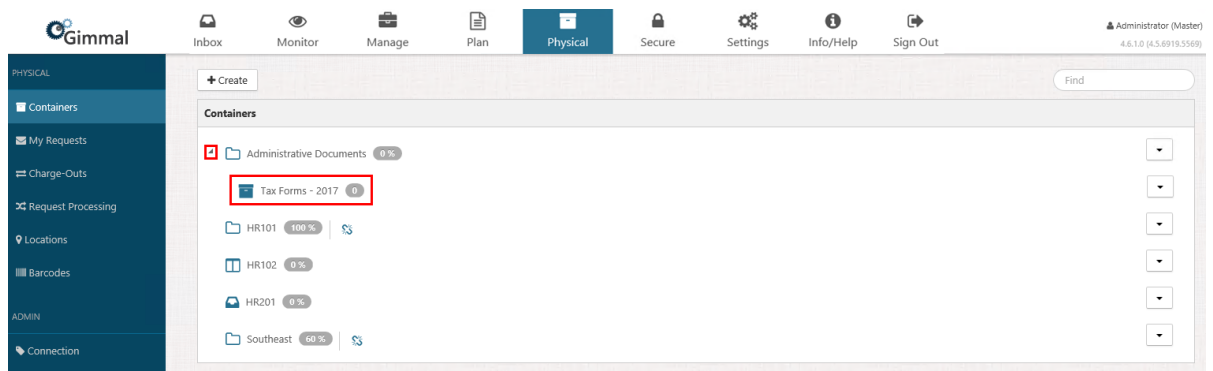
Creating a Child Container

1. Login to Records Management with either of the following roles/permissions:
 - A user with the **Physical Administrator** role, or
 - A Physical User with container permissions set to **Edit** or higher
2. On the Containers page referenced above, click the drop-down arrow for the container you want to create a child container for.

3. Click **+Create**. (The drop-down options you see may vary, depending on your permissions.)



4. Enter the required and optional fields as described in [Container Properties](#)(see page 140).
5. Click **Create**, and then expand the parent container. The new child container displays under the parent container.

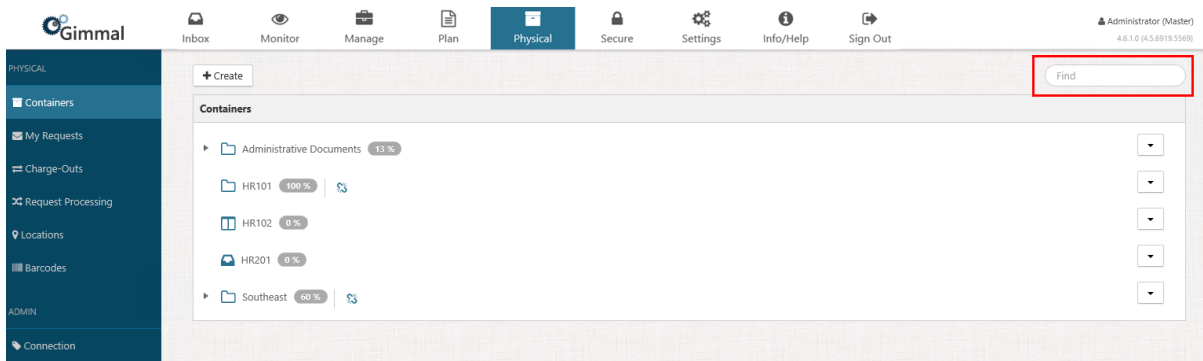


4.15.8.11 Searching for a Container

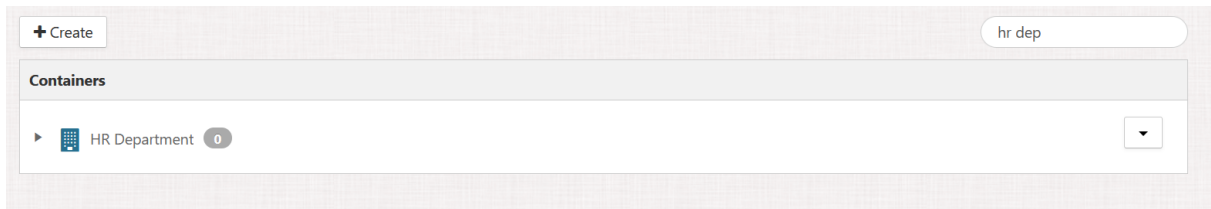
Your containers list can have potentially thousands of entries. As a result, Physical Records Management enables you to search the containers list by **name** or **title** to easily find a specific container.

To search for a container, perform the following steps:

1. Select **Physical** on the Main Menu, and then **Containers** on the left navigation menu. The **Containers** page displays, along with a list of all of your containers.



2. In the **Find** field in the upper right corner, start by entering the first few characters of the container name until the container results are filtered to match the characters you enter, and the desired container(s) display (provided that you have the appropriate container permissions applied).

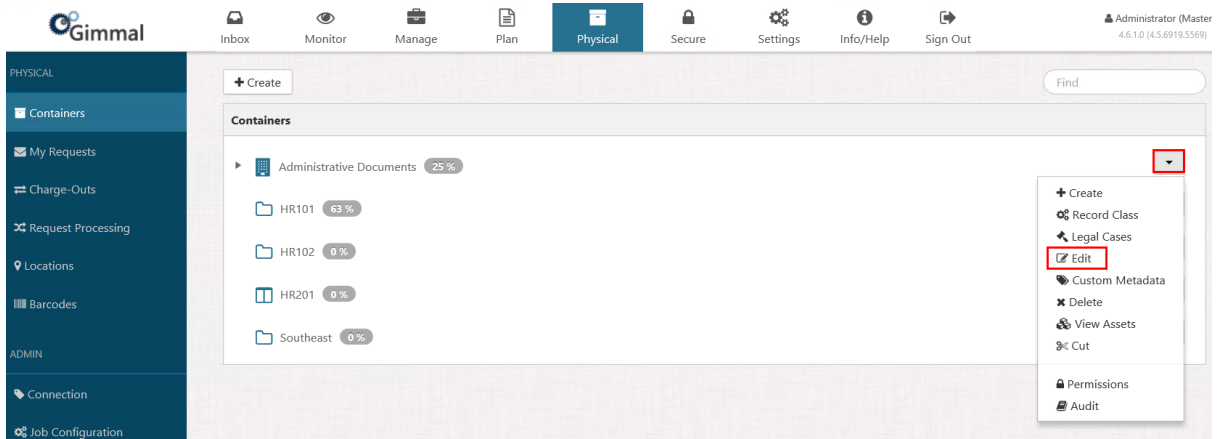


4.15.8.12 Making changes to containers

If you want to make changes to a container, you can edit the container's properties if you have the appropriate permissions. The following topic describes how to edit the properties of a parent container and how to edit the properties of a child container.

Editing a Parent & Child Container's Properties

1. Select **Physical** on the Main Menu, and then **Containers** on the left navigation menu. The Containers page displays.
2. **Parent:** Locate the container whose properties you want to edit, and click the drop-down arrow on the right side. The container context menu displays. (The drop-down options you see may vary, depending on your permissions.)
Child: Locate the container whose properties you want to edit, expand the container, and then click the drop-down arrow on the right side. The child container context menu displays. (The drop-down options you see may vary, depending on your permissions.)



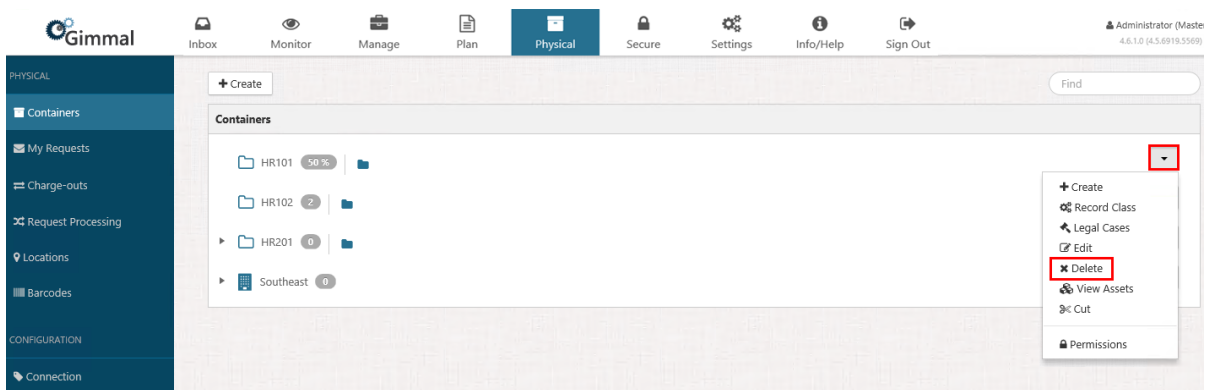
3. Click **Edit**. The Edit Container dialog opens.
4. Make your desired changes to the properties and then click **Save**. The container updates on the Containers page.

Deleting a Container

If you no longer need a container, you can delete it if you have the appropriate permissions. The following sections describe how to delete a parent container and how to delete a child container. There are some limits to when you can delete a container:

- You cannot delete a container that contains physical assets.
- You cannot delete a parent container that has a child container with physical assets.


1. Select **Physical** on the Main Menu, and then Containers on the left navigation menu. The **Containers** page displays.
2. **Parent:** Locate the container you want to delete, and click the drop-down arrow on the right side. The container context menu displays.
Child: Expand the parent container that has the child container you want to delete, and click the drop-down arrow on the right side. The container context menu displays. (The drop-down options you see may vary, depending on your permissions.)




3. Click **Delete** on the context menu. The Delete Container dialog opens.
4. Click **Delete** on the dialog*. The container is deleted, and no longer displays on the Containers – page. If a parent container has children, a confirmation message will display, asking you to confirm the deletion of the child containers as well. Click **Delete** to delete the parent container and all child containers.

Moving a Container

You can move a container from one container to another by cutting and pasting the container, or by dragging and dropping the container. In order to move a container, you must have Edit permissions on both the source container and the target parent container. You can also only move containers to other parents of the same type (Location to Location or Logical to Logical).

 When you move a container, all of its child containers and assets are moved with it.

 **Legal Holds**
A container that has a legal case/legal hold on it can be moved to another container and the hold will persist.

Cutting and Pasting a Container









Perform the following steps to move a container by cutting and pasting it.







1. Locate the container you want to move, and click the drop-down arrow on the right side. The container context menu displays. (The drop-down options you see may vary, depending on your permissions.)
2. Click **Cut**. The container "grays out" on the page, indicating that it's been selected for cutting.
3. Locate the target container you want to move the selected container to, and click the drop-down arrow on the right side. The target container context menu displays. (The drop-down options you see may vary, depending on your permissions.)
4. Click **Paste**. The selected container moves under the target container, as well as any physical assets of the selected container.

Dragging and Dropping a Location

Find the location you want to move, click and hold the pointer on the location row, and drag the location over to the target location. The location is moved under the target location.

During the dragging process, a small popup displays at the base of your pointer. One of several icons displays at the top of the popup, which indicates the dragging status. Each icon is described below.

  FIN1  	Dragging the container to this location is permitted
  FIN1  	Dragging the container to this location is not permitted

  <p>FIN1</p> <p>33 %</p> 	<p>Drag the container below this row</p>
  <p>FIN1</p> <p>33 %</p> 	<p>Drag the container above this row (Note: Parent/root containers display on this page in alphabetical order. If you drag a container whose name is lower in alphabetical order above a container whose name is higher in alphabetical order, the page will refresh, and place the dragged container back in proper alphabetical order on the page.)</p>

4.15.8.13 Record Classes and Containers

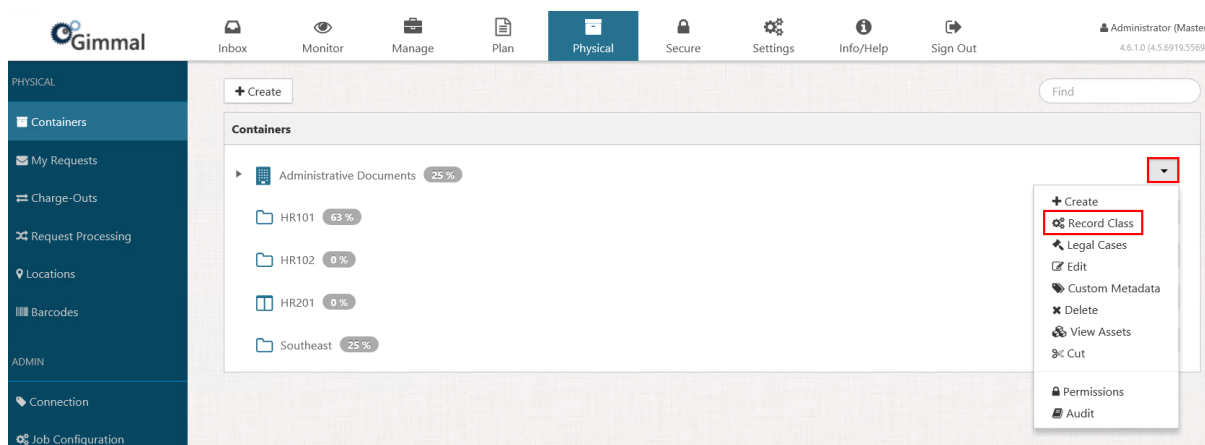
Associating a Container to a Record Class

A record class defines a named grouping in which containers, and their physical assets, can be assigned. Associated to this grouping, or record class, is a number of properties that define more detailed information about the container, as well as the Lifecycle that containers that are assigned to this grouping will follow. For more information on Record Classes, such as creating, editing, and deleting them, see [Records Classes](#)²¹ under the Records Management Core component. Assigning a record class to a container enables you to classify all physical assets in that container with a particular record class. Any current, or newly-created, child containers will inherit the assigned record class.

For a Physical Administrator to be able to add a record class to a container, the Administrator must have Declare permission, in Manager Web, on the relevant record class.

1. Select **Physical** on the Main Menu, and then **Containers** on the left navigation menu. The Containers page displays.
2. Locate the container you want to associate a Record Class to, and click the drop-down arrow on the right side. The container context menu displays. (The drop-down options you see may vary, depending on your permissions.)

²¹ <http://docs.gimmel.com/en/1641-record-classes.html>



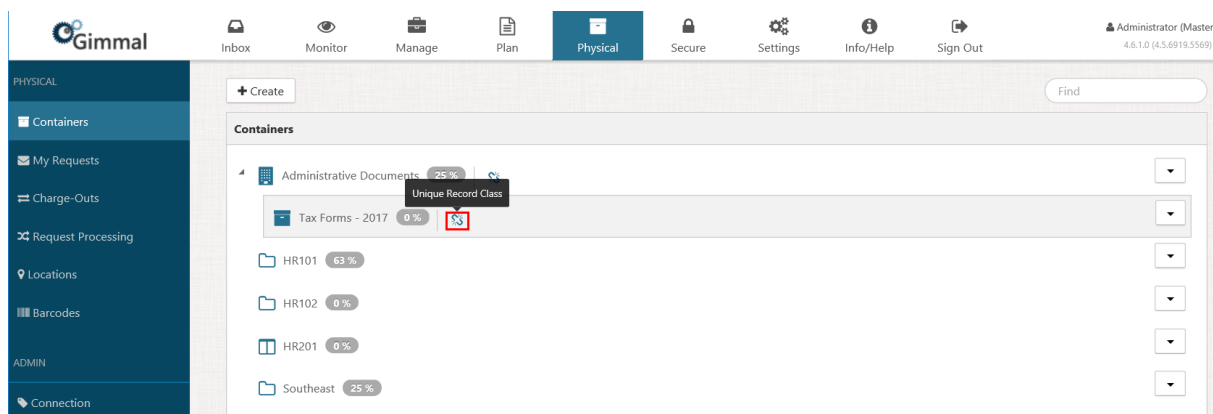
3. Click **Record Class**. The Record Class dialog opens.
4. Click the Record Class drop-down, select a record class, and then click **Save**. The changes are saved and the new record class is assigned to the container. A "Unique Record Class" icon displays to the right of the container, indicating that a record class has been assigned to it.

i When you create a child container, the child container inherits the same record class from the parent container. This is indicated by the "Inheriting Record Class" icon to the right of the child container.

Breaking Record Class Inheritance

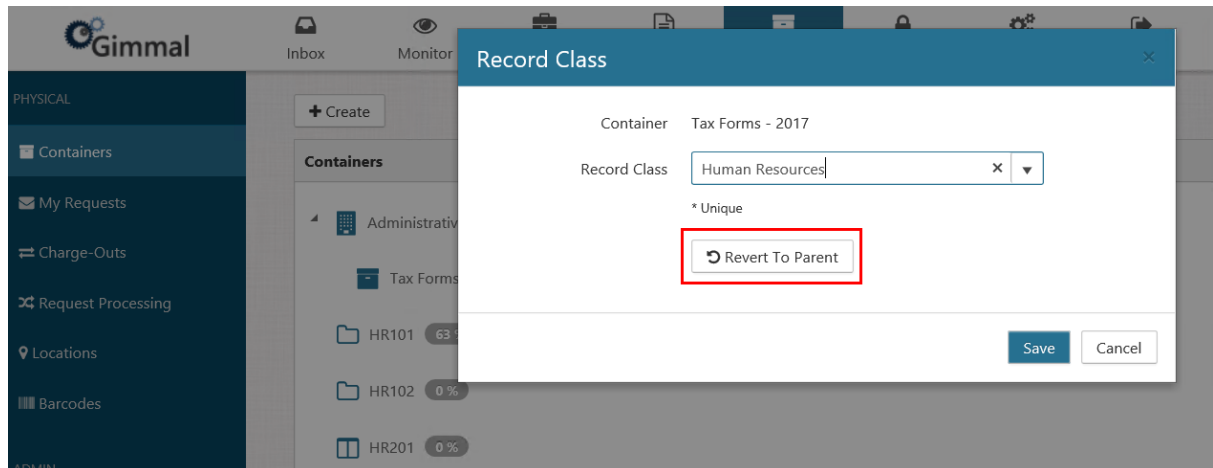
Record Class inheritance is the process by which a child container inherits the record class of its parent container. An authorized user (as described above) can break this inheritance and manually set a separate record class for a child container. If desired, you can revert the child container's record class back to the parent's record class.

1. Create a container, and then create a child container. (For more information, see [Creating Containers](#)(see page 142))
2. Assign a record class to the parent container. The child container inherits this record class.
3. Open the child container's Record Class dialog, select a new record class, and then click Save. The new record class is assigned to the child container, and the "Unique Record Class" icon displays next to the child container on the Containers page.

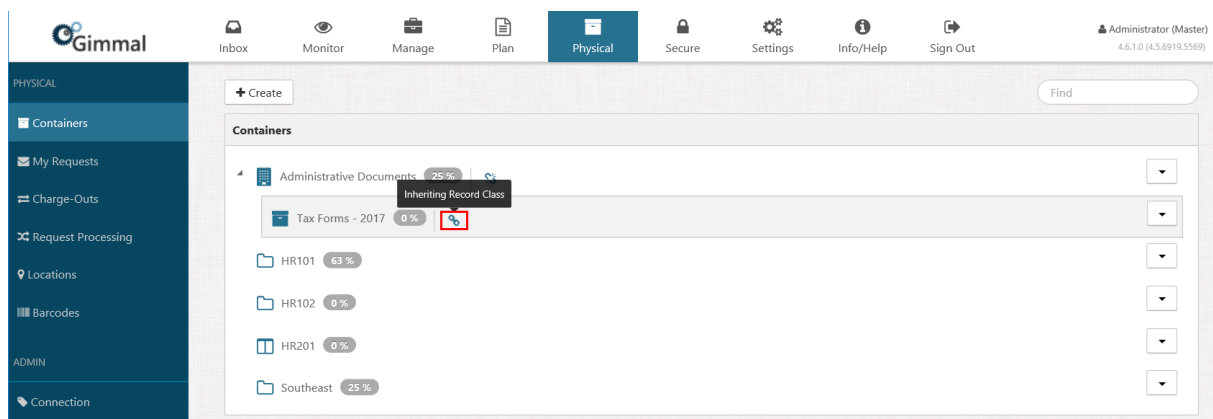


Reverting Back to a Parent Container's Record Class

1. Open the Record Class dialog for the child container with the broken inheritance, and click **Revert to Parent**.
2. The Record Class dialog closes, and the child's record class now matches the parent container's record class, as indicated by the "Inheriting Record Class" icon to the right of the child container's name.



The Record Class dialog closes, and the child's record class now matches the parent container's record class, as indicated by the "Inheriting Record Class" icon to the right of the child container's name.



4.15.8.14 Legal Cases and Holds on Containers

Legals holds created in Gimmel Records Management can be applied to physical assets, which in turn locks the physical assets.

For example, if "Company XYZ" is facing pending or imminent litigation, or if legal action is anticipated in the near future, it may become necessary to preserve paper-based (personnel files, legal contracts, etc.) or physical types of media (DVDs, CDs, microfiche, etc.) that pertain to a lawsuit or an audit. All processes leading to the disposal of these paper-based or physical media items are suspended to ensure these items are available for the legal discovery process. Note that the system doesn't actually put these items on hold in a physical sense. The application merely provides visual indicators of the holds, it locks down the item's properties (metadata), and it

prevents the disposition process from occurring. Physical Records Management enables you to manually assign legal cases/legal holds to containers and physical assets.

Adding a Legal Case to a Container

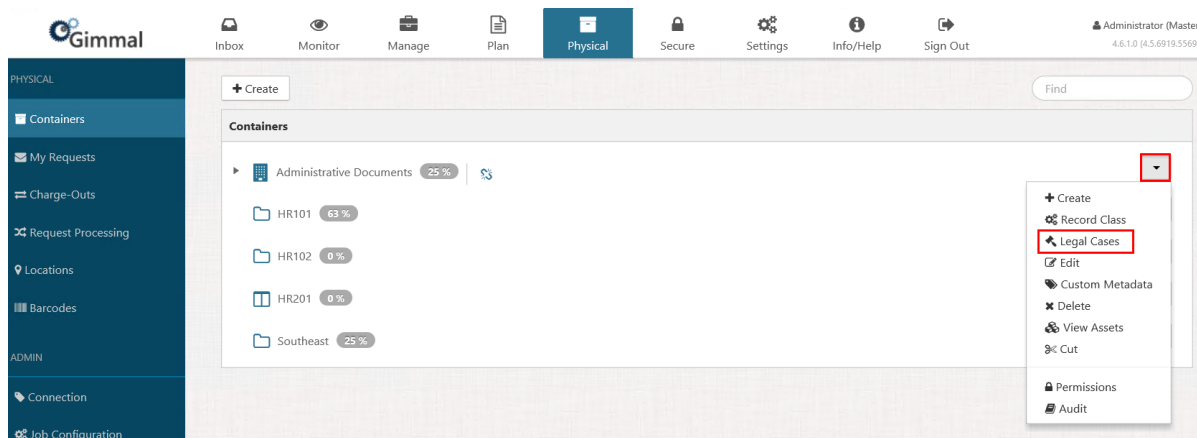
A legal case represents litigation or an audit in which items with various repositories need to be placed on legal hold as part of the Discovery process. A legal hold suspends a document's Lifecycle and prevents any disposition or modifications of the record/asset from occurring. You can assign a legal case to a container. This means that every physical asset that exists in this container, or that will be added to this container, will automatically inherit the legal case.

Legal holds do not "cascade" down to other child containers. You have to repeat this process for each container in the hierarchy.

- If you add a legal case to a container that has physical assets, and those physical assets are locked, you cannot create additional child assets.
- For information on creating legal cases, see [Creating a Legal Case](#)²².
- To add a legal hold to a physical asset, see [Adding a Legal Hold to a Physical Asset](#)²³.

To add a legal case to a container, perform the following steps:

1. Select **Physical** on the Main Menu, and then **Containers** on the left navigation menu. The Containers page displays.
2. Locate the container that you want to add a legal case to, and click the drop-down arrow on the right side. The container context menu displays. (The drop-down options you see may vary, depending on your permissions.)



3. Click **Legal Cases**. The Legal Cases window opens.
4. Select a legal case from the Available Legal Cases drop-down and click **Add**. The legal case displays under Active Legal Cases.
5. Click **Close** to close the window.

Removing a Legal Case/Legal Hold

When it is safe to do so, you can remove a legal hold from a physical item. This is typically when your in-house or outside legal counsel tells you to do so, after litigation or audits are complete and have been fully responded to. All holds must be removed from an item in order for it to be processed through to the next lifecycle phase of the policy.

²² <http://docs.gimmel.com/en/6127-adding-a-legal-hold-to-a-physical-asset.html>

²³ <http://docs.gimmel.com/en/6127-adding-a-legal-hold-to-a-physical-asset.html>

The steps you perform to remove a legal case/legal hold vary, depending on how the legal hold/legal case was originally applied. The following sections describe each method. Perform the following steps as a user or Physical Administrator who is assigned a Record Manager account.

Removing a Legal Case that was Added to a Container

- Removing a legal case from a container **does not** remove the legal hold from the container's assets.
- You can remove legal holds manually or wait until the case reaches the closed date.
- To remove the legal hold manually, click **Manage** on the Main Menu, and then click **Legal Cases** on the left navigation menu. On the Legal Cases page, click the drop-down for the desired legal case, click **Legal Holds**, and then click the **X** for each hold you want to remove.

An indirect (inherited) legal hold placed on a physical asset can only be removed by lifting the hold on the parent container. Perform the following steps:

1. Select **Physical** on the Main Menu, and then **Containers** on the left navigation menu. The Containers page displays.
2. On the container whose legal case you want to remove, click the drop-down on the right-hand side and select **Legal Cases**.

The Legal Cases dialog opens.

Legal Cases [X]

Container
HR101

Available Legal Cases
[X] [v] [Add]

Active Legal Cases

Jones vs. Harris	[X]
------------------	-----

[Close]

3. Click the **X** next to the legal case(s) you want to remove. The legal case is removed from the list.
4. Click **Close**.

Removing a Legal Hold that was Created with a Legal Hold Rule

1. Select **Manage** on the Main Menu, and then Legal Cases on the left navigation menu. The **Legal Cases** page displays.
2. On the legal case whose hold you want to remove, click the drop-down on the right-hand side and select **Legal Hold Rules**.

The Legal Hold Rules dialog opens.

Legal Hold Rules
✕

Clear

|
▼

Add Rule Set

Property	Operator	Value	Data Type	Join	
<input type="text" value="@folder"/>	= ▼	<input type="text" value="Legal"/>	Text ▼	None ▼	✕

Save
Cancel

3. Click the **X** next to the legal hold rule you want to remove. The rule is removed from the list.
4. Click **Save** to close the dialog and return to the Legal Cases page.

4.15.9 Assets

In Physical Records Management, a physical asset consists of something tangible, such as a document, a box, a folder, a carton, a DVD, etc. A physical asset is created and added to containers, where they are managed individually with respect to a lifecycle and requests. Physical assets can be created by any user with the appropriate permissions, and they must have a parent (either a container or another physical asset).

4.15.9.1 Asset Properties

4.15.9.2 Associating Assets to a Record Class

4.15.9.3 Creating Physical Assets

4.15.9.4 Modifying Existing Assets

4.15.9.5 Copying Assets

4.15.9.6 Searching for Assets

4.15.9.7 Viewing Asset Properties and Record Details

4.15.9.8 Asset Properties

The following table contains a list and description of the physical asset properties found on the Create and Edit Physical Asset dialog.

Property	Required	Default	Description
Name	Yes		The unique name for the physical asset; maximum characters allowed is 128; special characters are permitted
Title	No		An optional title.
Subject	No		An optional subject/description of the physical asset.
Keywords	No		An optional keyword(s) about the physical asset.
Home Location	Yes	<p>Location Based Container: full path to the container (node) where the asset is being created. It is calculated automatically based on container structure and cannot be changed.</p> <p>Logical-based Container: Unknown</p>	<p>The Home Location field is container (node)-specific.</p> <p>Location Based Container: The Home Location will always show the full path of the physical asset in relation to the way the containers are structured; for example: Parent Container > Child Container > Sub-child Container, and so on. The advantage of this is that organizations can create a "real-world" structure of where their physical items are being stored. All physical assets created in a location-based container will have the same Home Location.</p> <p>Logical-based Container: Select from a list of locations where the physical asset "lives" (for example, a street address). You can have multiple physical assets that each have a different Home Location. You must select a Home Location for each physical asset you create.</p>
Temporary Location	No		Defines a temporary location that you can assign to a physical asset when it has been moved to another location on a temporary basis. For example, if you have a box of documents that is located in a warehouse office, and the office receives flood damage, you can move that box to another location, and indicate this using the Temporary Location field. This field pulls from the Locations list. See Managing Locations ²⁴ for more information on creating locations and applying them to a physical asset.
Asset Type	Yes	Box	<p>Defines the type of physical asset you're creating. Possibilities are:</p> <ul style="list-style-type: none"> • Box • Document • Folder • Other

²⁴ <http://docs.gimmel.com/en/5905-managing-locations.html>

Property	Required	Default	Description
Other Asset Type	No		If the Asset Type "Other", this property becomes available.
Format	No	Yes	Defines the format of the physical asset. Possibilities are: <ul style="list-style-type: none"> • None • CD • DVD • Film • Microfiche • Microfilm • Mixed • Negative • Optical • Paper • Slide • Tape • Video • X-Ray • Other
Other Format	No		If the Format "Other", this property becomes available.
Owner	Yes	Current user(s)	Defines who owns the physical asset. Users of the system are part of the drop-down, however, other values to represent external users can be entered as well.
Allow Requests	Yes	Yes, unless parent is set to No, in which case the value is No and cannot be changed.	Determines whether the physical asset is available for request.
Barcode			Allows manual entry of a barcode to apply to an asset or displays the barcode schemes to allow selection from there (if configured). These values appear from the drop-down menu and the next available barcode number according to the scheme is entered automatically.
Barcode Symbology			The type of barcode symbology to use.

Property	Required	Default	Description
Barcode Alternate			A Barcode Alternate is useful when you have assets that may have need separate barcodes for internal and external usage. This property works the same way as Barcode.
Barcode Symbology Alternate			The type of barcode symbology to use for the Barcode Alternate.

4.15.9.9 Associating Assets to a Record Class

A record class defines a named grouping in which physical assets can be assigned. Associated to this grouping, or record class, is a number of properties that define more detailed information about the asset, as well as the Lifecycle that assets that are assigned to this grouping will follow.

1. Select **Physical** on the Main Menu, and then **Containers** on the left navigation menu. The Containers page displays.
2. Locate the container that has the physical asset you want to associate to a record class, click the drop-down arrow on the right side, and select **View Assets**. The Physical Assets dialog opens.

Physical Assets

/ Houston Corporate Office

+ Create + Create Request + Create Return Find

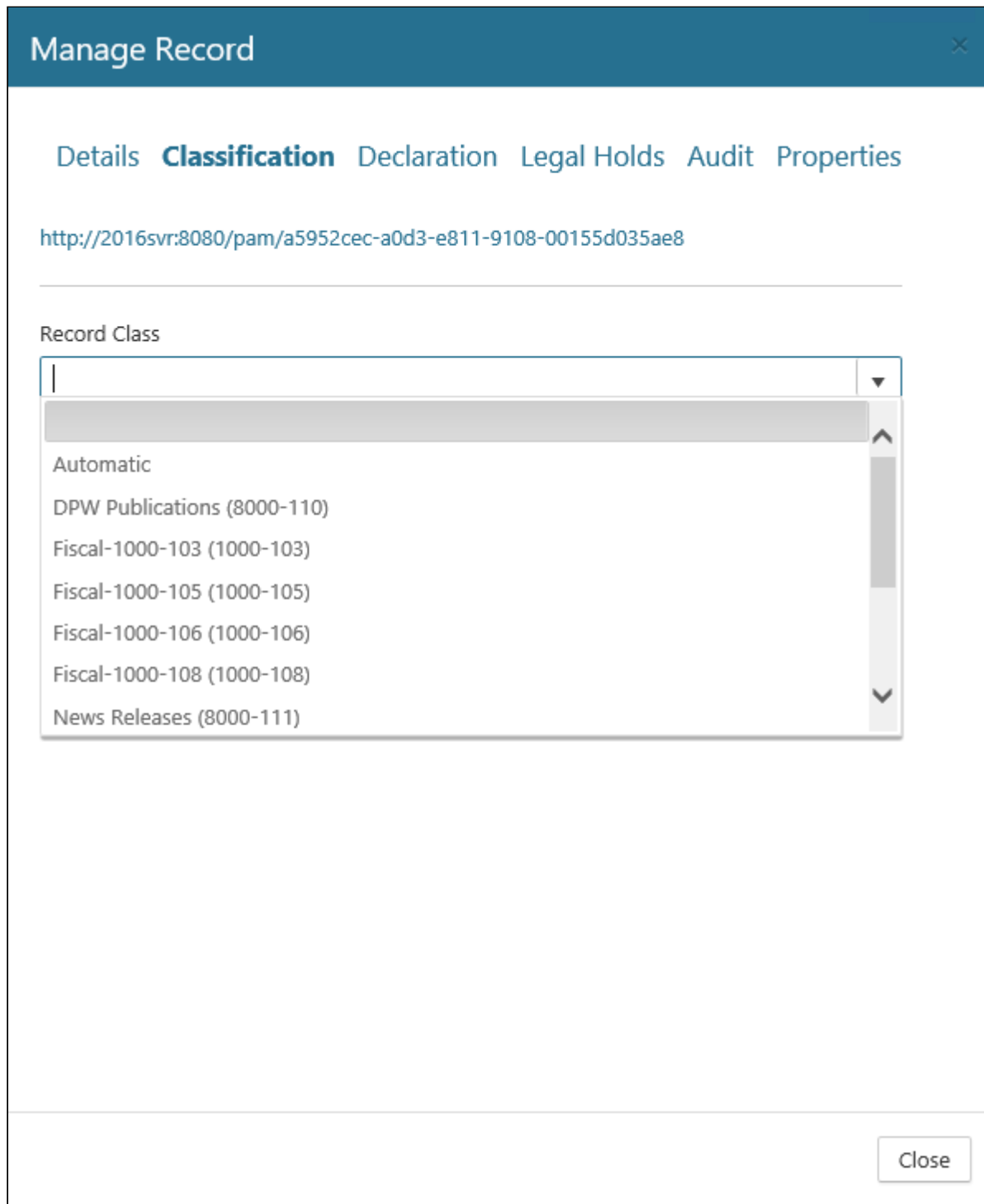
Name	Title	Owner	Availability Status
▶ Benefits Forms	Benefits Forms	Administrator	In
▶ Employee Tax Forms	Employee Tax Forms	Administrator	In
▶ Expired Legal Contracts	Expired Legal Contracts	2016devdomain\physicale...	In

Create Child
 Edit
 Move
 Delete
 Properties
 Add to Request
 Add to Return
 Custom Metadata
Manage Record
 Audit

1 - 3 of 3 items

Close

3. Right-click the desired asset, and select **Manage Record**. The Manage Record dialog opens.
4. Click the **Classification** tab.
5. Click the drop-down arrow, select the desired record class, and then click **Save**.



6. Click **Close** to close the dialog.

Adding a Legal Hold to an Asset

Legal holds can be added manually or automatically to physical assets. Automated legal holds are part of the core platform, and more information can be found by viewing the [Legal Case](#)(see page 191) topic.

To add a Legal Hold on a physical asset manually, perform the following steps:

1. Select **Physical** on the Main Menu, and then **Containers** on the left navigation menu. The Containers page displays.
2. Locate the container that has the asset you want to add the legal hold rule to, click the drop-down arrow on the right, and select **View Assets**. The Physical Assets window opens.

The screenshot shows the 'Physical Assets' window for the 'Houston Corporate Office'. It features a table with columns for Name, Title, Owner, and Availability Status. A context menu is open over the 'Expired Legal Contracts' row, with 'Manage Record' highlighted in red. The table contains the following data:

Name	Title	Owner	Availability Status
Benefits Forms	Benefits Forms	Administrator	In
Employee Tax Forms	Employee Tax Forms	Administrator	In
Expired Legal Contracts	Expired Legal Contracts	2016devdomain\physicale...	In

The context menu options are: Create Child, Edit, Move, Delete, Properties, Add to Request, Add to Return, Custom Metadata, **Manage Record**, and Audit. The 'Manage Record' option is highlighted with a red border. The window also includes a 'Close' button at the bottom right and a status bar at the bottom showing '1 - 3 of 3 items'.

3. Right-click the desired asset, and select **Manage Record**. The Manage Record dialog opens.
4. Click the Legal Holds tab.
5. Click the drop-down arrow, select the desired legal hold, and then click **Create**.

Manage Record ✕

[Details](#) [Classification](#) [Declaration](#) **Legal Holds** [Audit](#) [Properties](#)

<http://2016svr:8080/pam/8c5515ac-cedb-e811-9108-00155d035ae8>

Legal Case

Case 987654 ▼

Create

Close

4.15.9.10 Creating Physical Assets

Creating Physical Assets on a Container

- Physical assets must have a parent (either a container or another physical asset).
- Physical asset names only have to be unique for the container that they are in. You can have ten items called "Box 1" as long as they are located in different containers.

To create a physical asset, perform the following steps:

1. Select **Physical** on the Main Menu, and then **Containers** on the left navigation menu. The Containers page displays.
2. Locate the container that you want to add a physical asset to, and verify that the container is authorized to contain assets. Perform these steps:
 - Click the drop-down for the desired container, and then click **Edit**. The Edit Container dialog opens.

Edit Container ✕

Name ✕

Title

Subject

Keywords

Node Type **Location**

Location Type ▼

Capacity

Can Contain Assets ▼

Allow Requests ▼

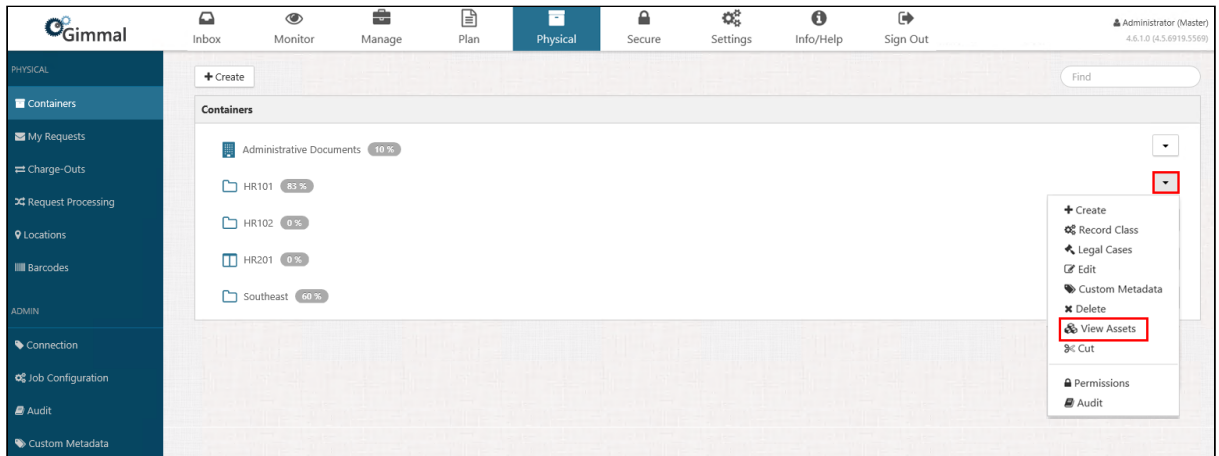
Barcode

Barcode Symbology ▼

Barcode Alternate

Barcode Symbology Alternate ▼

- Verify **Yes** is selected for the "Can Contain Assets" field, and then click **Cancel** to close the dialog and return to the Containers page.
3. Click the drop-down for the desired container and select **View Assets**. (The drop-down options you see may vary, depending on your permissions.)




The Physical Assets dialog opens. If the container has any physical assets, they will be listed alphabetically as shown below.

Physical Assets


/ HR101

+ Create + Create Request + Create Return Find

Name	Title	Owner	Availability Status
▶ Benefits Registration - Anderson	Benefits Registration - Anderson	2016DEVDOMAIN\techpubs	In
▶ Benefits Registration - Andrews	Benefits Registration - Andrews	2016DEVDOMAIN\techpubs	In
▶ Benefits Registration - Benson	Benefits Registration - Benson	2016DEVDOMAIN\techpubs	In
▶ Benefits Registration - Bentley	Benefits Registration - Bentley	2016DEVDOMAIN\techpubs	In
▶ Benefits Registration - Bush	Benefits Registration - Bush	2016DEVDOMAIN\techpubs	In

1 - 5 of 5 items 

Close

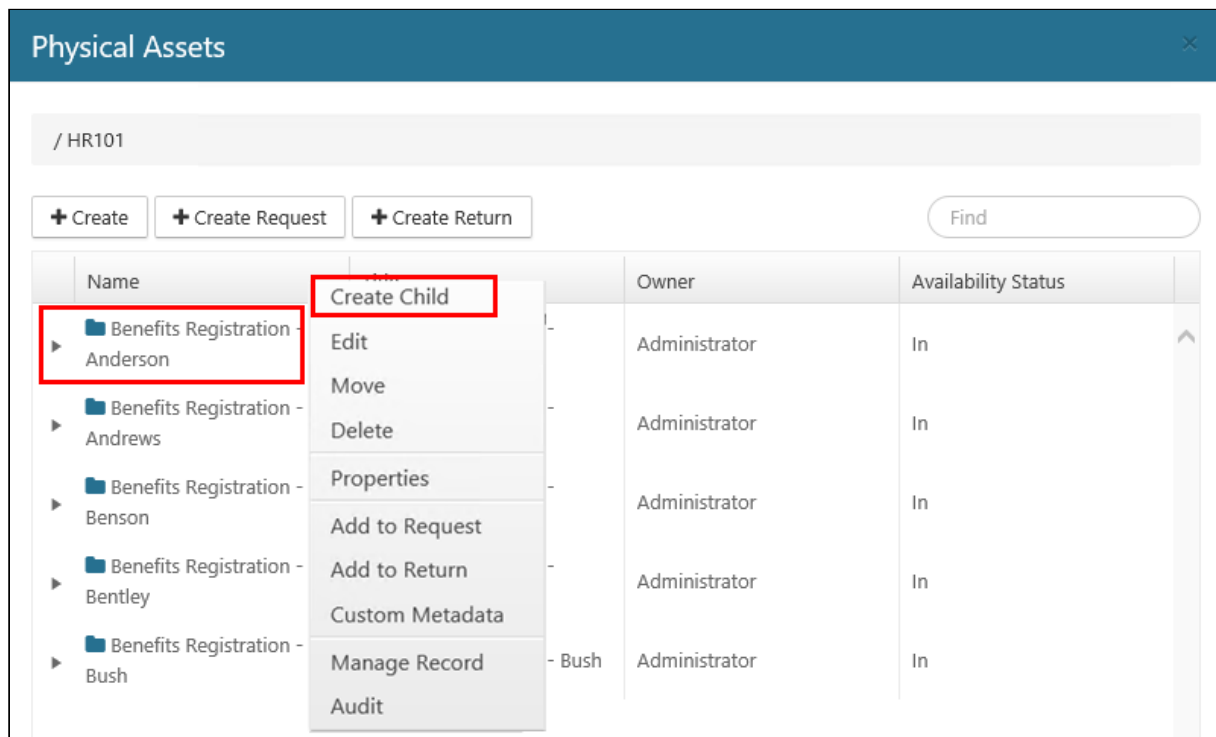
 If the asset you are expecting is not displayed, click the refresh icon on the lower right of the window.

4. Click **+Create**. The Create Asset dialog opens.
5. Enter the [asset properties](#)(see page 153).
6. Click **Create**. The Create Asset dialog closes, and the Physical Assets dialog opens. The new asset displays in a list on this dialog.
7. Click **Close** to close the Physical Assets dialog.

Creating a Child Asset

Physical Records Management enables you to create one level of children under a parent physical asset. The Home Location for a child asset is inherited from the parent asset. Child assets do not show up as records in the core Records Management system.

1. Follow steps 1 & 2 from Creating a Physical Asset above.
2. Click the drop-down for the desired container and select the **View Assets** option. The Physical Assets dialog opens.
3. Right-click the desired physical asset, and select the **Create Child** option.



4. Enter the [asset properties](#)²⁵. (The **Name (unique)**, **Home Location**, **Asset Type**, **Format**, and **Owner** fields are required.)

²⁵ <http://docs.gimmel.com/en/5901-managing-physical-assets.html>

5. Click **Create**. The new child asset is added to the Physical Assets dialog, under the parent asset.

The screenshot shows the 'Physical Assets' dialog with a breadcrumb path '/ HR101'. At the top, there are buttons for '+ Create', '+ Create Request', and '+ Create Return', along with a 'Find' search box. Below is a table with columns: Name, Title, Owner, and Availability Status. The table contains several rows, with the second row highlighted by a red box. This row is 'Tax Forms - Anderson' with title 'Tax Forms - Anderson', owner 'Administrator', and availability status 'In'. Below the table, there are pagination controls showing '1' of 1 items and a refresh icon, also highlighted by a red box.

Name	Title	Owner	Availability Status
Benefits Registration - Anderson	Benefits Registration - Anderson	Administrator	In
Tax Forms - Anderson	Tax Forms - Anderson	Administrator	In
Benefits Registration - Andrews	Benefits Registration - Andrews	Administrator	In
Benefits Registration - Benson	Benefits Registration - Benson	Administrator	In
Benefits Registration - Bentley	Benefits Registration - Bentley	Administrator	In
Benefits Registration - Bush	Benefits Registration - Bush	Administrator	In

4.15.9.11 Modifying Existing Assets

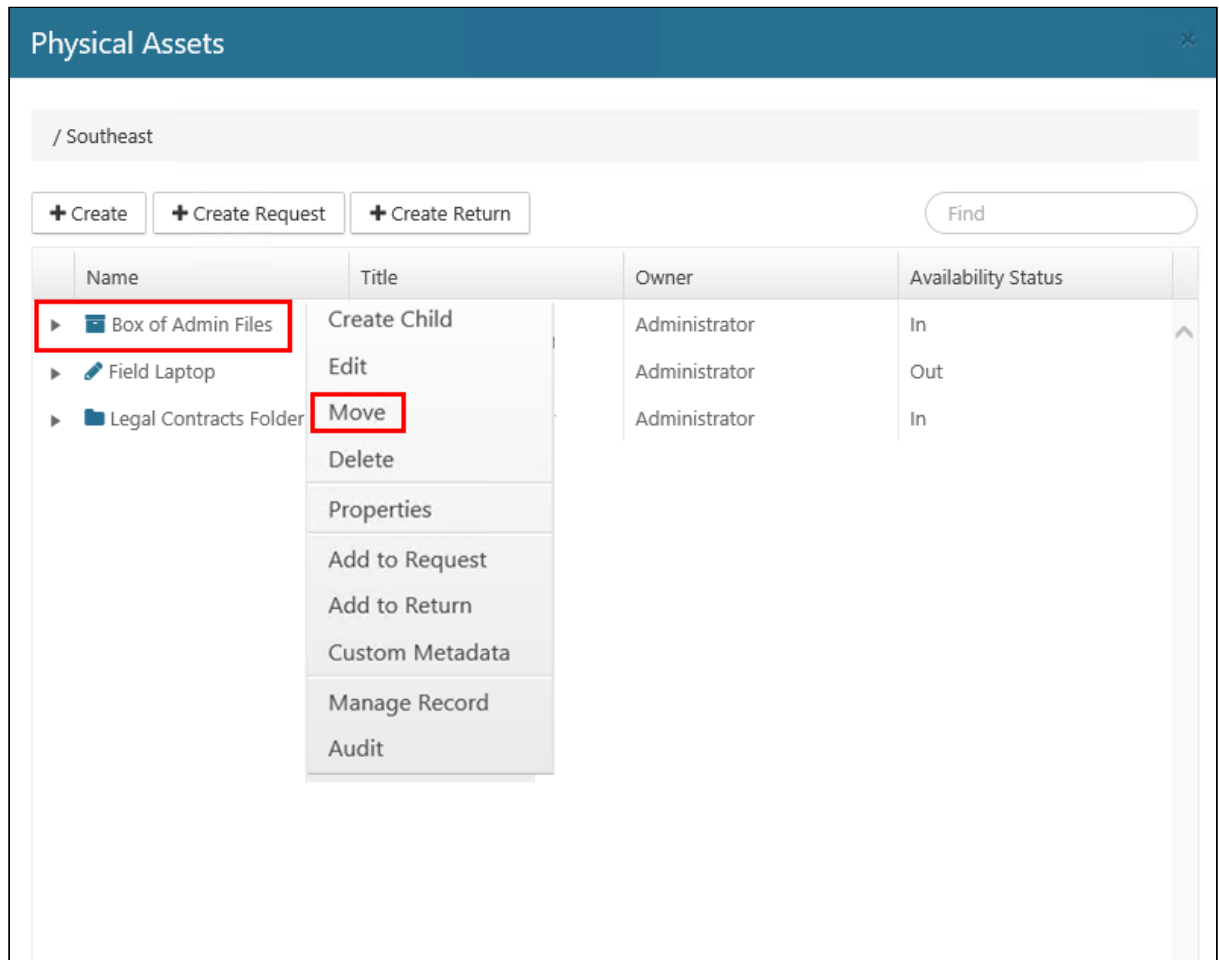
Moving an Asset

You can perform a move of a physical asset, whereby an asset is moved from one container to another, or the asset is moved under a parent asset.

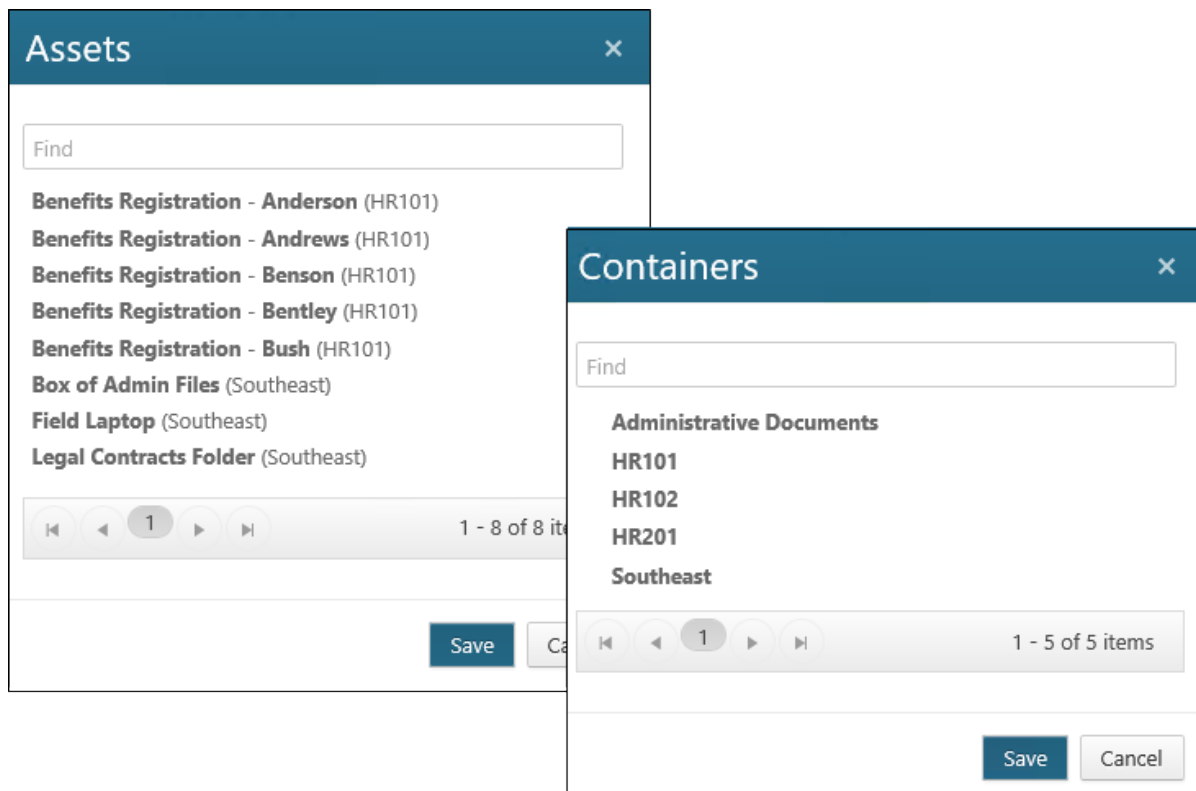
- An asset that has a direct hold placed on it (one that is applied manually to an asset/record) can be moved to another location and the hold will persist.
- An asset that has an indirect hold (one that is inherited either from the container or by the parent asset) cannot be moved unless the hold is removed from the parent.
- You cannot move a physical asset to a different parent container node type. For example, if a parent container has a node type of logical, the asset can only be moved to another container whose node type is logical.
- You cannot move an asset with children to another asset, as a child. You are only permitted one level of child assets.

To move a physical asset, perform the following steps:

1. Select **Physical** on the Main Menu, and then **Containers** on the left navigation menu. The Containers page displays.
2. In the Containers list, locate the container whose asset(s) you want to move, and click the drop-down arrow on the right.
3. Click **View Assets**. The Physical Assets dialog opens.
4. Right-click on the physical asset you want to move, and select **Move**.



5. From the Move To drop-down list, select **Container** or **Asset**.
6. Click the Parent Select icon to the right of the Parent field. The Containers dialog or the Assets dialog opens, providing a list of possible containers or assets that you can select and move the asset to.



7. Make your selection, and then click **Save**. If you moved the asset to another container or to an asset in another container, it will no longer appear on the Physical Assets dialog.

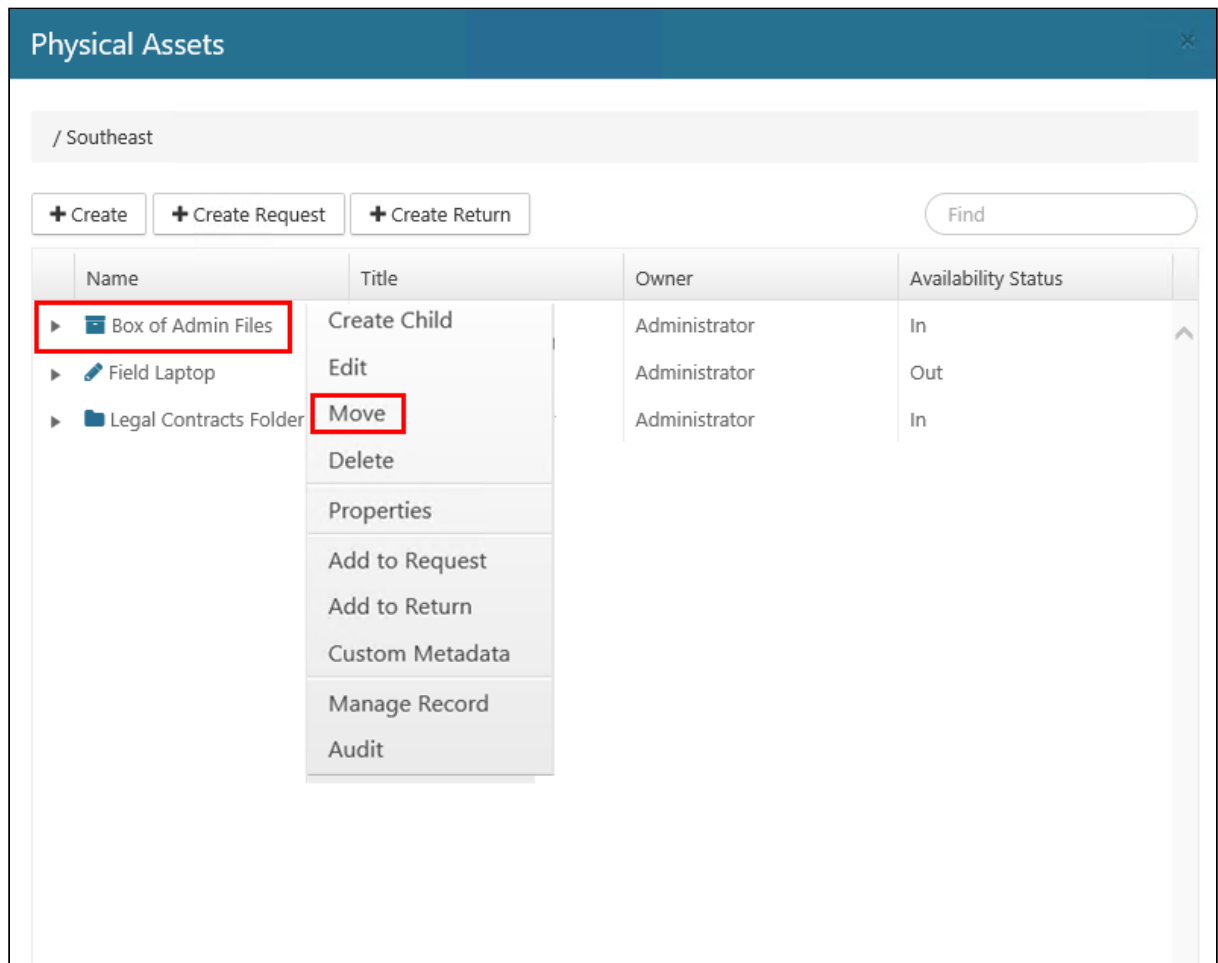
Editing & Deleting an Asset

Physical assets cannot be deleted if any of the following apply:

- An asset's container has a legal hold/legal case
- An asset has been declared a record
- An asset is charged-out

Follow these steps to Edit or Delete a Physical Asset:

1. Follow step 1, 2, and 3 from **Moving as Asset** above
2. Right-click on the asset you want to edit or delete. A context menu displays.

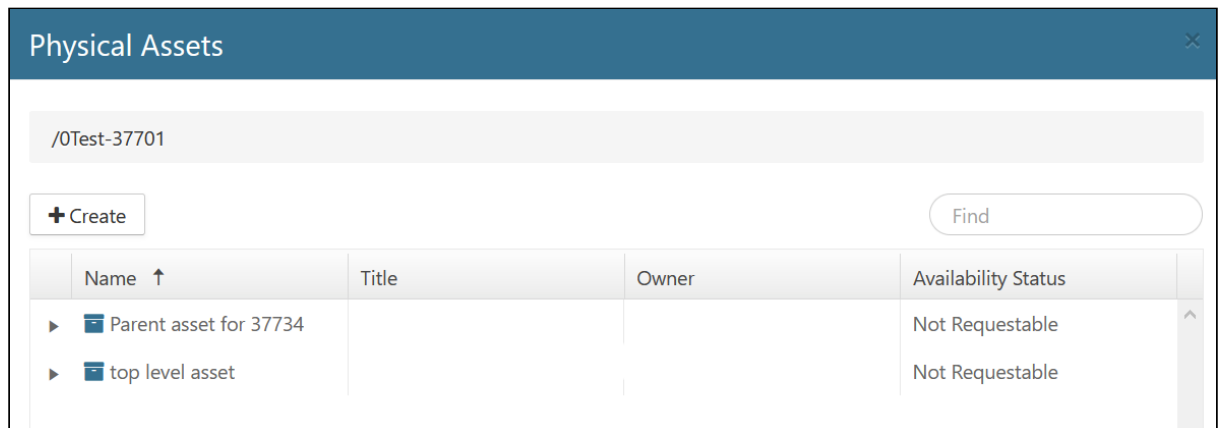


3. If you want to delete the physical asset, then select **Delete** and the Delete Asset dialog opens. **Click** Delete. The asset is removed from the list on the Physical Assets dialog. If you want to edit the physical asset move to step 4.
4. Select **Edit**. The Edit Asset dialog opens.
5. Change the [asset properties](#)(see [page 153](#)) as desired.
6. Click **Save**. The Edit Asset dialog closes, and the Physical Assets dialog opens. The edited asset displays in a list on this dialog.
7. Click **Close** to close the Physical Assets dialog.

4.15.9.12 Copying Assets

You can perform a copy of a physical asset, whereby an asset is copied to a container or to another asset. To copy an asset, perform the following steps:

1. Click Physical on the Main Menu, and then click Containers on the left navigation menu. The Containers page displays.
2. In the Containers list, locate the container whose asset(s) you want to copy, and click the drop-down arrow on the right.
3. Click View Assets. The Physical Assets dialog opens.



4. Right-click on the physical asset you want to copy, and select Copy.
5. The Copy Asset window opens, which lists the name of the asset you want to copy, and lets you select whether to copy it to a parent container or a parent asset.
6. From the Copy to drop-down list, select Container or Asset.
7. Click the Parent Select icon () to the right of the Parent field. The Containers dialog or the Assets dialog opens, providing a list of possible containers or assets that you can select and copy the asset to.
8. Make your selection, and then click Save. This will close the Containers dialog or the Assets dialog.
9. Enter or select the Owner.
10. Make any additional changes, and then click Copy. It may take a few moments for the window to close.
11. Click Close to close the Physical Assets window.

4.15.9.13 Searching for Assets

Physical Records Management has the ability to search for assets by **name** or **title** to easily find a specific asset.

To search for an asset, perform the following steps:

1. Login to Records Management with either of the following roles/permissions:
 - A user with the **Physical Administrator** role, or
 - A user with the **Physical User** role
2. Click **Physical** on the Main Menu, and then click **Containers** on the left navigation menu. The **Containers** page displays, along with a list of all of your containers.
3. Click the drop-down for the container that has the physical asset you're searching for, and select the **View Assets** option. The Physical Assets dialog opens.
4. In the **Find** field in the upper right corner, starting by entering the first few characters of the asset name or title until the results are filtered to match the characters you enter, and the desired asset(s) display.

The screenshot shows a window titled "Physical Assets" with a close button in the top right corner. Below the title bar, there is a breadcrumb path "/ HR101". A toolbar contains three buttons: "+ Create", "+ Create Request", and "+ Create Return". A search bar labeled "Find" is highlighted with a red rectangle. Below the toolbar is a table with the following data:

Name	Title	Owner	Availability Status
Benefits Registration - Anderson	Benefits Registration - Anderson	2016devdomain\techpubs	In
Benefits Registration - Andrews	Benefits Registration - Andrews	2016devdomain\techpubs	In
Benefits Registration - Benson	Benefits Registration - Benson	2016devdomain\techpubs	In
Benefits Registration - Bentley	Benefits Registration - Bentley	2016devdomain\techpubs	In
Benefits Registration - Bush	Benefits Registration - Bush	2016devdomain\techpubs	In

At the bottom of the table, there is a pagination control showing "1" and "1 - 5 of 5 items". A "Close" button is located at the bottom right of the window.

4.15.9.14 Viewing Asset Properties and Record Details

If you have view permission on a container, then you also have the ability to view any physical assets that are within that container. To view physical assets in a container, perform the following steps:

1. Select **Physical** on the Main Menu, and then **Containers** on the left navigation menu. The Containers page displays.
2. Locate the container whose physical assets you want to view, and click the drop-down arrow on the right side. The container context menu displays. (The drop-down options you see may vary, depending on your permissions.)
3. Click **View Assets**.

The Physical Assets window displays, showing a list of all the physical assets in that container.

The screenshot shows a window titled "Physical Assets" with a close button in the top right corner. Below the title bar, the container path "/ HR101" is displayed and highlighted with a red box. Below the path are three buttons: "+ Create", "+ Create Request", and "+ Create Return", along with a "Find" search box. The main area contains a table with the following columns: Name, Title, Owner, and Availability Status. The table lists five "Benefits Registration" assets, each with a unique name (Anderson, Andrews, Benson, Bentley, Bush) and an owner of "2016DEVDOMAIN\techpubs". All assets have an "In" availability status. At the bottom of the window, there are navigation controls (back, forward, refresh) and a "Close" button.

Name	Title	Owner	Availability Status
Benefits Registration - Anderson	Benefits Registration - Anderson	2016DEVDOMAIN\techpubs	In
Benefits Registration - Andrews	Benefits Registration - Andrews	2016DEVDOMAIN\techpubs	In
Benefits Registration - Benson	Benefits Registration - Benson	2016DEVDOMAIN\techpubs	In
Benefits Registration - Bentley	Benefits Registration - Bentley	2016DEVDOMAIN\techpubs	In
Benefits Registration - Bush	Benefits Registration - Bush	2016DEVDOMAIN\techpubs	In

Viewing Asset Properties

You can view the properties you entered when you initially created a physical asset. To view an asset's properties, perform the following steps:

1. Follow steps 1, and 2 from **Viewing Physical Assets in a Container** above
2. For the asset whose properties you want to view, right-click on the asset name. A drop-down menu displays. (The drop-down options you see may vary, depending on your permissions.)
3. Click Properties. The **Properties** dialog box opens, showing you the properties that were entered for that asset.

The screenshot shows a window titled "Physical Assets" with a breadcrumb "/ HR101". Below the breadcrumb are three buttons: "+ Create", "+ Create Request", and "+ Create Return", and a search box labeled "Find". The main area contains a table with the following columns: Name, Title, Owner, and Availability Status. The table lists five "Benefits Registration" assets, each with a lock icon. A context menu is open over the "Bentley" asset, with the "Properties" option highlighted in red. The menu options are: Create Child, Edit, Move, Delete, Properties, Add to Request, Add to Return, Custom Metadata, Manage Record, and Audit. At the bottom of the table, there are navigation arrows and a page indicator "1". The bottom right corner of the window has a "Close" button.

Name	Title	Owner	Availability Status
Benefits Registration - Anderson	Benefits Registration - Anderson	2016devdomain\techpubs	In
Benefits Registratic Andrews	Benefits Registratic Andrews	2016devdomain\techpubs	In
Benefits Registratic Benson	Benefits Registratic Benson	2016devdomain\techpubs	In
Benefits Registratic Bentley	Benefits Registratic Bentley	2016devdomain\techpubs	In
Benefits Registratic Bush	Benefits Registratic Bush	2016devdomain\techpubs	In

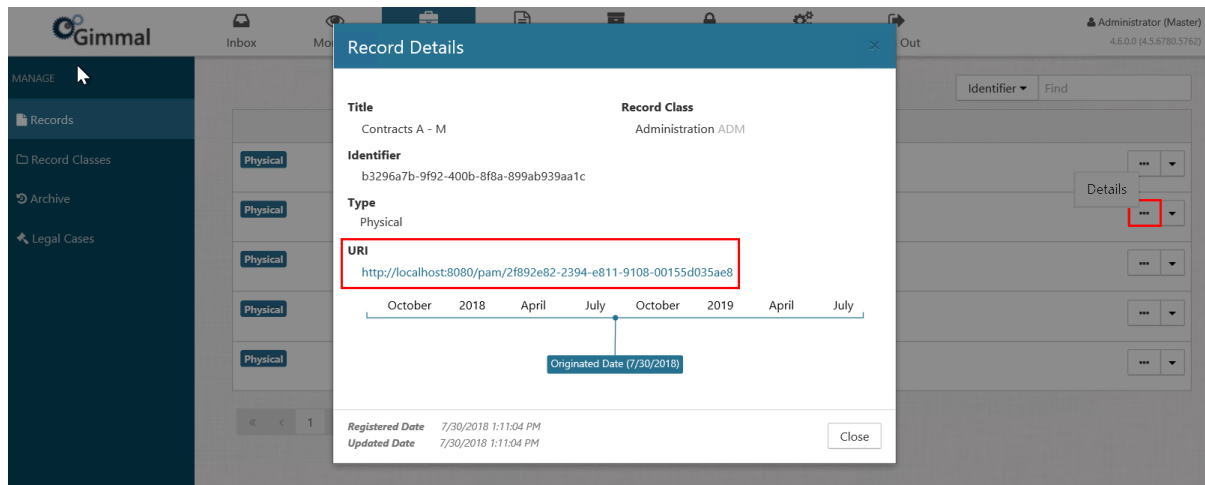
Viewing Asset Record Details

The core Records Management application provides a convenient way to view a physical asset's record details directly from the Records page. If a physical asset has child assets, they will display at the bottom of the Asset Details window as well.

Perform the following steps to view a physical asset's record details:

1. Follow step 1 from **Viewing Physical Assets in a Container** above
2. Click **Manage*** on the Main Menu, and then click **Records** on the left navigation menu. The Records page displays.

3. Locate the physical asset whose record details you want to view, and click the "Details" ellipsis (...) to the right of the asset name. The Record Details window opens.



4. Click the link under URI. The Asset Details page displays, showing the physical asset's metadata in View mode.

Asset Details ✕

/ Southeast

<p>Id e1d66226-72ba-e811-9109-00155d035ae8</p> <p>ParentId dd030ea9-71ba-e811-9109-00155d035ae8</p> <p>Name Field Laptop</p> <p>Title Field Laptop</p> <p>Subject --</p> <p>Keywords --</p> <p>Home Location / Southeast</p> <p>Temporary Location --</p> <p>Current Location / Southeast</p> <p>Charged-Out No</p>	<p>Asset Type Other</p> <p>Other Asset Type Laptop</p> <p>Format Other</p> <p>Other Format Hardware</p> <p>Owner Administrator</p> <p>Barcode --</p> <p>Barcode Alternate --</p> <p>Allow Requests Yes</p> <p>CreatedDate 9/17/2018 7:06:47 AM</p> <p>ModifiedDate 9/17/2018 7:06:47 AM</p>
---	---

+ Create

Child Assets

Name	Title	Owner	Availability Status
No items to display			

⏪ ⏩ 0 ⏪ ⏩

No items to display

Close

- If you choose to add additional child assets, click the **+Create** button, and perform the steps described in [Creating a Child Asset](#) (see page 161). (Physical Users must have container permissions set to **Edit** or higher on this container to create additional child assets.)

4.15.10 Barcode Schemes

The Barcodes option enables the creation of common barcode schemes that are used within your organization. Barcodes can be assigned to assets and containers, enabling you to easily look up information for the files in the physical world by tagging them with the assigned barcode.

4.15.10.1 Barcode Properties

The following table contains a list and description of the barcode properties found on the **Create** or **Edit Barcode Scheme** dialogs. Properties with an asterisk (*) are required.

Property	Required	Description
Title*	Yes	The unique name of the Barcode Scheme
Prefix	No	An optional static prefix that will be used in barcode generated from this scheme
Suffix	No	An optional static suffix that will be used in barcode generated from this scheme
Start Range	Yes	The start range in the barcode number
End Range	Yes	The end range in the barcode number
Barcode Padding	Yes	The number of zeros padding the generated barcode number
Opened Date	No	The date in which the barcode scheme will be available for tagging
Closed Date	No	The date in which the barcode scheme will stop being available for tagging

4.15.10.2 Barcode Uniqueness

Barcodes across the entire system must be unique. No two assets, regardless of whether or not they use the same barcode schema can use the same barcode.

4.15.10.3 Creating a New Barcode Scheme

- Select **Physical** on the Main Menu, and then **Barcodes** on the left navigation menu. The Barcodes page displays.

2. Click **+Create**. The Create Barcode Scheme window opens.

Create Barcode Scheme

Title

Prefix

Suffix

Start Range

End Range

Barcode Padding

Opened Date

Closed Date

Create **Cancel**

3. Enter the required and optional fields as described in Barcode Properties above.

Since barcodes must be unique throughout the system, it is highly recommended you use a Prefix, Suffix, and/or Padding to ensure schemes can never attempt to produce the same barcode.

4. Click **Create**. The new barcode displays on the Barcodes page.

Title	Prefix	Suffix	Is Full
Administration Barcode	ADM	RPT	No
Human Resources Barcode	HR	FIL	No
Legal Contracts Barcode	LGL	CON	No

Page 1 of 1 (3 Items)

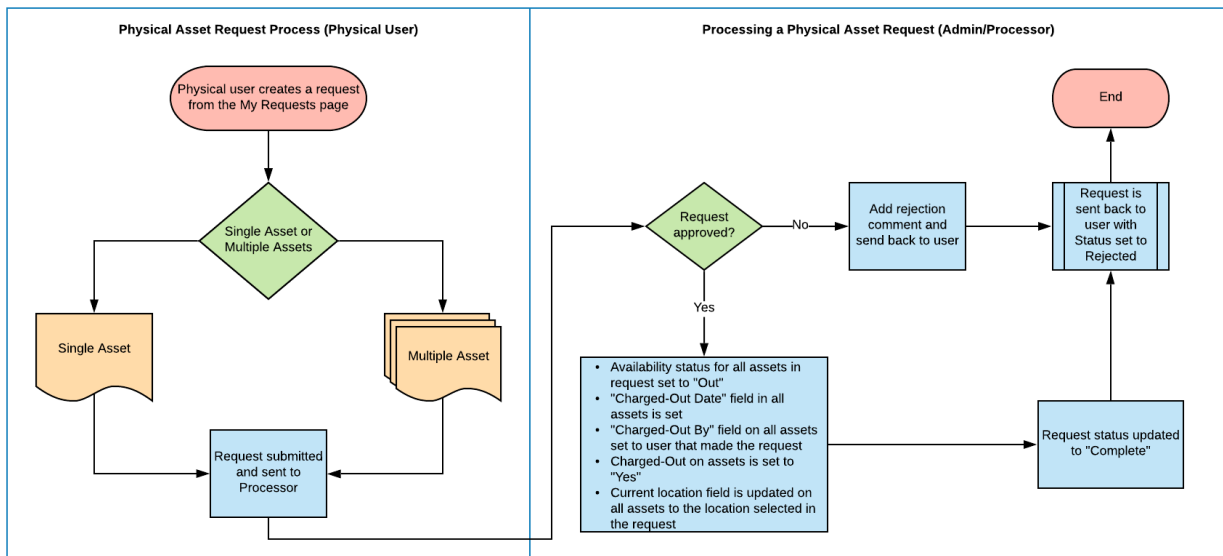
4.15.10.4 Editing or Deleting Barcode Scheme

1. Locate the barcode whose properties you want to edit, and click the drop-down arrow on the right side of the barcode name. The barcode context menu displays. (The drop-down options you see may vary, depending on your permissions.)
2. Click **Edit** and the Edit Barcode Scheme dialog opens. Click Delete on the context menu and the Delete Barcode Scheme dialog opens.
3. If editing, make your desired changes to the properties and then click **Save**. The barcode updates on the Barcodes page. If deleting, click **Delete** on the dialog. The barcode scheme is deleted, and no longer displays on the Barcodes page.

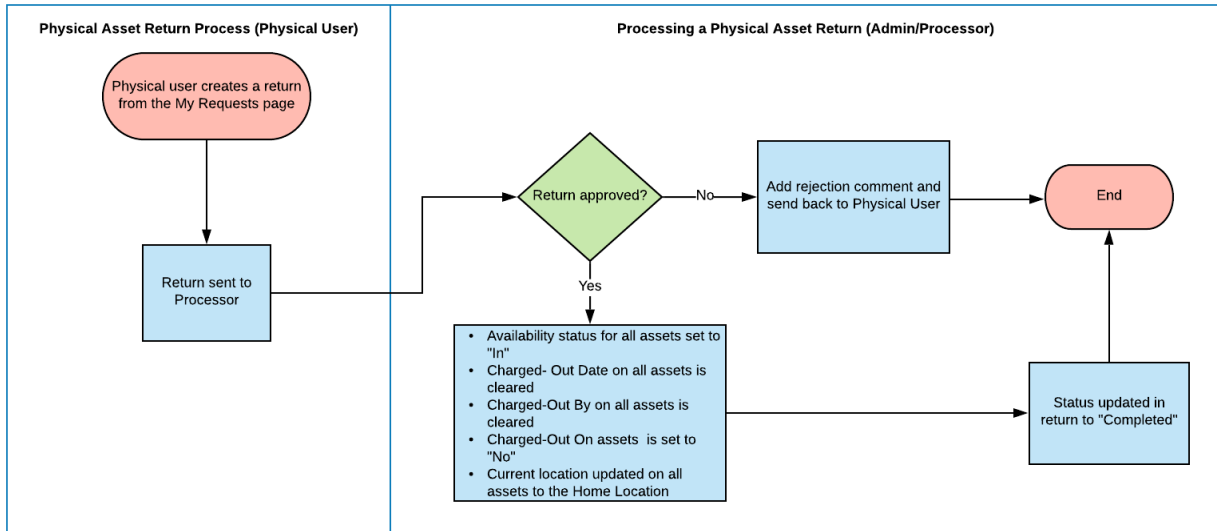
4.15.11 Request and Returns

The Physical Administrator is responsible for processing the requests and returns that have been submitted by the Physical User. The following flowchart illustrates the physical asset request/charge-out process, and the flowchart below illustrates the physical asset return/charge-in process. See the following topics for more information:

4.15.11.1 Processing Request



4.15.11.2 Processing Return



4.15.11.3 Managing All Charge-Outs

Managing charge-outs is generally covered in the [Managing Charge-Outs](#)(see page 69) topic in the User's Guide, however, Physical Administrators have a few more options available on charge-outs:

- The ability to see all users charge-outs
- Directly charge-in an asset, without a return

All Charge-Outs

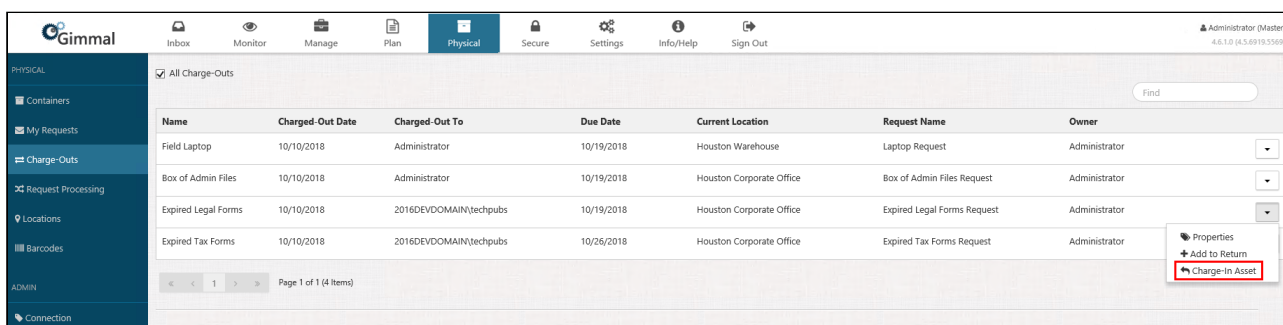
If you are logged in as a Physical Administrator you can see the additional checkbox in the upper left. Checking this box will allow you to view charge-outs for all users.

Name	Charged-Out Date	Charged-Out To	Due Date	Current Location	Request Name	Owner
Field Laptop	10/10/2018	Administrator	10/19/2018	Houston Warehouse	Laptop Request	Administrator
Box of Admin Files	10/10/2018	Administrator	10/19/2018	Houston Corporate Office	Box of Admin Files Request	Administrator
Expired Legal Forms	10/10/2018	2016DEVDOMAIN\techpubs	10/19/2018	Houston Corporate Office	Expired Legal Forms Request	Administrator
Expired Tax Forms	10/10/2018	2016DEVDOMAIN\techpubs	10/26/2018	Houston Corporate Office	Expired Tax Forms Request	Administrator

Charging-In a Single Asset

In the event that a user has possession of an asset and is not available to return the asset (for example, if the user is suddenly out on sick leave), you can return (charge-in) the asset in place of the that user. To charge-in a physical asset in place of the user, locate the asset you want to return, click the drop-down arrow on the right, and

select **Charge-In Asset**. A green confirmation message will display briefly in the upper right corner, indicating that the asset was successfully charged-in.



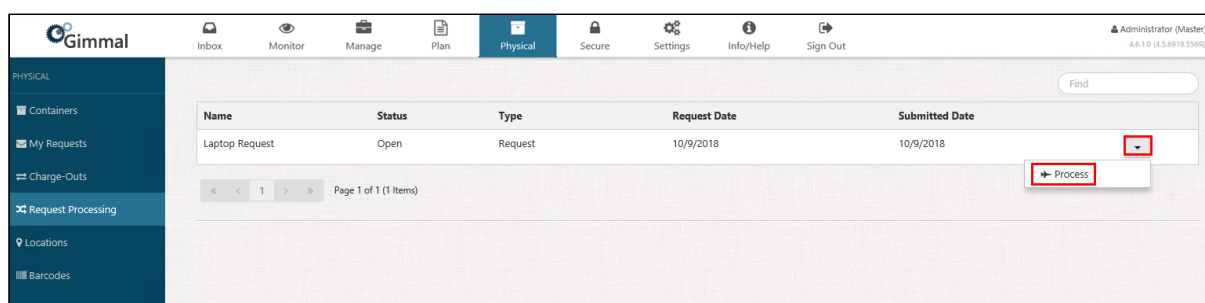
Name	Charged-Out Date	Charged-Out To	Due Date	Current Location	Request Name	Owner
Field Laptop	10/10/2018	Administrator	10/19/2018	Houston Warehouse	Laptop Request	Administrator
Box of Admin Files	10/10/2018	Administrator	10/19/2018	Houston Corporate Office	Box of Admin Files Request	Administrator
Expired Legal Forms	10/10/2018	2016DEVDOMAIN\techpubs	10/19/2018	Houston Corporate Office	Expired Legal Forms Request	Administrator
Expired Tax Forms	10/10/2018	2016DEVDOMAIN\techpubs	10/26/2018	Houston Corporate Office	Expired Tax Forms Request	Administrator

4.15.11.4 Processing a Request

The Request Processing page is where the fulfillment of physical asset requests (charge-outs) takes place. It is the responsibility of the Processor/Administrator to review the open requests, process them, and then mark the requests fulfilled (Charged-Out).

To process a charge-out request, perform the following steps:

1. Select **Physical** from the Main Menu, and then select **Request Processing** from the left navigation menu. The Request Processing page opens, along with a list of submitted requests. Note that the Status is "Open", indicating that the request is ready to be processed.
2. Click the drop-down next to the request that you want to process, and select **Process**.



Name	Status	Type	Request Date	Submitted Date
Laptop Request	Open	Request	10/9/2018	10/9/2018

The Process dialog opens, showing the properties associated with the request, as well as the physical asset that was requested (under the Assets section).

- The **Request Date** is the date the user wants the asset delivered to them.
 - The **Due Date** is the date the asset needs to be returned by.
 - The **Submitted Date** is the date the user submitted the request.
3. Determine if you will approve or reject the request by performing either of the following steps:
 - To approve the return, click **Approve**. The process starts to run and the request disappears from the Return Processing page. As soon as the Return Processor job is complete, the return reappears on the My Requests page, with the Status column updated to **Completed**. (Instead of waiting for the processor job to run, you can expedite the process by (link) forcing the job to run now.) To verify the approval process, see the next section.
 - To reject the return, enter a description in the Reason for Rejection field (optional) and then click **Reject**. The return is sent back to the user with a reason for rejection (if added by the processor). The user can modify the return and resubmit it.

Verifying Request Process Completion

To verify that the return approval process has completed properly, perform the following steps:

1. Navigate to the Physical Assets dialog from the container that is holding the asset that was requested.
2. Verify that the **Availability Status** column for that asset is "in".
3. Right-click on the asset and click **Properties**. (The drop-down options you see may vary, depending on your permissions.)

4. On the Properties dialog, verify that the **Charged Out** field is set to "No".

The screenshot shows the 'Physical Assets' interface with a table of assets. A context menu is open over the 'Field Laptop' asset, with the 'Properties' option highlighted. A red arrow points from this option to the 'Properties' dialog box. In the Properties dialog, the 'Charged-Out' field is highlighted with a red box and contains the value 'Yes'.

Name	Title	Owner	Availability Status
Box of Admin Files	Box of Admin Files	Administrator	In
Field Laptop	Field Laptop	Administrator	Out
Legal Contracts Folder	Legal Contracts Folder	Administrator	In

Field	Value
Name	Field Laptop
Title	Field Laptop
Subject	Laptop for field contractors
Keywords	--
Home Location	/ Southeast
Temporary Location	--
Current Location	Houston Warehouse
Asset Type	Other
Other Asset Type	Laptop
Format	Other
Other Format	Hardware
Owner	Administrator
Allow Requests	Yes
Charged-Out	Yes
Charged-Out Date	9/25/2018
Charged-Out To	Administrator
Is Child Asset	No
Barcode	--
Barcode Symbology	Code39
Barcode Alternate	--
Barcode Symbology Alternate	Code39

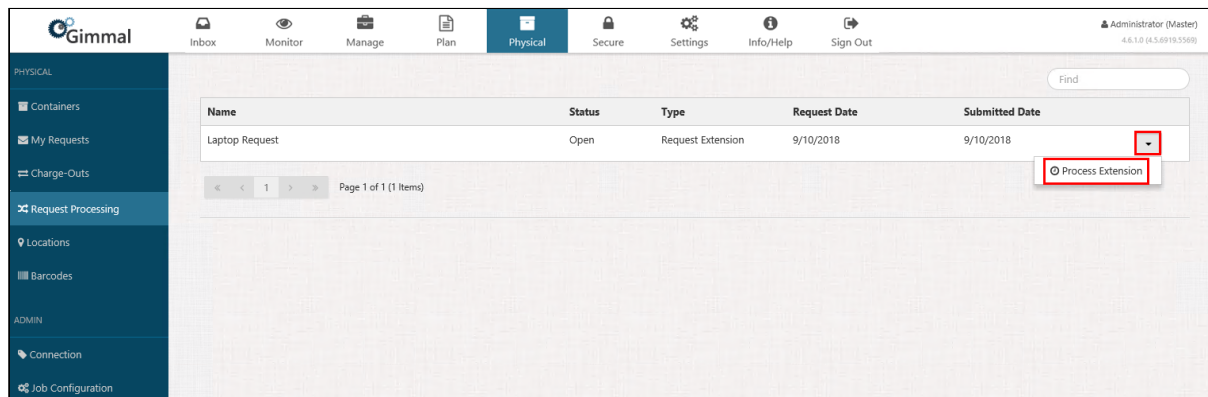
4.15.11.5 Processing a Request Extension

In addition to processing requests and returns, you can also process request extensions that take place when a user wants to extend the due date for returning a physical asset.

When a user submits a request extension, you can either approve the extension request with the new requested date, approve the request but change the date, or reject the request.

To process the request extension, perform the following steps:

1. Select **Physical** from the Main Menu, and then select **Request Processing** from the left navigation menu. The Request Processing page open, along with a list of submitted extension requests. Note that the Status is "Open", indicating that the request is ready to be processed.



The screenshot shows the Gimmal web application interface. The top navigation bar includes 'Inbox', 'Monitor', 'Manage', 'Plan', 'Physical' (selected), 'Secure', 'Settings', 'Info/Help', and 'Sign Out'. The left sidebar has 'PHYSICAL' and 'ADMIN' sections. Under 'PHYSICAL', 'Request Processing' is selected. The main content area displays a table with the following data:

Name	Status	Type	Request Date	Submitted Date
Laptop Request	Open	Request Extension	9/10/2018	9/10/2018

Below the table, there is a pagination control showing 'Page 1 of 1 (1 Items)'. A red box highlights a drop-down menu next to the 'Laptop Request' row, which is open and shows the option 'Process Extension'.

2. Click the drop-down next to the extension request that you want to process, and select **Process Extension**.

Process Extension ✕

Name Laptop Request

Reason Request for laptop to be used by contractor in the field

Request Date 9/25/2018 12:00:00 AM

Urgent No

User Administrator

Ship To Houston Warehouse

Submitted Date 9/25/2018 11:24:37 AM

Due Date 9/28/2018 12:00:00 AM

Extension Date

Notes

Reason for Rejection

Assets

Name	Title	Owner	Availability Sta...	Location
Field Laptop	Field Laptop	Administrator	In	/ Southeast

⏪ ⏴ 1 ⏵ ⏩

1 - 1 of 1 items

Approve
Reject

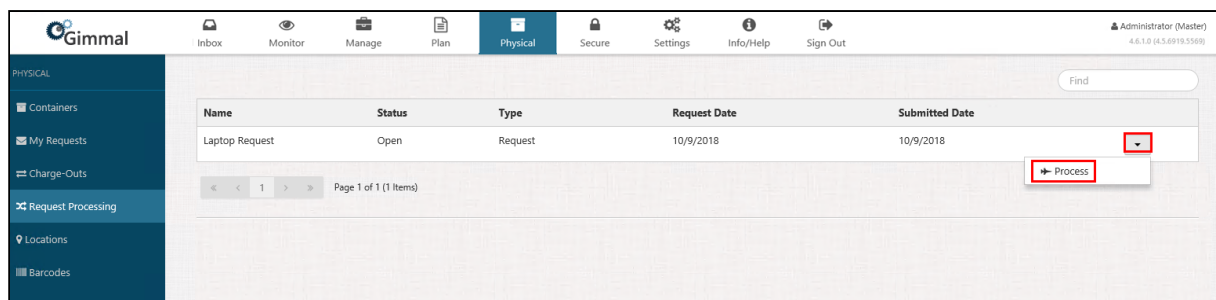
The Process Extension dialog opens, showing the properties associated with the request, as well as the physical asset that was initially requested (under the Assets section). Note that you can right-click on the asset to view its properties.

3. Determine if you will approve or reject the request by performing either of the following steps:
 - To approve the request, click **Approve**. The process starts to run and the request disappears from the Request Processing page. As soon as the Request Processor job is complete, the request reappears on the My Requests page, with the Status column updated to "Completed". (Instead of waiting for the processor job to run, you can expedite the process by (link) forcing the job to run now.) To verify the approval process, see the next section.
 - To approve the request, but change the request extension date, enter a new date in the Extension Date field, and then click **Approve**. You may want to enter a comment in the Notes field about why you changed the requested extension date.
 - To reject the request, enter a description in the Reason for Rejection box (required) and then click **Reject**. The request is returned to the user with a reason for rejection (if added by the processor). The user can modify the request and resubmit it.

4.15.11.6 Processing a Return

To process a charge-out request, perform the following steps:

1. Select **Physical** from the Main Menu, and then select **Request Processing** from the left navigation menu. The Request Processing page opens, along with a list of submitted requests. Note that the Status is "Open", indicating that the request is ready to be processed.
2. Click the drop-down next to the request that you want to process, and select **Process**.



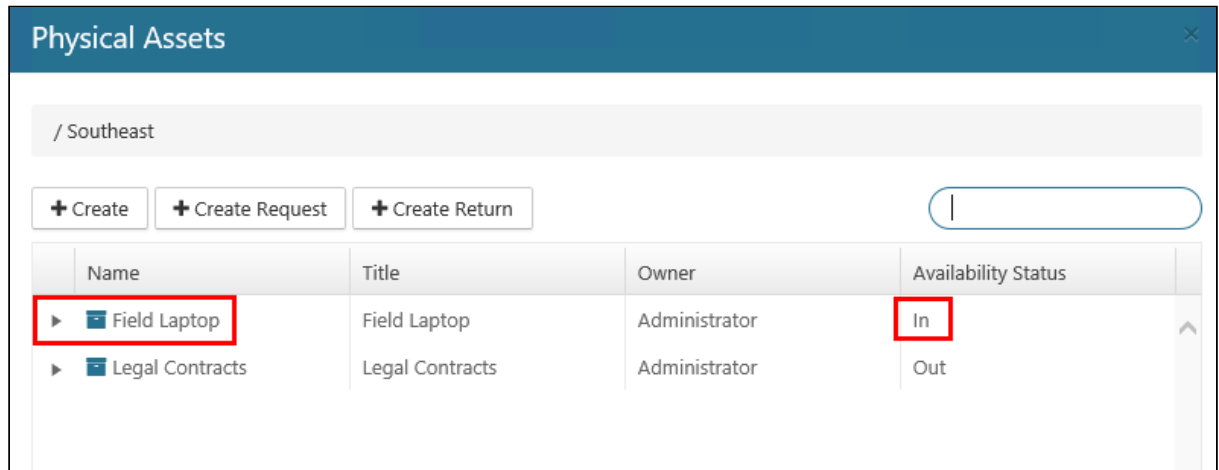
The Process dialog opens, showing the properties associated with the request, as well as the physical asset that was requested (under the Assets section).

- The **Request Date** is the date the user wants the asset delivered to them.
 - The **Due Date** is the date the asset needs to be returned by.
 - The **Submitted Date** is the date the user submitted the request.
3. Determine if you will approve or reject the request by performing either of the following steps:
 - To approve the return, click **Approve**. The process starts to run and the request disappears from the Return Processing page. As soon as the Return Processor job is complete, the return reappears on the My Requests page, with the Status column updated to **Completed**. (Instead of waiting for the processor job to run, you can expedite the process by (link) forcing the job to run now.) To verify the approval process, see the next section.
 - To reject the return, enter a description in the Reason for Rejection field (optional) and then click **Reject**. The return is sent back to the user with a reason for rejection (if added by the processor). The user can modify the return and resubmit it if desired.

Verifying Return Process Completion

To verify that the return approval process has completed properly, perform the following steps:

1. Navigate to the Physical Assets dialog from the container that is holding the asset that was requested.



The screenshot shows a 'Physical Assets' dialog window with a dark blue header and a close button. Below the header is a breadcrumb path '/ Southeast'. There are three buttons: '+ Create', '+ Create Request', and '+ Create Return', followed by a search input field. A table lists assets with columns: Name, Title, Owner, and Availability Status. The first row is 'Field Laptop' with status 'In', and the second row is 'Legal Contracts' with status 'Out'. Red boxes highlight the 'Field Laptop' name and its 'In' status.

Name	Title	Owner	Availability Status
▶ Field Laptop	Field Laptop	Administrator	In
▶ Legal Contracts	Legal Contracts	Administrator	Out

2. Verify that the **Availability Status** column for that asset is "in".
3. Right-click on the asset and click **Properties**. (The drop-down options you see may vary, depending on your permissions.)

- On the Properties dialog, verify that the **Charged Out** field is set to "No".

The screenshot shows the 'Physical Assets' interface with a table of assets. A context menu is open over the 'Field Laptop' asset, with the 'Properties' option highlighted. A red arrow points from this option to the 'Properties' dialog box. In the 'Properties' dialog, the 'Charged-Out' field is set to 'No' and is also highlighted with a red box.

Name	Title	Owner	Availability Status
Box of Admin Files	Box of Admin Files	Administrator	Out
Field Laptop	Field Laptop	Administrator	In
Legal Contracts Folder	Legal Contracts Folder	Administrator	In

Field	Value
Name	Field Laptop
Title	Field Laptop
Subject	--
Keywords	--
Home Location	/ Southeast
Temporary Location	--
Current Location	/ Southeast
Asset Type	Other
Other Asset Type	Hardware
Format	Other
Other Format	Laptop
Owner	Administrator
Allow Requests	Yes
Charged-Out	No
Is Child Asset	No
Barcode	--
Barcode Symbology	Code39
Barcode Alternate	--
Barcode Symbology Alternate	Code39

4.15.12 Custom Metadata and Templates

Physical Records Management enables you to create custom metadata fields with specific data types, add them to templates, which can then be associated with containers and assets. These custom metadata fields enable you to label an item with customized information that doesn't fit into any of the existing properties.

When associated with assets, the custom metadata will become part of the records and available for use in rules throughout the core Records Management product.

4.15.12.1 Custom Metadata

The following data types are available for Custom Metadata properties:

- Date
- Choice (drop-down)
- Choice (multiple)
- Number
- Single line of text
- True/False

To manage custom metadata, select Physical from the main menu and then Custom Metadata from the navigation menu:

Title	Type
Audited	True/False
Box Location	Text
Box Location ie11	Text
EmployeeID	Text
Inspected	True/False
My Date	Date
My Dropdown	Drop-down Choice
My Number	Number
Quarter	Drop-down Choice
Restricted	True/False

From here you can create new metadata by selecting +Create, or edit an existing property using the dropdown menu on the right side of any existing property.

4.15.12.2 Templates

Templates allow the creation of sets of Custom Metadata to group together and add to either Containers or Assets. Templates are available directly below Custom Metadata on the Navigation menu.

To create a new Templates follows the steps below:

1. Select **+Create** from the top left of the page and enter a unique Template name
2. Use the dropdown to select the Custom Metadata you want to add, then click the **Add** button

Create Template [Close]

Title * MyTemplate

Custom Metadata Audited [Add]

Template Metadata [Search]

- Audited
- Box Location
- Box Location ie11
- EmployeeID
- Inspected
- My Date
- My Dropdown

[Create] [Cancel]

3. Remove or rearrange the properties as necessary

Edit Template [Close]

Title * My Test CMD Template

Custom Metadata Audited [Add]

Template Metadata

- My Date
- My Dropdown
- My Number
- Box Location

*Drag and drop for ordering

[Save] [Cancel]

4. Click the **Create** button

i Delete Templates

Templates that are in use on either Containers or Assets cannot be removed.

4.15.12.3 Adding Custom Metadata to Containers and Assets.

When creating or editing Container or Assets, the ability to add a Template is available at the bottom of the window:

Custom Metadata Template

Personnel File ▼

Remove

Personnel File

EmployeeID

You can add as many Templates as necessary, and remove any that are no longer needed. Once added, the metadata will be available to populate.

4.16 Creating and Managing Legal Cases and Legal Holds

A Legal Case represents litigation or an audit in which items within various repositories need to be placed on Legal Hold as part of the discovery process. A Legal Hold suspends an item's Lifecycle and prevents any disposition or modifications of the item from occurring.

4.16.1 Legal Case Properties

Property	Description
Title	Defines the unique name of the Legal Case
Description	Defines the description of the Legal Case for informational purposes
Court	Defines the Court who is seeing this Legal Case
Case Number	Defines the Case Number for the Legal Case
Opened Date	Defines the date the Legal Case became active. Once this date has occurred, items can be placed on Legal Hold for the Legal Case.
Closed Date	Defines the date the Legal Case closed. Once this date has occurred, the Legal Holds will be lifted.

4.16.2 Creating a Legal Case

To create a Legal Case, perform the following steps:

1. Select **Manage** from the Main Menu.
2. Select **Legal Cases** from the left Navigation Menu.
3. Click **Create**.

4. Provide the necessary Legal Case Properties.
5. Click **Create**.

Create Legal Case ✕

Title	
Description	
Court	
Case Number	
Opened Date	5/25/2016 📅
Closed Date	📅

Create
Cancel

4.16.3 Managing Legal Holds

Legal Holds can be created both manually and automatically. To automatically create Legal Holds, Legal Hold Rules must first be defined on the Legal Case.

To create a Legal Hold Rule, perform the following steps as a user or Physical Administrator who is assigned a Record Manager account:

1. Click **Manage** on the Main Menu, and then click **Legal Cases** on the left navigation menu. The Legal Cases page displays
2. Click the drop-down for the desired Legal Case, and then select **Legal Hold Rules**. The Legal Hold Rules Editor opens. See the [Rule Builder page](#)(see page 125) for more information about how to build rules.
3. You can create the rules for the Legal Hold in two different ways. Refer to (Link) Understanding Rule Sets & Rule Groups for more information.
 - Select **Create** to manually define the rules.
 - Specify the Properties that should be used for the rule. The Properties are identical to the Classification Rule Properties. (Refer to (Link) Classification Rule Properties for a detailed description of each of the properties.)
 - Select **Add Rule Set** to add a Rule Set that has been pre-defined.
4. Click **Save**

4.16.4 Viewing Legal Holds for a Legal Case

To view the Legal Holds for a Legal Case, perform the following actions:

1. Select **Manage** from the Main Menu.
2. Select **Legal Cases** from the left Navigation Menu.
3. Click the drop-down for the desired Legal Case.
4. Select the **Legal Holds** option. The Legal Hold dialog opens, providing a list of legal holds for that Legal Case.

Legal Holds
×

Created Date	Uri	
5/17/2016 11:35:02 AM	\\rldemo\managed shares\tax\return\2000\2000 return.pdf	×
5/10/2016 11:35:44 AM	\\rldemo\managed shares\tax\return\2001\2001 return.pdf	×

«
<
1
>
»

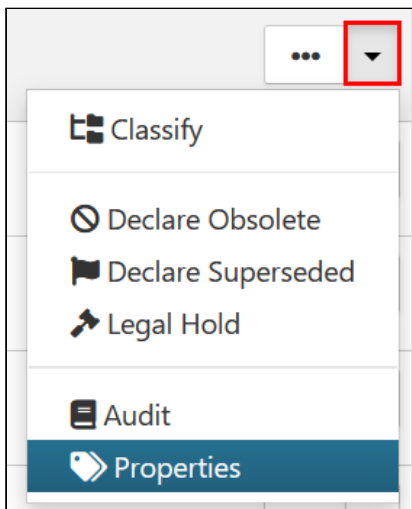
Page 1 of 1 (2 Items)

Close

4.17 Filtering Records by Rules and Metadata

Gimmel Records Management has the capability to allow records to be secured by a set of rules that can include virtually any type of metadata. Metadata is known as data that provides information about data, and for the purposes of this system, virtually everything known about the content is added as a **Property** to each record.

Whenever you see a record in the system, there is typically a quick way to see the properties by selecting a dropdown on the right side of the row and selecting Properties.



These properties can be used to filter records to specific users or groups by creating Record Filters and associating them to Record Classes. The following topics detail this process.

- [Intro to Record Filters](#)(see page 194)
- [Creating Record Filters](#)(see page 198)
- [Adding Filters to Record Classes](#)(see page 200)

4.17.1 Intro to Record Filters

Record Filters allow records to be filtered by a specific set of rules. These filters only apply to Users and Record Managers (not Global Record Managers). They apply to all aspects of the system such as Managing Records, Disposition tasks, and Reports.

Record Filters are assigned to Record Classes and secure records according to all the filters for Record Classes. Filters work in an inclusive manner, meaning that once a Record Class has been assigned at least one filter, only members of that Record Filter will have access to those records. Users will continue to be bound by the permissions given to them for a specific Record Class.

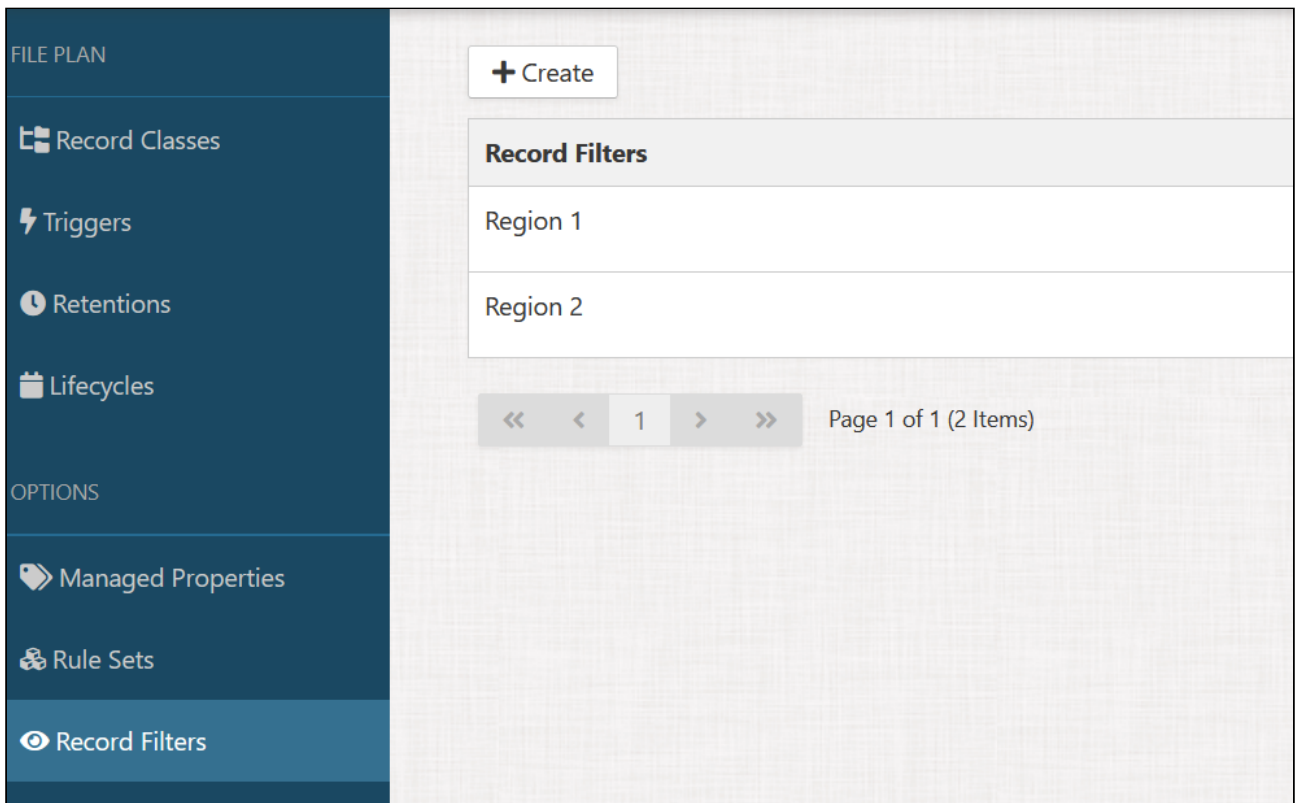
4.17.1.1 Record Filters in Practice

If an organization has multiple regions that they operate in, and each region has its own records manager, a Record Filter could be created for each region to secure records within the system to the appropriate records managers. This accomplished by having some metadata that was consistent throughout all records in that region. This could be a SharePoint Site Collection, a folder on your network file system, or specific property(s) that are common to all records in a particular region.

In the following example, an organization with two regions, each with a different records manager, Record Filters could be added to separate the records without needing to make any changes to the File Plan.

The URI would need the third part to identify the specific region; <https://mysharepoint/sites/region X> or <\\myserver\shares\region X>.

Two Record Filters would be created, Region 1 and Region 2:



Set the group membership and rules for Region 1:

Group Membership ✕

Select a user... + Add

Group Members

Region 1 Record Managers 🗑️

<< < 1 > >> Page 1 of 1 (1 Items)

Close

Record Filter Rules ✕

Clear 👤 Add Rule Set

Property	Operator	Value	Data Type	Join	
@uri_level3	=	Region 1	Text	None	✕

Save Cancel

Set the group membership and rules for Region 2:

Group Membership ✕

Select a user... + Add

Group Members

Region 2 Record Managers ✕

<< < 1 > >> Page 1 of 1 (1 Items)

Close

Record Filter Rules ✕

Clear Add Rule Set

Property	Operator	Value	Data Type	Join	
<input type="text" value="@uri_level3"/>	=	<input type="text" value="Region 2"/>	Text	None	✕

Save Cancel

Once the group membership and rules are created, you can add each of the Record Filters to the necessary Record Classes:

Record Filters ✕

Available Record Filters + Add

Record Class Record Filters

Region 2 ✕

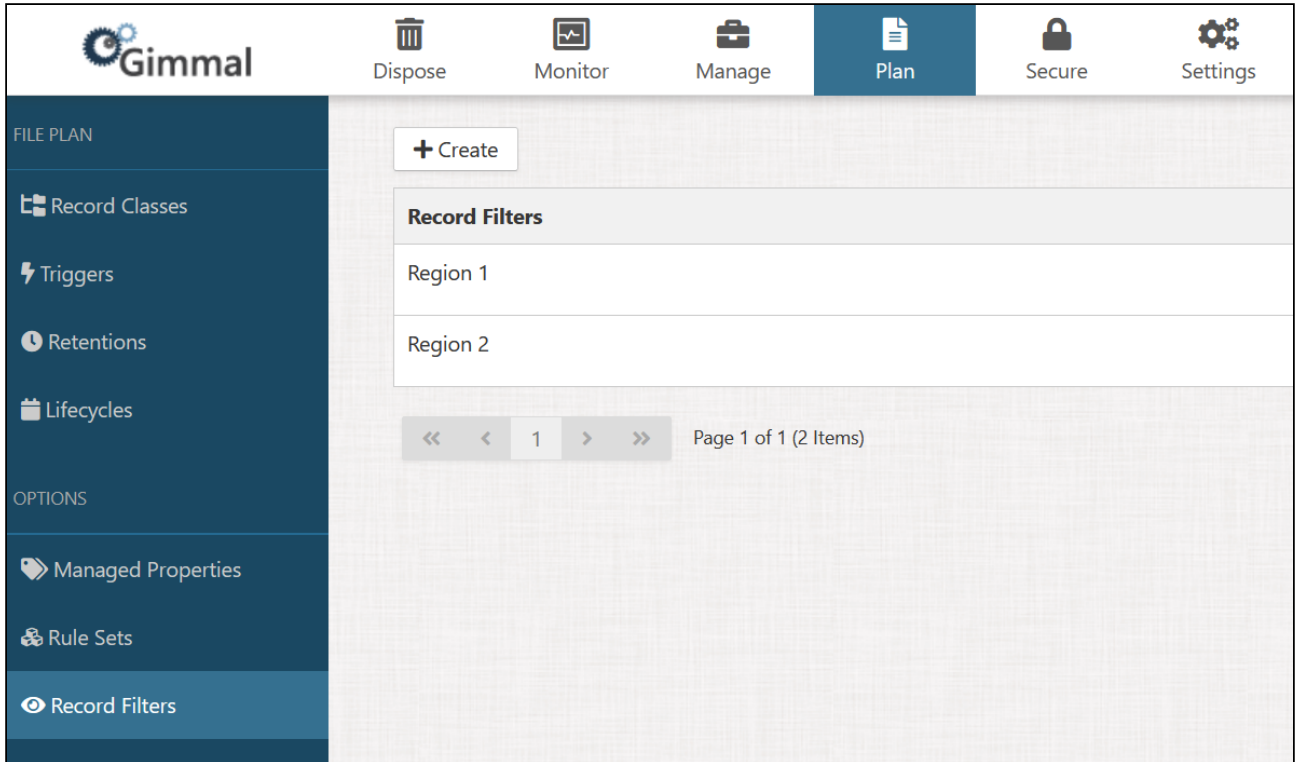
Region 1 ✕

Save Cancel

Once this is complete, the system will make updates to the records in a background service to apply the filters. Once finished, the members of Region 1 and Region 2 groups will only have access to records that meet the given rules.

4.17.2 Creating Record Filters

Record Filters are created and managed from the Plan main menu selection.



When you select the Create button, the following window appears, where you should enter a unique name for the new Record Filter.

 A dialog box titled 'Create Record Filter' with a close button (X) in the top right corner. The dialog contains a text input field labeled 'Name *'. Below the input field, there are two buttons: 'Create' and 'Cancel'.

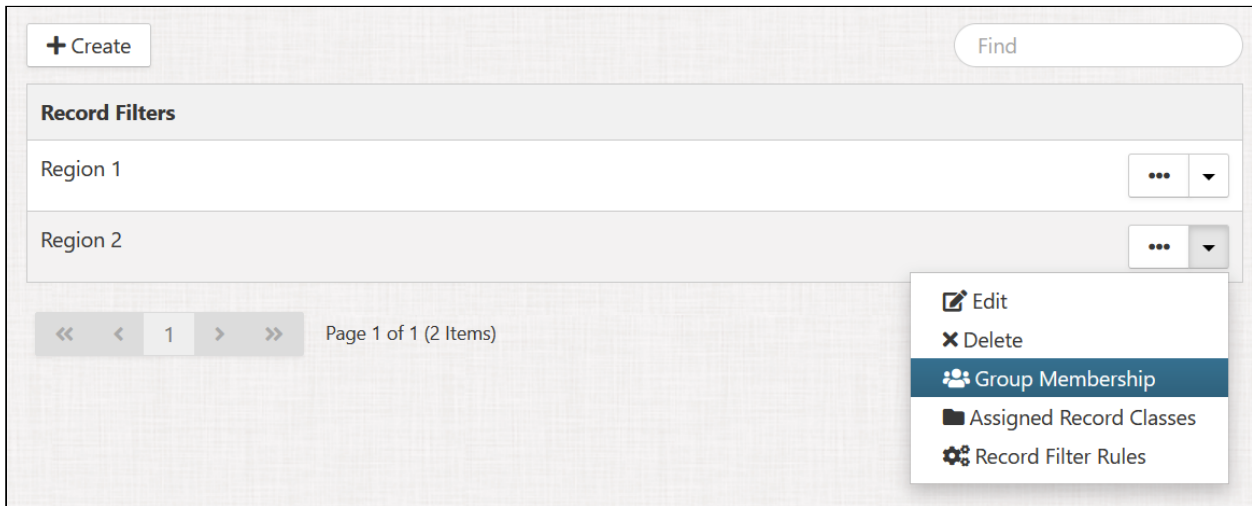
Once a filter is created, the drop-down menu on the right side of each filter allows the following actions:

- Edit
- Delete
- Group Membership
- Viewing and removing assigned Record Classes
- Rules

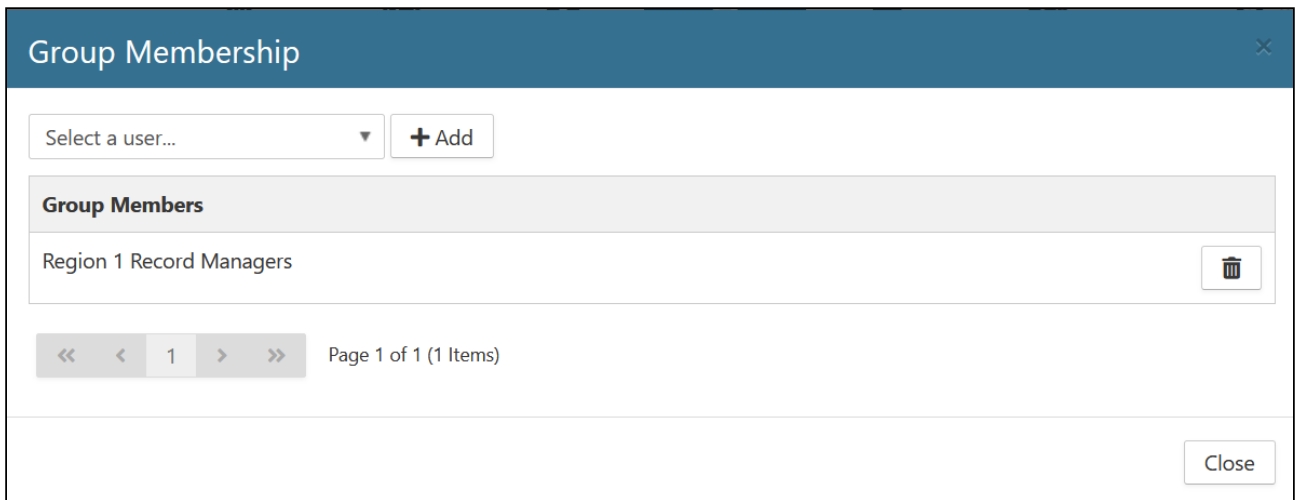
4.17.2.1 Group Membership

Group membership works in an inclusive manner, meaning that all members added to the group will gain access to records for a particular Record Class when the rules for the filter result in a positive outcome. If there are no Record Filters that include a specific user, that user will not be able to see any records that belong to that Record Class.

To create Group Memberships, select the drop-down menu for a Record Filter and select Group Membership.

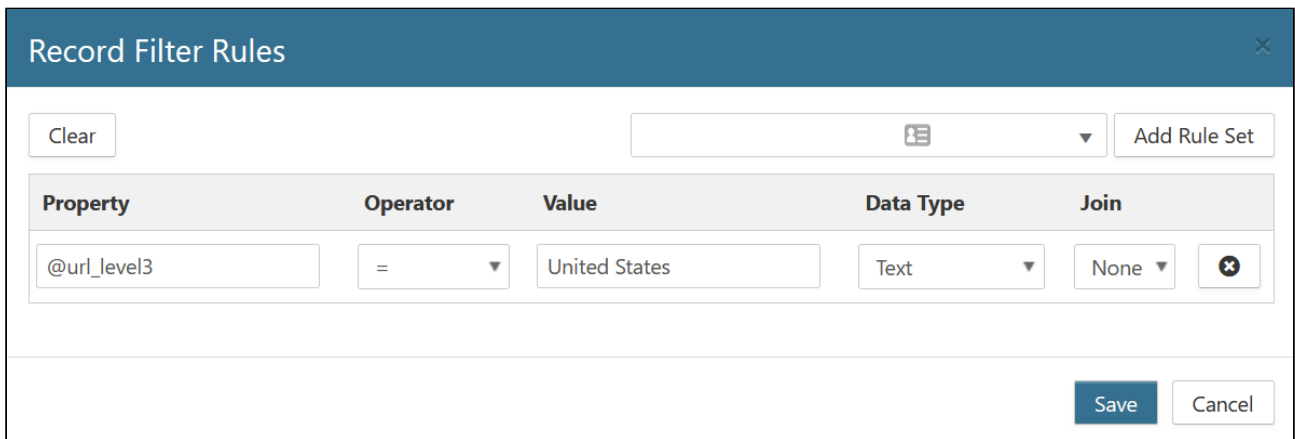


You may add either individual users or user groups to the Group Membership.



4.17.2.2 Record Filter Rules

Record Filter Rules determine which records should be filtered to the specific group. For example, if you wanted to narrow down a specific region to only show records for the SharePoint site "Region 1" at the URL https://mysharepoint/sites/region_1, you could create the following rule:



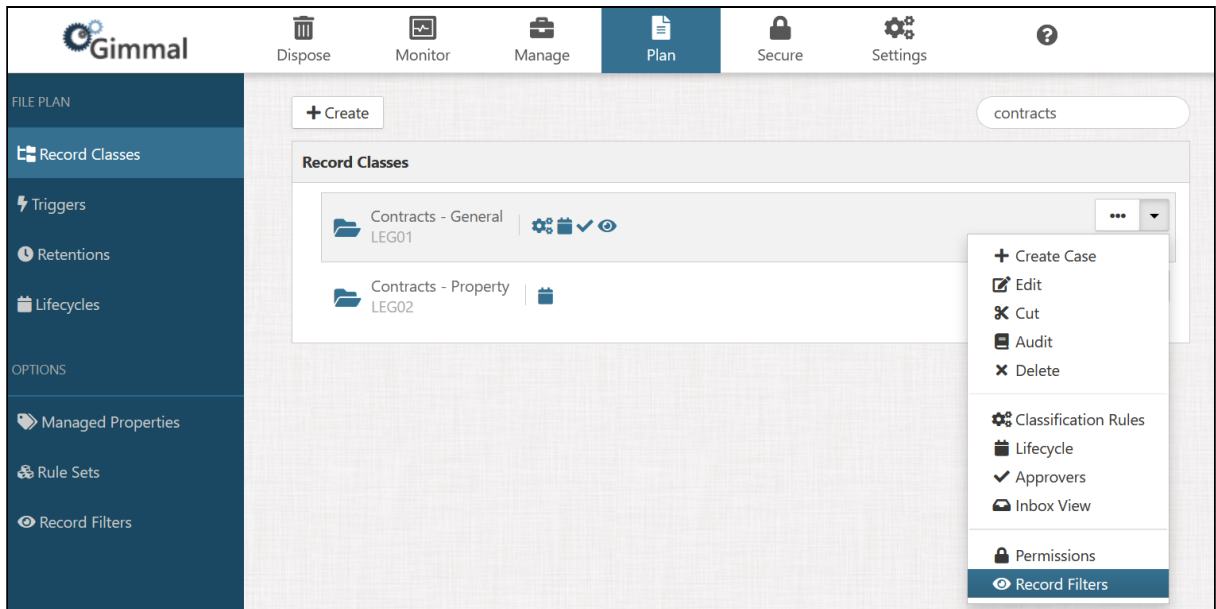
For detailed information on creating rules, see the [Rule Builder](#)(see page 125) topic.

4.17.3 Adding Filters to Record Classes

In order for a Record Filter to be applied, it must be added to a Record Class. Each filter will have a set of users/groups that for the specific rules, and any number of Record Filters can be added to a Record Class.

Record Filters can be added to Record Classes by Global Administrators and System Admins. To add a Record Filter to a Record Class, follow the steps below:

1. Browse to or search for the Record Class that should receive the Record Filter
2. Select Record Filters on the drop-down menu on the right side of the Record Class



3. Add the appropriate Record Filters

4. Click Save

i The Record Filters will not apply immediately, as they must be processed by the Lifecycle Processing Service. For cloud implementations this could take up to 30 minutes, for server based installations, this is configured by your System Admins.

4.18 Record Class Permissions

4.18.1 Granting Permissions

To assign user permissions to specific Record Classes, you must add the user to the system as a User account.

After adding the user, perform the following steps:

1. Click **Plan** from Main Menu.
2. Click the drop-down for the desired Record Class.
3. Select **Permissions**.
4. Click **Assign**.
5. Select the User or Group.
6. Select Permissions to be granted.
7. Click **Save**.

4.18.2 Revoking Permissions

You can revoke a user's permissions from a specific Record Class using either of the following options:

- Revoking from Record Class, or
- Revoking from User Profile

4.18.2.1 Revoking from Record Class

To remove a user's permissions from a Record Class using the Record Class navigation, perform the following steps from the Plan menu.

1. Click **Plan** from the Main Menu.

2. Click the drop-down for the desired Record Class.
3. Select **Permissions**.
4. Click **Edit** Button next to user.
5. Uncheck **Permissions** to remove.
6. Click **Save**

4.18.2.2 From User Profile

To remove a user's permissions from a Record Class using the User Profile, perform the following steps from the Secure menu.

1. Click **Secure** from the Main Menu.
2. Check the **Edit** Button for the desired User.
3. Click the **Permission** button for the specific Record Class.
4. Uncheck the desired permissions.
5. Click **Save**.

4.18.3 Permission Inheritance

Record Classes support permission inheritance. When permissions are assigned to a Record Class, permissions are propagated to all child Record Classes. However, once permissions are edited for a specific Record Class, the inheritance chain is broken and permissions will no longer be propagated from the parent if the parent's permissions are changed.

To re-enable permission inheritance, open the Permissions for a specific Record Class and click the **Revert to Parent** button, which will remove all permissions specific to the Record Class and then automatically propagate the parent's permissions back down.

5 Getting started

First of all, thank you for being a client. We appreciate that you trusted Gimmel for your purchase.

For the most part, the Records Management documentation is separated into guides for each role, starting with system administration and moving through to developers. Some of the topics you are interested may be in other guides, for instance, if you are a Global Records Manager setting up the File Plan, you will need to move down to the Record Manager guide.

- [\(5.2.4\) Administrator Guide](#)(see page 221)
- [\(5.2.4\) Record Manager Guide](#)(see page 73)
- [\(5.2.4\) User Guide](#)(see page 20)
- [\(5.2.4\) Developer Guide](#)(see page 432)

You can go directly to the guides above, or work through the steps we have put together around the topics that should help you get started using the system.

5.1 1. Deployment

Gimmel Records Management is a part of the Gimmel Cloud, however it can also be deployed on your servers (or your cloud servers, such as Azure). However, even if you use the Gimmel Cloud, you may still need or want to deploy the connectors on your own. The following planning topic will help understand your options.

[\(5.2.4\) Plan Your Deployment](#)(see page 221)

If you are deploying the core software on your servers, start with the following topic:

[\(5.2.4\) Deploying On-Premise](#)(see page 222)

5.1.1 Connector Deployment

To deploy connectors on your own services, start with the [\(5.2.4\) Connector Deployment](#)(see page 264) topic.

5.1.2 Physical Records Management Deployment

If you have licensed Physical Records Management, you will need to ensure it is correctly deployed on order to use it. If you are deploying the physical records management software on your servers, start with the [\(5.2.4\) Physical Records Management Server Deployment](#)(see page 392) topic. You will also need to configure the Physical Records Management extension, start with the [\(5.2.4\) Physical Records Management Configuration](#)(see page 404) topic to learn more.

5.2 2. First time setup

If this is the first time you are personally using Gimmel Records Management, you should start here. Even if you are the first person in your organization to use the software, start here for setting it up the first time.

[\(5.2.4\) First time setup](#)(see page 210)

If you are a user, and not configuring the File Plan, skip down to step 6, using the Inbox.

5.3 3. Creating the File Plan

The first step for almost any records management implementation is to build your file plan, which contains the retention schedule and lifecycles for you content. Build each of the following components in order to fully prepare your File Plan. Start with the topic on [\(5.2.4\) Building Your File Plan](#)(see page 73).

5.4 4. Add classification rules

Once the File Plan is complete you will need to build classification rules in order to classify content in your sources to the Record Classes in the File Plan.

[\(5.2.4\) Classification](#)(see page 95)

5.5 5. Adding policies to Record Classes

Once you have information classifying correctly, it's time to assign the lifecycles (policies) to each Record Class.

[\(5.2.4\) Lifecycles and Record Classes](#)(see page 97)

5.6 6. Using the inbox

Now that content is being classified to your File Plan and adhering to policies, records ready for disposition will start showing up in your Inbox.

[\(5.2.4\) Inbox](#)(see page 21)

5.7 7. Setting up Crawl Overrides in SPOC

By default, the SharePoint Online Connector manages content in Document Libraries that are not hidden and are not excluded from a search. The Crawled Libraries tab allows for customized control of this behavior, allowing the creation of overrides to crawl content in hidden libraries or to ignore content in non-hidden libraries.

[Setting Up Crawl Library Overrides](#)(see page 424)

5.8 Terminology

The following table lists the terminology that is used within the guides.

For Physical Records Management terminology, see [Physical Records Management Terminology](#)(see page 208).

Term	Description
Unclassified Document	<p>Any file, document, or other type of information that has been registered into Records Management. Records Management is aware of the metadata and the document is subject to Legal Holds.</p> <p>If an Unclassified Document cannot be assigned to a Record Class, it remains unclassified and is assigned to the Undefined Record Class.</p>
Record (Classified Document)	<p>Any file, document, or other type of information that has been classified to a Record Class. When a Record Class is given a Lifecycle, all classified items will adhere to the policies of the Lifecycle. All classified documents within Records Management are considered Records for the purposes of having a Lifecycle.</p>
Declared Record (Immutable)	<p>Any record (Classified Document) that has been automatically or manually declared a record. Declared records are made immutable (locked) by Records Management and are not editable by users. The property "Declared Record" is marked as "Yes".</p>
Administration Records	<p>Administrative Records are time-based records. A record is made up of one document. The retention and disposition are based on the date from each individual record.</p>
Case Records	<p>Case Records are based on a person, place, or thing. A record is made up of one or more documents. The retention and disposition are based on a future event (event-based records). All of the documents have a common Case ID and all belong to a Case Record Class.</p>
Vital Records	<p>Any record that has been automatically or manually declared as vital. Vital Records are made immutable (locked) by Records Management and are not editable by users. The property "Vital Record" is marked as "Yes".</p>
Classification	<p>The process by which an Unclassified item gets associated to a Record Class. Classification can happen manually or automatically. Automatic classification is accomplished by specifying a set of Classification Rules.</p>
Rules	<p>A set of simple expressions that define how an action will take place. Rules are used for Classification, Rule Triggers, and Legal Holds.</p>
Rule Sets	<p>Provides the ability to create pre-defined rules that can be used when creating Classification Rules, Rule Triggers, and Legal Hold Rules. This enables a set of rules to be re-used.</p>

Term	Description
Undefined Record Class	A pre-defined Record Class that contains items that cannot be classified to another Record Class because the item did not match any of the rules defined for automatic classification.\
Record Class	The central entity that makes up the File Plan. A Record Class is a node in the hierarchical File Plan. It contains records that have related activity. The Record Classes are all linked via a parent/child relationship. This is often referred to as the "Category" in the Retention Schedule.
Trigger	Represents a re-usable entity that defines the structure of how a retention period begins. Triggers are a building block for defining another type of entity called Retentions. There are four types of Triggers supported: Date Property Triggers, Event Triggers, Rule Triggers, and Special Triggers.
Retention	Represents a reusable entity that defines a time period from an associated Trigger. It is used to represent a regulation or policy that refers to some duration. A Retention is used to build a Lifecycle.
Lifecycle	<p>Brings together the existing Triggers and Retentions to define what action should happen to an item at specific points in time. Each of these points in time is represented within a Lifecycle by a Phase. The Lifecycle ensures an item is guided through the defined phases so that they carry out each Action indicated by the Phase at the time specified by the Retention.</p> <p>Once a Lifecycle has been created, it can be assigned to any number of Record Classes. When an item is assigned to a Record Class, it will take on the associated Lifecycle.</p>
Inbox	<p>There are several Inbox types: An Action Item Inbox and a Requests Inbox.</p> <ul style="list-style-type: none"> • Action Items Inbox - Provides a single location where Record Managers and Approvers will go to approve and submit Action Items. Action Items can be Automatic or Manual, dictated by the specific Lifecycle Phase that is being approved. • Requests Inbox - This is for physical records; it is where the fulfillment of Record Requests take place.
File Plan	A comprehensive outline for how records will be organized (classification, retention, permissions, settings, etc.). The File Plan is based on the client's Retention Schedule.

Term	Description
Retention Schedule	<p>A Retention Schedule is a policy that defines how long records must be retained in order to meet the legal, regulatory, or operational requirements of an organization. A Retention Schedule typically contains the following elements: Records Categories, Description, Retention Period and Event Trigger, Disposition Authority/Citations. It typically does not specify where the information is located or specify the event or property that starts retention.</p> <p>To create a File Plan in Records Management, you must have a Retention Schedule. The Retention Schedule is either imported during the project implementation or it is manually entered into Records Management.</p>
Managed Properties	Provides the ability to map multiple metadata properties to a single property name that can be used in Rule Sets, Classification Rules, Legal Hold Rules, Event-Based Triggers, and Event Targeting conditions.
Approval Groups	Represents users that are required to approve retention in the Action Items inbox. A Record Class can have multiple Approval Groups and each Approval Group may be assigned multiple users.
Archive	A separate location to send record information to, after the record is disposed. The Archive contains Record Details, Record Properties (Connector metadata included), and the Record Audit Trail. The Record Details will always be included, while the Properties and Audit Trail are optional. The Archive options are set by Record Class. The Archive is considered permanent; it does not have a Retention.
Legal Cases	Represents litigation or an audit in which items are placed on Legal Hold as part of a Discovery process.
Legal Holds	Suspends the Lifecycle of a record(s) and prevents any disposition or modifications of the document from occurring. Each Legal Case will have one or more Legal Hold rules.

5.8.1 Physical Records Management Terminology

Term	Description
Container	<p>A container is an entity that represents an organizational hierarchy for physical records repositories. It serves as a holding place for physical assets.</p> <p>There are two types of containers: Location and Logical</p> <p>A Location container refers to an actual physical location where physical assets can be located, such as an office, a warehouse, a filing cabinet, etc. The Home location of a physical asset is calculated automatically in this case, and is the full path of the hierarchy in which it resides.</p> <p>A Logical container can be any representation used to organize and catalog physical assets. It does not have to mirror any structure or organization in the "real world". The Home location of a physical asset is not automatically calculated, but is derived from a location that is selected from the Locations list.</p> <p>You can create and use both location-based and logical-based containers.</p>
Create Request	<p>If you are a user, you will perform this task when you want to take possession of a physical asset. You can also request an extension of the due date for the physical asset, if you want to keep the item a bit longer.</p>
Create Return	<p>If you are a user, you will perform this task when you want to return a physical asset back to its Home location.</p>
Direct Hold	<p>A direct hold is a legal hold that you apply manually (directly) to an asset/record.</p>
Indirect Hold	<p>An indirect hold is a legal hold that you apply at the physical container level. Thereafter, any physical assets that are created and added to that container will inherit that legal case/legal hold.</p>

Term	Description
Location	<p>A location can be a logical address or a real-world address that is attached to physical assets when they are created and is used in the routing and management of the items in the system. There are several types of locations that you can specify:</p> <ul style="list-style-type: none"> • Home – The Home location is the "resting place" of the physical asset when it is not charged-out. This location differs slightly, depending on which Container/Node Type you are using. <ul style="list-style-type: none"> • If the container is Location-based, the Home location is the full path to the container where the physical asset is being created. It is generated automatically, and cannot be edited. • If the container is Logical-based, the Home location can be specified by clicking the Location picker. The picker pulls from the Locations list and is security-trimmed. An "Unknown" value is also available. • Current – Where the physical asset is residing at this moment. If it were charged-out to a user, then the Current Location would be the Ship To Location selected in the request. • Temporary – A temporary location for a physical asset that you enter manually, or select from the Location picker. (The Location picker draws from the (Link) Locations list). An example of this would be the physical asset is not in its Home location but a temporary one (maybe the warehouse shelves were being repaired), or it was charged out to a user and the user is not in their current location (they temporarily moved offices or are working from somewhere else). • Ship To Location – The location where a physical asset will be shipped. This location is specified during the (Link) Create Request process. • Pickup Location – The location where a physical asset can be picked up to be returned to its Home location. This location is specified during the (Link) Create Return process.
Metadata	<p>Metadata is information that describes an entity and is contained in metadata definitions. It can describe any record, whether it is paper, media-based, or electronic.</p>
Physical Asset	<p>A physical asset is an item that is created and added to a container to which you have Edit access (e.g., a box, a folder, a DVD, etc.). A containing asset is managed in terms of lifecycle at the Parent level (the children are included, but are not managed independently).</p> <p>When requesting a physical asset, you can request a parent (containing) asset but you get all of the child assets as well. The charge-outs list will individually list the parent and children assets. For example, you request a parent physical asset (Box A) that has a single child (Folder A), and this is processed to a charge-out. The charge-out list includes Box A and Folder A, so that each asset can be returned independently.</p>
Processing an Extension	<p>A process performed by the Physical Administrator in which the user requests an extension to the due date of a physical asset return and the administrator either approves the extension, approves the extension but revises the new due date, or rejects the extension.</p>

Term	Description
Processing a Return	A process performed by the Physical Administrator in which a physical asset has been returned* by the user. The Processor must return the asset, mark it as returned (charged-in), and make the asset available to be charged-out by other users. (*See the Return entry below.)
Processing a Request	A process performed by the Physical Administrator in which a request* is received from a user for a physical asset. The request must be reviewed and approved, or denied. If the request is approved, the item is marked as charged-out. (*See the Request entry below.)
Processor	The Physical Administrator who processes asset requests and returns and is responsible for making final charge-outs and charge-ins.
Request	The process of asking for an asset to be delivered to a user or to be picked up for return. This asset is a real-world item that a user is requesting to have delivered to them (a box for example). Once the request is processed (approved) by the Physical Administrator, the asset is delivered to the user and is now considered "charged-out".
Return	The process of returning a physical asset back to its Home location. Once the return is processed (approved) by the Physical Administrator, the item is considered "charged-in" (i.e., now in its Home location and available to be charged-out again).

5.9 First time setup

This is where you should start if you are signing in or setting up Gimmel Records Management for the first time. There are topics for both Admins and Users, please follow the link to the one that best describes your role.

5.9.1 Admin

5.9.2 Users and Record Managers

5.9.3 Admin

5.9.3.1 Creating the Master Account

5.9.3.2 Assign System Admin Users

5.9.3.3 Global Preferences and Theme

5.9.3.4 Email Settings

5.9.3.5 Creating the Master Account

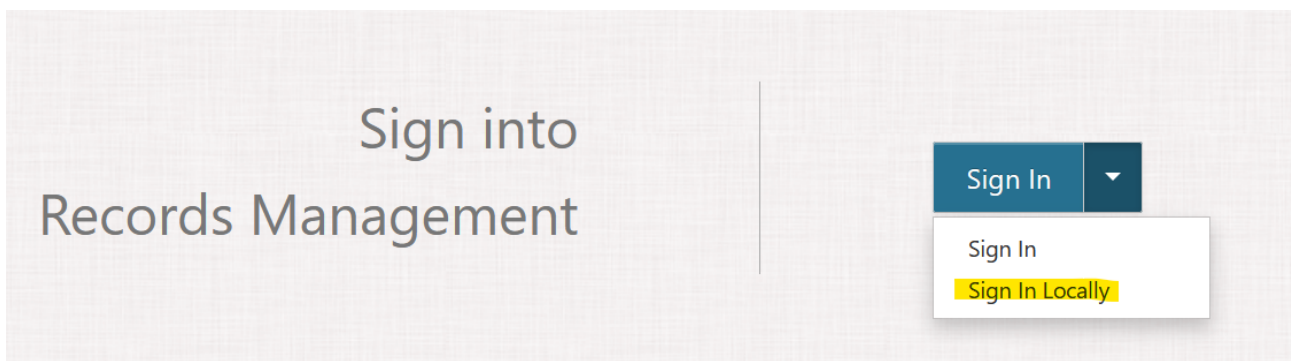
To begin using Records Management for the first time, the first thing you must do is Sign In Locally using the Master Account, so that you can provision other users in the system. To sign in locally, enter the username **administrator** and then enter any password you desire.

Because this is the first login, the password that is first entered here will automatically become the password of the Master Account. After the first login, to re-login with the Master Account, enter the username **administrator** and the password that you provided upon first sign in

When signing into Records Management for the first time you will need to Sign In Locally, which will create your Master Account. When signing in you must enter a user name and password.

Username - You must enter administrator as the user name

Password - Enter a secure password that you can remember as it will be used to sign back into the Master Account.



i The password entered here will automatically become the password of the Master Account. After the first sign in, to re-sign in with the Master Account, enter the username **administrator** and the password that you provided.

i The Master Account password can only be changed from PowerShell (see [\(Link\) Change Master Account Password](#)).
The Master Account has full control over all of Records Management and can be used to provision new Users and Service Accounts, as well as administer any aspect of the system. This account information should be kept secure!

5.9.3.6 Assign System Admin Users

As an administrator to Records Management, It is recommended that the Master Account is only used when needed, and you should immediately create add the System Admin role to your administrator to use going forward. Select the Secure option on the Main Menu, and then select New User.



While you may create as many System Admins as necessary, but these should be limited to individuals who need to control all aspects of the system.

1. Enter each user on a separate line in the text box.
2. Check the System Admin box.
3. Select the Assign Button.

New Users and Groups ✕

Please enter a list of users or groups, each on a separate line

user1@mycompany.com
 user2@mycompany.com

System Admin
 Record Manager
 User
 Physical Administrator
 Physical User

Assign
Cancel

5.9.3.7 Global Preferences and Theme

Time Zone

Times are stored in the system as GMT times and are converted within the user interface to the individual users' personal preference. As an administrator, you can set the default time zone for all users.

1. Select **Settings** from the Main Menu
2. Select **Global Preferences**
3. Set the Time Zone accordingly

Default Inbox View Properties

Each Record Class can have specific properties set so those properties will be shown as columns when using Views on the Inbox. As an administrator, you can set the default view properties for all Record Classes. Individual users also have the ability to set specific Inbox View Properties that can only be seen in the views by them.

Enter each property on a new line.


Theme

You can change the theme of the existing layout by changing the product logo or color scheme.

Changing the Logo

Records Management displays two different logos. One logo displays on the sign-in screen and the other logo displays within the application. Perform the following steps to change the built-in logos:

1. Select **Settings** from the Main Menu, and then click **Theme** from the left navigation menu.
2. Choose a .PNG file for the logo and/or the alternate logo. (See the table below for logo dimensions.).
3. Click **Update**.


 You may need to refresh your browser after you change your logo due to browser caching.

Maximum Preferred Logo Dimensions	
Logo (Login Logo)	W: 300px X H: 100px
Alternate Logo (Application Logo)	W: 200px X H:50px

Changing the Color Scheme

You can change the color scheme of the theme by performing the following steps:

1. Select **Settings** from the Main Menu, and then click **Theme** from the left navigation pane.
2. Choose the desired theme from the list of pre-configured options.
3. Click **Update**.

 To restore the default theme (color scheme and logos), click the **Defaults** button.

5.9.3.8 Email Settings

Email Server

To send out notifications, you must configure a valid email server that will be used to send the Records Management notifications. You can set up your email server by performing the following steps:


1. Select **Settings** from the Main Menu.
2. Select **Email** from the left navigation menu.
3. In the "From" field, enter the "From" address that will be used in the email notification.
4. In the "Host" field, enter the "Host" which represents the address of the actual email server.
5. In the "Port" field, enter the "Port" on the host which is used for SMTP.
6. Indicate whether "SSL" is used on the email server.
7. Indicate if "Default Credentials" should be used to access the email server.
 - If "Yes", the email server will be connected to using the Records Management Web's App Pool.
 - If "No", the specified "Username" and "Password" will be used.

8. Click **Save**.

The screenshot shows the Gimmal Settings interface. The top navigation bar includes options like Dispose, Monitor, Manage, Plan, Physical, Secure, and Settings. The left sidebar lists settings categories: My Preferences, Global Preferences, Theme, Email, Email Template, and Notifications. The main content area is titled 'Email' and features a 'Not Configured' warning. The configuration fields include: 'From' (text input), 'Host' (text input), 'Port *' (text input with value 25), 'Use SSL *' (dropdown menu with 'No' selected), 'Use Default Credentials *' (dropdown menu with 'No' selected), 'Username' (text input), and 'Password' (text input). At the bottom of the form are 'Save' and 'Defaults' buttons.

Email Template

Customize an email template for your Records Management approval notifications by performing the following steps. This will be used when the system sends emails for approvals. An asterisk (*) indicates that the property is mandatory.

 Only enter plain text in these fields. No markup is allowed.

1. Select **Settings** from the Main Menu.
2. Select **Email Template** from the left navigation menu.
3. Enter a custom subject, message body, signature and logo that will be used in the email notification.
4. Choose a .PNG file for the logo. The maximum preferred logo dimensions are W: 300px X H: 100px

5. Click **Update**.

The screenshot shows the Gimmal web interface. At the top, there is a navigation bar with icons for Dispose, Monitor, Manage, Plan, Physical, Secure, and Settings. The Settings menu is open, showing options like My Preferences, Global Preferences, Theme, Email, Email Template (selected), and Notifications. The main content area is for configuring an email template. It includes fields for Subject (with a red asterisk), Message Body (with a red asterisk), and Signature. The Subject field contains the text "Retention actions require your approval". The Message Body field contains "Please sign in and review the items needing your approval." Below these fields is a "Logo" section with the text "No logo has been uploaded" and an "Upload" button. A note at the bottom states: "*Only enter plain text in the fields above. No markup is allowed." At the bottom of the form is a blue "Update" button.

Notifications

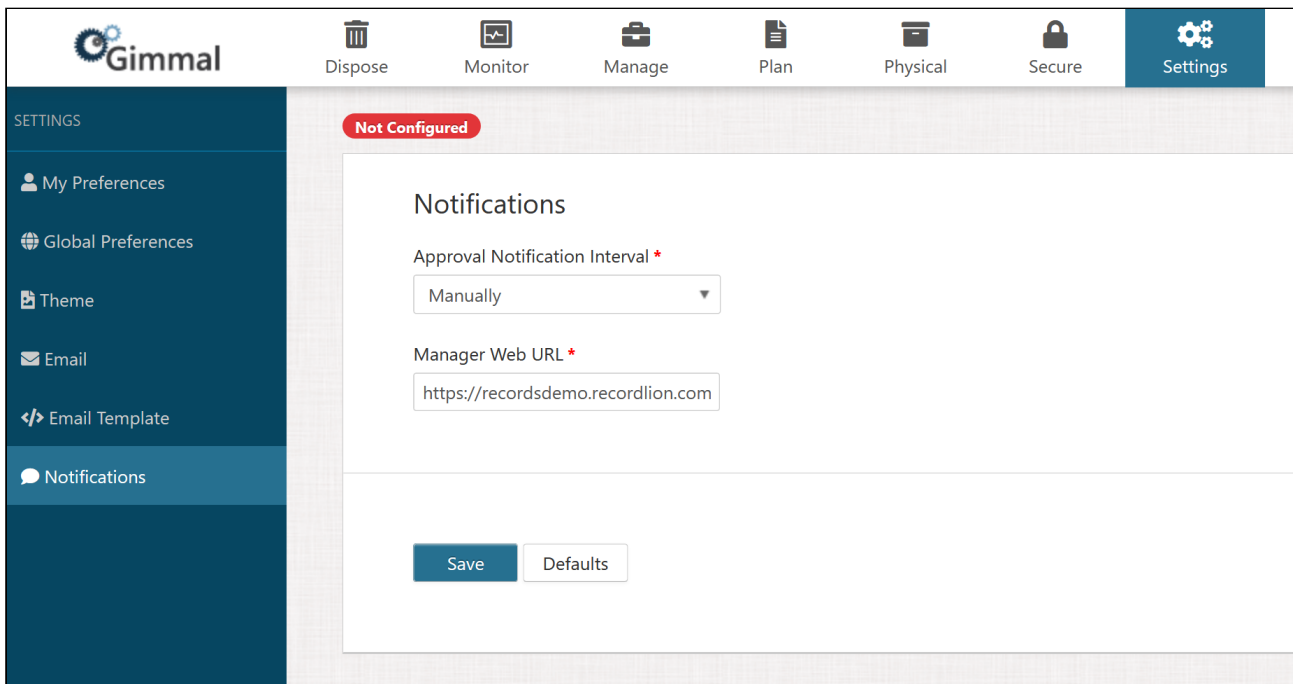
Approvers with any pending action items will be sent a notification based on when they last received an approval notification and the configured schedule. If the schedule is set to Weekly and an approver receives a notification Tuesday afternoon and still has pending approvals the following Tuesday afternoon, they will receive another notification.

Once your Email server is configured, you can configure the interval in which notifications should be sent to users by performing the following steps:

1. Select **Settings** from the Main Menu.
2. Select **Notifications** from the left navigation menu.
3. Choose how often to notify users of Pending Action Items (Daily, Weekly, Monthly).
4. Enter the “base” URL that should be used to generate the link contained in the notification, which will be used to guide the user to the appropriate location based on the notification type. (**Note:** This defaults to the current URL in the browser’s address bar, but can be changed to account for load balancing or FQDN names.)
5. Click **Save**.



When Notifications are configured, a **Push Notifications** button will be shown on the **Secure** screen that will, when clicked, manually send notifications to approvers with pending action items. This button will not be displayed until your Email Server is also configured.



5.9.4 Users and Record Managers

- [Requirements](#)(see page 217)
- [Signing In](#)(see page 217)
- [User Preferences](#)(see page 218)

5.9.4.1 Requirements

Browser Requirements

Unless otherwise noted for a specific connector, extension, or other related application, Gimmal Records Management is compatible with the following browsers.

- Mozilla Firefox (latest)
- Google Chrome (latest)
- Microsoft Edge (latest)

5.9.4.2 Signing In

Sign In

To access Records Management, use a web browser to navigate to ([https://\[yourURL\]](https://[yourURL])). You must use the fully qualified domain name (FQDN) of your server (e.g., <https://demo.recordsmanagement.com:8080>.) Because Records Management is a secure system, the first thing you must do is sign in using your credentials. Your administrator will provide you with the necessary credentials, however, since the system uses Single Sign-On technology, they should be the same as the credentials used to access your other corporate systems.



Sign Out

To sign out of the system, click on your user name in the upper right of the page, and then select Sign Out.



5.9.4.3 User Preferences

You can access the My Preferences screen by clicking **Settings** from the Main Menu and then **My Preferences** from the left navigation menu. My Preferences enables you to configure settings that are specific to you, the current logged in user.

Time Zone

This setting enables you to configure your personal Time Zone setting, which affects how dates display. The default setting is based on the time zone setup by your systems administrator.



Inbox View Properties

The Inbox, as well as the Rejected Records area (and Expired Records if you are a Record Manager), can contain different views that you can create yourself. One of the options on each view is to modify the columns that are available for viewing and filtering. The columns that are available for your user are either configured by your system administrator or added in the My Preferences settings.

The screenshot shows the 'My Preferences' settings page in the Gimmel Records application. The page has a dark blue sidebar on the left with 'My Preferences' selected. The main content area is titled 'My Preferences' and contains a 'Time Zone' dropdown menu set to '(UTC-06:00) Central Time (US & Canada)'. Below this is a red-bordered box labeled 'Available Inbox View Properties' containing a text input field with the text 'My Column'. At the bottom of the page are 'Update' and 'Defaults' buttons.

In the **Available Inbox View Properties** text box, enter each column you'd like to have an option for using on a separate line, and then click the Update button.

Now each of these columns will be available to use within the different areas of Disposition.

Source	Phase	Action	Expiration
			<input checked="" type="checkbox"/> Approved
			<input checked="" type="checkbox"/> Record Class
			<input checked="" type="checkbox"/> Record / Case File
			<input checked="" type="checkbox"/> Source
			<input checked="" type="checkbox"/> Phase
			<input checked="" type="checkbox"/> Action
			<input checked="" type="checkbox"/> Expiration
			<input checked="" type="checkbox"/> My Column

6 Administrator Guide

The Administrator Guide covers topics that are only available to administrators, such as deployment, global configurations, and security.

6.1 Plan Your Deployment

6.2 Deploying On-Premise

6.3 Records Management Core Deployment

6.4 Managing Security

6.5 Connector Deployment

6.6 Physical Records Management Deployment

6.7 Monitoring Services

6.8 Migration Utility

6.9 Setting Up Crawl Library Overrides

6.10 Plan Your Deployment

These are the deployment options for the Gimmel Records Management products.

	Server	Cloud	UK Cloud	CAN Cloud
Gimmel Records Management Core	Yes	Yes	Yes	Yes
Altitude Connector	Yes	No	No	No
Box Connector	Yes	Yes	No	No

	Server	Cloud	UK Cloud	CAN Cloud
Documentum Connector	Yes	No	No	No
FileNet Connector	Yes	No	No	No
Physical Records Management Extension	Yes	Yes	No	No
SharePoint Connector	Yes	No	No	No
SharePoint Online Connector	Yes	Yes	Yes	Yes
Universal File Share Connector	Yes	No	No	No

6.11 Deploying On-Premise

While Gimmal Records Management can be deployed as service in the Gimmal Cloud, it also may be deployed on-premise to ensure the strictest record security and have complete control of your environment. The steps below will walk you through an on-premise deployment of Gimmal Records Management.

1. [6.11.1 Plan Your Deployment](#)
2. [6.11.2 Install Records Management Core](#)
3. [6.11.3 Configure Records Management Core](#)
4. [6.11.4 Administrators first time setup](#)

6.12 Records Management Core Deployment

6.12.1 [Records Management Core Planning \(On-Premises\)](#)

6.12.2 [Records Management Core Installation \(On-Premises\)](#)

6.12.3 [Records Management Core Configuration \(On-Premises\)](#)

6.12.4 [Uninstalling the Core Platform](#)

6.12.5 [Records Management Core Planning \(On-Premises\)](#)

Gimmel Records Management may be deployed on-premise to ensure the strictest record security and have complete control of your environment. This section will walk you through an on-premise deployment of the software.

6.12.5.1 Topology and Architecture

6.12.5.2 System Requirements and Considerations

6.12.5.3 Scalability

6.12.5.4 Disaster Recovery

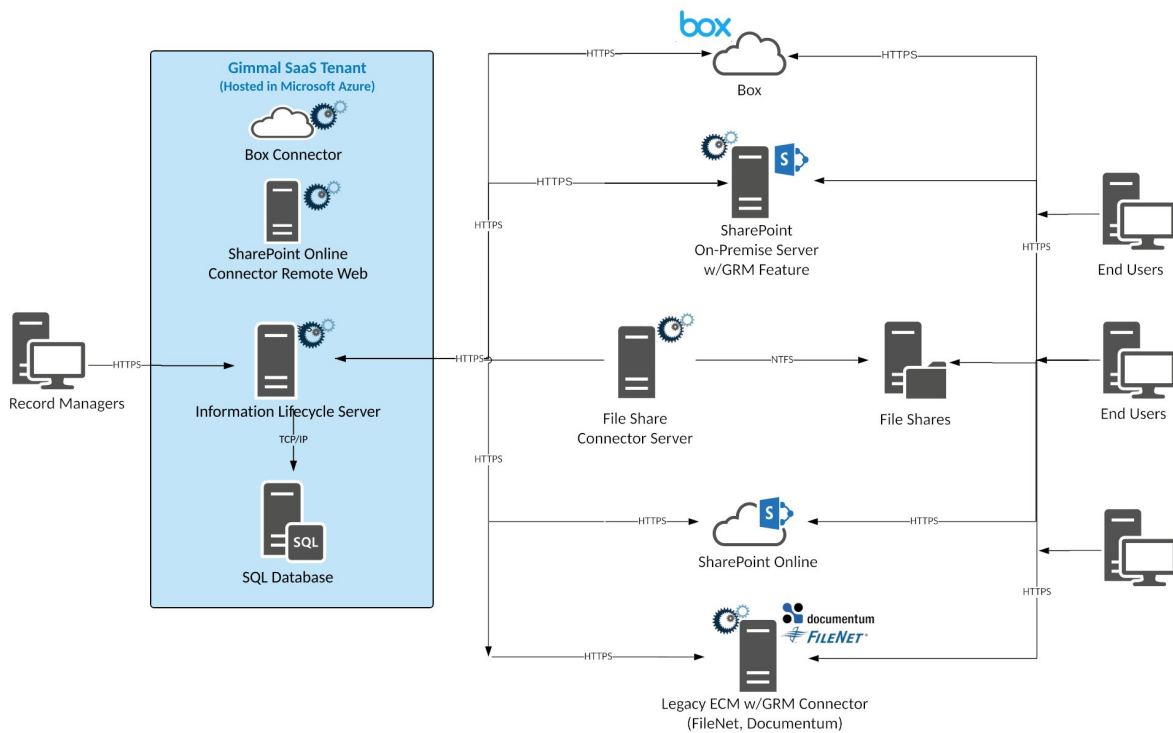
6.12.5.5 High Availability

6.12.5.6 Load Balancing

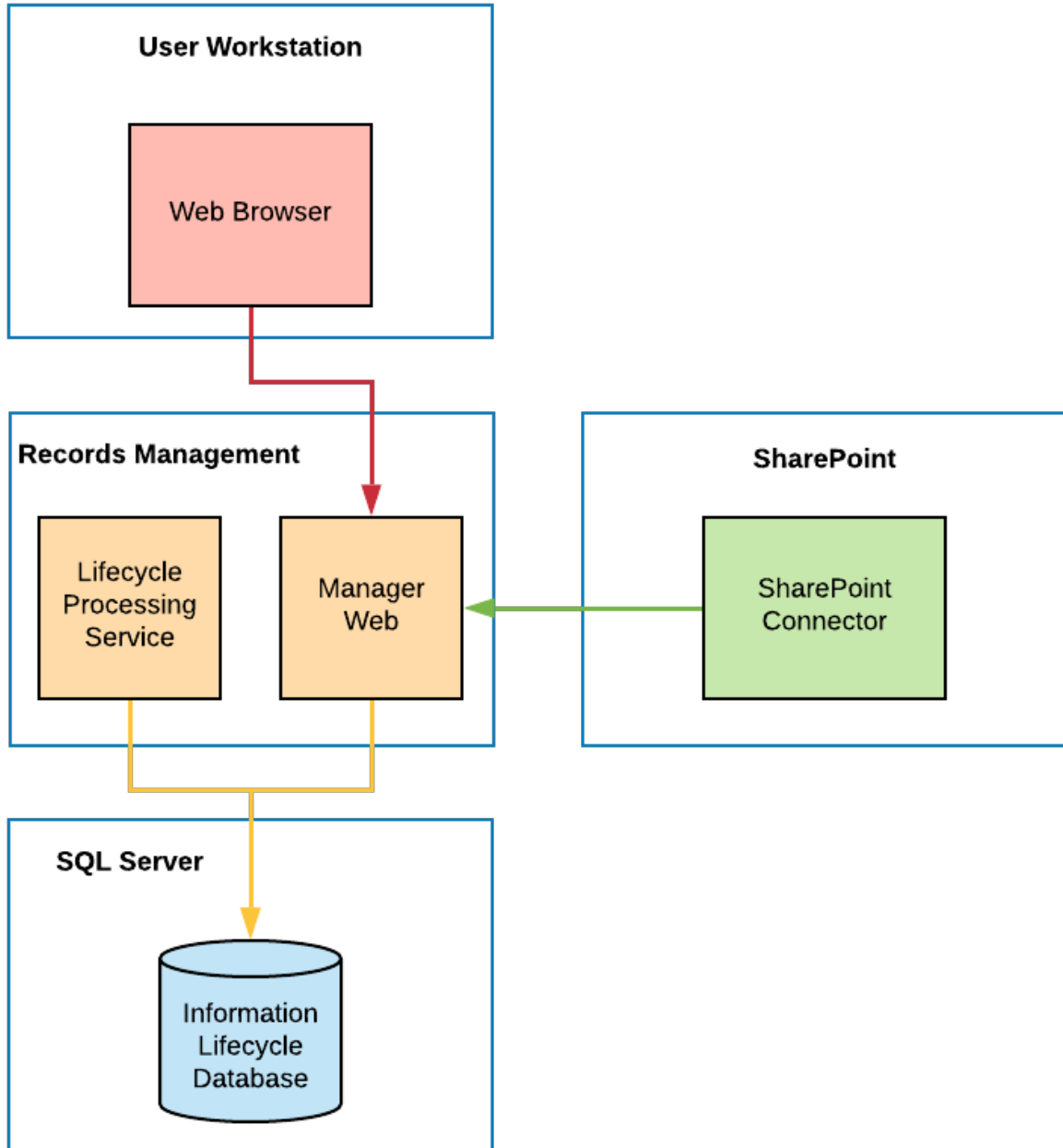
6.12.5.7 Authentication

6.12.5.8 Topology and Architecture

Platform Topology



Architecture



6.12.5.9 System Requirements and Considerations

System Requirements

Before you install Records Management and any of its components, verify that your system meets or exceeds the following requirements:


Records Management Server		
	Cores	Memory (MB)
Minimum	2	4096
Recommended	4	8192


- Windows Server 2012 or later (x64)
- Windows Server 2012 R2* or later (x64)
 - For Windows Server 2012 R2, the WebClient service must be running. To enable the WebClient service, ensure that the Desktop Experience feature is enabled on the server.
- .NET Framework 4.8 (only for Records Management v5.0)
- .NET Framework 4.5
- .NET Framework 3.5
- Internet Information Services 7 or later
- PowerShell 3+
- 250 MB Disk Space for software and 200 MB for log files

July 1, 2021: HTTPS Requirement

Today, it is exceedingly rare to have non-sensitive web traffic. By always using HTTPS connections, people's changing expectations for how websites handle sensitive traffic make everyone safer. By always using HTTPS connections, web services don't have to make a subjective judgment call about what's "sensitive". By always using HTTPS connections, there is less room for error and deployment is simpler and more consistent across all of your environments.

Some modern web browsers now have default behavior that does not allow certain authentication schemes over HTTP. **As a result, Gimmel now requires using HTTPS with Gimmel Records for any version of the software.** The version of Gimmel Records you're using doesn't change the behavior of the browser with HTTP. The exact behavior when using HTTP depends on your choice of web browser and its related security configuration. For these reasons, Gimmel will provide limited, best-effort support for HTTP and **will require HTTPS to be configured before troubleshooting any support tickets.**

-  As a security best practice, Gimmel recommends that you configure your server to use Transport Layer Security (TLS) 1.2.

-  As a security best practice when using the .NET Framework, Gimmel recommends that you enable Transport Layer Security (TLS) 1.2, which provides communications security for client/server applications.

To enable TLS 1.2, you must add the following Windows registry settings to the Records Management Core server(s) and the servers of any Records Management connectors you are using (if applicable), and then reboot your system.

- HKLM:\SOFTWARE\Microsoft\.NETFramework\v4.0.30319 "SchUseStrongCrypto"= dword:00000001
- HKLM:\SOFTWARE\Microsoft\.NETFramework\v4.0.30319 "SystemDefaultTlsVersions"= dword:00000001
- HKLM:\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319 "SchUseStrongCrypto"= dword:00000001
- HKLM:\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319 "SystemDefaultTlsVersions"= dword:00000001

Note that some operating systems require additional steps to enable TLS 1.2. For more information, see [Microsoft's TLS documentation](#)²⁶ To verify that your operating system supports TLS 1.2, read the [Support for TLS 1.2 section of Microsoft's documentation](#)²⁷.

SharePoint on-Premises Requirements:

- SharePoint Server 2016
- SharePoint Server 2019

Database Requirements

Effectively managing a database requires familiarity with collation, maintenance plans, recovery models, backups, and techniques for minimizing file system fragmentation, such as creating a database file large enough for any anticipated growth.

SQL Server Versions

- SQL Server 2016 or later



If it is necessary to upgrade from an older version of SQL Server (pre 2016), after you upgrade SQL Server and BEFORE installing the latest version of Gimmel Record Management, verify the SQL Compatibility Level of the "InformationLifecycle" database by running the following query:
`select compatibility_level from sys.databases where name = 'InformationLifecycle'`
 This query should return a minimum value of 130. If this is not the case, refer to the following Microsoft documentation for updating the compatibility level [here](#)²⁸.

Sizing

The following table shows database sizing estimates in GB. The "m" in the Data File headings represents millions.

Data File	1m	25m	50m	100m
Information Lifecycle Data	25	600	1200 (1.1 TB)	2400 (2.4 TB)

²⁶ <https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls#systemdefaulttlsversions>

²⁷ <https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls#support-for-tls-12>

²⁸ <https://docs.microsoft.com/en-us/sql/relational-databases/databases/view-or-change-the-compatibility-level-of-a-database?view=sql-server-ver15>

Data File	1m	25m	50m	100m
Information Lifecycle Log	15	50	100	200
Temp Data	100	100	100	100
Temp Log	10	10	10	10

Collation

Records Management requires a case insensitive collation as a minimum system requirement for the SQL Server database. The default EN-US collation is SQL_Latin1_General_CP1_CI_AS, which meets the Records Management minimum system requirements. Guidance on collations is available here: [https://msdn.microsoft.com/en-us/library/ms143508\(v=sql.105\).aspx](https://msdn.microsoft.com/en-us/library/ms143508(v=sql.105).aspx)

Maintenance Plans

The Database Administrator should be familiar with tuning and monitoring a SQL Server instance. If there are no efforts made to track database performance over time, it becomes highly likely that database performance may be negatively impacted.

These monitoring efforts should be documented in reports containing empirical information about the database. From these reports, it is possible to construct and maintain a well-designed SQL Server maintenance plan. A SQL maintenance plan is highly recommended for any Records Management implementation.

The plan should address, but not be limited to, the following:

- Index Fragmentation
- Transaction Logs
- Backups/disaster recovery
- VerifyBackups
- Maintenance Plan Cleanup



Database administrators must run the stored procedure ProcBlock_RebuildIndexes to rebuild the Records Manager indexes to improve query performance if they experience slowness.

Message Queue Considerations

Records Management is now using a message queue to improve the performance and reliability of the system. By default SQL Server is used as the queuing mechanism, but to improve performance and reliability Azure Queues can be used. This works with an Azure Service Bus instance located in your Microsoft Azure account and will distribute work across **n** number of machines where the service is installed and is configured to listen to the same set of queues. To configure your system to use Azure Queues, make the following additions to the <appSettings> section in the config file for both the Lifecycle Processing Service (RecordLion.RecordsManager.ServiceV2.exe.config) and Physical Records Management (RecordLion.RecordsManager.PhysicalAssets.Service.exe.config).

```
<add key ="r\l.queue_type" value="azure"/>
```



```
<add key="rl.servicebus_connection_string" value="{service bus connection string}"/>
value comes from the azure service bus instance and should include the security
information for accessing the service bus
<add key="rl.azure_job_queue_name" value="{queue name}"/> value represents the name
of the Queue in the Azure Service Bus Namespace that will be used
<add key="rl.job_worker_count" value="1"/> value represents the number of parallel
active messages, please set to 1 unless instructed by Gimmel to increase
```

6.12.5.10 Scalability

Records Management Web	
What comprises the solution...	<ul style="list-style-type: none"> • ASP.NET-based web application • Data stored in SQL • Provides a user interface for user interaction • Provides a web API for external component integration such as connectors and client software integrations
How Scaling Works...	<ul style="list-style-type: none"> • The web can be installed to multiple servers that all point to the same SQL server instance • Network or hardware load balancing can be used to distribute among the multiple servers • Session affinity should be set to "none"
When to Scale...	<ul style="list-style-type: none"> • When CPU utilization is consistently above 90% for an extended duration more cores should be added or new servers should be added to the load balancer • When Memory Pressure is consistently above 80% for an extended duration, more memory should be added or new servers should be added to the load balancer
General Sizing Guidelines...	<ul style="list-style-type: none"> • $(\text{total User Count} * \text{Avg. \% Hourly Users}) * 5 / 60 = \# \text{ of request per second}$ • $\text{Ceiling} (\# \text{ of requests per second} / 50) = \# \text{ of servers}$ • Minimum of 2 servers recommended

Records Management Processing Service	
What comprises the solution...	<ul style="list-style-type: none"> • .NET-based Windows Service • Data stored in SQL Server • Performs reclassification of items • Manages lifecycle for each item being tracked

Records Management Processing Service	
How Scaling Works...	<ul style="list-style-type: none"> • The service can be installed to multiple servers that all point to the same SQL Server instance • The service supports failover, not load distribution • The service acts as a controller off-loading the bulk of its workload to SQL Server stored procedures
Where to Scale...	<ul style="list-style-type: none"> • Not Applicable
General Sizing Guidelines	<ul style="list-style-type: none"> • Should have at least 2 servers for failover • Recommended installing services on each Manager Web Server

6.12.5.11 Disaster Recovery

Preparing for Disaster Recovery

Preparing for disaster recovery of Records Management is a matter of ensuring that you have a proper SQL Server Maintenance Plan in place to handle the backing up of the Records Management database on regular intervals.

It is important to note that the Web and Services that makeup Records Management can simply be re-installed on another server and pointed to any Records Management database and, therefore, have no relevance in terms of disaster recovery. The database, on the other hand, is where all of the mission-critical information is stored and maintained. Therefore, it is absolutely critical that regular backups are captured and stored in a secure location where they can be accessed should the need arise.

In the event that a disaster does occur, having ensured that you have a working SQL Server backup in place, you should have nothing to worry about when recovering the system.

Review the following SQL Server documentation for information on SQL Server backup and restore strategies: <http://technet.microsoft.com/en-us/library/ms189647.aspx>

Backing up the Records Management Database

To perform a backup of the Records Management database, follow the referenced SQL Server documentation: <http://technet.microsoft.com/en-us/library/ms187510>

In production scenarios, a SQL Server Maintenance Plan should be created, which backs up the Records Management Database on regular intervals. The SQL Server documentation for this can be found at the following location: <http://technet.microsoft.com/en-us/library/ms189647.aspx>

Considerations

When choosing a backup strategy for Records Management, you should analyze the backup strategies used by each repository where the content being managed by Records Management is actually stored, and choose a strategy that most closely resembles what they use. This will ensure that if both systems are lost, they can be restored to a similar point in time.

Recovering From a Disaster

Restoring the Records Management Database

In order to restore a backup of the Records Management database, see the following SQL Server documentation.

1. [Full Recovery Model](#)²⁹
2. [Simple Recovery Model](#)³⁰

Installing Records Management using a Recovered Database

Once the Records Management Database has been restored, the next step is to install both the Records Management Web and Service.

Records Management Web

To install the Records Management Web, when the Database Settings screen displays, enter the name of the Server and Database to which the backup was restored and de-select the option to “Automatically Create the Database.”

²⁹ <https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/complete-database-restores-full-recovery-model?view=sql-server-2017>

³⁰ <https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/complete-database-restores-simple-recovery-model?view=sql-server-2017>

The screenshot shows the 'Records Manager' window with the 'Database Settings' section. The 'Database Server' field contains 'SERVER NAME' and the 'Database Name' field contains 'DATABASE NAME'. Both fields are highlighted with red boxes. Below these fields are two checkboxes: 'Automatically Create Database' (checked) and 'Use SQL Authentication' (unchecked), both also highlighted with red boxes. At the bottom right, there are 'Previous' and 'Next' buttons, with 'Next' being a dark blue button.

Records Management Processing Service

To install the Records Management Processing Service, when the Database Settings screen displays, enter the name of the Server and Database to which the backup was restored.

Gimmel Records Manager Services

Service Settings

Username Password

Database Settings

Database Server Database Name

SERVER NAME DATABASE NAME

Use SQL Authentication

Username Password

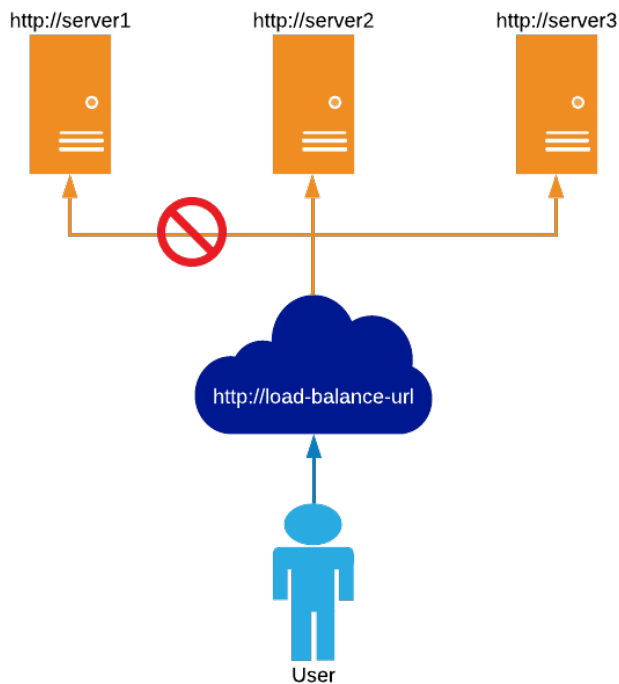
Previous Next

6.12.5.12 High Availability

Records Management Web

To support high availability from the Records Management Web, you must leverage either software or hardware load balancing to create a load balanced cluster. By doing so, you will not only provide the ability of being able to service more concurrent requests, but you will inherently provide for high availability by allowing the load-balanced cluster to redistribute load to other servers in the cluster should a node be lost.

The following diagram depicts how this scenario functions:



Lifecycle Processing Service

The Lifecycle Processing Service supports high availability using failover capabilities built into the service itself. To support Lifecycle Processing Service failover, install Lifecycle Processing Service onto multiple machines and point them to the same Records Management Database instance to form a failover cluster.

Once the services are installed, they must still be started. Upon doing so, the services will non-deterministically negotiate which server becomes the primary server that will perform Lifecycle Processing for managed records.

Should a server in the failover cluster be lost, another server will step in and take over the processing responsibilities.

By reviewing the Services screen in the Records Management Web, you can see which server is the primary by noticing the “P” next to the line in which it is listed, as shown in the following image:

The screenshot shows the Gimmal Monitor interface. The top navigation bar includes icons for Inbox, Monitor (selected), Manage, Plan, Physical, Secure, Settings, Info/Help, and Sign Out. The user is logged in as Administrator (Master) with version 4.6.0.0 (4.5.6744.5701). The left sidebar has sections for REPORTING (Dashboard, Reports, Destruction Certificates) and ACTIVITY (Audit, Event Occurrences, Pending Automation, Services). The main content area displays a table with the following data:

Host	Source	Last Heartbeat	Status	Actions
2016SVR	Lifecycle Processing Service	6/25/2018 1:30:40 PM	Green Heartbeat	More options, Close
2016SVR	Physical Records Service	6/25/2018 10:07:53 AM	Red Heartbeat	Close
2016SVR	SharePoint Audit Timer Job	6/25/2018 1:30:02 PM	Green Heartbeat	Close
2016SVR	SharePoint Classification Timer Job	6/25/2018 1:30:17 PM	Green Heartbeat	Close
2016SVR	SharePoint Retention Timer Job	6/24/2018 11:23:19 PM	Green Heartbeat	Close
2016SVR	SharePoint System Timer Job	6/25/2018 1:30:02 PM	Green Heartbeat	Close

6.12.5.13 Load Balancing

After setting up load balancing, you must update Records Management to accommodate the new load-balanced URL. To do this, perform the steps on each server hosting Records Management in the load balanced cluster.

⚠️ Two file shares are needed for load balancing the Manager Web: a reports_share and a cache_share. The reports_share is used to store custom user created reports. The cache_share is used for all reports regardless of the report type - OOTB or Custom. These file shares should be accessible from all Manager Web (Records Management Core) servers by the Manager Web Application Pool account/Service Account with Full Control.

Open a PowerShell Command Window and execute the following commands:

```
Set-RecordsManagerWeb -SiteName "Information Lifecycle"
-SiteUrl "https://load-balanced-url:8080"
-WSFedMetaUrl "https://load-balanced-sts-url:8081/metadata/federationmetadata.svc/xml"
-WSFedMetaRealm "https://load-balanced-url:8080"
-WSFedMetaReply "https://load-balanced-url:8080"
-WSFedMetaAudience "https://load-balanced-url:8080"
-WSTrustUrl "https://load-balanced-sts-url:8081/Trust.svc"
-ReportDirectory "\\server\reports_share"
-ReportCacheDirectory "\\server\cache_share\"
```

```
Set-RecordsManagerSTSWeb -SiteName "Information Lifecycle STS"
-BaseUrl "https://load-balanced-sts-url:8081"
-ExpectedAddress "https://load-balanced-url:8080"
```

6.12.5.14 Authentication

Records Management uses claims-based authentication for users, specifically the WS-Federation protocol. A default Identity Provider web site is always installed and configured as part of the Records Management Core installation. However, an administrator can easily use another Identity Provider to authenticate users. Any Identity Provider that supports WS-Federation can be used to authenticate users instead of the default Identity Provider web site.

Required Claims

Claim	Schema
Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name [schemas.xmlsoap.org] ³¹
NameIdentifier	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier [schemas.xmlsoap.org] ³²
Role	http://schemas.microsoft.com/ws/2008/06/identity/claims/role [schemas.microsoft.com] ³³

Optional Claims

Claim	Schema
Email	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress [schemas.xmlsoap.org] ³⁴

³¹[https://urldefense.proofpoint.com/v2/url?](https://urldefense.proofpoint.com/v2/url?u=http-3A__schemas.xmlsoap.org_ws_2005_05_identity_claims_name&d=DwMFAG&c=YC-d702opsuYKpiO2Bmlzg&r=lfBJH7oZg59df1-psrRWAAlTY3lzDOKwZVEEdCBjEctU&m=bMllv5eNy5YgP6c2UZ7-P87wrqynLOZJrVJgMrXzV2Y&s=Y4xXbCsQSRpasWqp7f_n3yfs1g8nYJO9Lb1aJCVgoSY&e=)

[u=http-3A__schemas.xmlsoap.org_ws_2005_05_identity_claims_name&d=DwMFAG&c=YC-d702opsuYKpiO2Bmlzg&r=lfBJH7oZg59df1-psrRWAAlTY3lzDOKwZVEEdCBjEctU&m=bMllv5eNy5YgP6c2UZ7-P87wrqynLOZJrVJgMrXzV2Y&s=Y4xXbCsQSRpasWqp7f_n3yfs1g8nYJO9Lb1aJCVgoSY&e=](https://urldefense.proofpoint.com/v2/url?u=http-3A__schemas.xmlsoap.org_ws_2005_05_identity_claims_name&d=DwMFAG&c=YC-d702opsuYKpiO2Bmlzg&r=lfBJH7oZg59df1-psrRWAAlTY3lzDOKwZVEEdCBjEctU&m=bMllv5eNy5YgP6c2UZ7-P87wrqynLOZJrVJgMrXzV2Y&s=Y4xXbCsQSRpasWqp7f_n3yfs1g8nYJO9Lb1aJCVgoSY&e=)

³²[https://urldefense.proofpoint.com/v2/url?](https://urldefense.proofpoint.com/v2/url?u=http-3A__schemas.xmlsoap.org_ws_2005_05_identity_claims_nameidentifier&d=DwMFAG&c=YC-d702opsuYKpiO2Bmlzg&r=lfBJH7oZg59df1-psrRWAAlTY3lzDOKwZVEEdCBjEctU&m=bMllv5eNy5YgP6c2UZ7-P87wrqynLOZJrVJgMrXzV2Y&s=3D-mDpqtNPJ6rnn0TpuakAMpHEPguXVL5gLHV5CKps&e=)

[u=http-3A__schemas.xmlsoap.org_ws_2005_05_identity_claims_nameidentifier&d=DwMFAG&c=YC-d702opsuYKpiO2Bmlzg&r=lfBJH7oZg59df1-psrRWAAlTY3lzDOKwZVEEdCBjEctU&m=bMllv5eNy5YgP6c2UZ7-P87wrqynLOZJrVJgMrXzV2Y&s=3D-mDpqtNPJ6rnn0TpuakAMpHEPguXVL5gLHV5CKps&e=](https://urldefense.proofpoint.com/v2/url?u=http-3A__schemas.xmlsoap.org_ws_2005_05_identity_claims_nameidentifier&d=DwMFAG&c=YC-d702opsuYKpiO2Bmlzg&r=lfBJH7oZg59df1-psrRWAAlTY3lzDOKwZVEEdCBjEctU&m=bMllv5eNy5YgP6c2UZ7-P87wrqynLOZJrVJgMrXzV2Y&s=3D-mDpqtNPJ6rnn0TpuakAMpHEPguXVL5gLHV5CKps&e=)

³³[https://urldefense.proofpoint.com/v2/url?](https://urldefense.proofpoint.com/v2/url?u=http-3A__schemas.microsoft.com_ws_2008_06_identity_claims_role&d=DwMFAG&c=YC-d702opsuYKpiO2Bmlzg&r=lfBJH7oZg59df1-psrRWAAlTY3lzDOKwZVEEdCBjEctU&m=bMllv5eNy5YgP6c2UZ7-P87wrqynLOZJrVJgMrXzV2Y&s=HjvT_J0OCZ7OWt97dhpXFz8S-Frb_gG31XvLMhEgaw0&e=)

[u=http-3A__schemas.microsoft.com_ws_2008_06_identity_claims_role&d=DwMFAG&c=YC-d702opsuYKpiO2Bmlzg&r=lfBJH7oZg59df1-psrRWAAlTY3lzDOKwZVEEdCBjEctU&m=bMllv5eNy5YgP6c2UZ7-P87wrqynLOZJrVJgMrXzV2Y&s=HjvT_J0OCZ7OWt97dhpXFz8S-Frb_gG31XvLMhEgaw0&e=](https://urldefense.proofpoint.com/v2/url?u=http-3A__schemas.microsoft.com_ws_2008_06_identity_claims_role&d=DwMFAG&c=YC-d702opsuYKpiO2Bmlzg&r=lfBJH7oZg59df1-psrRWAAlTY3lzDOKwZVEEdCBjEctU&m=bMllv5eNy5YgP6c2UZ7-P87wrqynLOZJrVJgMrXzV2Y&s=HjvT_J0OCZ7OWt97dhpXFz8S-Frb_gG31XvLMhEgaw0&e=)

³⁴[https://urldefense.proofpoint.com/v2/url?](https://urldefense.proofpoint.com/v2/url?u=http-3A__schemas.xmlsoap.org_ws_2005_05_identity_claims_emailaddress&d=DwMFAG&c=YC-d702opsuYKpiO2Bmlzg&r=lfBJH7oZg59df1-psrRWAAlTY3lzDOKwZVEEdCBjEctU&m=bMllv5eNy5YgP6c2UZ7-P87wrqynLOZJrVJgMrXzV2Y&s=YAQQC5mhss5Ww9-dcHa_ANIZQyeIjDB0Nr4ZEW8_Wql&e=)

[u=http-3A__schemas.xmlsoap.org_ws_2005_05_identity_claims_emailaddress&d=DwMFAG&c=YC-d702opsuYKpiO2Bmlzg&r=lfBJH7oZg59df1-psrRWAAlTY3lzDOKwZVEEdCBjEctU&m=bMllv5eNy5YgP6c2UZ7-P87wrqynLOZJrVJgMrXzV2Y&s=YAQQC5mhss5Ww9-dcHa_ANIZQyeIjDB0Nr4ZEW8_Wql&e=](https://urldefense.proofpoint.com/v2/url?u=http-3A__schemas.xmlsoap.org_ws_2005_05_identity_claims_emailaddress&d=DwMFAG&c=YC-d702opsuYKpiO2Bmlzg&r=lfBJH7oZg59df1-psrRWAAlTY3lzDOKwZVEEdCBjEctU&m=bMllv5eNy5YgP6c2UZ7-P87wrqynLOZJrVJgMrXzV2Y&s=YAQQC5mhss5Ww9-dcHa_ANIZQyeIjDB0Nr4ZEW8_Wql&e=)

Claim	Schema
GivenName	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname [schemas.xmlsoap.org] ³⁵
Surname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname [schemas.xmlsoap.org] ³⁶

6.12.6 Records Management Core Installation (On-Premises)

Gimmel Records Management may be deployed on-premise to ensure the strictest record security and have complete control of your environment. The installation media consists of a single ISO that contains everything necessary to install and set up Records Management and its components.

To initiate the setup process, regardless of the component, double-click the setup.hta file in the root folder of the ISO.

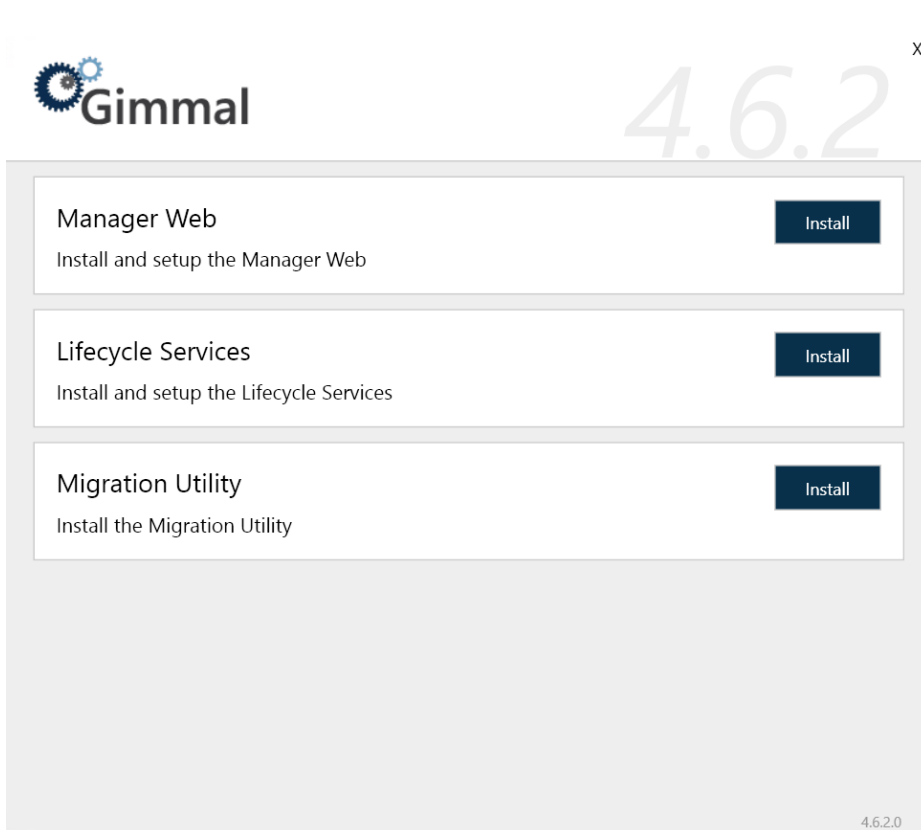
6.12.6.1 Setup Screen

i Ensure that you run the installer as the Local Administrator.

Upon initiating setup, the Records Management splash screen launches, which provides a link to each component's respective installer.

³⁵https://urldefense.proofpoint.com/v2/url?u=http-3A__schemas.xmlsoap.org_ws_2005_05_identity_claims_givenname&d=DwMFAG&c=YC-d702opsuYKpiO2Bmlzg&r=lfBJH7oZg59df1-psrRWAAlTY3lzDOKwZVEdCBJEctU&m=bMllv5eNy5YgP6c2UZ7-P87wrqynLOZJrVJgMrXzV2Y&s=bt-cgK4O5JjxCMzU0q5V3mKjOLljalFmYAghmE7YXxU&e=

³⁶https://urldefense.proofpoint.com/v2/url?u=http-3A__schemas.xmlsoap.org_ws_2005_05_identity_claims_surname&d=DwMFAG&c=YC-d702opsuYKpiO2Bmlzg&r=lfBJH7oZg59df1-psrRWAAlTY3lzDOKwZVEdCBJEctU&m=bMllv5eNy5YgP6c2UZ7-P87wrqynLOZJrVJgMrXzV2Y&s=6MribuZLJ26ewdp4vNc2FtMmCgF7xmWocs1OnTrHowg&e=



This screen presents each installable component that is a part of the Core Platform. Click **Install** next to the component that you want to install. This will launch the specific installation wizard for that component.

Each of these components can be installed on the same machine or on a separate machine for scale-out scenarios.

Perform the following steps on the following pages for a successful deployment of the core platform.

1. [Pre Installation of Manager Web](#)(see page 238)
2. [Installation of Manager Web](#)(see page 239)
3. [Installation of Lifecycle Services](#)(see page 241)
4. [Ensuring Successful Authentication with NTLM](#)(see page 243)

6.12.6.2 Manager Web Pre-Installation

Prior to installing the Manager Web, you must configure Windows Roles and Features as follows:

Roles

- Web Server (IIS)
 - Common HTTP Features
 - Static Content
 - Health and Diagnostics
 - HTTP Logging
 - Performance
 - Static Content Compression
 - Security
 - Windows Authentication
 - Application Development

- ASP.NET 3.5
- ASP.NET 4.5

Features

- .NET Framework 3.5 Features
 - .NET Framework 3.5
- .NET Framework 4.5 Features
 - WCF Services
 - HTTP Activation



July 1, 2021: HTTPS Requirement

Today, it is exceedingly rare to have non-sensitive web traffic. By always using HTTPS connections, people's changing expectations for how websites handle sensitive traffic make everyone safer. By always using HTTPS connections, web services don't have to make a subjective judgment call about what's "sensitive". By always using HTTPS connections, there is less room for error and deployment is simpler and more consistent across all of your environments.

Some modern web browsers now have default behavior that does not allow certain authentication schemes over HTTP. **As a result, Gimmel now requires using HTTPS with Gimmel Records for any version of the software.** The version of Gimmel Records you're using doesn't change the behavior of the browser with HTTP. The exact behavior when using HTTP depends on your choice of web browser and its related security configuration. For these reasons, Gimmel will provide limited, best-effort support for HTTP and **will require HTTPS to be configured before troubleshooting any support tickets.**

6.12.6.3 Installing Manager Web



Ensure that the [Pre-Installation](#)(see page 238) steps have been completed prior to beginning installation.

To install Manager Web, perform these steps:

1. On the [Core Platform setup screen](#)³⁷, click **Install** to the right of Manager Web. The first screen that displays is the Check for Prerequisites. This screen validates the following information before allowing the installation to proceed:
 - a. Current User is Local Administrator
 - b. IIS 7+ is Installed
2. Click **Next**. The installation location screen displays, which determines where the software will be installed.
3. Click the **...** icon next to the installation location field, select the desired installation location, and then click **Next**. The IIS settings page displays.
4. Configure the IIS settings for the Manager Web, based on the information below:
 When you install the Manager Web, two web applications will be created in IIS. One is the Manager Web site and the other is the Records Management STS.
 The Records Management STS is used for Claims-Based Security, which is used by Records Management. Out of the box, the built-in STS uses Integrated Windows Authentication, but you have the ability to leverage another STS if desired.
 The following options determine what the respective site will be named in IIS:

³⁷ <http://docs.gimmel.com/en/14318-launching-the-setup-screen.html>

- Web Application Name
- STS Application Name

The following options determine which port the respective site will use in IIS:

- Web Application Port
- STS Application Port

The following options determine how authentication is configured and whether to create IIS bindings with *SSL (*highly recommended) or without SSL (see [Pre-Installation](#)(see page 238) requirement on HTTPS):

- Fully Qualified Domain Name (This is the load-balanced URL or DNS name used to access Records Management.)
- SSL Certificate (If selected, this certificate is used to create SSL bindings in IIS, otherwise, if not specified, SSL will not be used.)

When you install the Manager Web, a new Application Pool will be created that is used by each of the created web applications. The following options specify which user account to use for this Application Pool: (This should be a domain account.)

- **Username** (ex. DOMAIN\Username)
- **Password**

5. Click **Next**. The Database Settings screen displays, where you can configure the database that will be used by Records Management.

The following options determine the connection information that will be used by Records Management to connect to SQL Server.

Enter the following information:

- **Database Server:** The name of the SQL Server Install (ex. SERVERNAME\InstanceName)
- **Database Name:** The name of the actual SQL Server Database
- **Use SQL Authentication:** Specifies that the connection information should use SQL Authentication with the Username and Password indicated below
- **Username:** The SQL Server username to use if SQL Authentication is specified
- **Password:** The SQL Server password to use if SQL Authentication is specified

If SQL Authentication is not specified, the connection information will use Windows Authentication by specifying a trusted connection. This means that the Application Pool account will be used to connect to SQL Server, therefore this account will need the following database permissions. If SQL Authentication is specified, the SQL user will also require the following permissions.

- db_datareader
- db_datawriter
- **GRANT EXECUTE** on all Stored Procedures
- **GRANT EXECUTE** on all Scalar User Defined Functions
- **GRANT SELECT** on all Table and Inline User Defined Functions
- **GRANT ALTER** on the following Tables
 - ClassificationContexts
 - DateAssignmentContexts

If you select "Automatically Create Database", the installation will automatically attempt to create the database using the Database Server and Database Name indicated. The appropriate account will also be automatically granted the appropriate rights to this database. **This option requires that the current user has permission to create databases and manage security in the SQL Server instance indicated.**

If "Automatically Create Database" is **not** specified, the installation will configure connection information but will not attempt to create the database. In this case, you will need to leverage the SQL Scripts at the following location (in the order listed) to manually create the database in the SQL Server instance indicated. You will also need to manually configure security as indicated above.

- %Install Path%\Web\Sql\RecordLion.RecordsManager.sql
- %Install Path%\Web\Sql\RecordLion.RecordsManager.Optimize.sql
- %Install Path%\Web\Sql\RecordLion.RecordsManager.Elmah.sql
- %Install Path%\Web\Sql\RecordLion.RecordsManager.Seed.sql

6. Click **Next**. The Installed screen displays, indicating that the installation will take place using the configuration options you specified. The progress bar indicates the current state of the installation.
7. When the application is finished installing, click **Next** to continue to the final screen. The final screen indicates that everything installed successfully.
8. Click **Finish** to return to the main Setup screen, which should now indicate that Manager Web has been installed.
9. After Managed Web has installed, you must create the Master Administrator account by performing the following steps:
 - a. Open the Manager Web using a web browser.
 - b. Click the Sign-In dropdown and select **Sign In Locally**.
 - c. Enter the username **administrator** and a password of your choosing. Note the following:
 - i. The credentials you enter represent your **Master Account**.
 - ii. This account has full permission over Records Management.
 - iii. To log back in with this account, use the credential you provided above.
 - iv. You can use this account to provision new users.

6.12.6.4 Installing Lifecycle Services

The Lifecycle Services component is a critical part of Records Management because it is the engine that is used to process retention periods and direct the actions that ultimately drive records and information through its lifecycle. Without this component, information will not move through its lifecycle, so it must be installed.

To install Lifecycle Services, perform these steps:

1. On the [Core Platform setup screen](#)³⁸, click **Install** to the right of Lifecycle Services. The first screen that displays is the Check for Prerequisites. This screen validates the following information before allowing the installation to proceed.
 - Current User is Local Administrator
2. Click **Next**. The installation location screen displays, which determines where the software will be installed.
3. Click the **...** icon next to the installation location field, select the desired installation location, and then click **Next**. The Service Settings screen displays.

The following fields determine the connection information that will be used by Records Management to connect to SQL Server. Enter the following information:

 - **Username:** The name of the domain account (ex. DOMAIN\Username)
 - **Password:** The password of the domain account
4. Click **Next**. The Database Settings screen displays, where you will configure the database settings for Lifecycle Services.

The following options determine the connection information that will be used by Records Management to connect to SQL Server. Enter the following information:

- **Database Server:** The name of the SQL Server Install (ex. SERVERNAME\InstanceName)
 - **Database Name:** The name of the actual SQL Server Database
 - **Use SQL Authentication:** Specifies that the connection information should use SQL Authentication with the Username and Password indicated below
 - **Username:** The SQL Server username to use if SQL Authentication is specified
 - **Password:** The SQL Server password to use if SQL Authentication is specified
- If SQL Authentication is not specified, the connection information will use Windows Authentication by specifying a trusted connection. This means that the Application Pool account will be used to connect

³⁸ https://docs.gimmel.com/Archived_Site/Records_Management_V462_Release/Launching_Setup_V462.htm

to SQL Server, therefore this account will need the following database permissions. If SQL Authentication is specified, the SQL user will also require the following permissions.

- db_datareader
- db_datawriter
- GRANT EXECUTE on all Stored Procedures
- GRANT EXECUTE on all Scalar User Defined Functions
- GRANT SELECT on all Table and Inline User Defined Functions
- GRANT ALTER on the following Tables
- ClassificationContexts
- DateAssignmentContexts

If you select the "Automatically Create Database" checkbox, the installation will automatically attempt to create the database using the Database Server and Database Name indicated. The appropriate account will also be automatically granted the appropriate rights to this database. This option requires that the current user has permissions to create databases and manage security in the SQL Server instance indicated.

If you do **not** select the "Automatically Create Database" checkbox, the installation will configure connection information but will not attempt to create the database. In this case, you will need to leverage the SQL Scripts at the following location (in the order listed) to manually create the database in the SQL Server instance indicated. You will also need to manually configure security as indicated above.

- %Install Path%\Web\Sql\RecordLion.RecordsManager.sql
- %Install Path%\Web\Sql\RecordLion.RecordsManager.Optimize.sql
- %Install Path%\Web\Sql\RecordLion.RecordsManager.Elmah.sql
- %Install Path%\Web\Sql\RecordLion.RecordsManager.Seed.sql

5. Click **Next**. The Installed screen displays, where installation takes place using the configuration options specified. The progress bar indicates the current state of the installation.
6. When the application is finished installing, click Next to continue to the final screen.
7. The Finish screen displays, indicating that everything installed successfully.
8. Click **Finish** to return to the main Setup screen. This screen should now indicate that Lifecycle Services has been installed.
9. Once the installation is complete for Lifecycle Services, you must manually start Lifecycle Services for it to start processing.

6.12.6.5 Installing the Migration Utility



To use the Migration Utility "Import" function, the Microsoft Access 2013 Runtime must first be installed. It can be downloaded directly from Microsoft [here](#)³⁹. Typically, the x86 version will be installed.

To install the Migration Utility, perform these steps:

1. On the [Core Platform setup screen](#)⁴⁰, click **Install** to the right of Migration Utility. The first screen that displays is the Check for Prerequisites.
2. Click **Next**. The installation location screen displays, which determines where the software will be installed.
3. Click the **...** icon next to the installation location field, select the desired installation location
4. Click **Next**. The Installed screen displays, where installation takes place using the configuration options specified. The progress bar indicates the current state of the installation.
5. When the application is finished installing, click Next. The Finish screen displays, indicating that everything installed successfully.

³⁹ <https://www.microsoft.com/en-us/download/details.aspx?id=39358>

⁴⁰ https://docs.gimmel.com/Archived_Site/Records_Management_V462_Release/Launching_Setup_V462.htm

- Click **Finish** to return to the main Setup screen. This screen should now indicate that the Migration Utility has been installed.

6.12.7 Records Management Core Configuration (On-Premises)

6.12.7.1 Ensuring Successful Authentication with NTLM

6.12.7.2 Configuring Fully Qualified Domain Name (FQDN)

6.12.7.3 Supporting FQDN from Browser on Localhost

6.12.7.4 IIS Configuration

6.12.7.5 Ensuring Successful Authentication with NTLM

Once you create the Information Lifecycle STS, it is configured to leverage Windows Authentication in IIS. If Kerberos Authentication is not enabled, many modern browsers may have an issue successfully authenticating users using NTLM, even though both providers exist in IIS configuration. To ensure successful authentication, you should disable Kerberos authentication by performing the following steps:

- Open IIS
- Select **Records Management STS**
- Click **Authentication Feature**
- Select **Windows Authentication**
- Click the **Providers...** option in the pane on the right
- Select the **Negotiate** option and click **Remove**
- Click **OK** to close the Providers window

6.12.7.6 Configuring Fully Qualified Domain Name (FQDN)

To change the Records Management URL so that it uses a Fully Qualified Domain Name (FQDN), you must configure Records Management so that it knows the URLs that will be used to access the site. To do so, after configuring DNS, perform the following steps:

Open a PowerShell command window, and execute the following commands:

```
Set-RecordsManagerWeb -SiteName "Records Management"
-SiteUrl "https://url-to-manageweb"
-WSFedMetaUrl "https://url-to-sts/metadata/federationmetadata.svc/xml"
-WSFedMetaRealm "https://url-to-manageweb"
-WSFedMetaReply "https://url-to-manageweb"
-WSFedMetaAudience "https://url-to-manageweb"
-WSTrustUrl "https://url-to-sts/Trust.svc"
```

```
Set-RecordsManagerSTSWeb -SiteName "Records Management STS"
```

```
-BaseUrl "https://url-to-sts"
-ExpectedAddress "https://url-to-manageweb"
```


6.12.7.7 Supporting FQDN from Browser on Localhost

If you attempt to access Records Management using a Fully Qualified Domain Name from the local machine where Records Management is installed, IIS prevents you from being able to access the site with an HTTP 401.1 status code. This is because Windows performs a loopback check in this scenario to prevent reflection attacks on your computer, which causes Authentication to fail.

To enable access to the site, refer to the following Microsoft knowledge base article:

<http://support.microsoft.com/kb/896861>

6.12.7.8 IIS Configuration

 The topics on configuring IIS apply to the core platform running on-premise.

[Configuring the IIS Binding Securely using SSL](#)

[Configuring the IIS Binding Unsecurely without SSL](#)

[Allowing HTTP](#)

[Installing a Custom Signing Certificate](#)

[Configuring the IIS Binding Securely using SSL](#)

To secure Records Management with SSL, you must configure the IIS Bindings. You can configure the IIS Bindings for SSL in two ways, manually or by using the provided PowerShell script.

Binding Manually


To configure SSL Bindings manually, perform the following actions:

1. Open IIS.
2. Select **Records Management Web**.
3. Select **Bindings...**
4. Change or Add HTTPS Binding and Choose Open Port.
5. Select **Certificate to use for SSL**.
6. Select **Records ManagementSTS Web**.
7. Select **Bindings...**
8. Change or Add HTTPS Binding and Choose Open Port.
9. Select **Certificate to use for SSL**.

Open a PowerShell command window, and execute the following commands:


```
Set-RecordsManagerWeb -SiteName "Records Management" -SiteUrl "https://url-to-manageweb" -WSFedMetaUrl "https://url-to-sts:444/metadata/federationmetadata.svc/xml" -WSFedMetaRealm "https://url-to-manageweb" -WSFedMetaReply "https://url-to-manageweb" -WSFedMetaAudience "https://url-to-manageweb" -WSTrustUrl "https://url-to-sts:444/Trust.svc" -AllowHttp $false
```

```
Set-RecordsManagerSTSWeb -SiteName "Records Management STS" -BaseUrl "https://url-to-sts:444" -ExpectedAddress "https://url-to-manageweb" -AllowHttp $false
```

 If you use port 443, you should exclude the port number in the above PowerShell commands for the respective URL, as in the example.

Binding Using the Powershell Script

To configure SSL Bindings using the provided PowerShell script, perform the following actions:

1. Open the PowerShell Prompt.
2. Change Current Directory to “%Manager Web Path%\Ps1”.
3. Execute the Script in the folder named Set-RecordsManagerSSL.ps1 as in the example below:

```
.\Set-RecordsManagerSSL.ps1 -WebName "Information Lifecycle" -WebUrl "https://url-to-manageweb" -WebPort 443 -StsName "Information Lifecycle STS" -StsUrl "https://url-to-sts:444" -StsPort 444 -CertThumbprint "BE41D8EA75A18AB565EF1622C8622336F482A0E3"
```

Finding the SSL Certificate Thumbprint

Use the following PowerShell script to find the Thumbprint for a certificate that is already installed in the local computer's Personal certificate store. Be sure to replace the **CN=*.domain.local** string with your certificate's subject name.

```
$cert = Get-ChildItem cert:\LocalMachine\My | Where-Object {$_.Subject.StartsWith("CN=*.domain.local")}  
$cert.Thumbprint
```

Configuring the IIS Binding Unsecurely without SSL

To set up Records Management, you must configure the IIS Bindings. You can configure the IIS Bindings in two ways: manually, or by using the provided PowerShell script. Each method is described below.

Binding Manually


To configure bindings manually, perform the following steps:

1. Open IIS.

2. Select **Records Management Web**.
3. Select **Bindings ...**
4. Change or Add HTTP Binding and Choose Open Port.
5. Select **Records Management STS Web**.
6. Select **Bindings...**
7. Change or Add HTTP Binding and Choose Open Port.
8. Open a PowerShell command window, and execute the following commands:

```
Set-RecordsManagerWeb -SiteName "Records Management"
-SiteUrl "http://url-to-manageweb"
-WSFedMetaUrl "http://url-to-sts:8081/metadata/federationmetadata.svc/xml"
-WSFedMetaRealm "http://url-to-manageweb"
-WSFedMetaReply "http://url-to-manageweb"
-WSFedMetaAudience "http://url-to-manageweb"
-WSTrustUrl "http://url-to-sts:8081/Trust.svc"
-AllowHttp $true
```

```
Set-RecordsManagerSTSWeb -SiteName "Records Management STS"
-BaseUrl "https://url-to-sts:8081"
-ExpectedAddress "https://url-to-manageweb"
-AllowHttp $true
```

 If you use port 80, you should exclude the port number in the above PowerShell commands for the respective URL, as in the example.


Binding Using Powershell Script

To configure bindings using the provided PowerShell script, perform the following steps:

1. Open the PowerShell Prompt
2. Change Current Directory to “%Manager Web Path%\Ps1”.
3. Execute the Script in the folder named Set-RecordsManager.ps1, as in the example below:

```
.\Set-RecordsManager.ps1
-WebName "Records Management"
-WebUrl "http://url-to-manageweb"
-WebPort 80
-StsName "Records Management STS"
-StsUrl "http://url-to-sts:8081"
-StsPort 8081
```

Allowing HTTP

 Using HTTP for Gimmel Records Management is not recommended and may be a security risk.

By default, Records Management cannot be used over HTTP. If you attempt to access Records Management without binding the Web to SSL, you receive an error.

However, for some scenarios (such as demos) you may want to allow HTTP access. To do so, open a PowerShell command window, import the Records Management PowerShell Module, and execute the following commands:

```
Set-RecordsManagerWeb -SiteName "Information Lifecycle" -AllowHttp $true
Set-RecordsManagerSTSWeb -SiteName "Information Lifecycle STS" -AllowHttp $true
```

Installing a Custom Signing Certificate

Once the Records Management STS is created, an X.509 certificate is registered in IIS that is responsible for signing issued tokens, which ultimately ensures that Claims-Based Security is secure.

Because the out-of-the-box signing certificate that is used is common to all installations of Records Management, you should deploy your own certificate specific to your environment by performing the following steps on each of the Web Servers that will be hosting the Manager Web.

1. Obtain an X.509 certificate for token signing.

There are several ways to obtain a X.509 certificate for token signing.

- Commercial Certification Authority – You can purchase an X.509 certificate from a commercial certification authority.
- Generate a Self-Signed Certificate – You can generate your own self-signed certificate by following the steps at the following link: <https://docs.microsoft.com/en-us/powershell/module/pki/client/new-selfsignedcertificate?view=win10-ps>

1. Once you have generated a certificate, open IIS and select **Certificates**.
2. Select your newly generated certificate and choose **Export** from the Actions Pane.
3. On each server hosting the Manager Web, open IIS and select **Certificates**.
4. Select **Import** from the Actions Pane and choose the certificate that you previously exported.
5. On each server hosting the Manager Web, execute the following PowerShell command:

```
Set-RecordsManagerStsWeb -SiteName "Records Management STS" -
SigningCertificateSubjectName CN=<YourSubjectName>
```

6.12.8 Uninstalling the Core Platform

To uninstall the Core Platform, perform the following steps:

1. Open Add/Remove Programs on Servers hosting the Manager Web.
2. Double-click Gimmel Manager Web.
3. Click **Uninstall**.
4. Open Add/Remove Programs on Servers hosting Lifecycle Services.
5. Double-click Gimmel **Lifecycle Processing Service**.
6. Click **Uninstall**.

After you uninstall the Core Platform, the database will remain intact on the database server. You may keep this database in case you will be reinstalling the Core Platform, or you can delete the database manually if it is no longer needed.

6.13 Managing Security

Security in Gimmel Records Management is made up of accounts, security roles, permissions, and record filters.

- Accounts - A user name and password that allows access to the system.
- Security Roles - A role defines which features a user account will have access to. A user may have more than one role.
- Permissions - Permissions are given to user accounts granting them certain types of access to records associated with record classes and containers.
- Record Filters - A rule-based filter that can limit which records a user has access to.

This section covers the security administration tasks that are available in Records Management. It includes the following topics:

6.13.1 Account Types

6.13.2 Security Roles

6.13.3 Security Role Privilege Overview

6.13.4 Permission Overview

6.13.5 File Plan Editor Permissions

6.13.6 Creating a Service Account

6.13.7 Granting and Revoking User Access

6.13.8 Creating Local Groups

6.13.9 Changing the Master Account Password

6.13.10 Account Types

There are three types of account types available in the system; **Master Account**, **User Account**, and **Service Account**.

6.13.10.1 Master Account

The Master Account is a specific account that has full control over all of Records Management (not Physical Records Management) and can be used to provision new Users and Service Accounts, as well as administer any aspect of the system. This account information should be kept secure!

If you are the system administrator, you should have [created the Master Account](#)(see page 211) the first time you logged in.

6.13.10.2 User Account


The User Account is the typical account that is created in the system. User accounts are given [Security Roles](#)(see page 249) once they are created. In order to add a User Account, they must belong to the registered Identity Provider, such as Windows Accounts if you are using the out-of-the-box Identity Provider.

6.13.10.3 Service Account

A Service Account differs from the other account types because these accounts are created locally and not associated with the registered Identity Provider, such as Windows Accounts if using the out-of-the-box Identity Provider.

The purpose of a Service Account is to have an account that can be used from the various Connectors or any Third-Party Services that will be communicating with Records Management.

As a best practice, you should create a separate Service Account for each Connector that will be used. This will make it easier to identify a specific Connector's related activity within the system. Service Accounts possess a high level of rights within the system and should be kept secure.

 When you enter your Service Account credentials, the Service Account username format depends on whether or not you are connecting the Gimmel Cloud for Records Management. If the Gimmel Cloud is being used, the username format is: {service account name}@{tenant domain} (e.g. spocservice@gimmel.com⁴¹, or fscservice@companyname.com⁴²), otherwise, the format is just: {service account name}. For more information, see [Directing the Connector to Records Management](#).

6.13.11 Security Roles

In Records Management, there are many security roles available in the system. When adding a new account to the system, they will need to be assigned to at least one security role. Accounts can only be created and managed by those logging with a Master Account or with the System Admin role.

6.13.11.1 System Admin

The System Admin role grants a user full access to Records Management. System Admins can manage all aspects of Records Management, including the management of security. As a best practice, after logging in for the first time as the Master Account, we recommend provisioning the first user account as a System Admin. You should then login with this newly provisioned account to administer the system going forward. The Master Account should only be used if needed, such as when setting up the first System Admin account or configuring custom branding.

⁴¹ <mailto:spocservice@gimmel.com>

⁴² <mailto:fscservice@companyname.com>

The Physical Records Management extension has a different security system and not even this System Admin role will grant a user access to that system. If a user should be the administrator of both systems, add the user to both System Admin and Physical Administrator roles.

6.13.11.2 Global Record Manager

The Global Record Manager role allows a single user or group of users to have complete control over the File Plan and associated records within the system. A Global Record Manager will be able to grant users access to specific Record Classes as well as manage Record Filters in order to lock down access to records meeting a specific set of rules. The Global Record Manager role will not grant permission to manage accounts or to the global system settings.

A Global Record Manager is not an administrator of the Physical Records Management system by default, the user would also need to be given the Physical Administrator role.

6.13.11.3 Record Manager

The Record Manager role is used to provide record managers who may not have access to all records in an organization due to geographic or departmental boundaries. If your organization does not have these types of boundaries you may not need to assign any accounts to this role and can possibly make all records managers a Global Record Manager in the system.

The Record Manager role can actively manage the File Plan, with the exception of permissions and Record Filters. They will also be able to manage Legal Cases and to see monitoring information to better understand what is happening to information in the system in real-time.

The Record Manager account is bound by any Record Filters configured and applied to Record Classes.

6.13.11.4 Users

The User role grants an account access to the system but does not assign them any permissions to see records. Permissions are assigned for a specific user to individual Record Classes in order to give a user a certain level of access to the records and information assigned to that Record Class. A Global Record Manager will be able to set these specific permissions. An account must first be added to the system in order for it to be granted permission.

There are two levels of permissions that can be assigned at the Record Class level:

- **View** permissions grant a user view access for individual Record Classes in Records Management. When users who are assigned View permission sign into Records Management, they will have the ability to view existing records and details, as well as create physical record requests as needed.
- **Declare** permissions grant a user Declare access for individual Record Classes in Records Management. When users who are assigned Declare permission sign into Records Management, they will have the ability to view existing records and also Declare official records pertaining to the Record Classes in which they have been given access.

In addition, an account with the User role may be assigned Approver permissions. Approver permissions grant a user the ability to approve records for disposition for individual Record Classes. The ability to assign Approve permissions is discussed in the [Approvers](#) (see page 98) topic.

6.13.11.5 Physical Administrator

An account with the Physical Administrator role has complete access to all components of Physical Records Management. However, a Physical Administrator does not have System Admin role in the core Record Management system unless they are given that role as well. Because of the integration of Physical Records Management into the

core system, a Physical Administrator will not have access to the following components unless assigned the proper role in the core software:

- Assigning a record class to a container
- Placing a container on hold
- Placing an asset on hold
- Reporting

6.13.11.6 Physical User

The Physical User role will only be able to use features if they are given specific permission on the different components of Physical Records Management, which includes Containers, Assets, Locations, Charge In/Out, and using a Barcode Schema.

6.13.12 Security Role Privilege Overview

Each security role has different privileges within the software.

Permission	System Admin	Global Record Manager	Record Manager	User
Change Branding Options	X			
Plugins (Master Account only)				
Global Preferences	X			
Theme	X			
Email Server Settings	X			
Create Template for Approval Notification Emails	X			
Notification Settings	X			
My Preferences	X	X	X	X
Access Secure Option from Main Menu	X			
Create Users	X			
Assign User Permissions to a Record Class	X			
Monitor Services	X			

Permission	System Admin	Global Record Manager	Record Manager	User
Create and Manage File Plan	X	X	X	
Record Filters	X	X		
Access Monitor from Main Menu	X	X	X	
Inbox	X	X	X*	X*
Physical Confirmation	X	X	X*	
Expired Records	X	X	X*	
Rejected Records	X	X	X*	X*
Exceptions	X	X	X	
View Destruction Certificates	X	X	X	
View Disposed Records	X	X	X*	
View Record Details	X	X	X	X**
View Record Properties	X	X	X	X**
View Record Audit	X	X	X	
Declare Records	X	X	X	X**
Undeclare Records	X	X	X	
Classify Records	X	X	X	
Approve, Submit, Pause, Reject Inbox Items	X†	X†	X†	X†
Hold or Reclassify Expired Items	X	X	X	

Permission	System Admin	Global Record Manager	Record Manager	User
Legal Holds (Creating/viewing of cases, applying holds, configuring hold rules, removing holds)	X	X	X	
Services (Deletion)	X			
Access Manage option from Main Menu	X	X	X*	
Declare Obsolete	X	X	X	X**
Declare Superseded	X	X	X	X**
Generate and View Reports	X	X	X	
View Event Occurrences	X	X	X	
View Pending Automation	X	X	X	

*Subject to Records Filter

**Only when given specific permissions

†Only when made an approver

6.13.13 Permission Overview

Permissions allow users certain type of access to records and containers. The specifics permissions are detailed in this section.

6.13.13.1 Record Classes

Accounts with the User security role, will need to be given specific permissions on a Record Class for access to any records that that belong to it.

Permission	Comment
View Record Details	The ability to view details about the records including properties and lifecycle details.
Declare	Declare as a record. Also allows a record to be marked superseded or obsolete.

See the topic on [Record Class Permission](#)(see page 201) for more information.

6.13.13.2 Physical Records

Accounts with the Physical User role will need to be given specific permissions in order to access container and assets.

Child Containers

A Physical User cannot be given create/edit/delete permission to root containers regardless of the permissions that are set and must be assigned specific access to child containers. In the following table, the permissions are shown from least privileged to most privileged, meaning View is the least, and Delete is the most.

Permission	Comment
View	View a container. Without View, a user won't be able to see or search for any assets. This is the lowest privileged assignment and does not adopt any other permissions.
Create	Create a new child container under the given container.
Edit	Edit the container all the properties for a container, apply custom metadata, as well as the ability to drag/drop and cut/paste.
Edit Permission	Edit the permission of a container.
Delete	Delete the container. This is the highest privileged assignment and adopts all the other permission with it.

Assets

In the following table, the permissions are shown from least privileged to most privileged, meaning View is the least, and Delete is the most. Some of the permission may also require permissions on the container itself in order to get the expected results.

Permission	Comment
View	View the properties, metadata, and record details on assets in the container. This is the lowest privileged assignment and does not adopt any other permissions.
Create	Create a new asset in the container. Edit must also be given on the container.
Edit	Edit the metadata on assets in the container. Edit must also be given on the container.
Delete	Delete the asset. Edit must also be given on the container.

In addition to the permissions above, the following permissions require specific assignments in order for them to work.

Permission	Comment
Copy	Copy the asset to another location. The user must have Edit access to the target location for Copy/Paste or Drag/Drop to work.
Move	Move the asset to a new location. The user must have Edit access on both the source and target location for Copy/Paste or Drag/Drop to work. In addition, users are only allowed to move assets to the same Node type.

Locations

Physical users can only View locations, and cannot be assigned permissions to create, edit, or delete locations.

Barcode

A Physical User does not have the ability to create, edit, or delete barcode schemas. They will have the ability to enter barcodes if they have at least Edit permissions on both the container and the asset. Once a barcode is saved on an asset, a user can no longer edit them.

6.13.14 File Plan Editor Permissions

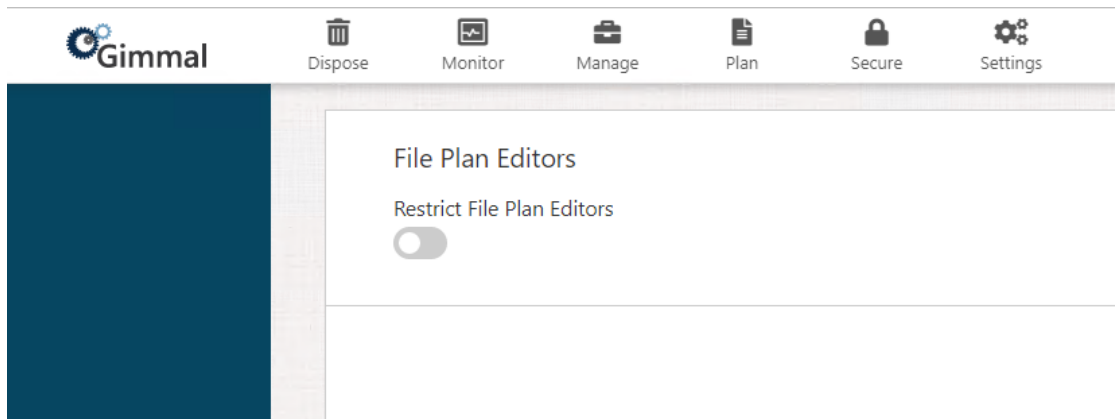
Permissions to File Plans can be restricted to individual users irrespective of the roles they've been granted. For example, you may have multiple Global Record Managers in your organization and only want one of them to be permitted to modify File Plans.

6.13.14.1 Accessing and Using the File Plan Editors Feature

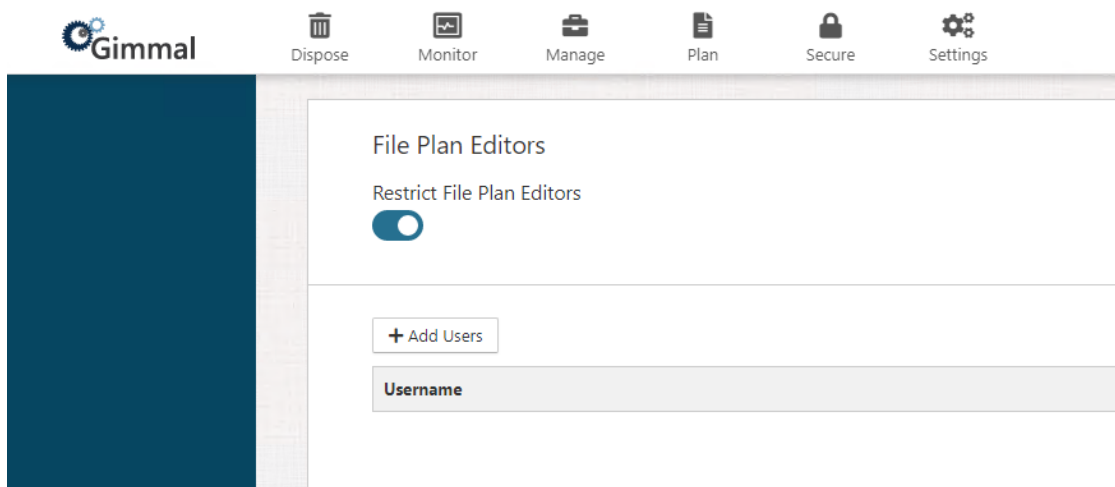
The File Plan Editors page can only be accessed by adding the */FilePlanEditors* endpoint to your Manager Web's URL. For example, if you are using the SaaS version of Gimmel Records, you would enter <https://records.gimmel.cloud/FilePlanEditors> into the address bar of your web browser.

NOTE: Only users with the System Admin role can access this page.

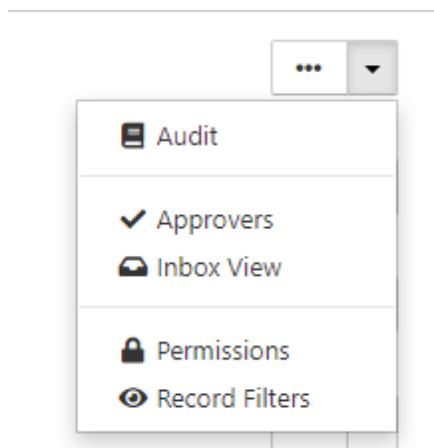
Upon navigating to the appropriate URL, you will see this page:



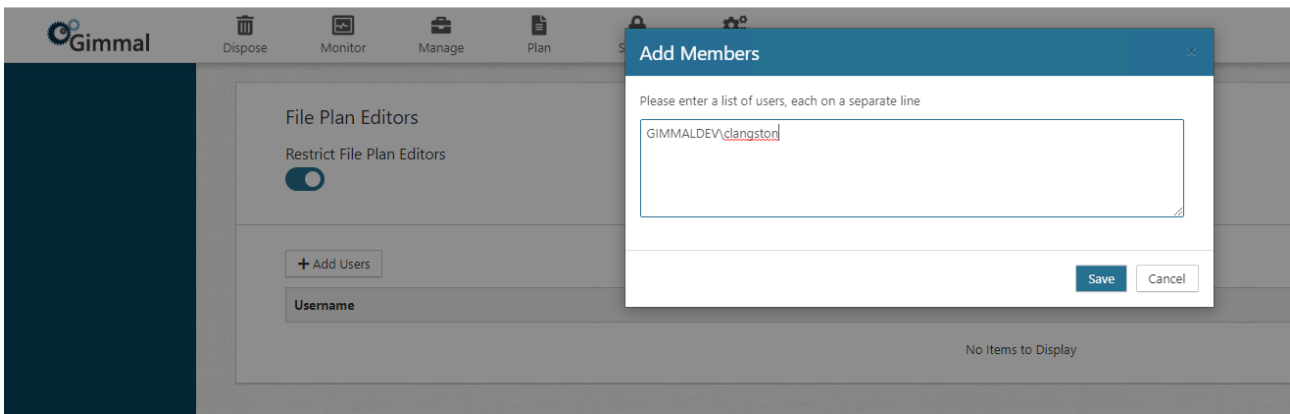
By default, this feature is disabled. Clicking on the slider will enable the feature, like so:



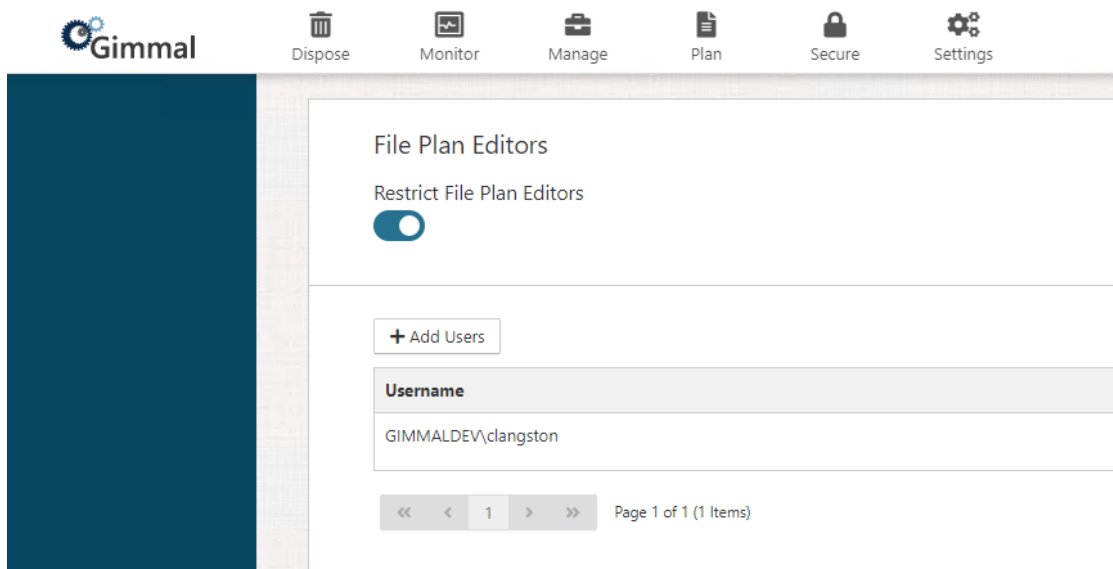
Once enabled, access to File Plans will be restricted to only the users supplied in the list on this page. If no users are specified, then no users will be able to create, modify, audit, or delete file plans. Here is what the options set looks like for File Plans when access is restricted:



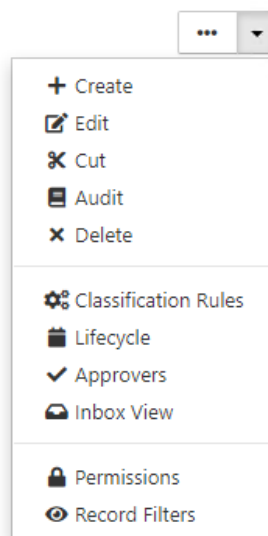
To grant File Plan Editor permission to a user, simply click on the *Add Users* button. A modal window will appear asking you to supply the *full username* for anyone you wish to grant permission. If you wish to submit multiple users at a time, supply each username on a separate line within the text box. Here’s an example of what a full username will look like:



Click the *Save* button to submit the list of users you wish to grant File Plan Editor permission. Upon doing so, you should see the list of users you submitted appear on the page, like so:



Once done, the users submitted will have full access to create, modify, audit, and delete File Plans. The options set within File Plans for users who have File Plan Editor permission will look like this:



At any time, this feature can be disabled by toggling the slider to the off position. Once disabled, File Plan permissions will be determined by Security Roles. For more information on what roles have access to File Plans, please see the [Security Role Privilege Overview page](#)(see page 251).

6.13.14.2 Limitations

The File Plan Editors feature has several limitations. They are as follows:

- The Manager Web interface contains no navigable link to this page. It can only be accessed by entering the appropriate URL into your web browser's address bar.
- The File Plan Editors page is the only location that indicates whether this feature is enabled. Neither the *Secure* nor *Settings* provide any indication that the File Plan Editors feature has been enabled or which users have been granted File Plan Editor permission.
- No operations within the File Plan Editors feature are audited. As such, there will be no audit trail available to see when the feature was enabled, who enabled it, what users were granted permission and when, and so forth. *(Note: File Plans themselves are audited as normal even when this feature is enabled. The only component lacking auditing is the File Plan Editor feature itself.)*
- If the File Plan Editors feature is enabled and no users are granted permission, then no one in the organization can interact with File Plans. This can only be resolved by granting at least one user File Plan Editor permission or by toggling the feature off.
- The File Plan Editors feature supersedes all other security permissions, meaning only users in the list of File Plan Editors have access to File Plans. Even the Master Account will not have access to File Plans while this feature is enabled.

6.13.15 Creating a Service Account

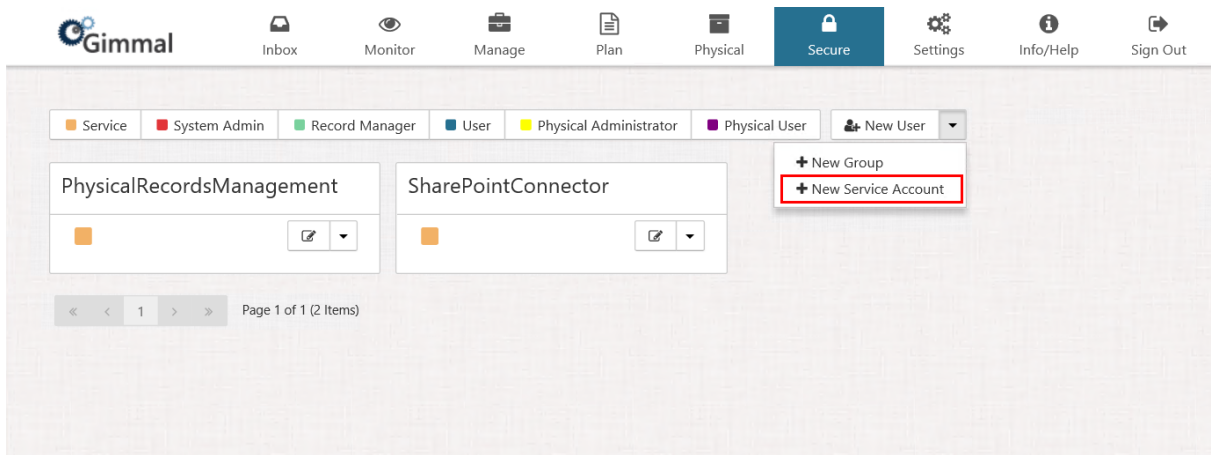
Service Accounts are created and managed locally within Records Management. They differ from the other account types because these accounts are created locally and not associated with the registered Identity Provider, such as Windows Accounts if using the out-of-the-box Identity Provider. The purpose of a Service Account is to have an account that can be used from the various Connectors or any Third-Party Services that will be communicating with Records Management.

As a best practice, you should create a separate Service Account for each Connector that will be used. This will make it easier to identify a specific Connector's related activity within the system. Service Accounts possess a high level of rights within the system and should be kept secure.

To create a Service Account, perform the following steps:

1. Login to Records Management as a user with a **Master** account or a **System Admin** account.
2. Select **Secure** on the Main Menu.

The Security page displays.



3. Select the New User drop-down, and then select **+New Service Account**.

The New Service Account window opens.

The 'New Service Account' dialog box is shown. It has a title bar with the text 'New Service Account' and a close button (X). Below the title bar, there are three input fields: 'Username *', 'Password *', and 'Confirm Password'. Each field has a small icon to its right: a user icon for Username, a key icon for Password, and a key icon for Confirm Password. At the bottom right of the dialog, there are two buttons: 'Save' and 'Cancel'.

4. Enter a username and password for the new account

⚠ When you enter your Service Account credentials, the Service Account username format depends on whether or not you are connecting to a Gimmel Cloud deployment for Records Management. If the cloud tenant is being used, the username format is: {service account name}@{tenant domain} (e.g. spocservice@gimmel.com⁴³, or fscservice@companyname.com⁴⁴), otherwise the format is just: {service account name}. For more information, see [\(Link\) Directing the Connector to Records Management](#).

Service Account passwords are limited to 18 characters. While the interface may let you enter more than 18 characters, connectors will not be able to use the service account.

5. Select the **Save** button

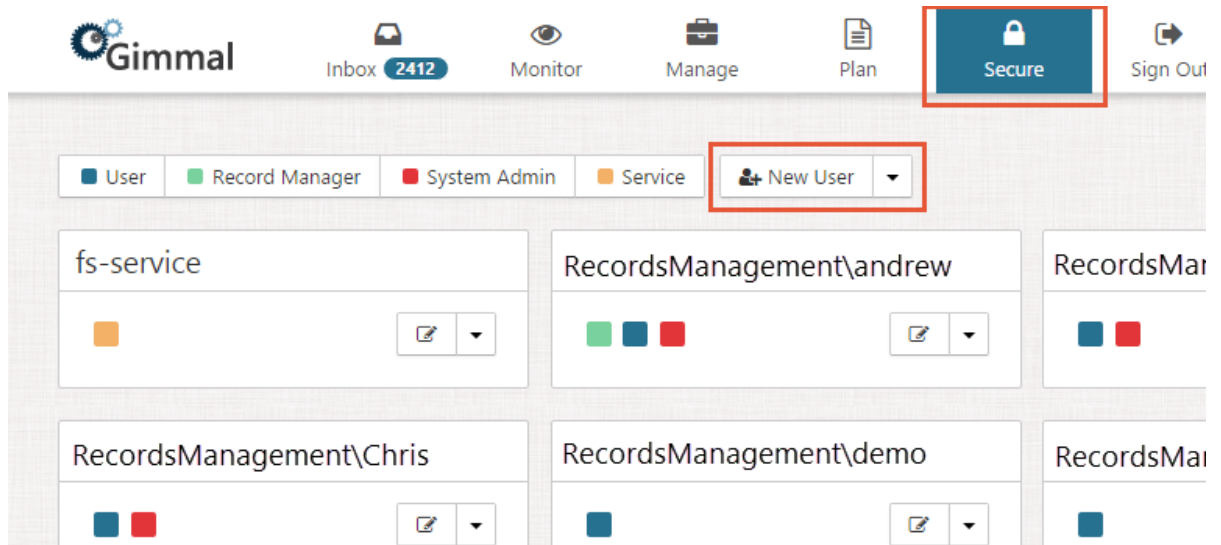
⁴³ <mailto:spocservice@gimmel.com>
⁴⁴ <mailto:fscservice@companyname.com>

6.13.16 Granting and Revoking User Access

6.13.16.1 Granting Access

To grant users access to the system, perform the following actions:

1. Select **Secure** from Main Menu
2. Select **New User**



The New Users and Groups window appears.


New Users and Groups
✕


Please enter a list of users or groups, each on a separate line

DOMAIN\User
 DOMAIN\Group


User
 Record Manager
 System Admin

3. Enter the names of each Login you are granting access (one per line)
4. Select check boxes for the type of access you want to grant
5. Select **Assign**

 In addition to performing the steps provided above, Gimmel Cloud customers must also email support@gimmel.com⁴⁵ and provide Gimmel their users' email address(es). Gimmel must add these email addresses to the Records Management permitted users list. This will enable Gimmel to authenticate users for the Gimmel Cloud environment.

 Use Windows Domain Users and/or Groups in the following format:

- DOMAIN\User
- DOMAIN\Group

 When giving a domain group access, you must ensure that the pre-Windows 2000 group name, also known as the SAMAccountName, is used or the group will not be granted access. This is typically the same as the Active Directory group name, but it does not have to be.

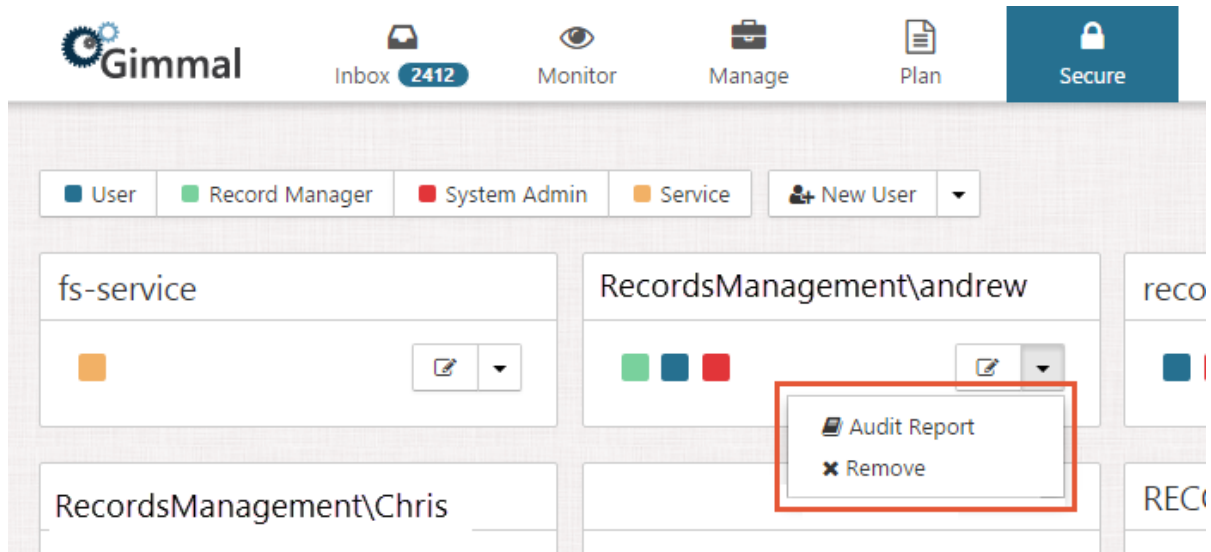
6.13.16.2 Revoking User Access

In order to remove users from the system, perform the following actions:

1. Select **Secure** from the Main Menu.
2. Select the drop-down for a specific user.

⁴⁵ <mailto:support@gimmel.com>

3. Select **Remove** from the menu and confirm.



6.13.17 Creating Local Groups

6.13.17.1 User Profile Properties

When a user is added to the system, either by attempting to sign in or by being manually added by an administrator, a User Profile is generated to represent the current user. Each user profile has the following properties that can be populated with data.

Property	Description	Claim
First Name	The user's first name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
Last Name	The user's last name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
Email	The user's Email Address (Used to send notification to the user)	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

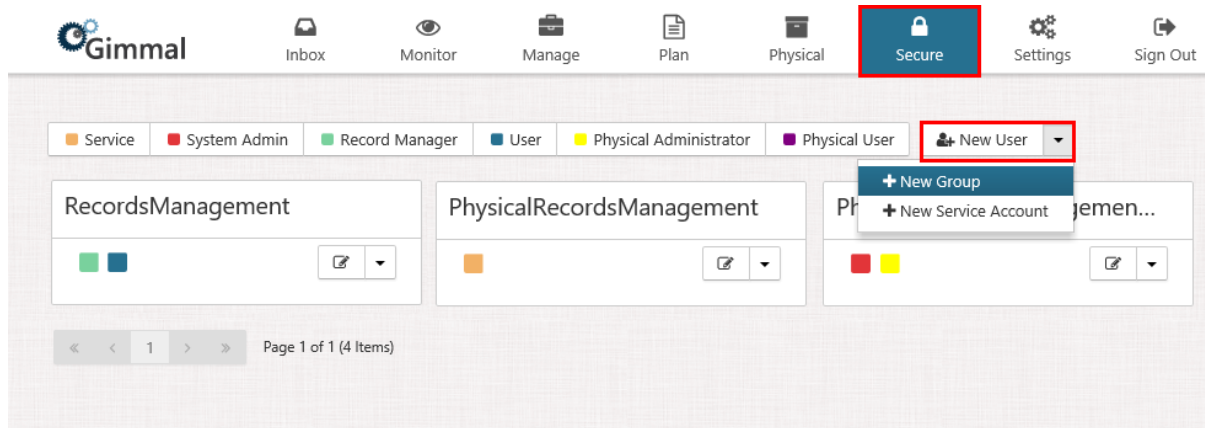
6.13.17.2 Local Groups

Version: Cloud, 4.2 and above

Local Groups give administrators the ability to create groups within the system instead of relying on the security providers (typically Active Directory) for groups. This is especially important for Gimmal Cloud users, as groups are not possible when using Azure Active Directory sync for single sign-on.

To create a Local Group, perform the following steps:

1. Select **Secure** from the Main Menu.
2. Select the New User drop-down list.
3. Select **New Group**.



4. Enter a name for the Local Group.
5. Select valid account types.
6. Enter a valid email address in order to send notifications to group members.
7. Select **Save**.

6.13.18 Changing the Master Account Password

Versions: 4.0 and above

To change the Master Account password, perform the following steps:

1. On the Records Management server, open a PowerShell window as the System Administrator.
2. At the prompt, enter Set-UserAccount and press Enter. The PowerShell credentials dialog opens.
3. Enter the username (administrator), the existing password, and press Enter. The PowerShell credentials dialog opens again.
4. Enter the same username (administrator), enter a new password, and Press Enter.

Further information about the Set-UserAccount cmdlet can be found on the [Manager Web page](#)(see page 440) of the PowerShell section.

6.14 Connector Deployment

6.14.1 [Box Connector](#)

6.14.2 [Documentum Connector](#)

6.14.3 [FileNet Connector](#)

6.14.4 [SharePoint Online Connector](#)

6.14.5 [SharePoint Server Connector](#)

6.14.6 [Universal File Share Connector](#)

6.14.7 [Box Connector](#)

The Box Connector enables you to securely manage document objects on a Box platform, as part of the Records Management system. It provides a way to manage all versions of a document that exist in the Box cloud. You will need a box enterprise account. Once you have acquired that, you will need to add two Box Applications to the account. (This is done on the Box Enterprise Admin Console).

If you are using the Gimmel Cloud for Records Management, the Box Connector is typically also hosted by the Gimmel cloud environment. However, you may also deploy the Box Connector on-premise. If you are running the Records Management Core on-premise, then you must also deploy the Box Connector on-premise

6.14.7.1 [Box Connector Planning and Requirements](#)

6.14.7.2 [Box Connector On-Premise Installation](#)

6.14.7.3 [Box Connector Configuration](#)

6.14.7.4 [Removing the On-Premise Box Connector](#)

6.14.7.5 [Configuring Box](#)

6.14.7.6 [Box Connector Jobs](#)

6.14.7.7 [Box Connector Planning and Requirements](#)

Planning

In order for the Box Connector to work properly, you will need the following:

- Box Business or higher
- Box Custom Subdomain
- Web browser compatible with the core Records Management platform

Box Governance

If your organization is using Box Governance, send a request to Box support to add the "GCM" and "Manage Legal Hold Policies" scopes to both your user and server applications. These are authorizations.

When using Box Governance, a Legal Hold is created called "Gimmel Hold" to manage record declaration. The connector creates the Hold upon the initial record declaration.

System Requirements for on-premise installations

Before you install the Records Management Box Connector on-premise, verify that your system meets or exceeds the following requirements.


Box Connector Server		
	Cores	Memory (MB)
Minimum	2	4096
Recommended	4	8192

- Windows Server 2012 or later (x64)

- Windows Server 2012 R2 or later (x64)
- Windows Server 2016.NET Framework 4.7.2
- 200 MB Disk Space for Software

Database Server


- SQL Server 2016 or greater
- 100 MB for Box Connector Database

 As a security best practice when using the .NET Framework, Gimmel recommends that you enable Transport Layer Security (TLS) 1.2, which provides communications security for client/server applications. To enable TLS 1.2, you must add the following Windows registry settings to the Records Management Core server(s) and the servers of any Records Management connectors you are using (if applicable), and then reboot your system.

- HKLM:\SOFTWARE\Microsoft\.NETFramework\v4.0.30319 "SchUseStrongCrypto"= dword:00000001
- HKLM:\SOFTWARE\Microsoft\.NETFramework\v4.0.30319 "SystemDefaultTlsVersions"= dword:00000001
- HKLM:\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319 "SchUseStrongCrypto"= dword:00000001
- HKLM:\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319 "SystemDefaultTlsVersions"= dword:00000001

Note that some operating systems require additional steps to enable TLS 1.2. For more information, see [Microsoft's TLS documentation](#)⁴⁶ To verify that your operating system supports TLS 1.2, read the [Support for TLS 1.2 section of Microsoft's documentation](#)⁴⁷.

6.14.7.8 Box Connector On-Premise Installation

 On-Premise installation of the Box Connector is not required if your connector is being hosted by Gimmel.

The Box Connector on-premise installation consists of a Web Application and a Service that relies on SQL Server Database for storing configuration data. After installation and configuration, it enables Gimmel Records Management to manage content stored in Box.

Box Connector Web

When the Box Connector Web is installed, a Web Application is created, which provides the interface for registering a Box app to a Box account as well as configuring the Box Connector to communicate with Gimmel Records Management.

Prior to installing the Box Connector Web, have access to the following information as it will be entered during installation. See **Configure Box** section for **Box User app**.

- Box User app Client ID
- Box User app Client Secret
- Box Url
- Box Enterprise ID

⁴⁶ <https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls#systemdefaulttlsversions>

⁴⁷ <https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls#support-for-tls-12>

1. Click **Install** to the right of the Box Connector Web option to begin the installation. The first screen that displays is the check for prerequisites. This screen validates that .NET Framework 4.7.2 is installed and the Current User is Local Administrator before allowing the installation to proceed.
2. Enter the path for the installation location. Leave the default, or to change it to the desired installation location.
3. Enter **IIS Settings** values.
4. Enter **App Registration Settings**. These values are found in the Configuration of the Box application.
5. Enter **Data Provider** values. This information determines the connection information that the Box Connector will use to connect to SQL Server.
6. Continue through the remaining screens to complete the installation for Box Connector Web.

Box Connector Service

When the Box Connector Service is installed, a Windows Service called Gimmel Box Service is created in Windows to perform the actions necessary to enable Gimmel Records Management to manage the lifecycle of records and information stored in Box. The Box Connector Service relies upon a SQL Server Database for storing configuration data.

1. Click **Install** to the right of the Box Connector Services option to begin the installation. The first screen that displays is the check for prerequisites. This screen validates that .NET Framework 4.7.2 is installed and the Current User is Local Administrator before allowing the installation to proceed.
2. Enter the path for the installation location. Leave the default or to change it to the desired installation location.
3. Enter **Service Settings** values. This is the user account that will be used to run the Windows Service.
4. Enter **Data Provider** values. This information determines the connection information that the Box Connector will use to connect to SQL Server.
5. Continue through the remaining screens to complete the installation for Box Connector Services.

6.14.7.9 Box Connector Configuration

The Gimmel Box Connector allows a Box admin or co-admin to configure settings via a web page. The following sections explain how to configure the Connector after it has been deployed for you.

Sign In to Box Connector

When you sign into Box Connector, you will be asked for your Box URL in order to authenticate you against your Box account. Only a user that belongs to the Box admin or co-admin role will be able to configure the connector. Box will ask for your consent to allow the connector to access your Box account.

After you have signed in to your Box account, then you will be redirected back to the connector. If your Box session expires, even if you have **NOT** closed your web browser, you will automatically be redirected to authenticate with Box and grant access to the Connector again.

Create a Service Account

Before continuing with configuration a Gimmel Records Management administrator will be required to create a service account for the Box Connector.

Records Management Configuration

After signing in to the connector, you should configure the Records Management Configuration section first.

- URL - This field is the URL for your Gimmel Records Management server. If you are hosting your own instance of the product, then you must ensure public inbound HTTPS traffic is allowed for it. Configuring your

network firewall or router is beyond the scope of normal Gimmal support. However, Gimmal support can provide your network or security operations team with the list of IP addresses the Connector uses. If your Gimmal Records Management tenant is hosted by Gimmal, then no additional configuration is required.

- **Username** - This is a service account created in your Records Management instance. If your Records Management is hosted by Gimmal, then your service account Username must include your tenant domain and will resemble an email address. For example, a Gimmal hosted Records Management service account should resemble the following: `box-svc@domain.com`⁴⁸. If you are hosting your own instance of Records Management, then your service account Username does not use a tenant domain. For example, it should resemble the following: `box-service`.
- **Password** - This field represents the password for the box service account created in your Records Management instance.

Box Configuration

This screen requires you to provide the Connector with the information obtained from the topic [Configuring Box](#) (see page 269).

It is critical to configure the User Authentication and Server Authentication sections correctly, or you may have to contact Gimmal Support.

This section has two fields that are global for your Connector:

- **URL:** This field is the URL to your Box account. Be sure to include your custom subdomain. For example, `https://acme.app.box.com`⁴⁹.
- **Enterprise ID:** This field is your Box enterprise ID.

⁴⁸ <mailto:box-svc@domain.com>

⁴⁹ <https://acme.app.box.com/>

Authentication Sections

There are two separate authentication types for each of the two apps configured in your Box Account. Each authentication type requires you to configure the appropriate OAuth 2.0 credentials required to communicate with your Box apps required above in the Configuring Box section

- User Authentication
- Server Authentication

User Authentication

This section is pre-populated by Gimmel during your Connector deployment. It contains the client ID and client secret for the app that allows a Box admin or co-admin to manage the connector. **WARNING:** misconfiguring this section could cause you to be locked out of your Connector and would require opening a Gimmel support ticket in order to have it reset.

- **Client ID:** This field is the client ID for the Box User App.
- **Client Secret:** This field is the client secret for the Box User App.

Server Authentication

This section requires you to know the RSA keypair you configured for the Box Server-to-Server app. If you do not know them, then you will need to regenerate the keypair since Box cannot retrieve them for you.

- **Client ID:** This field is the client ID for the Box Server-to-Server app.
- **Client Secret:** This field is the client secret for the Box Server-to-Server app.
- **Public Key ID:** This field is the value (do NOT include the quotation marks) of the publicKeyID element in the JSON config file for your RSA keypair.
- **Private Key:** This field is the value (do NOT include the quotation marks) of the privateKey element in the JSON config file for your RSA keypair.
- **Private Key Passphrase:** This field is the value (do NOT include the quotation marks) of the passphrase element in the JSON config file for your RSA keypair.
- **Box User Email:** This user must be a member of the admin or co-admin roles in your Box account and have the “Run new reports and access existing reports” permission. The Connector uses the Box API Admin Events stream to detect changes to files in your Box account.

6.14.7.10 Removing the On-Premise Box Connector

To uninstall the Box Connector, perform the following steps:

1. On the server that hosts the Box Connector, navigate to the Windows Control Panel and select **Uninstall a Program** from the Programs section.
2. On the “Uninstall or change a program screen”, locate the **Gimmel Box Connector** and double-click it. A dialog displays, asking you to confirm the uninstallation.
3. Click **Yes** to confirm the uninstallation. The User Account Control dialog displays, asking you to confirm the uninstallation.
4. Click **Yes** to begin the uninstallation process. When the uninstallation has completed, the Records Management Box Connector program will be removed from the Programs list
5. Repeat to uninstall the **Gimmel Box Connector Web**.
6. Verify that the **Gimmel Box Service** is no longer displayed in the Windows Services list.

6.14.7.11 Configuring Box

The following sections explain the required information, settings, and apps needed in your Box account before you can start using the Connector.

Box Enterprise ID

Your enterprise ID is available in several places throughout Box. You can easily find it within the [Admin Console under the Account & Billing](#)⁵⁰ page.

Custom Subdomain

You must configure your box account to use a custom subdomain. This enables the Gimmel Box Connector to uniquely identify requests to/from your Box account back to your Gimmel Box Connector subscription. For more details, please follow Box's instructions on their [Custom Setup for your Enterprise page](#)⁵¹.

- Sign in to your Box Account.
- Access your admin console.
- Navigate to the Custom Setup tab.
- Under the Custom Subdomain section, ensure you have entered a value and click **Save**.

Box App

You are required to create two Box **Custom Apps** in order for the connector to communicate with your Box account —both a Box User App and a Box Server-to-Server App. Please note that the majority of this information comes from Box's documentation. For more details beyond what is provided by Gimmel, please see Box's [Creating Your First Application](#)⁵² page.

Box User App

This is a standard OAuth 2.0 app in Box (which Box also refers to as *User Authentication*). For more details, please see Box's [Setup with OAuth 2.0 developer page](#)⁵³. This app allows you to manage the connector through a web browser.

1. Create a new **Custom App** Box app that uses the **User Authentication (OAuth 2.0)** authentication method.

⁵⁰ <https://app.box.com/master/settings/accountBilling>

⁵¹ <https://support.box.com/hc/en-us/articles/360043693574-Custom-Setup-for-your-Enterprise>

⁵² <https://support.box.com/hc/en-us/articles/4636617907731-Creating-Your-First-Application>

⁵³ <https://developer.box.com/guides/authentication/oauth2/oauth2-setup/>

Custom App ✕

Select an authentication method and enter a name for your app. You can change the name later in General Settings.

Authentication Method

Server Authentication (with JWT)

- Best for building integrations or apps with external collaborators - [Learn More](#)
- The app authenticates using a JSON Web Token. Requires a public/private key-pair for added security.

User Authentication (OAuth 2.0)

- Best for building mobile or web apps - [Learn More](#)
- Users must authenticate with their Box login.

Server Authentication (Client Credentials Grant)

- Best for scripting and back office integrations - [Learn More](#)
- The app authenticates using Client ID and Client Secret.

App Name

By clicking 'Create App', you agree to the terms of the [Box Developer Agreement](#) and the [Box Privacy Policy](#).

2. Configure the app:

- a. **Redirect URI** – This will be the URI of the server where the Box Connector will be installed. You will need to supply the URI by itself, the URI with **/sign-in** appended to the end, and the URI with **/signin-box** appended to the end. Below is an example of how that should look:

Gimmal Records Box Connector – User Authentication

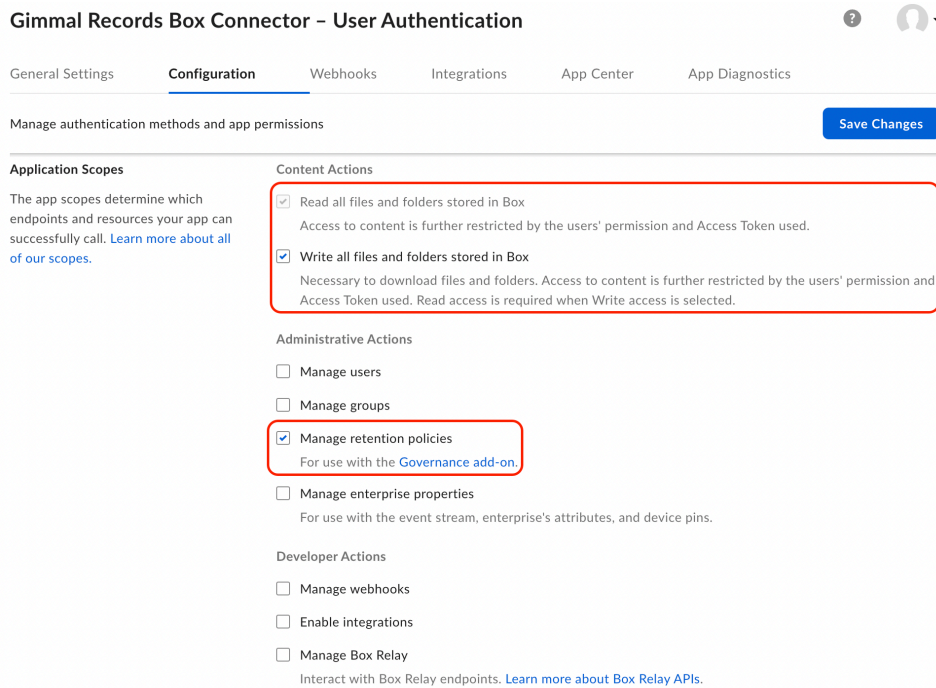
General Settings **Configuration** Webhooks Integrations

Manage authentication methods and app permissions

<p>OAuth 2.0 Redirect URI</p> <p>The redirect URI is the URL within your application that will receive OAuth 2.0 credentials.</p>	<p>Redirect URIs</p> <input type="text" value="https://records.gimmal.com"/> <input type="text" value="https://records.gimmal.com/sign-in"/> <input type="text" value="https://records.gimmal.com/signin-box"/> <p style="text-align: center;"><input type="button" value="Add a URI"/></p>
--	--

Application Scopes - Select all of the following:

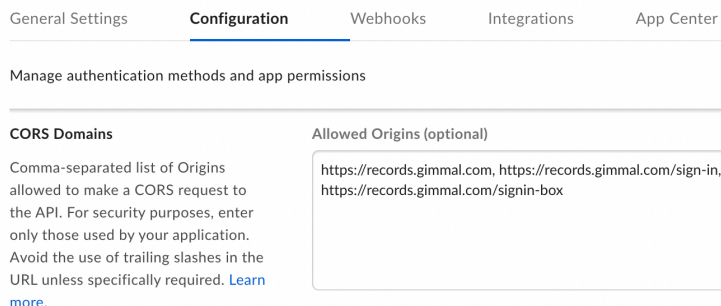
- i. Read all files and folders stored in Box.
- ii. Write all files and folders stored in Box.
- iii. If your organization is using Box Governance, also select Manage Retention Policies.



b. **CORS Domains** – This should be the same set of URIs supplied for the *Redirect URIs* section.

(Note: these URIs are **comma-separated**.)

Gimmel Records Box Connector – User Authentication



c. Click **Save Changes**.

Box Server-to-Server App

This is an OAuth 2.0 with JWT app in Box (which Box also refers to as *Server Authentication*). For more details, please see Box's [Setup with JWT developer page](#)⁵⁴. This app enables the connector to communicate with your Box account as a background service without any user interaction.

1. Create a new **Custom App** that uses the **Server Authentication (with JWT)** authentication method.

⁵⁴ <https://developer.box.com/guides/authentication/jwt/jwt-setup/>

Custom App ✕

Select an authentication method and enter a name for your app. You can change the name later in General Settings.

Authentication Method

- Server Authentication (with JWT)**
 - Best for building integrations or apps with external collaborators - [Learn More](#)
 - The app authenticates using a JSON Web Token. Requires a public/private key-pair for added security.
- User Authentication (OAuth 2.0)**
 - Best for building mobile or web apps - [Learn More](#)
 - Users must authenticate with their Box login.
- Server Authentication (Client Credentials Grant)**
 - Best for scripting and back office integrations - [Learn More](#)
 - The app authenticates using Client ID and Client Secret.

App Name

By clicking 'Create App', you agree to the terms of the [Box Developer Agreement](#) and the [Box Privacy Policy](#).

Cancel Create App

2. Configure the app:

a. **Application Access** is Enterprise.

Gimmel Records Box Connector – Server Auth

General Settings **Configuration** Webhooks Authorization App Diagnostics

Manage authentication methods and app permissions

App Access Level

The app access level determines which users and content your app may access. All Server-Server apps authenticate using an access token for the Service Account (Automation User) by default. [Read more about the Service Account.](#)

App Access Only

- ✓ Service Account and App Users only. [Learn more.](#)
- ✓ Access to content created by your app.
- ✗ Cannot manage Enterprise settings, content, or users.

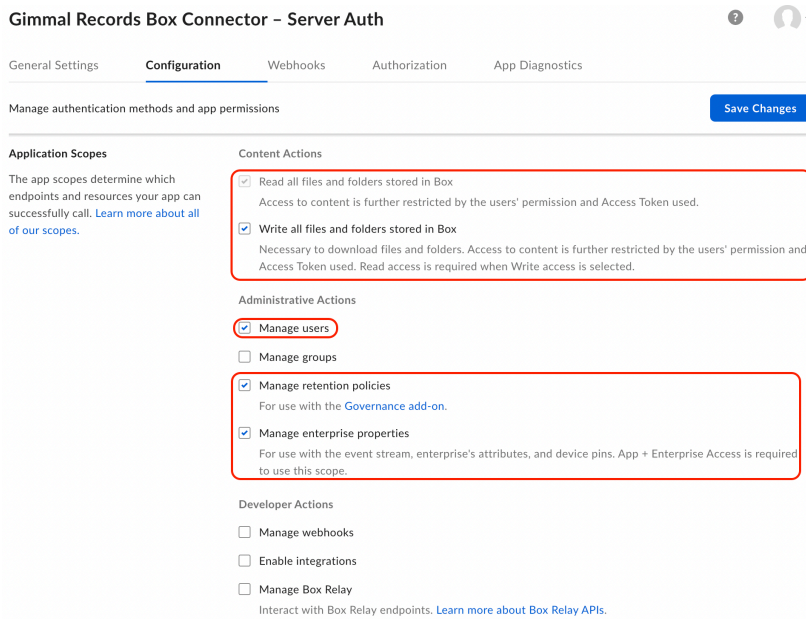
App + Enterprise Access

- ✓ All users
- ✓ Manage Enterprise settings, content, and users.
- ✗ Limited access to External Unmanaged Users.

b. **Application Scopes** - Select all of the following:

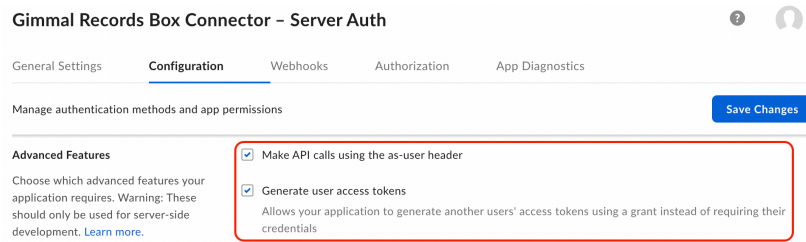
- i. Read all files and folders stored in Box.
- ii. Write all files and folders stored in Box.
- iii. Manage users.
- iv. Manage enterprise properties.
- v. If your organization is using Box Governance, also select Manage Retention Policies.

Administrator Guide – 273

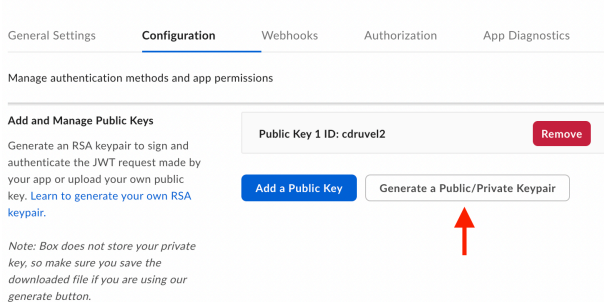


c. Advanced Features:

- i. *Make API calls using the as-user header* is enabled.
- ii. *Generate user access tokens* is enabled.



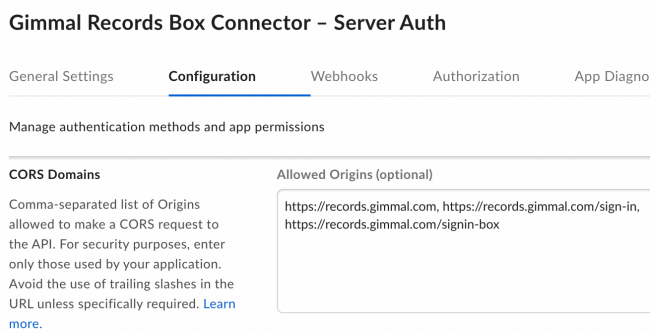
3. **Generate a Public/Private Keypair** by following the [instructions in Box's documentation](#)⁵⁵ (please note that this requires [Multi-factor Authentication](#)⁵⁶ be enabled on your Box account).



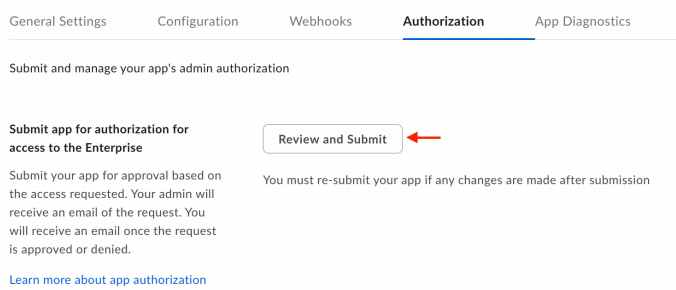
4. **CORS Domains** – This should be the same set of URIs used for the OAuth 2.0 User App that was configured earlier. (Note: these URIs are **comma-separated**.)

⁵⁵ <https://developer.box.com/docs/setting-up-a-jwt-app#section-step-2-generate-a-public-private-keypair>

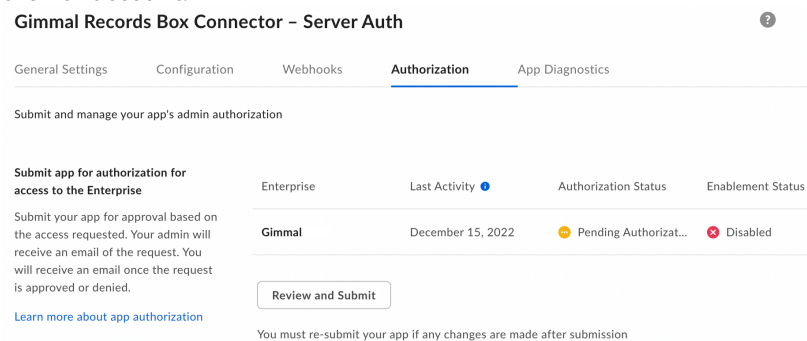
⁵⁶ <https://support.box.com/hc/en-us/articles/360043697154-Two-Factor-Authentication-Set-Up-for-Your-Account>



5. Click **Save Changes**.
6. Authorize and Approve the app. For full details, please see [Box's documentation for Authorizing Custom Applications in Sandbox and Production Environments](#)⁵⁷.
 - a. Under the **Authorize** tab, click the *Review and Submit* button.



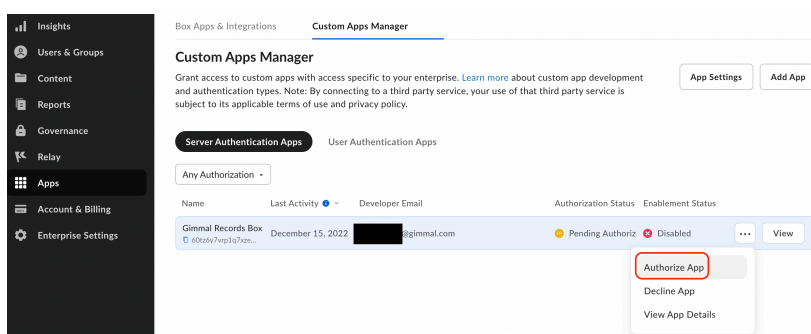
The authorization status will be *Pending Authorization*. This must be reviewed by an Administrator on the Box account.



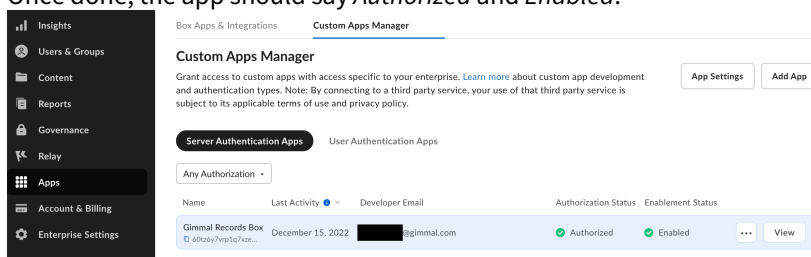
- b. Go to the [Admin Console](#)⁵⁸ on the Box account and navigate to the **Apps** tab.
- c. Click on **Custom Apps Manager** at the top of the page.
- d. The Server Authentication (with JWT) app you created should be present. Click the ellipsis (...) next to the app and select **Authorize App** from the drop down menu.

⁵⁷ <https://support.box.com/hc/en-us/articles/360043697014-Authorizing-Custom-Applications-in-Sandbox-and-Production-Environments>

⁵⁸ <https://app.box.com/master/settings/apps>



Once done, the app should say *Authorized* and *Enabled*.



6.14.7.12 Box Connector Jobs

The Connector has 3 jobs that are configurable. Each job can be run on a recurring schedule with an option to run it on-demand to override the schedule. Finally, each job can also be disabled to prevent it from running at all.

- Incremental Classification Job
- Retention Job
- Custom Classification Job

Incremental Classification Job

The incremental classification job is one of the most important jobs in the Connector. It is responsible for identifying any documents that have been created, updated, or deleted in your Box account since the last time the job ran. Once these documents are identified, the Connector sends the appropriate change notification (create, update, or delete) to the Records Management Service for the Record. The default interval for this job is 5 minutes.

Retention Job

The retention job asks the Records Management service for any action items that need to be processed by the Connector. The end result is the appropriate action is applied to the document inside your Box account. The default interval for this job is 5 minutes. The currently supported action items are:

- Lock item (declare record, permanent, and legal holds)
- Unlock item (undeclare record and legal holds)
- Dispose and delete



If using Box Governance, the retention job will use box legal hold functionality to lock items. Items on legal hold will not have a graphical indicator. There is no option to permanently delete an item on legal hold, only to “Restore”.

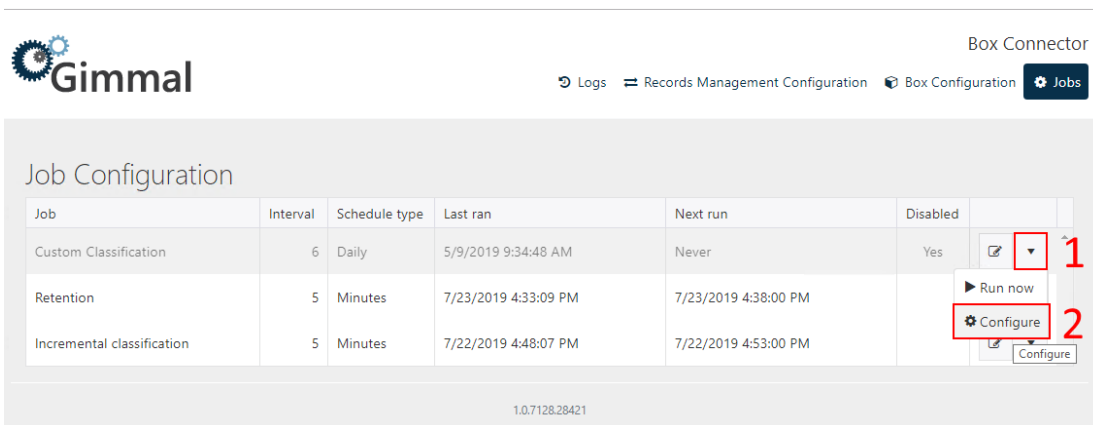


Naming box legal holds

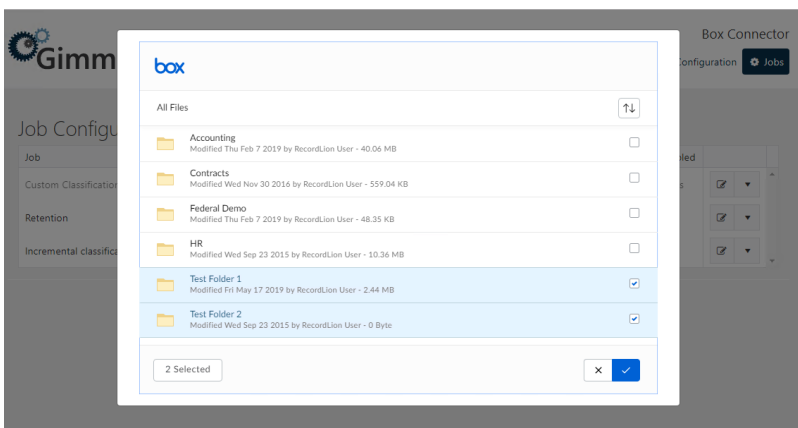
The default name for legal holds is “Gimmel Record”. If “Release” is selected for an active legal hold, the hold disappears, and all the documents are released from the hold. However, that name cannot be reused for new legal holds.

Custom Classification Job

Typically, this job would only be used once when the Connector is initially deployed in your Box account. It is primarily used recursively to classify all the existing documents within the selected root folders of your Box account. To configure the Custom Classification Job, first select Configure from the drop-down.



Once open, select the root folders in Box to crawl.




After selecting the desired folders, they will be crawled every time the job runs. Thus, we recommend leaving the job disabled until you are ready to run the job. This is because the incremental classification job is responsible for handling all document changes in your Box account but it will not pick up existing documents unless they are first modified.

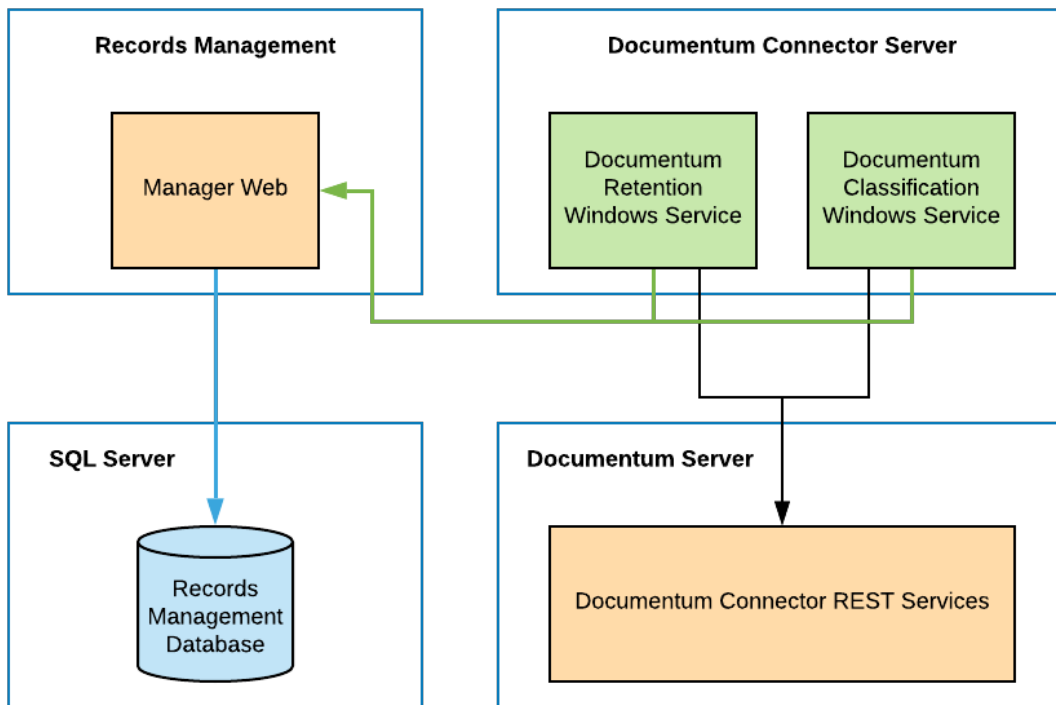
Once the custom classification job is enabled, you should run it on-demand by clicking the “Run now” option on the job action menu. Be sure to disable the job after it has completed successfully and updated the **Last Ran** column. For these reasons, the job is disabled by default and has a default interval of six days.

6.14.8 Documentum Connector

The Documentum Connector enables you to manage document objects in a Documentum DocBase, as part of the Records Management system. It provides a way to manage all versions of a document that exists in Documentum. This section described how to install and configure the Documentum Connector.

 The Documentum Connector does not support managing records that are part of the Documentum Physical Records solution.

6.14.8.1 Documentum Connector Architecture



[Documentum Connector Upgrade from 5.0 to 5.1](#)

[Documentum Connector System Requirements](#)

[Documentum Connector Installation](#)

[Applying Documentum Foundation Class Properties](#)

[Enable Documentum Audit Events](#)

[Documentum Connector Configuration](#)

[Uninstall Documentum Connector](#)

[Documentum Connector Upgrade 5.1 to 5.1.1](#)

[Documentum Services Installation](#)

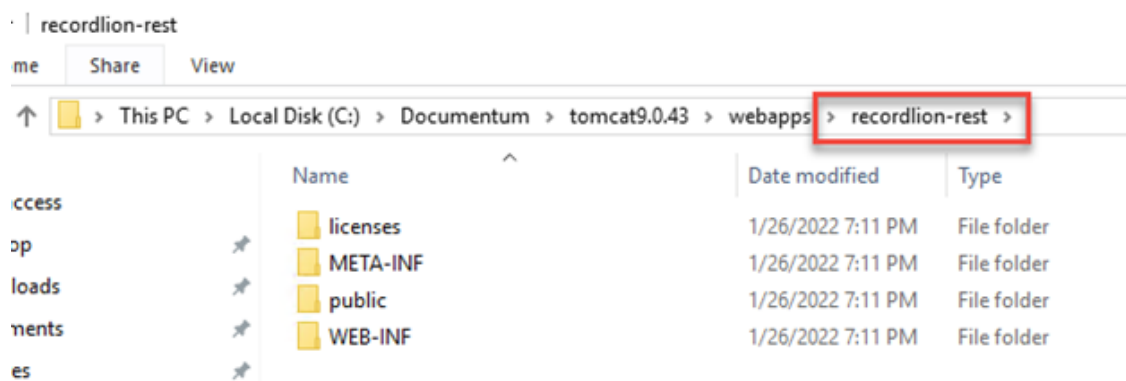
6.14.8.2 Documentum Connector Upgrade from 5.0 to 5.1

For the 5.1 release, major changes were made to the Documentum Connector as called out in the release notes. This topic will help you upgrade from 5.0 to 5.1.

Prerequisites

Before upgrading the Documentum Connector, complete the following prerequisite steps:

1. Make a copy of the **dfc.properties** file to use during the upgrade.
 - a. Remote Desktop into the Documentum web server with Administrative privileges.
 - b. Locate the **recordlion-rest** folder (see below)



- c. Copy the **dfc.properties** file (\recordlion-rest\WEB-INF\classes) to a location you can reference during the upgrade
2. Create a backup of the database (**DocumentumConnector** if it was not renamed during installation) for a backup plan.
3. Make a note of all repositories and docbases that are currently being managed by Gimmel Records.

- a. Remote Desktop into the Documentum web server with Administrative privileges.
- b. Launch the Documentum Connector.
- c. Make a note of all selected repositories and the docsbases selected.




Upgrade

Upgrade to version 5.1

⚠ Be sure you have completed the prerequisites before upgrading the Documentum Connector to 5.1,


1. Remote into the server as an Administrator on which the Documentum Connector is installed.
2. Stop the following Documentum Connector Services:
 - Gimmel Documentum Classification Service

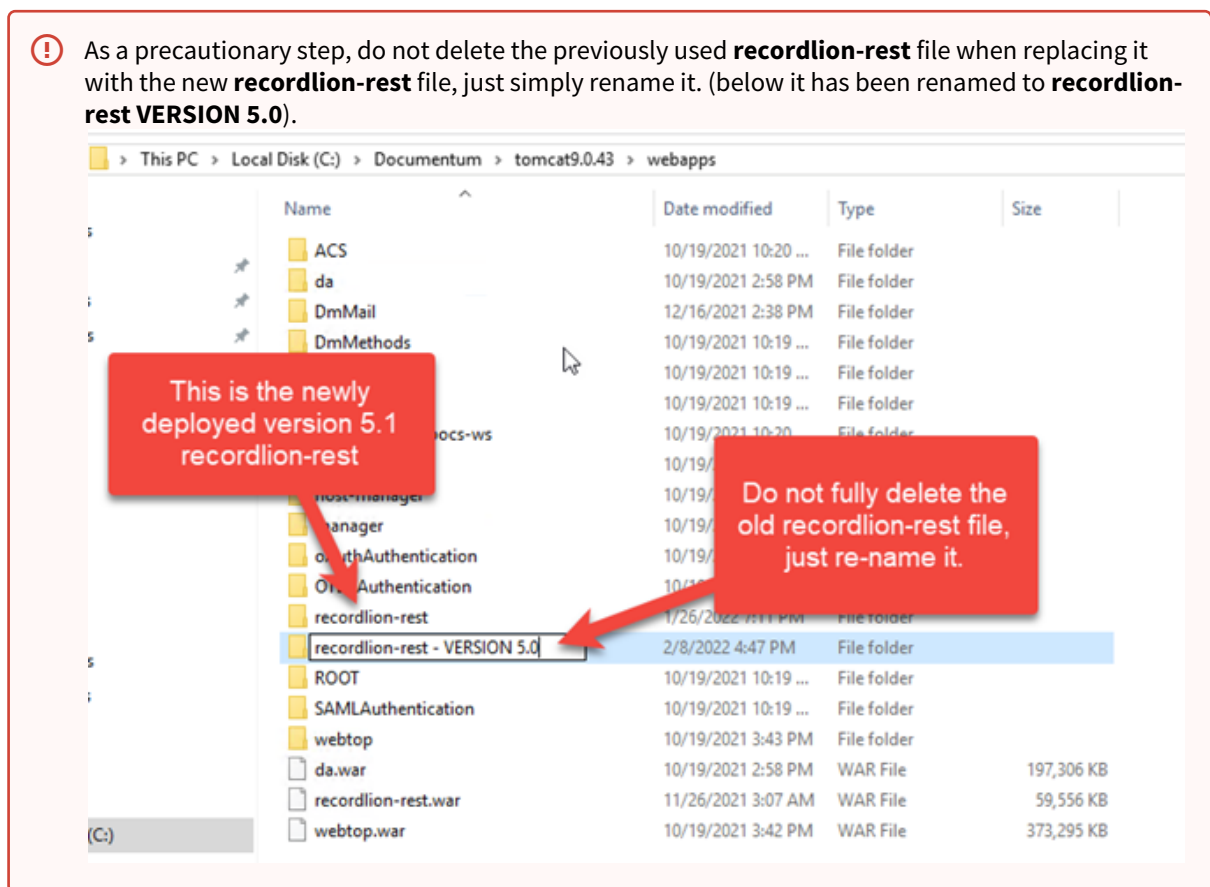
- Gimmel Documentum Retention Service
- Download the Documentum Connector ISOs from the [Gimmel Software Downloads](#)⁵⁹ site. If you do not have access to the software download site, please contact [Gimmel Support](#)⁶⁰
 - Using the provided ISO, install version 5.1 of the Documentum Connector by using [these steps](#)⁶¹.

 The documentation refers to 'Install' but since the Documentum Connector version 5.0 is currently still installed, the ISO will show the option to 'Upgrade' instead.

 Ensure that you run the installer as the Local Administrator.

- Deploy the **recordlion-rest** war file by following [these steps](#)⁶².

 As a precautionary step, do not delete the previously used **recordlion-rest** file when replacing it with the new **recordlion-rest** file, just simply rename it. (below it has been renamed to **recordlion-rest VERSION 5.0**).



- Update the **dfc.properties** file for the **recordlion-rest** by following [these steps](#)⁶³.


⁵⁹ <https://gimmel1.sharepoint.com/sites/EXT-Software/SitePages/Home.aspx>

⁶⁰ <https://support.gimmel.com>

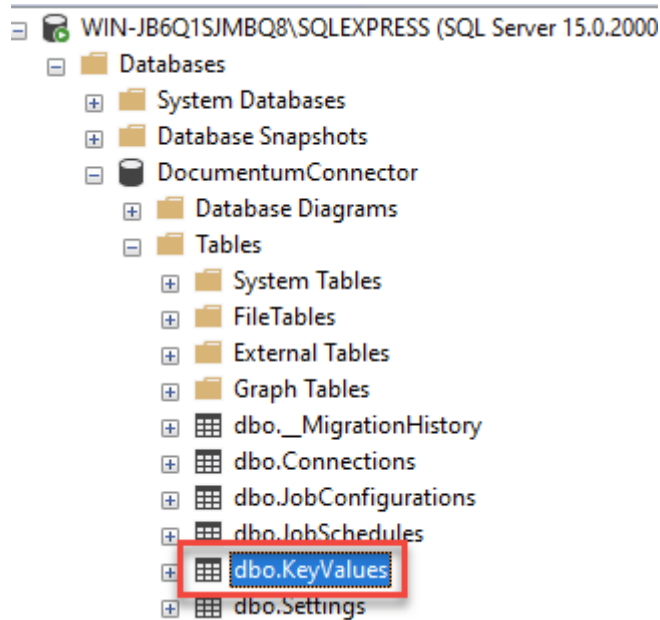
⁶¹ <https://docs.gimmel.com/rm/5.1/Server/documentum-connector-installation>

⁶² <https://docs.gimmel.com/rm/5.1/Server/documentum-services-installation>

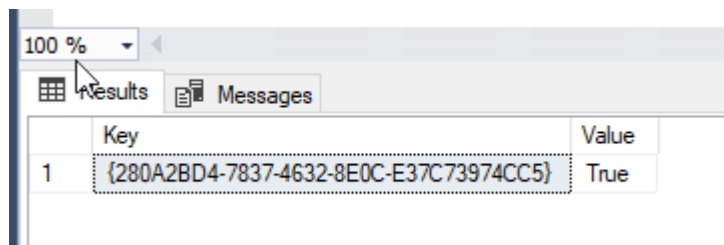
⁶³ <https://docs.gimmel.com/rm/5.1/Server/applying-documentum-foundation-class-properties>

 If you do not know where to find the dfc. properties, reference step 1 in the prerequisites.

7. Confirm the KeyValue tables have been added to the **DocumentumConnector** table
 - a. Expand the **DocumentumConnector** table in SQL Server Management Studio, then expand **Tables**



- b. Confirm that there is an initial entry in the **KeyValues** table that has a value of **True**

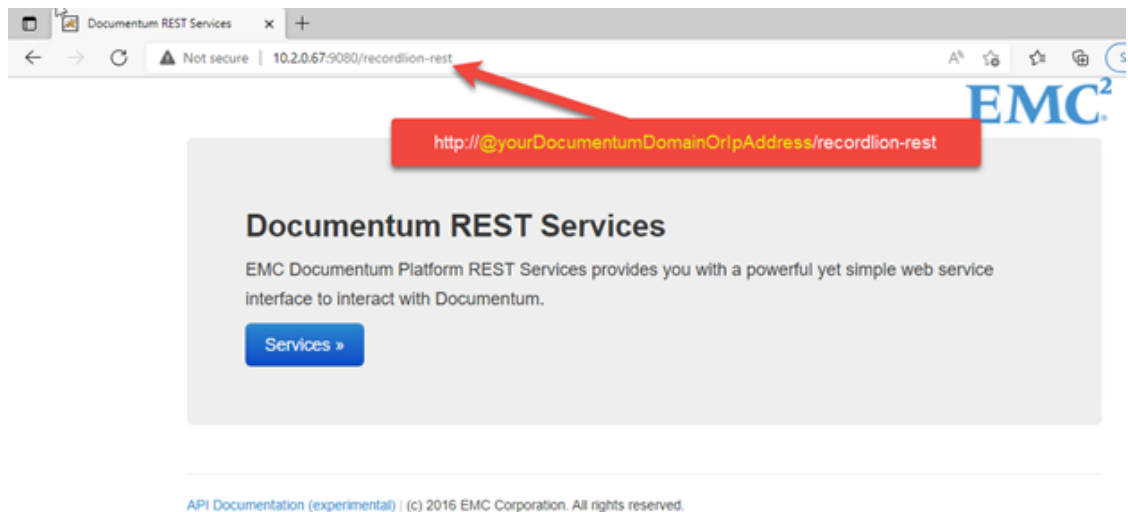


The screenshot shows the 'Results' grid in SQL Server Enterprise Manager. The grid has two columns: 'Key' and 'Value'. There is one row of data with the following values:

	Key	Value
1	{280A2BD4-7837-4632-8E0C-E37C73974CC5}	True

- c. Confirm **recordlion-rest** have been successfully deployed by opening a web browser to the URL <http://@yourDocumentumDomainOrIpAddress/recordlion-rest>⁶⁴-, and confirm that the web page below renders

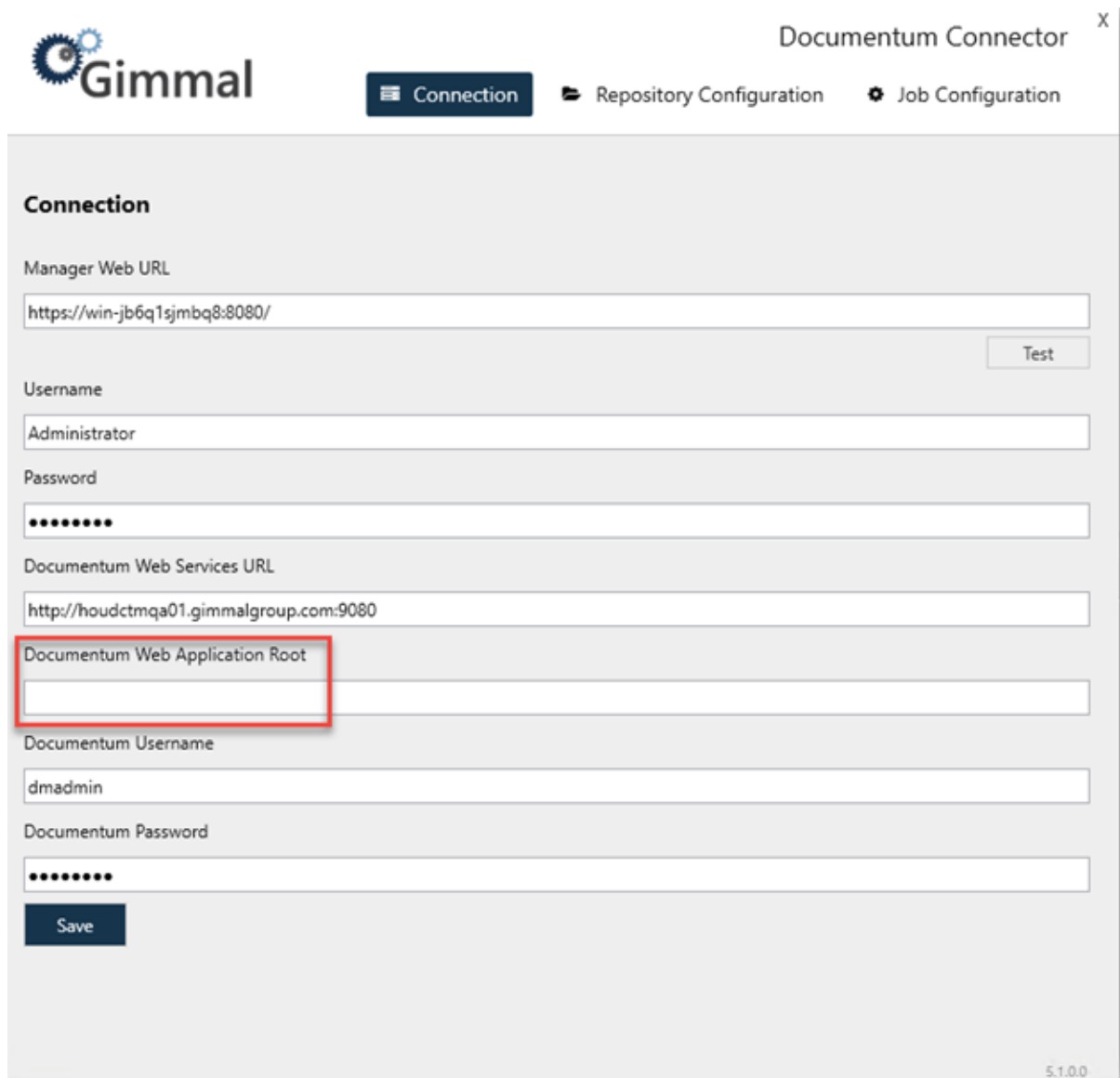
⁶⁴ <http://yourdocumentumdomainoripaddress/recordlion-rest>



Documentum Connector Initial Re-recordization

Version 5.1 of the Documentum Connector has a new feature where URIs will now be in a clickable format. However, if you are upgrading from version 5.0 to 5.1, you must go through the initial process of re-recordizing all the previous records to switch out the old URI format with the new clickable URI format. After completing these steps, you continue to proceed to use the connector as usual.

1. Remote into the machine where the Documentum Connector is installed.
2. Launch the Documentum Connector.
3. In the 'Connection' tab, all the information should already be populated with the previous connection information.



Gimmel Documentum Connector X

Connection Repository Configuration Job Configuration

Connection

Manager Web URL

Username

Password

Documentum Web Services URL

Documentum Web Application Root

Documentum Username

Documentum Password

5.1.0.0

4. Enter the 'Documentum Web Application Root' value, then click 'Save'. You will receive a confirmation if this is successful.

The screenshot shows the 'Documentum Connector' configuration window. The 'Connection' tab is selected. The fields are filled with the following values:

- Manager Web URL: `https://win-jb6q1sjmbq8:8080/`
- Username: `Administrator`
- Password: `*****`
- Documentum Web Services URL: `http://houdctmqa01.gimmelgroup.com:9080`
- Documentum Web Application Root: `webtop`
- Documentum Username: `dmadmin`
- Documentum Password: `*****`

A 'Save' button is located below the password field. A message box below the 'Save' button displays the text 'Save was successful'.

⚠ It is highly recommended to not adjust any of the Documentum information in the **Connection** tab after saving. Changing this setting can result in duplicate records being added.

- Restart the machine to clear any potential credential caches before proceeding to the next steps.
- Click the 'Repository Configuration' -> select the docbases and object types that you made note of in the prerequisites.


⚠ Only select repositories and docbases that were noted in the prerequisites at this time.



7. Start Documentum Connector Services:
 - Gimmel Documentum Classification Service
 - Gimmel Documentum Retention Service
8. Click **Job Configuration**, then click **Custom Classification Job**.

 Please do not set a **Next Run Time** for **Incremental Classification Job** or **Retention Job** before you run this essential step first.

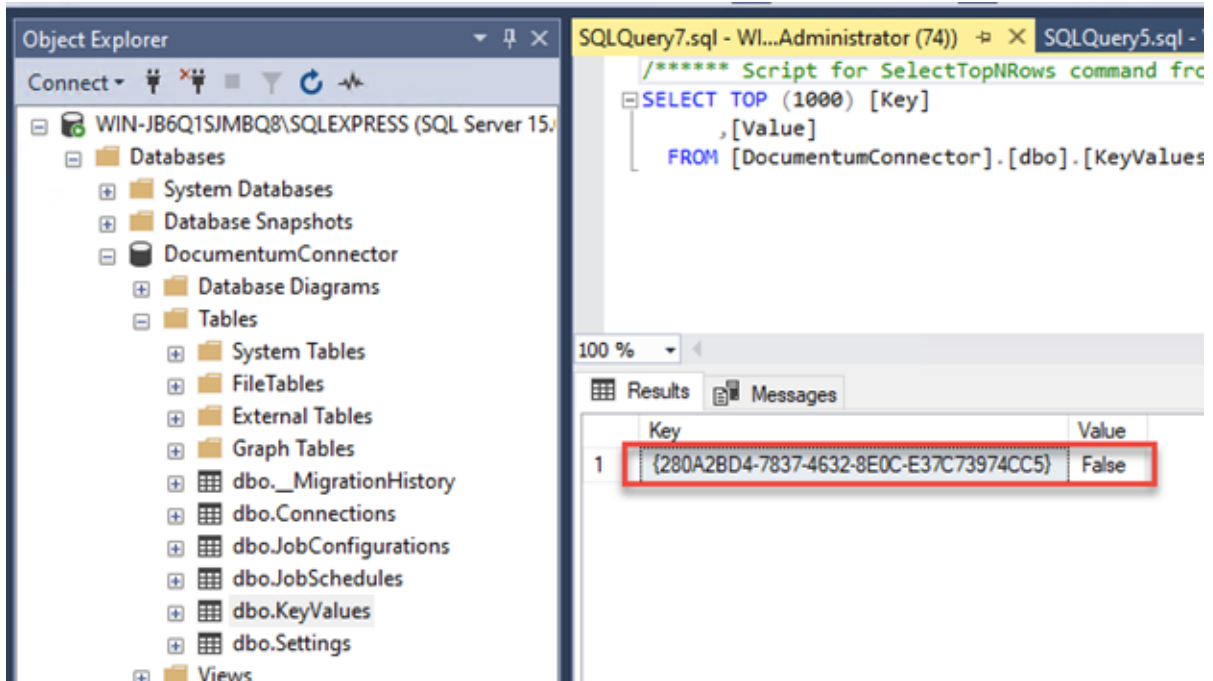
9. Select all the docbases and object types you wish to undergo the initial step of re-recordizing all the records to update to the new clickable URI format and press 'Run now'.

 This should again be the repositories and docbases noted in the prerequisites.



- Open SQL Server Management Studio and double-check that the **KeyValue** entry in the Documentum Connector database has been populated.

⚠ If you've made the mistake of forgetting a docbase or object type that you forgot to initially re-recordize to use the new URI format, just edit this entry to display **True** and follow steps 5-9 again.



- Upgrade to version 5.1 is complete. If you wish, you can go ahead and re-enable retention and incremental classification and proceed normally.


6.14.8.3 Documentum Connector System Requirements

Before you install the Records Management Documentum Connector, verify that your system meets or exceeds the following requirements.

- You are using the Gimmel Cloud, or you are using version 4.6.2 of the core Records Management software
- Documentum version 16.4 is installed and configured
- A TomCat web application server (v7.x or higher) to host the Documentum Services (REST Services) is installed and configured. Other application servers will likely work, however, Gimmel has only tested and only fully support TomCat.

Documentum Connector Server		
	Cores	Memory (MB)
Minimum	2	2048
Recommended	4	4096

- Windows Server 2012 or later (x64)
- Windows Server 2012 R2 or later (x64)
- .NET Framework 4.5** (x64)
- .NET Framework 3.5**
- 100 MB Disk Space for software

 As a security best practice when using the .NET Framework, Gimmel recommends that you enable Transport Layer Security (TLS) 1.2, which provides communications security for client/server applications. To enable TLS 1.2, you must add the following Windows registry settings to the Records Management Core server(s) and the servers of any Records Management connectors you are using (if applicable), and then reboot your system.

- HKLM:\SOFTWARE\Microsoft\.NETFramework\v4.0.30319 "SchUseStrongCrypto"= dword:00000001
- HKLM:\SOFTWARE\Microsoft\.NETFramework\v4.0.30319 "SystemDefaultTlsVersions"= dword:00000001
- HKLM:\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319 "SchUseStrongCrypto"= dword:00000001
- HKLM:\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319 "SystemDefaultTlsVersions"= dword:00000001

Note that some operating systems require additional steps to enable TLS 1.2. For more information, see [Microsoft's TLS documentation](https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls#systemdefaulttlsversions)⁶⁵ To verify that your operating system supports TLS 1.2, read the [Support for TLS 1.2 section of Microsoft's documentation](https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls#support-for-tls-12)⁶⁶.

Database Server

- SQL Server 2016 or greater
- 100 MB for Documentum Database

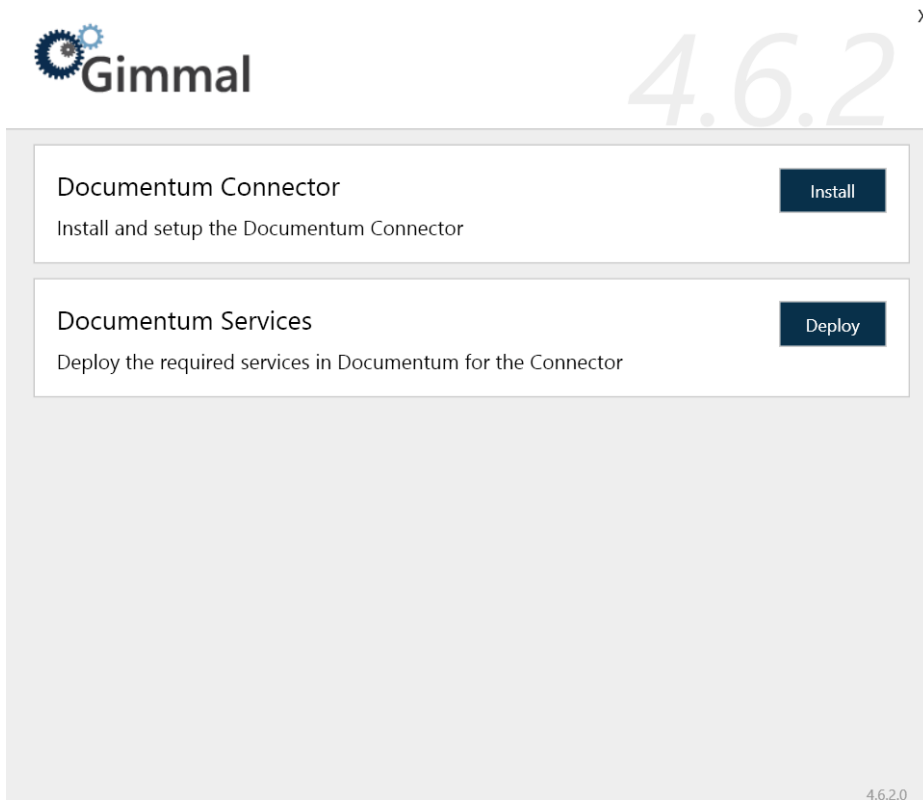
6.14.8.4 Documentum Connector Installation

 Ensure that you run the installer as the Local Administrator.

Upon launching the Documentum Connector installer, the following screen displays:

⁶⁵ <https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls#systemdefaulttlsversions>

⁶⁶ <https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls#support-for-tls-12>



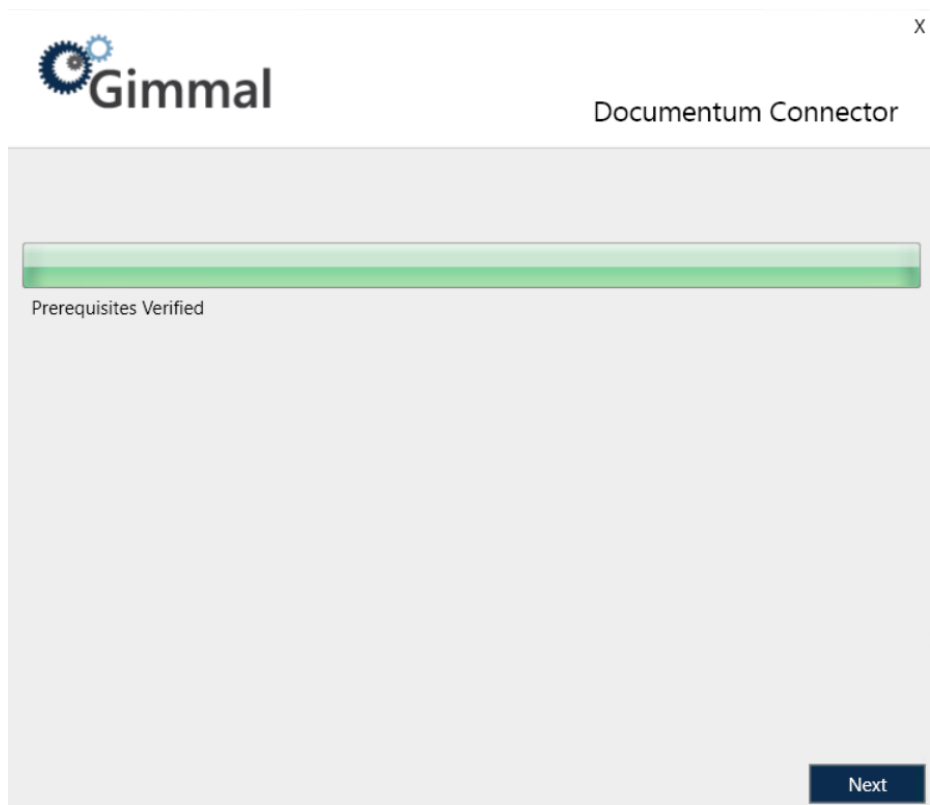
Installing the Documentum Connector

Before you install the Documentum Connector, verify the Connector [system requirements](#) (see page 288). This installation section also assumes that you have already installed the Records Management Core platform.

i When you install the Documentum Connector, a Configuration Utility and two Records Management related Windows Services are installed automatically as part of this process.

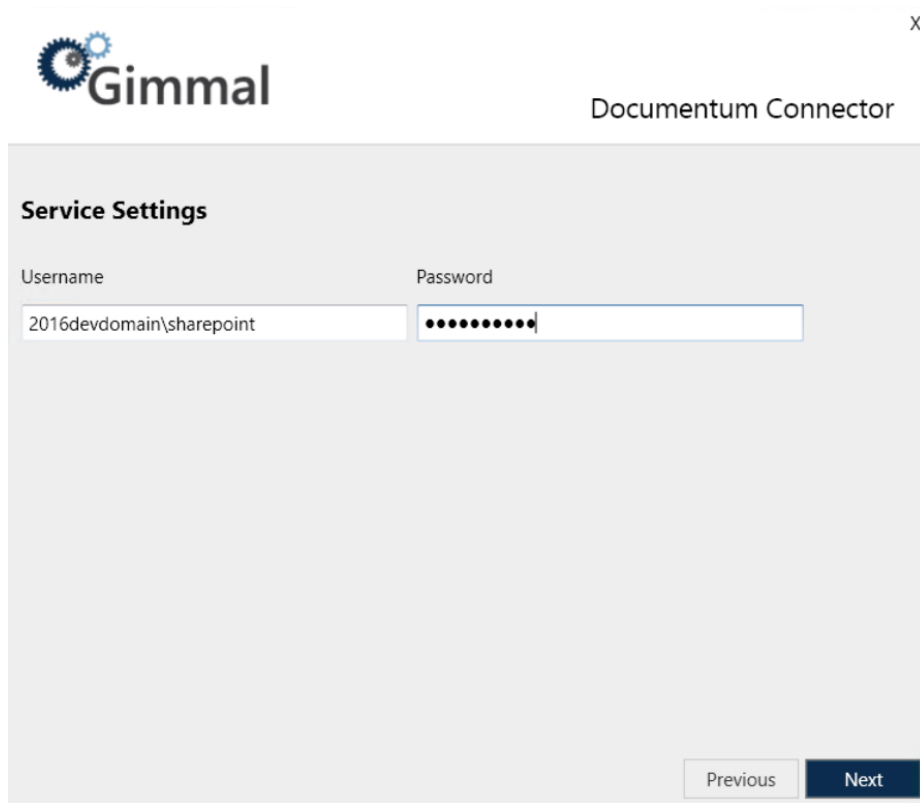
To install the Documentum Connector, perform the following steps:

1. From the Records Management splash screen, click the **Install Documentum Connector** link and the User Account Control window opens.
2. Click Yes to allow the installer to make changes to your computer. The Documentum Connector installation window opens.
3. On the Documentum Connector installation screen, click **Install** to the right of the Documentum Connector option. The first window that displays is the check for prerequisites. This window validates the following information before allowing the installation to proceed:
 - The current user is Local Administrator
 - You have installed .NET Framework 4.5
 - You have installed .NET Framework 3.5



4. Click **Next**. The installation location screen displays, which determines where the connector will be installed.
5. Leave the installation path as the default, or to change it, click the ... icon next to the installation location field, select the desired installation location, and then click **Next**.

 You must have at least 100MB of disk space available.




The screenshot shows a window titled "Documentum Connector" with the Gimmel logo in the top left corner. The window contains a "Service Settings" section with two input fields: "Username" and "Password". The "Username" field contains the text "2016devdomain\sharepoint" and the "Password" field contains ten black dots. At the bottom right of the dialog, there are two buttons: "Previous" and "Next".

6. Enter the following required information to specify which user account to use when you run the Windows Services:
 - **Username** (Ex. DOMAIN\Username)
 - **Password**The user account must be a domain account and must have the following file system permissions:
 - Read/Write: %Install path%\Logs

7. Click **Next**. The Database Settings screen displays.

The screenshot shows the 'Database Settings' window for the Documentum Connector. It includes the following fields and options:


- Database Server:** 2016SVR
- Database Name:** DocumentumConnector
- Automatically Create Database**
- Use SQL Authentication**
- Username:** (empty field)
- Password:** (empty field)
- Navigation:** Previous (disabled), Next (active)

 The "Database Server" and the "Database Name" settings, and the "Automatically Create Database" checkbox, will be populated automatically, however, you can change these settings. For information on the settings, see below.

8. Enter/select the following database settings to determine the connection information that will be used by the Documentum Connector to connect to SQL Server:
- **Database Server:** The name of the SQL Server Install (ex. SERVERNAME\InstanceName)
 - **Database Name:** The name of the actual SQL Server Database (The default name for the database is "DocumentumConnector", but you can change it here.)
 - **Automatically Create Database:** See description below
 - **Use SQL Authentication:** Specifies that the connection information should use SQL Authentication with the Username and Password indicated below
 - **Username:** The SQL Server username to use if SQL Authentication is specified
 - **Password:** The SQL Server password to use if SQL Authentication is specified

If **SQL Authentication** is not specified, the connection information will use Windows Authentication by specifying a trusted connection. This means that the Service account will be used to connect to SQL Server, and therefore, this account will need the following database permissions.

- **db_datareader**
- **db_datawriter**
- **GRANT EXECUTE** on all Stored Procedures
- **GRANT EXECUTE** on all Scalar User Defined Functions
- **GRANT SELECT** on all Table and Inline User Defined Functions


 If SQL Authentication is specified, the SQL user will also require the above permissions.

If **Automatically Create Database** is specified, the installation process will automatically attempt to create the database using the Database Server and Database Name indicated and will grant the appropriate database rights and permissions to the Service account. This option requires that the user running the installation has permission to create databases and manage security in the SQL Server instance indicated.

If **Automatically Create Database** is not specified, the installation will configure connection information but will not attempt to create the database. In this case, you will need to leverage the SQL script provided at the following location to manually create the database in the SQL Server instance indicated. You will also need to manually configure security as indicated above.

%Install Path%\Configuration\Sql\RecordLion.RecordsManager.Documentum.sql

9. Click **Next** to perform the final installation using the database settings you specified above. The progress bar indicates the state of the installation
10. When the application finishes installing, click **Next** to continue to the Finish screen. This screen indicates that everything installed successfully.

 If you experience any errors during the installation process, refer to the installer log in your Windows Temp folder (typically c:\temp).

11. Click **Finish** to return to the main Setup screen, which should now indicate that the Documentum Connector was installed successfully.
12. After you have finished installing the Documentum Connector, you must perform the following steps to run the newly installed Windows Services. (For information on how to run Windows Services, see Microsoft's online documentation.)
 - Open the Windows Services Manager.
 - In the Services window, verify that the **Gimmel Documentum Classification Service** and the **Gimmel Documentum Retention Services** are listed.
 - Start both services. When the services begin, the Status column will display "Running".
 - Using the SQL Server Management Studio, connect to the SQL database and navigate to the Databases folder. The database you applied settings to in step 9 is located under this Databases folder.
 - Verify that **DocumentumConnector** is listed.
 - Expand the nodes: **DocumentumConnector > Security > Users**, and then verify that the Service/User account that was created during the installation steps above is listed and has the correct permissions.
13. Continue the installation process by installing the Documentum Services component. For information, see [Installing Documentum Services](#)(see page 323).

6.14.8.5 Applying Documentum Foundation Class Properties

When you install Documentum Services, a WAR file is deployed as part of the process. This WAR file includes a **dfc.properties** file (located at WEB-INF/classes) that provides the configuration settings for the Documentum Foundation Classes runtime and it must be edited to provide the correct settings for the connector to be able to access the Documentum repository.

There are several ways to update the settings in this file:

1. **Include:** Use an #include statement to point to another dfc.properties file that is located outside of the web application on the local file system. This operation enables easy access to the settings and allows you to modularize your configuration settings. For example, you can add the following line as the only entry in the dfc.properties file that is included in the WAR file:

```
#include C:\Documentum\config\dfc.properties
```

2. **Copy:** Copy the contents of the Content Server's dfc.properties file (usu. located at **C:\Documentum\config\dfc.properties**) into your own **dfc.properties** file in the WEB-INF/classes folder.

Docbroker and Global Registry Properties

The **dfc.properties** file includes critical settings that are required for Documentum Services to reach a connection broker (also called a **Docbroker**) and connect to the Content Server. The following table summarizes the key DFC properties and a description of each:

Property	Value
dfc.docbroker.host[0]	The fully qualified hostname for the connection broker. You can add backup hosts by adding new properties and incrementing the index number within the brackets.
dfc.docbroker.port[0]	When you use a port for the connection broker other than the default of 1489, add a port key.
dfc.globalregistry.repository	The global registry repository name.
dfc.globalregistry.username	The username of the global registry user. The global registry user, who has the default username dm_bof_registry, must have read access only to the objects that are in the /System/Modules directory and the /System/NetworkLocations directory.
dfc.globalregistry.password	An encrypted password value for the global registry user.

For the global registry username and password, you have the following options:

1. Copy the username and encrypted password for the global registry user from the **dfc.properties** file on the global registry Content Server host, or
2. Select another global registry user and encrypt the password using the following command:

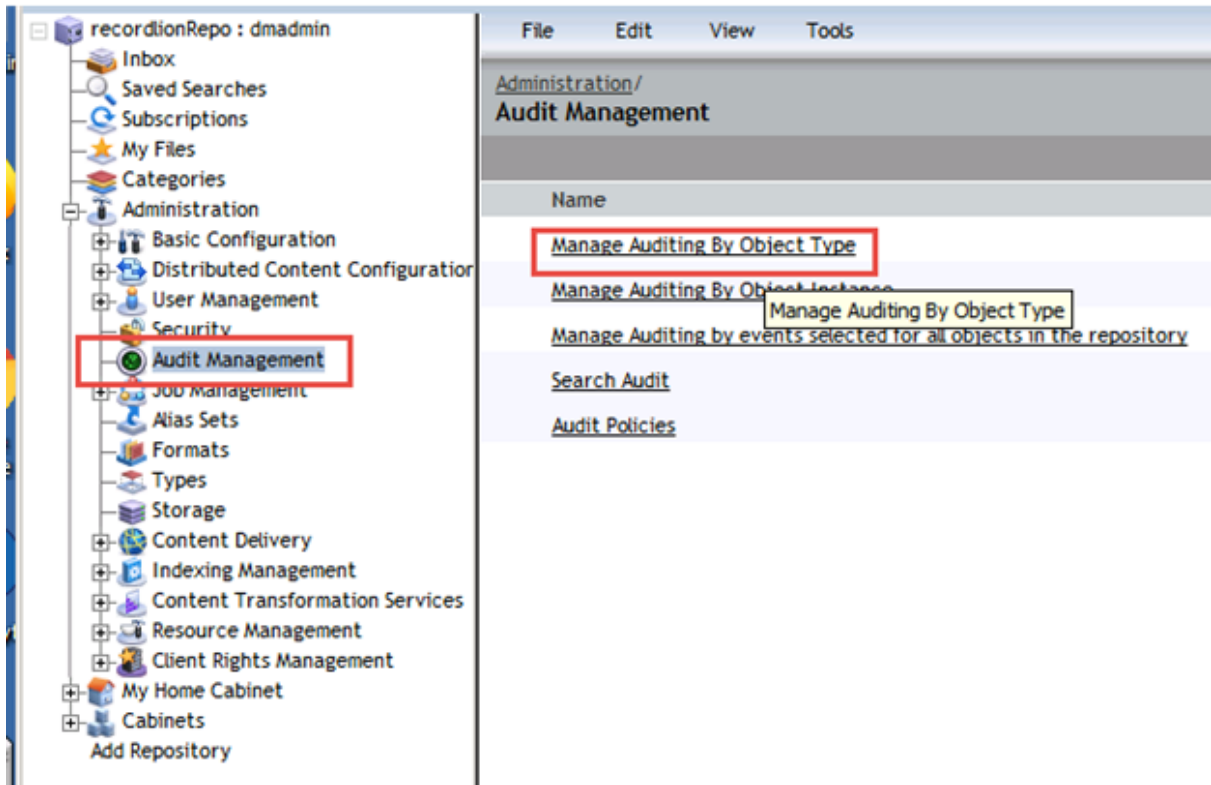
```
java -cp dfc.jar com.documentum.fc.tools.RegistryPasswordUtils <password_to_be_encrypted>
```

6.14.8.6 Enable Documentum Audit Events

Before you can perform incremental classification, you must ensure that certain Documentum Audit Trail event objects are present. Perform the following steps to enable these event objects:

1. Log into Documentum Administrator as a Superuser.
2. Select **Audit Management** from the left navigation pane.

3. Select **Manage Auditing by Object Type** on the Audit Management screen.



4. Select **dm_document** as the document type. **NOTE:** this **MUST be configured** at the dm_document level and NOT at the dm_sysobject level. While inheritance would result in audit events getting applied to dm_document, the connector requires an explicit definition of auditing for the dm_document.

Register Audit : dm_document

Application Code :

Lifecycle : [None Selected]

State :

Attributes : [None Selected]

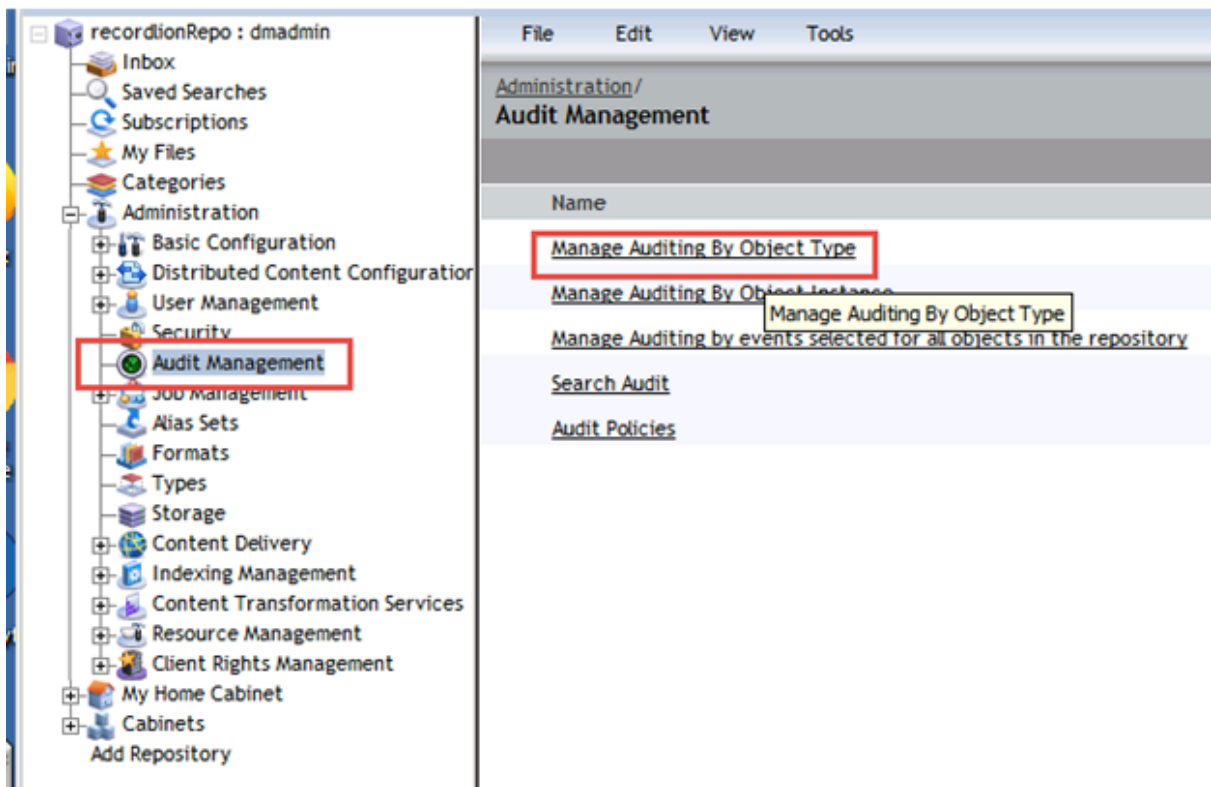
Has signature manifested

Include all subtypes

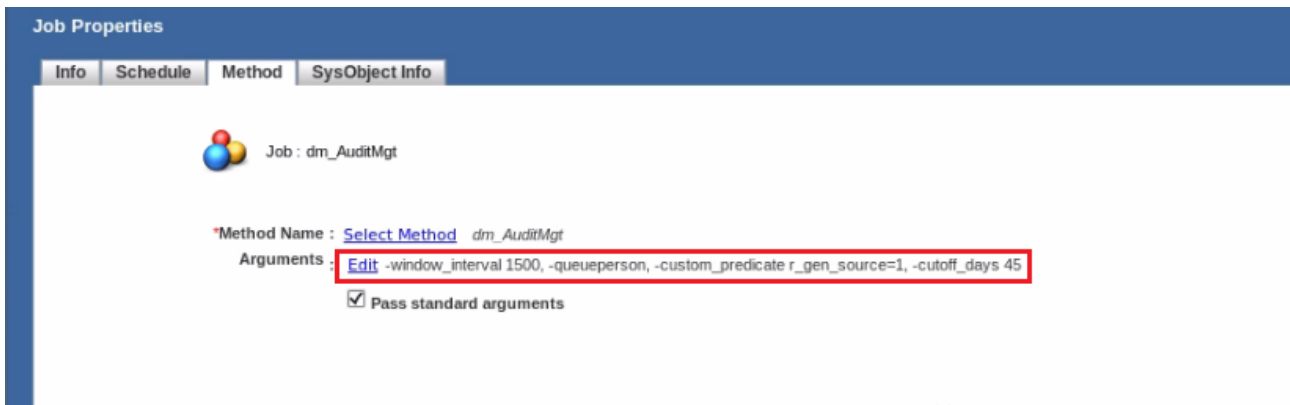
Authentication Required

Event Name

5. Click **Add** to add audited events. Ensure that the "Include all subtypes" option is checked.
6. Add the **dm_destroy** and **dm_prune** events for auditing.



7. Click **Save** to save the settings and close the dialog.
8. Select **Job Management** from the left navigation pane.
9. Select **Jobs > dm_AuditMgt** on the Jobs screen. Next select **Properties > Method tab > Edit** > set the cutoff_days value to 30 or higher.
10. Click **OK** to save, and then click **OK** to close the dialog.



6.14.8.7 Documentum Connector Configuration

The Documentum Connector Configuration component is a desktop application that is installed along with the Documentum Connector. The Configuration dialog provides three "tabs" that enable you to configure your Documentum connection settings, select your Documentum DocBases, view the available jobs in the connector, and schedule the job intervals.

The screenshot shows the 'Documentum Connector' application window with the 'Connection' tab selected. The window title is 'Documentum Connector' with a close button 'X'. The navigation menu includes 'Connection' (active), 'Global Configuration', and 'Job Configuration'. The main content area is titled 'Connection' and contains the following fields and buttons:

- Manager Web URL:** A text input field with a 'Test' button to its right.
- Username:** A text input field.
- Password:** A text input field.
- Documentum Web Services URL:** A text input field.
- Documentum Username:** A text input field.
- Documentum Password:** A text input field.
- Save:** A dark blue button at the bottom left.

Configuring the Documentum Connection Settings

The Connection tab enables you to enter the required credentials so you can access the Documentum server.



Before you begin these configuration steps, ensure that you have created the Manager Web account username and password.

To configure the Connection settings, perform these steps on the same machine where you are running the Records Management Documentum Connector.

1. Launch the Documentum Connector Configuration application. The application should be found in the installation location you specified during the Documentum Connector installation process, or you can launch the application from the Windows Start menu. The Documentum Connector window opens on the Connection page.

The screenshot shows the 'Documentum Connector' configuration window with the 'Connection' tab selected. The window title is 'Documentum Connector' with a close button 'x'. The navigation bar includes 'Connection' (active), 'Global Configuration', and 'Job Configuration'. The 'Connection' section contains the following fields:

- Manager Web URL: A text input field with a 'Test' button to its right.
- Username: A text input field.
- Password: A text input field.
- Documentum Web Services URL: A text input field.
- Documentum Username: A text input field.
- Documentum Password: A text input field.

A 'Save' button is located at the bottom left of the configuration area.

2. Enter the following information


- **Manager Web URL:** The URL to the Manager Web (i.e., where Records Management is installed)
- **Username:** The username of the Service Account created in Records Management
- **Password:** The password of the Service Account created in Records Management
- **Documentum Web Services URL:** The URL to your Documentum Services API (i.e., the base address of the Documentum Connector's web service API set; points to a deployed application running on a web application server in the Documentum environment.) Note that multiple Documentum Web Services instances are not supported.
- **Documentum Username:** The user ID of a Documentum superuser; ID is used to carry out all Connector activities within Documentum
- **Documentum Password:** The password of a Documentum superuser

3. Click **Save**

4. Continue to next section

Configuring the Documentum Global Configuration

The Global Configuration dialog enables you to select which DocBases (or repositories) you would like to classify and apply retention actions to. Different DocBases support different users, departments, operations, etc.

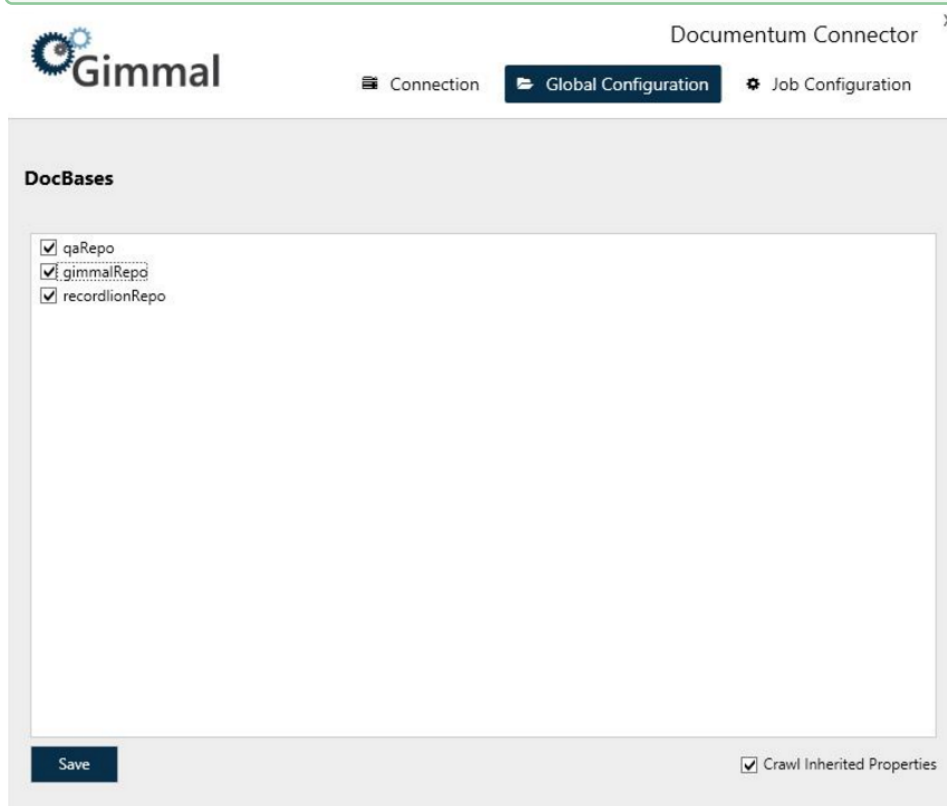
 To ensure that all documents are entered into Records Management accurately, the DocBases you select on this tab must initially be crawled by the Custom Classification job described in Configuring the Documentum Job Configuration.

⚠ One or more DocBases, containing content (documents), must exist. They must share a common superuser ID for the Records Management Documentum Connector to use when carrying out its tasks. (You configured this Documentum user on the Connection screen. You must configure a user first, or you will not be able to access the Global Configuration dialog.)

To select your DocBases, perform the following steps:

1. On the Documentum Connector Configuration dialog, click **Global Configuration**. The Global Configuration DocBases page opens, showing a list of available DocBases in Documentum.


✓ The Documentum Superuser ID being used requires at least read access to all DocBases within a DocBroker. Option to create a dedicated DocBroker to limit access to chosen DocBases is available.



2. Select the desired DocBase(s).
3. Indicate if you want the system to crawl the inherited properties for the selected DocBase(s) by clicking the **Crawl Inherited Properties*** checkbox in the lower right corner. (Defaults to checked.)
4. Click **Save**
5. Continue with the next section

Setting up the Documentum Job Configuration

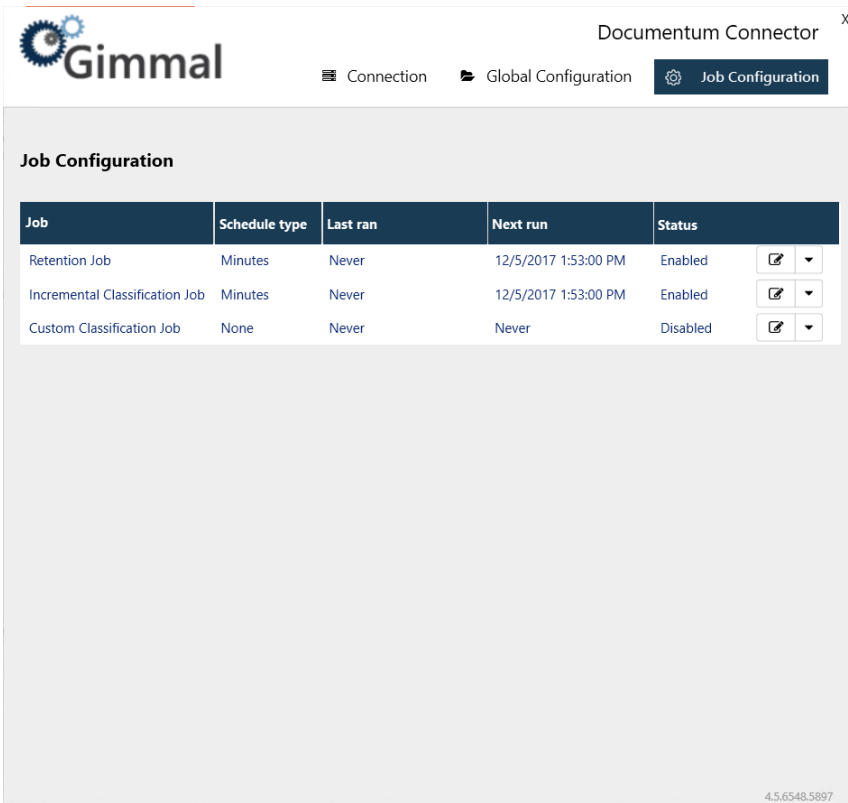
The Job Configuration dialog displays the retention and classification jobs included in the Documentum Connector, and enables you to either run the jobs immediately, or schedule how often you want the jobs to run. The jobs default to running every five minutes.


 The only way to schedule the retention and classification jobs is through the Connector configuration application.


To configure your retention and classification jobs, perform the following steps:

1. Ensure that you have started both the Documentum Retention Service and the Documentum Classification Service either manually or from the Windows Services dialog.
2. On the Documentum Connector Configuration screen, click Job Configuration. The **Job Configuration** dialog opens, showing a list of retention and classification jobs.
3. To run a job, perform either of the following steps:

To run a job immediately, click the drop-down arrow to the right of the desired job and then click Run Now. To schedule how often a job is to be run, click the Edit icon to the right of the desired job and set the Schedule Type (Minutes, Hourly, Daily), and the Time Interval; then click Save. The Next Run column will update with the time when the job is to be run next.

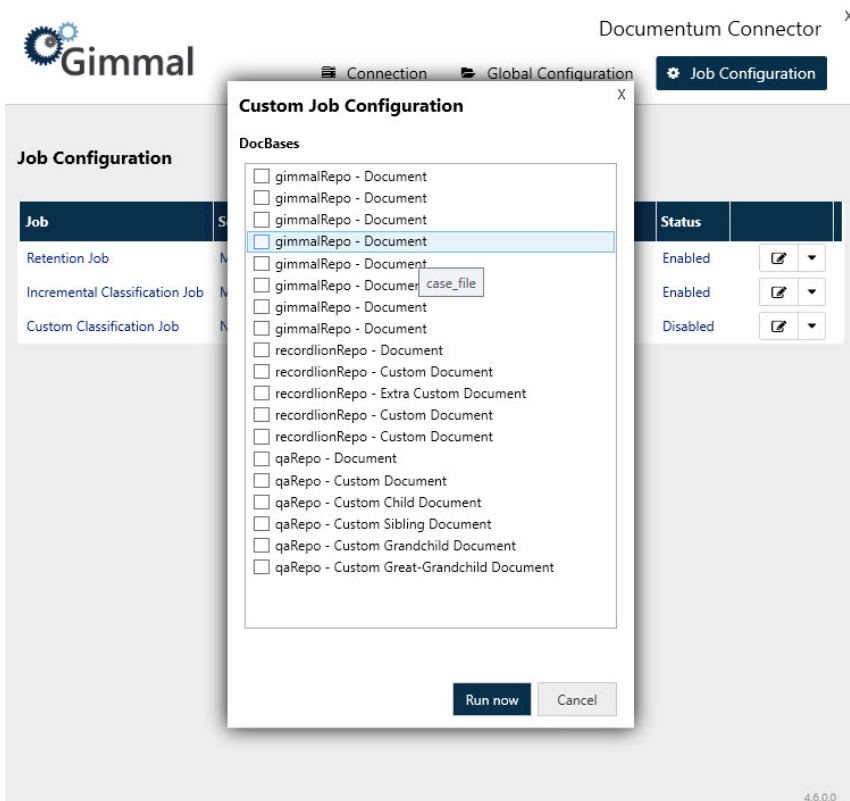


 There are three jobs listed on this screen. When initially setting up a system, the Custom Classification job must be run first (disable the Incremental Classification Job initially). Once the Custom Classification job has completed, disable it and reenale the Incremental Classification Job.

 The Custom Classification Job is essential when configuring a system for the first time.

To configure a job, click the Edit icon, which will open a separate dialog that displays all of the DocBases, along with Object Types that are available in that DocBase. This dialog enables you to select which Object Types under each DocBase you want to be included in the initial classification of a Documentum Server.

✔ The Object Types list on the Custom Job Configuration page may display duplicate Object Type names. This is because the list displays the "labelText" property of the Object Type, and multiple Object Types can have the same label. For convenience, if you hover your pointer over any Object Types in the list, a tooltip displays, showing the "name" field. This "name" field is unique for every item in the list and helps you differentiate between duplicate Object Type names.



The Documentum Connector Configuration application will show all descendants of **DM_document** except the following:


'dm_staged','dm_plugin','dm_java','dm_message_container','dm_email_message','dmc_search_template','dmc_jar','dm_esign_template','dm_format_preferences','dm_menu_system','dmc_tcf_activity_template','dmc_tcf_activity','dm_xml_config','dm_xml_style_sheet','dm_xml_zone','dm_xml_custom_code','dm_docset','dm_docset_run','dmc_preset_package'


In addition, the Configuration application does not support any Object Types found in these cabinets:


- 'Temp'
- 'System'
- 'Resources'
- 'Templates'

After you make your selections and activate the job, it will run immediately. Caution must be used when you perform this task if you are dealing with a large volume of documents. It could take many hours (possibly days) to

complete and can consume an exorbitant amount of resources from the Documentum and Records Management Documentum Connector servers.

 To ensure that all documents will be entered into Records Management accurately, ensure that the DocBases you selected on the Global Configuration tab are initially crawled by the Custom Classification job.

 By design when you enable a specific Object Type to be in scope for classification - that any child descendant of that Object Type will be automatically included for classification. Take for example if you had an Object Type named "dm_contract" and then created a child of that type called "dm_contract_legal". If you then selected "dm_contract" for classification - then automatically both "dm_contract" and "dm_contract_legal" types would automatically be included for classification because the parent Object Type was selected.

 After you select a DocBase/Object Type option and run a job, the selections do not persist. The next time you open the job scheduler, the check boxes will be unchecked.

Windows Services

When you install the Documentum Connector, two Windows Services are added during the installation process. These Services enable Records Management to manage the lifecycle of records and information stored in Documentum. A description of the Services follows:

Service Types	Description
Gimmel Documentum Classification Service	The Classification Service is responsible for discovering the content that exists in Documentum and notifying Records Management of its existence, including any updates and removals of this content.
Gimmel Documentum Retention Service	The Retention Service is responsible for executing the lifecycle actions, as indicated by Records Management at various points in time according to the specified File Plan.

6.14.8.8 Uninstall Documentum Connector

To uninstall the Documentum Connector, perform the following steps:

1. On the server that hosts the Documentum Connector, navigate to the Windows Control Panel and select **Uninstall a Program** from the Programs section.
2. On the "Uninstall or change a program screen", locate the **Gimmel Documentum Connector** and double-click it. (You can also select Gimmel Documentum Connector and then click the **Uninstall** option above the program list.) A dialog displays, asking you to confirm the uninstallation.
3. Click **Yes** to confirm the uninstallation. The User Account Control dialog displays, asking you to confirm the uninstallation.
4. Click **Yes** to begin the uninstallation process. When the uninstallation has completed, the Records Management Documentum Connector program will be removed from the Programs list.
5. Verify that the Gimmel Documentum Classification Service and the Gimmel Documentum Retention Service no longer display in the Windows Services list.

6.14.8.9 Documentum Connector Upgrade 5.1 to 5.1.1

Upgrade from version 5.1 to version 5.1.1

Prerequisites

- The current user is a Local Administrator
- You have installed .NET Framework 4.5
- You have installed .NET Framework 3.5
- Connector [system requirements](#)⁶⁷.
- 100 MB of space available for the Documentum Connector
- A service account with Read / Write permissions to %Install path%\Logs

Be sure you have completed the prerequisites before upgrading the Documentum Connector to 5.1.1

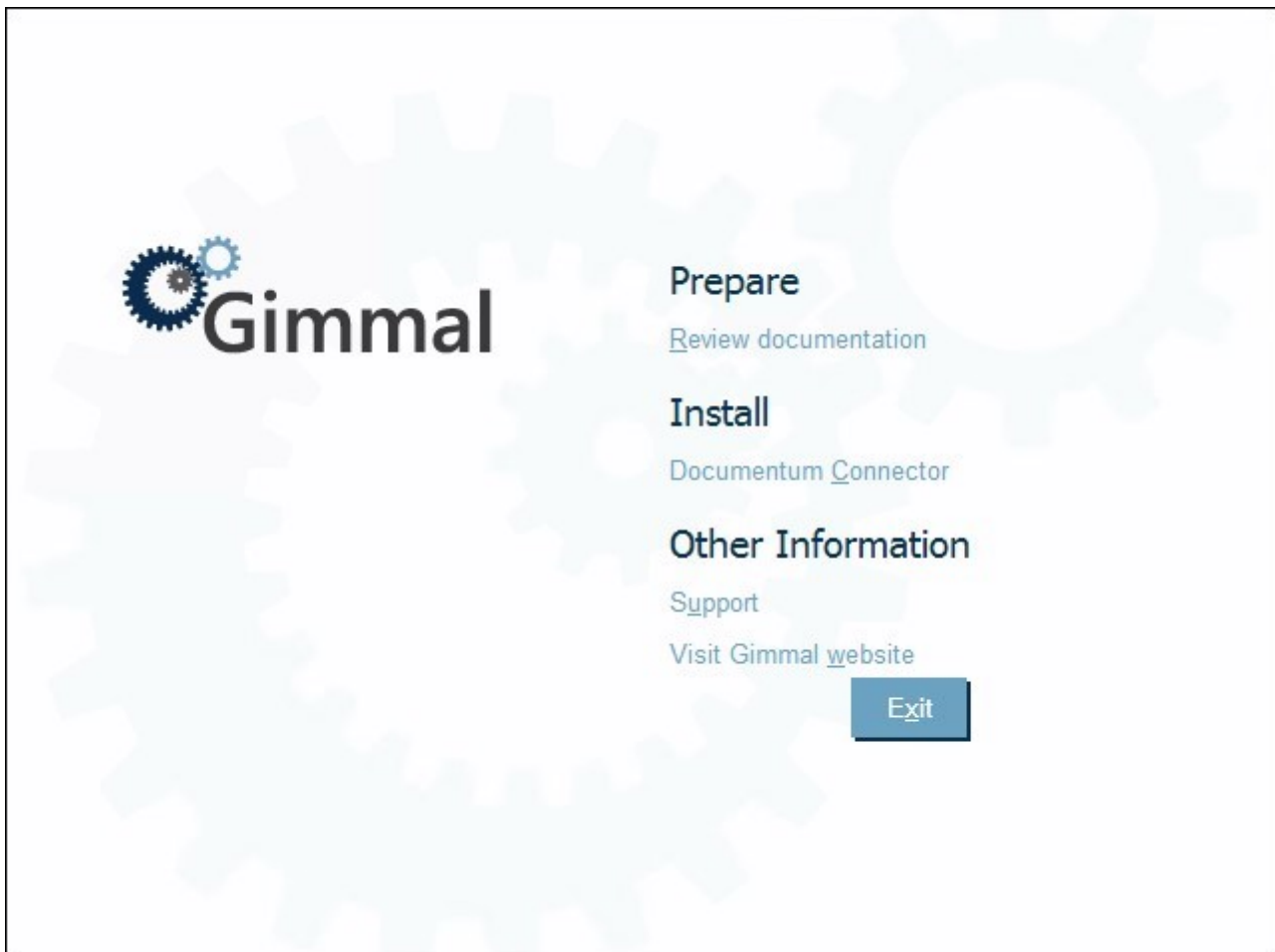
1. Remote into the server as an Administrator on which the Documentum Connector is installed.
2. Stop the following Documentum Connector Services:
 - Gimmel Documentum Classification Service
 - Gimmel Documentum Retention Service
3. Download the Documentum Connector ISO (Documentum Connector v5.1.1.iso) from the [Gimmel Software Downloads](#)⁶⁸ site. Once in the Gimmel Software downloads site click on the Documentum Connector link to see the Documentum Connector downloads. If you do not have access to the software download site, please contact [Gimmel Support](#)⁶⁹.

Upon launching the Documentum Connector installer as the Local Administrator, the following screen displays:

⁶⁷ <https://docs.gimmel.com/rm/5.1/Server/documentum-connector-system-requirements>

⁶⁸ <https://gimmel1.sharepoint.com/sites/EXT-Software/SitePages/Home.aspx>

⁶⁹ <https://support.gimmel.com>



Upgrading the Documentum Connector

Before you upgrade the Documentum Connector, verify the Connector [system requirements](#)⁷⁰. This upgrade section also assumes that you have already installed the Records Management Core platform.

To upgrade the Documentum Connector, perform the following steps:

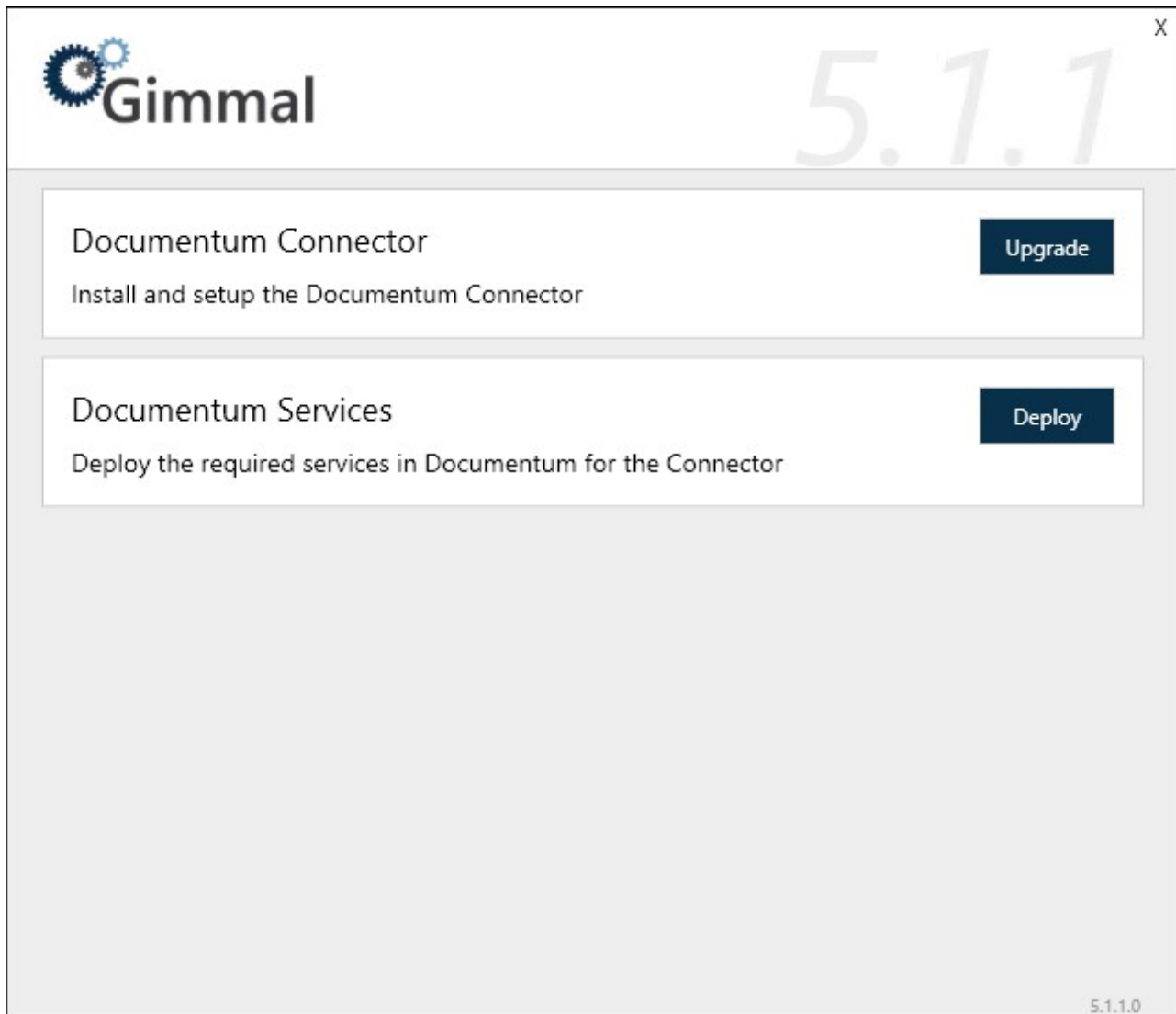
4. From the Records Management splash screen, click the

Install Documentum Connector link, and the User Account Control window opens.

5. On the Documentum Connector installation screen, click

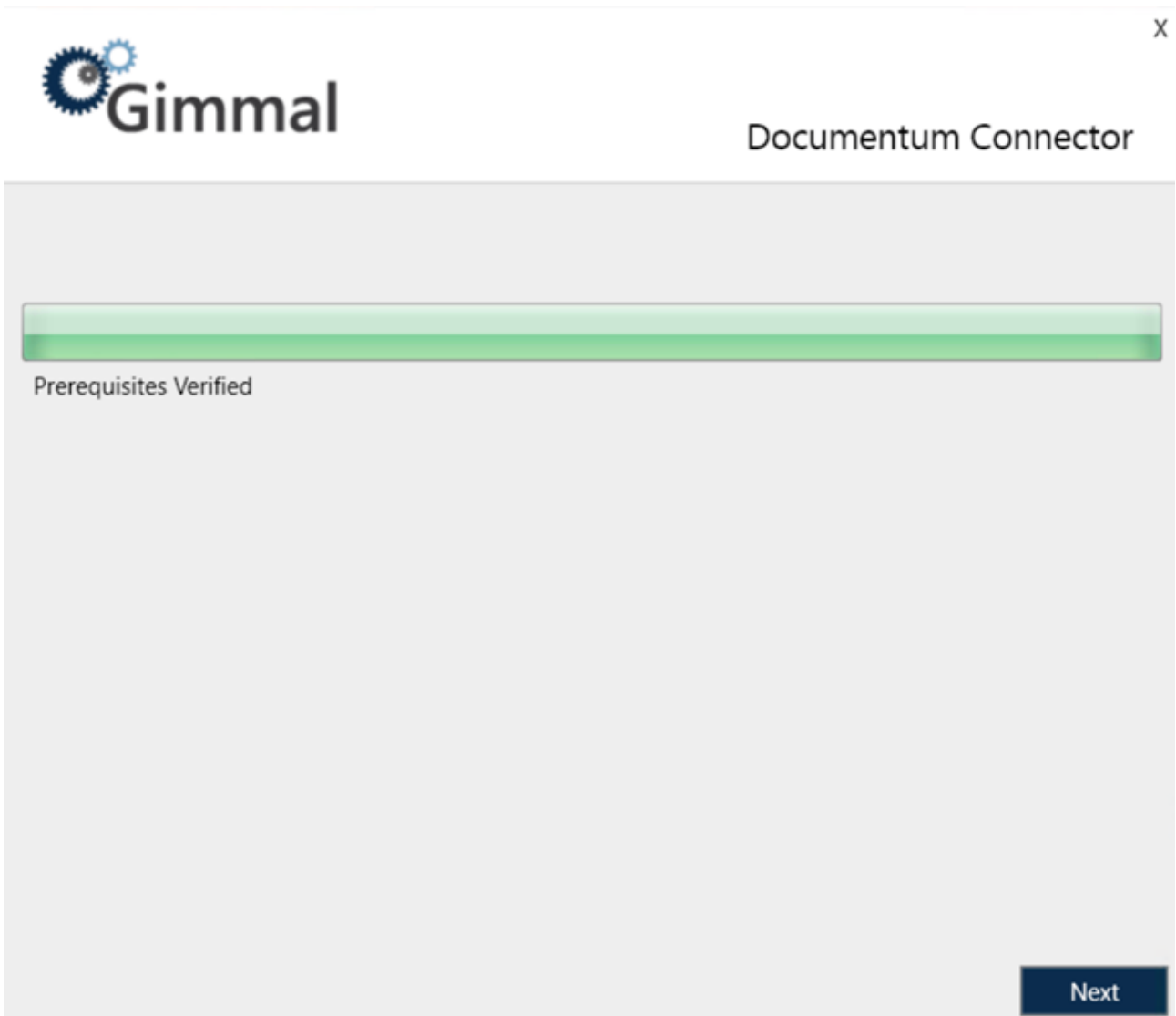
Upgrade to the right of the Documentum Connector option. The first window that displays is the check for prerequisites.

⁷⁰ <https://docs.gimmel.com/rm/5.1/Server/documentum-connector-system-requirements>



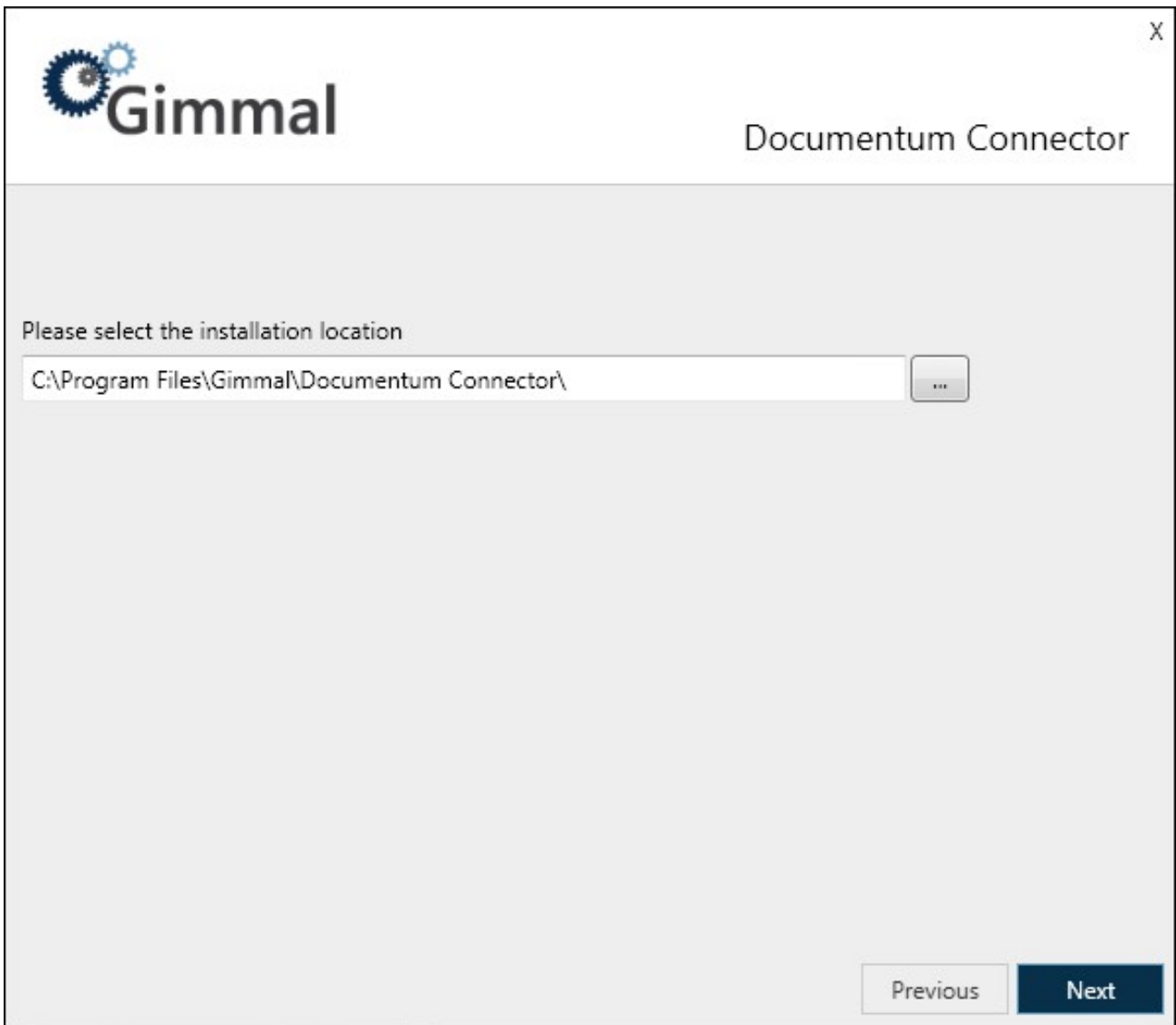
This window validates the following information before allowing the installation to proceed:

- The current user is a Local Administrator
- You have installed .NET Framework 4.5
- You have installed .NET Framework 3.5

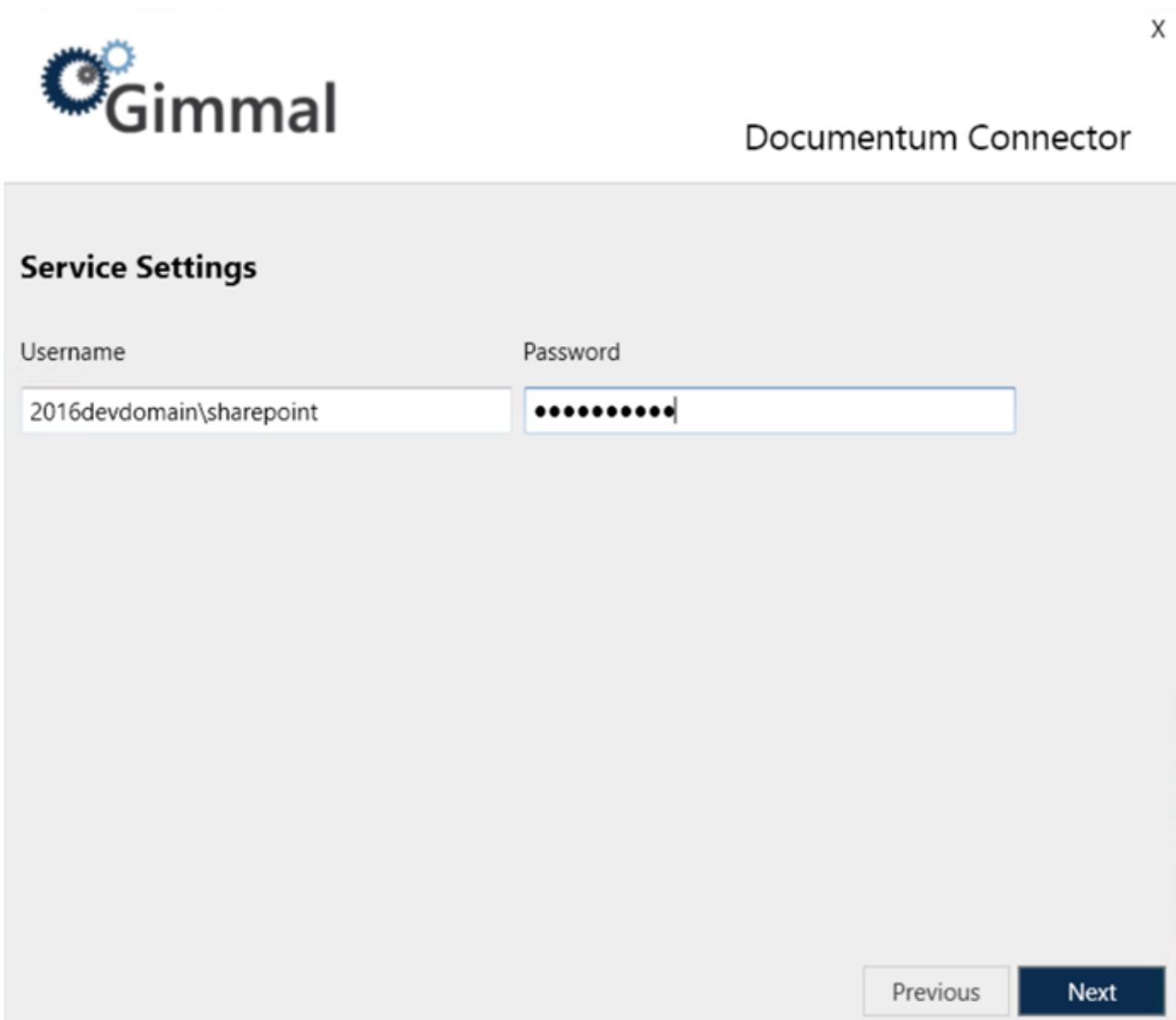


6. Click **Next**. The installation location screen is displayed. This determines where the connector will be installed.

7. Leave the installation path as the default, or to change it, click the ... icon next to the installation location field, select the desired installation location, and then click **Next**.



You must have at least 100MB of disk space available.



The screenshot shows a window titled "Gimmal Documentum Connector" with a close button (X) in the top right corner. The main content area is titled "Service Settings" and contains two input fields: "Username" and "Password". The "Username" field contains the text "2016devdomain\sharepoint". The "Password" field contains a series of black dots, indicating a masked password. At the bottom right of the form, there are two buttons: "Previous" and "Next". The "Next" button is highlighted in a dark blue color.

8. Enter the following required information to specify which user account to use when you run the Windows Services:

- o **Username** (Ex. DOMAIN\Username)
- o **Password**

The user account must be a domain account and must have the following file system permissions:

- o Read/Write: %Install path%\Logs

9. Click **Next**. The Database Settings screen displays.

Gimmel Documentum Connector

Database Settings

Database Server: SSDJTWIN2016 Database Name: DocumentumConnector

Automatically Upgrade Database Use SQL Authentication

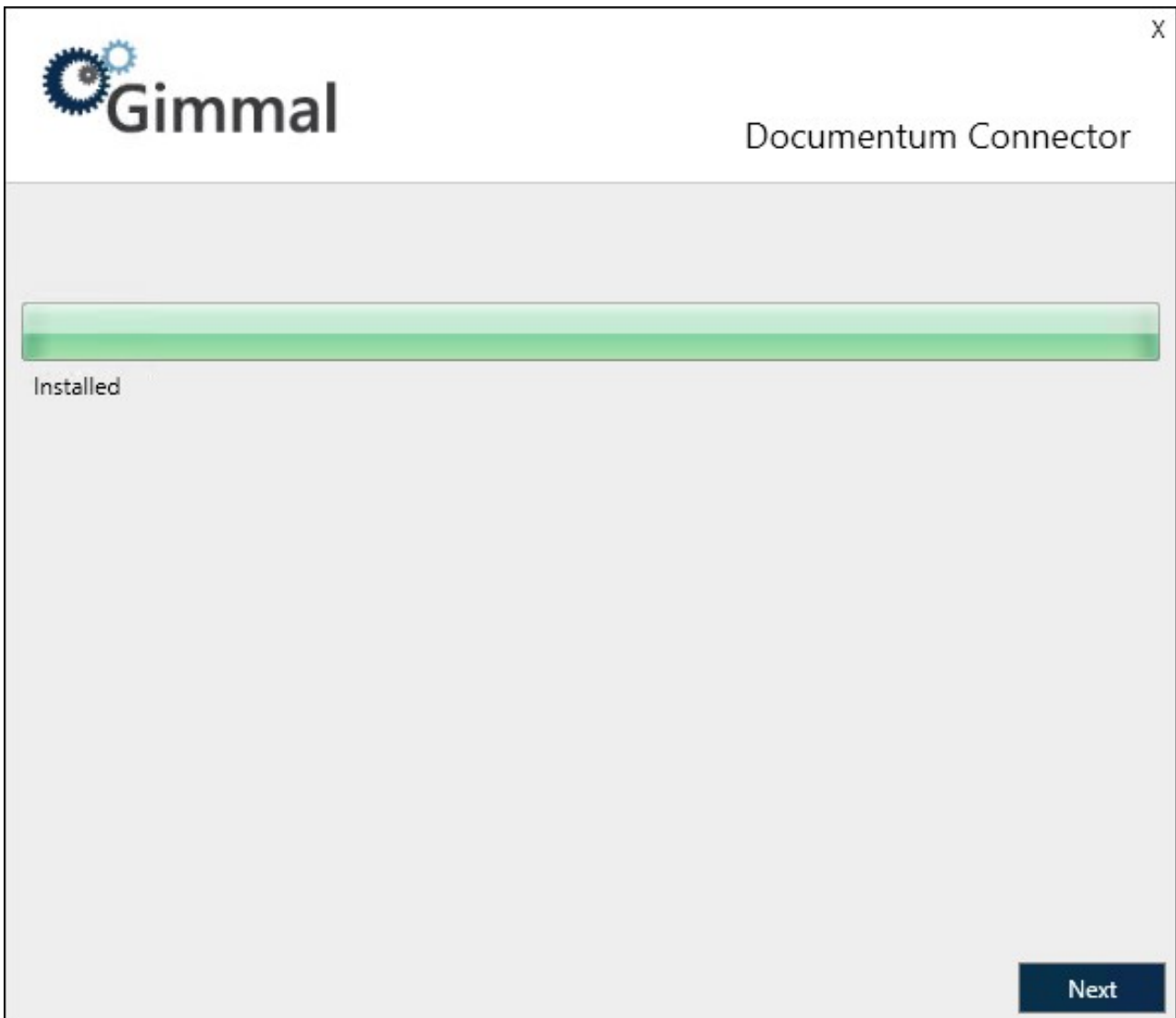
Username: Password:

Previous Next

The "Database Server" and the "Database Name" settings, and the "Automatically Upgrade Database" checkbox, will be populated automatically, however, you can change these settings. For information on the settings, see the picture above.

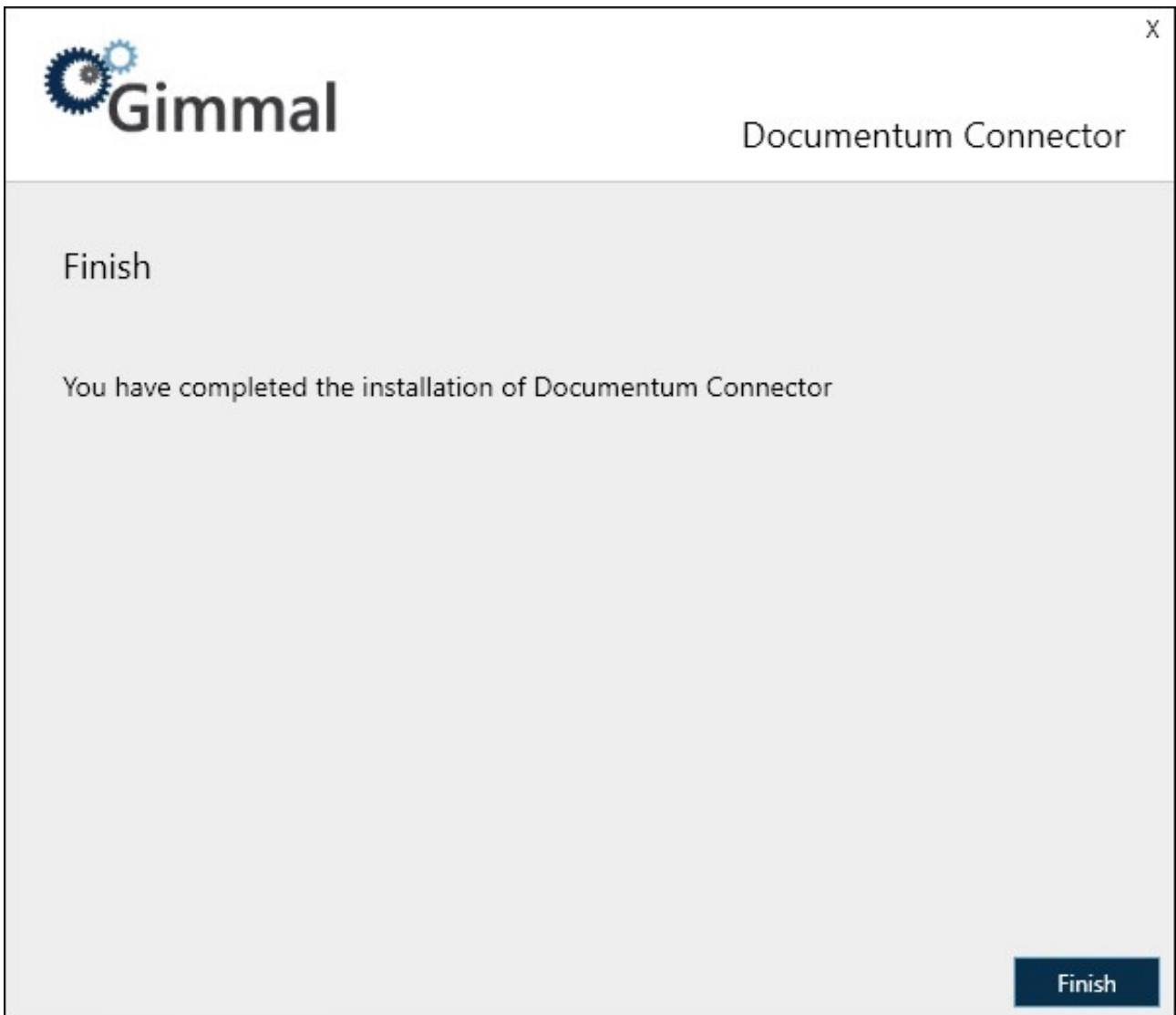
Click **Next** to perform the final installation using the database settings you specified above. The progress bar indicates the state of the installation

10. When the application finishes installing, click **Next** to continue to the Finish screen. This screen indicates that everything was installed successfully.

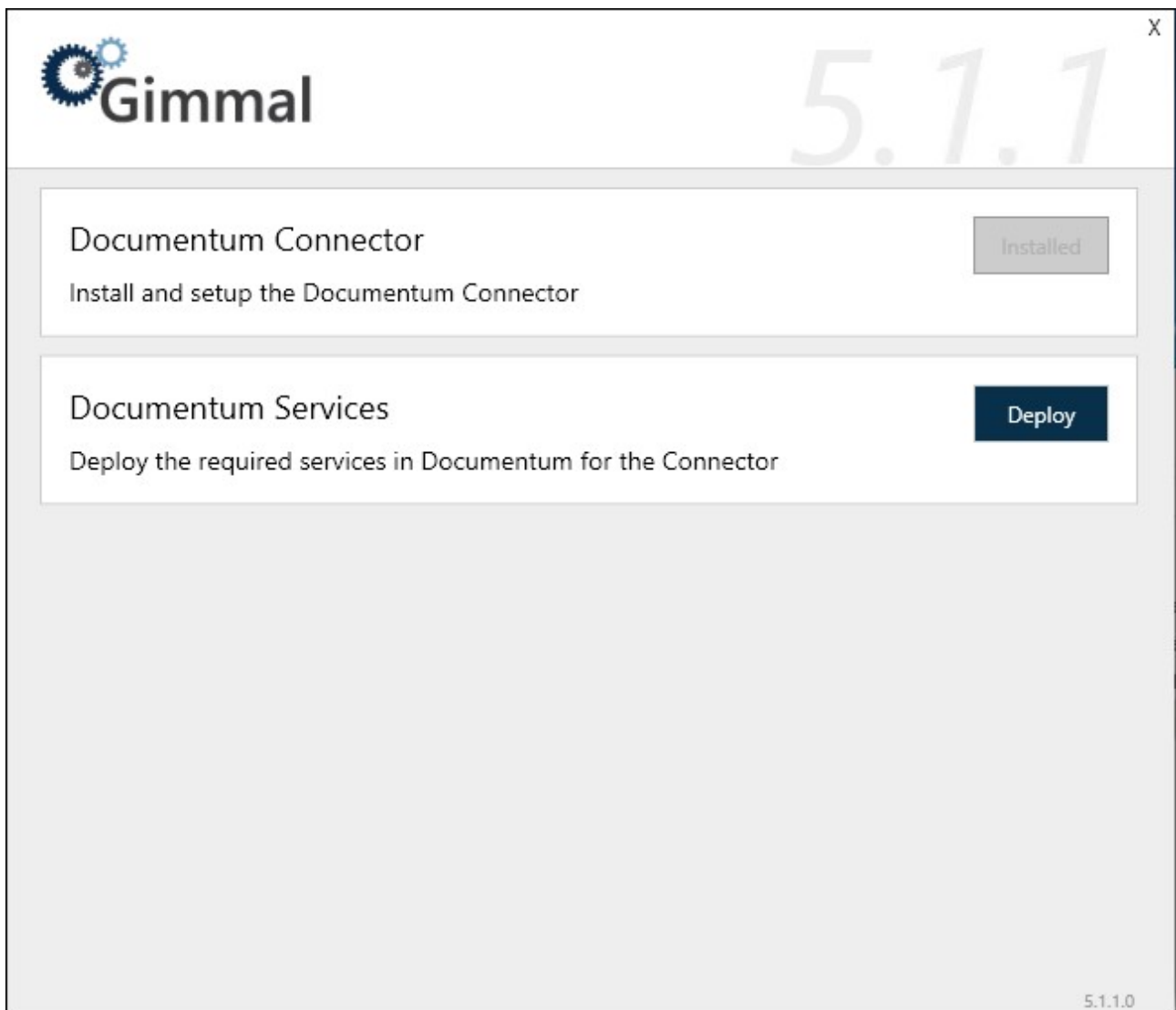


If you experience any errors during the installation process, refer to the installer log in your Windows Temp folder (typically c:\temp).

11. Click **Finish** to return to the main Setup screen, which should now indicate that the Documentum Connector was installed successfully.



12. After clicking Finish, you will see the initial installation screen showing that the Documentum Connector was installed.



13. Next, click on the Deploy button on the installation screen.

14. After you have finished installing the Documentum Connector, you must perform the following steps to run the newly installed Windows Services. (For information on how to run Windows Services, see Microsoft's online documentation.)

- a. Open the Windows Services Manager.
- b. In the Services window, verify that the **Gimmal Documentum Classification Service** and the **Gimmal Documentum Retention Services** are listed.
- c. Start both services. When the services begin, the Status column will display "Running".
- d. Using the SQL Server Management Studio, connect to the SQL database and navigate to the Databases folder. The database you applied settings to in step 9 is located under this Databases folder.
- e. Verify that **DocumentumConnector** is listed.
- f. Expand the nodes: **DocumentumConnector > Security > Users**, and then verify that the Service/User account that was created during the installation steps above is listed and has the correct permissions.

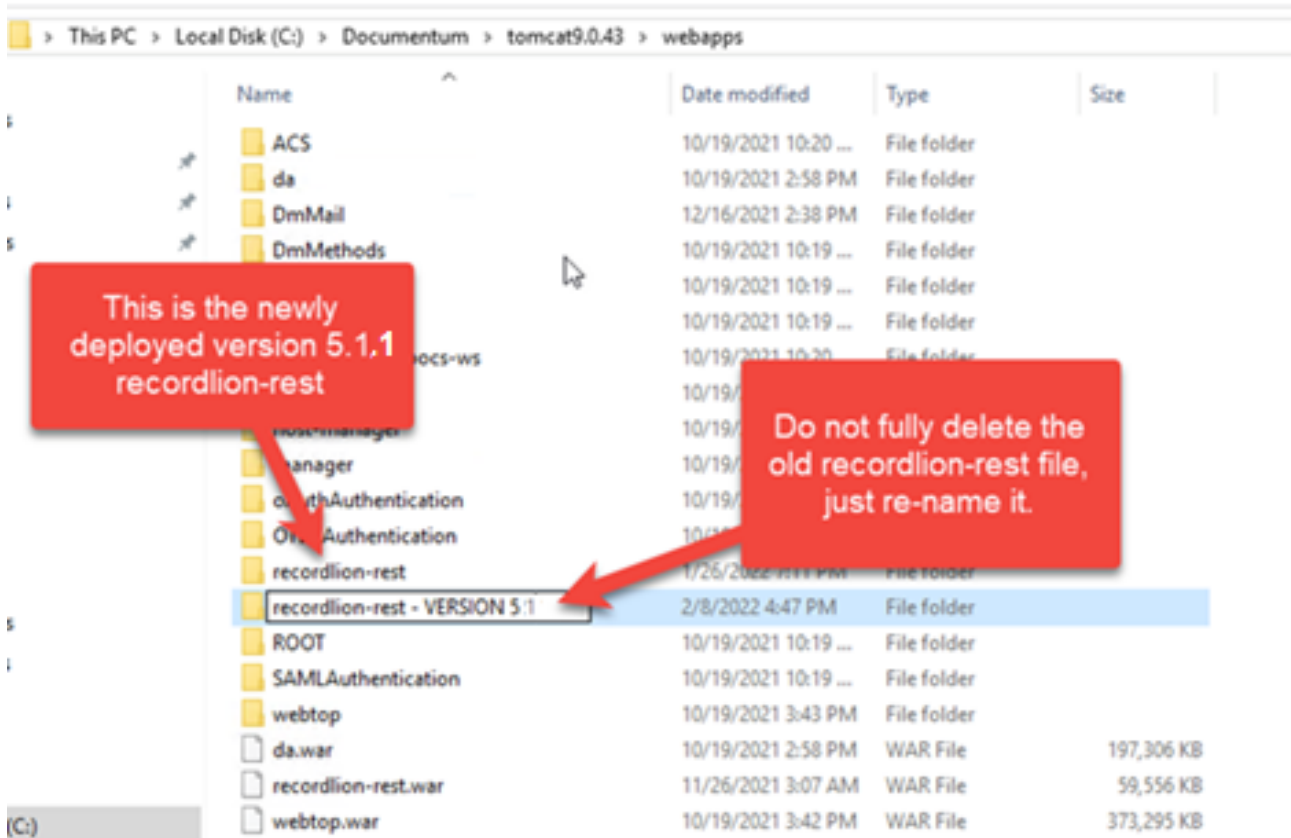
15. Continue the installation process by installing the Documentum Services component. For information, see

Installing Documentum Services⁷¹.

16. Deploy the recordlion-rest war file by following [these steps](#)⁷².

As a precautionary step, do not delete the previously used **recordlion-rest** file when replacing it with the new **recordlion-rest** file, just simply rename it. (Below it has been renamed to **recordlion-rest VERSION 5.1**)

FYI: For the precautionary step, I don't do this, but I would keep what's there.



17. Perform this step if you are deploying a new recordlion-net.war file in Step 16 above:

Update the **dfc.properties** file for the **recordlion-rest** by following [these steps](#)⁷³.

If you do not know where to find the dfc. properties, reference step 1 in the prerequisites.

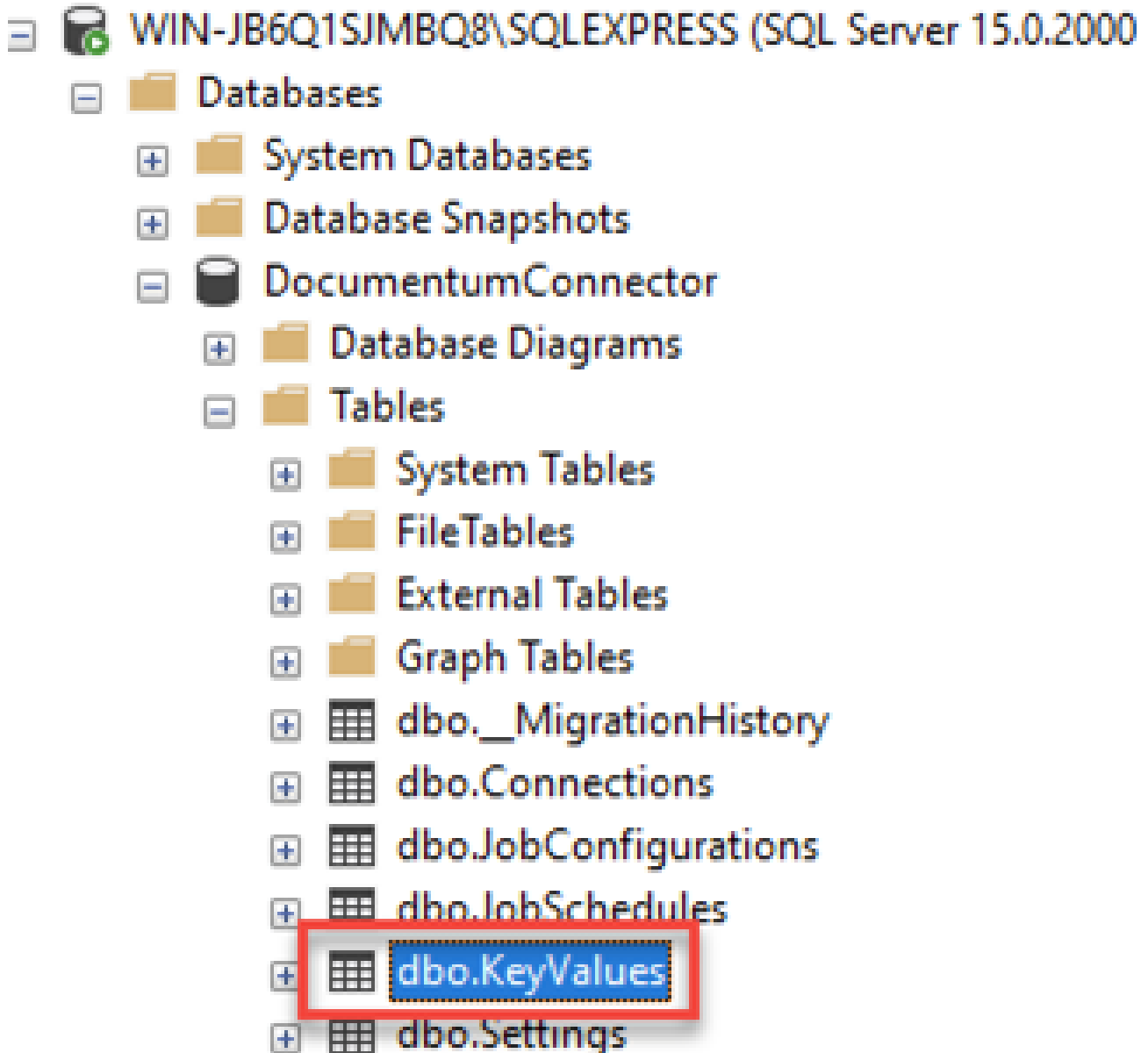
18. Confirm the KeyValue tables have been added to the **DocumentumConnector** table

o Expand the **DocumentumConnector** database in SQL Server Management Studio, then expand **Tables**. Then right-mouse-click on the KeyValue table and choose Select Top 1000 Rows...

⁷¹ <https://docs.gimmel.com/rm/5.1/Server/documentum-services-installation>

⁷² <https://docs.gimmel.com/rm/5.1/Server/documentum-services-installation>

⁷³ <https://docs.gimmel.com/rm/5.1/Server/applying-documentum-foundation-class-properties>



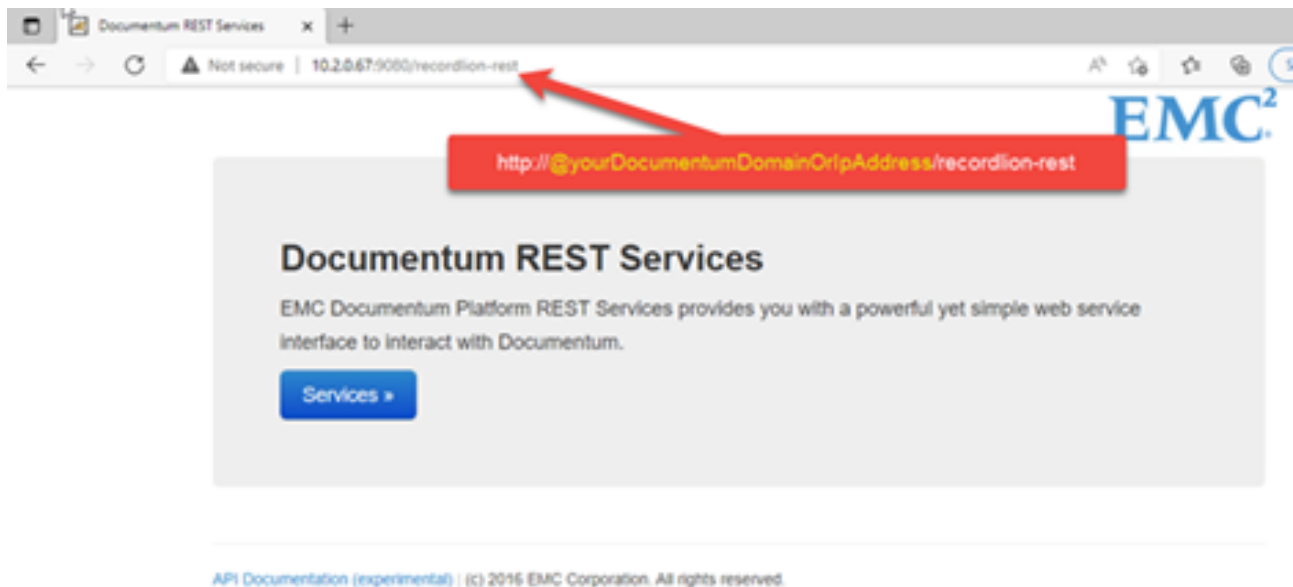
o Confirm that there is an entry in the **KeyValues** table that has a value of **false**

100 %

Results Messages

	Key	Value
1	{280A2BD4-7837-4632-8E0C-E37C73974CC5}	false

Confirm **recordlion-rest** has been successfully deployed by opening a web browser to the URL <http://@yourDocumentumDomainOrIpAddress/recordlion-rest>⁷⁴, and confirm that the web page below renders.



Documentum Connector Initial Re-Recordization

Next, you must go through the initial process of re-recordizing all the previous records to switch out the old URI format with the new clickable URI format. After completing these steps, you continue to proceed to use the connector as usual.

1. Remote into the machine where the Documentum Connector is installed.
2. Launch the Documentum Connector Configuration.
3. In the 'Connection' tab, enter the full Url path to the Documentum Web Url (login page) – see the setting in red below.

⁷⁴ <http://yourdocumentumdomainoripaddress/recordlion-rest>

Documentum Connector

Connection

Manager Web URL

Username

Password

Documentum Web Services URL

Documentum Web URL

Documentum Username

Documentum Password

5.1.1.0

4. Enter the 'Documentum Web URL (this is the absolute path to the login URL for Documentum Web) value, then click 'Save'. You will receive a confirmation if this is successful at the bottom of the web page.

Gimmel Documentum Connector

Connection Repository Configuration Job Configuration

Connection

Manager Web URL

Username

Password

Documentum Web Services URL

Documentum Web URL

Documentum Username

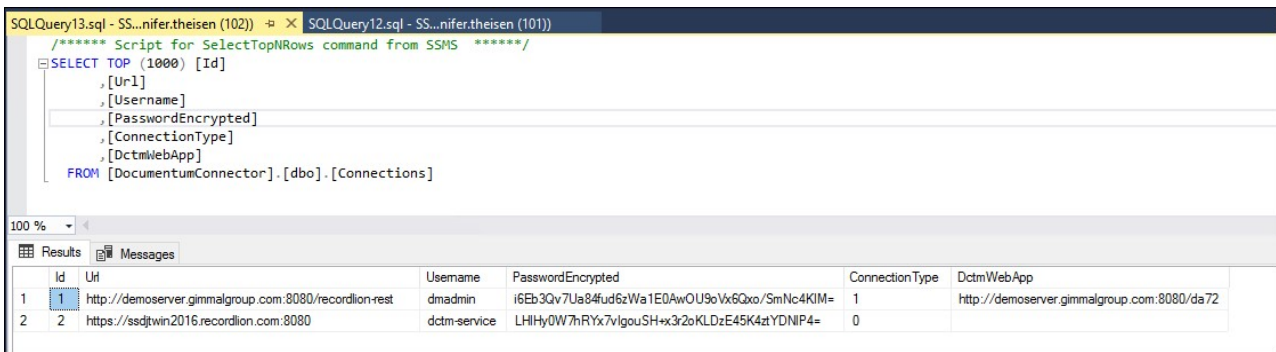
Documentum Password

Save was successful

5.1.1.0

It is highly recommended to not adjust any of the Documentum information in the **Connection** tab after saving. Changing this setting can result in duplicate records being added.

5. Open SQL Server Management Studio and make sure that the Documentum Web Url was entered in the database with an absolute path by querying the Connections table as follows; you should see the DctmWebApp column populated correctly:



6. Restart the machine to clear any potential credential caches before proceeding to the next steps.

7. Click the 'Repository Configuration' -> select the docbases and object types that you made note of in the prerequisites, and click Save.

Only select repositories and docbases that were noted in the prerequisites at this time.



8. Start Documentum Connector Services:

- Gimmel Documentum Classification Service
- Gimmel Documentum Retention Service

9. Click **Job Configuration**, then click **Custom Classification Job**.

Please do not set a **Next Run Time** for **Incremental Classification Job** or **Retention Job** before you run this essential step first.

10. Select all the docbases and object types you wish to undergo the initial step of re-recording all the records to update to the new clickable URI format, select the "Remap Legacy Documentum URLs" checkbox, and press 'Run now'.

This should again be the repositories and docbases noted in the prerequisites.

Job Configuration

Job	Schedule type
Retention Job	Minutes
Incremental Classification Job	Minutes
Custom Classification Job	None

Custom Job Configuration

DocBase - Object Type

- MyRepo - a1_child
- MyRepo - b1_child

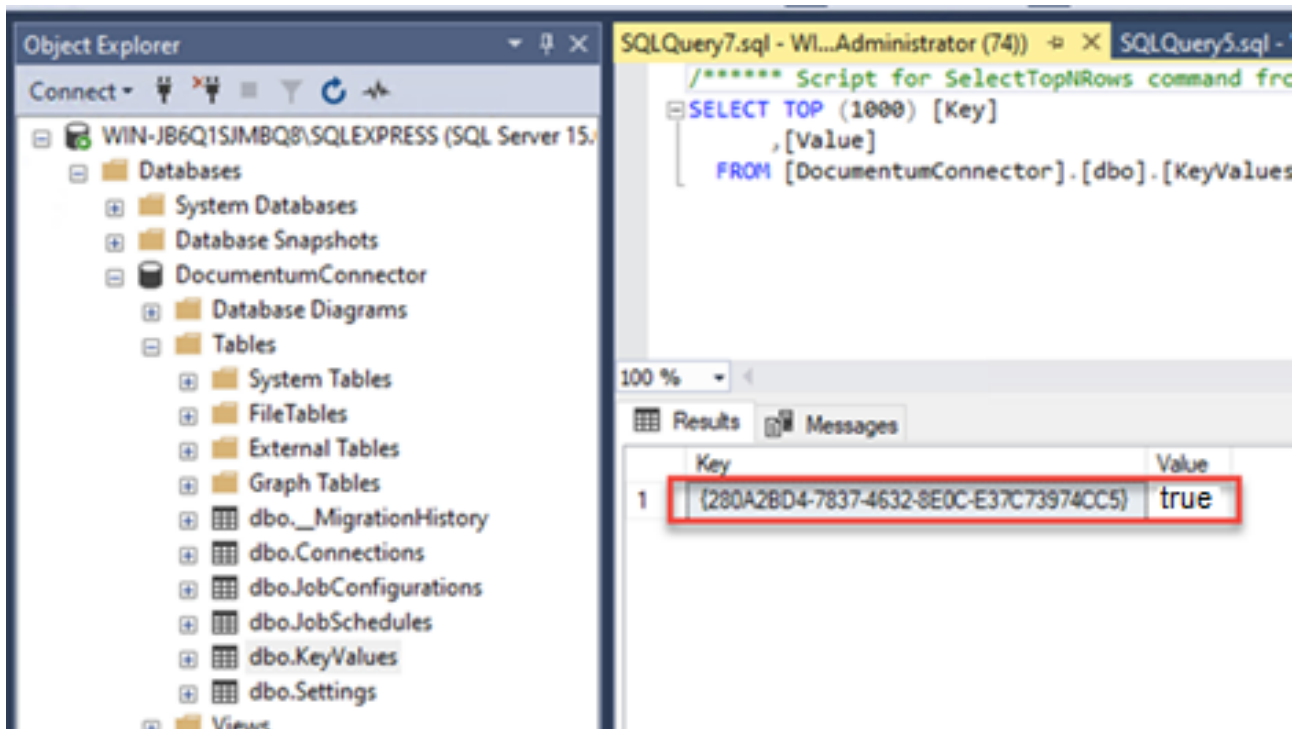
Remap Legacy Documentum URLs

Run now Cancel

5.1.1.0

11. Open SQL Server Management Studio and double-check that the **KeyValue** entry in the Documentum Connector database has been populated – could be true or false.


If you have not included all of the docbases or object types so that it did not initially re-recordize to use the new URI format, just edit this entry to display **True** and follow steps 6-10 again.



12. The upgrade to version 5.1.1 is complete. Please re-enable retention and incremental classifications to proceed.

6.14.8.10 Documentum Services Installation

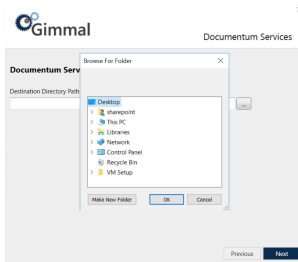
The Documentum Services component deploys required services and components to a Web Application Server that acts as a frontend to the Document Content Server. The Documentum Connector will leverage this server and the deployed services to communicate with Documentum. Specifically, a .WAR file*, which contains the required services is deployed to the Web Application Server. The Documentum Connector uses these services to manage documents inside of Documentum.

 The .WAR file that is installed as part of the Documentum Connector is supported only for deployment to an Apache Tomcat server. Tomcat must be version 7.x or higher.

Deploying to a Windows-based Documentum Web Application Server

To install Documentum Services, perform these steps on the same machine where the Documentum Web Application Server is installed:


1. On the Documentum Connector installation screen, click **Deploy** to the right of the Documentum Services option. The Destination Directory Path screen displays.
2. Click the ... icon next to the Destination Directory Path field. The Browse For Folder dialog opens.



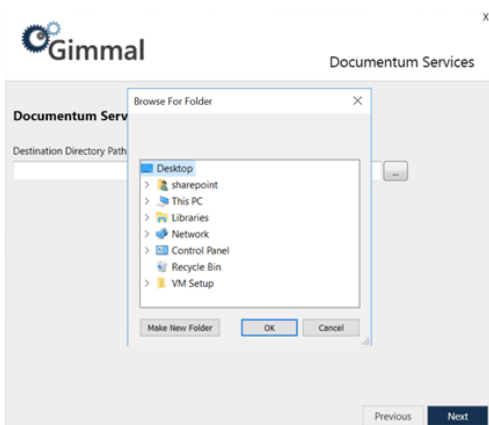
3. Browse to and select the **\webapps** folder of the TomCat web server that will host the Documentum Services, and then click **Next**. The installation begins, with a progress bar indicating the state of the installation.
4. Click **Next**. The Finish window displays, indicating the component was installed successfully.
5. Click **Finish** to close the installer.
6. Complete the installation by updating the [Documentum Foundation Properties](#)(see page 294) settings
7. Start the Documentum Retention and Classification Windows services on the Documentum Connector server.

Deploying to a Non-Windows Documentum Web Application Server

If desired, you can deploy the Documentum Connector .WAR file to a non-Windows Web Application Server*. To do so, perform the following steps on a Windows machine:

 The .WAR file that is installed as part of the Documentum Connector is deployed only to the web application server.

1. On the Documentum Connector installation screen, click **Deploy** to the right of the Documentum Services option. The Destination Directory Path window displays.
2. Click the ... icon next to the Destination Directory Path field. The Browse For Folder window opens.



3. Choose a temporary folder location (on current server or a safe network location) to which the the .WAR file should be extracted.
4. Click **Next**. The Finish screen displays, indicating the component was installed successfully.
5. Click **Finish** to close the installer.

6. Now take the .WAR file from the temporary folder location and copy it to the appropriate \webapps (or equivalent) folder of the JAVA web server that will host the Documentum REST services.
7. Complete the installation by updating the [Documentum Foundation Properties](#)(see page 294) settings
8. Start the Documentum Retention and Classification Windows services on the Documentum Connector server.

6.14.9 FileNet Connector

The FileNet Connector enables you to manage document objects in an IBM FileNet P8 platform, as part of the Records Management system. It provides a way to manage all versions of a document that exists in a FileNet repository.

6.14.9.1 FileNet Connector System Requirements

6.14.9.2 FileNet Connector Installation

6.14.9.3 FileNet Services Installation

6.14.9.4 Applying FileNet Property Settings

6.14.9.5 FileNet Connector Configuration

6.14.9.6 Uninstall FileNet Connector

6.14.9.7 FileNet Connector System Requirements


Before you install the Records Management FileNet Connector, verify that your system meets or exceeds the following requirements:

- You are using the Gimmel Cloud, or you are using version 4.6.2 of the core Records Management software
- IBM FileNet P8 Version 5.2.1 is installed and configured

FileNet Connector Server		
	Core	Memory (MB)
Minimum	2	2048
Recommended	4	4096

- Windows Server 2012 or later (x64)
- Windows Server 2012 R2 or later (x64)
- .NET Framework 4.5** (x64)

- .NET Framework 3.5**
- 100 MB Disk Space for software

 **As a security best practice when using the .NET Framework, Gimmel recommends that you enable Transport Layer Security (TLS) 1.2, which provides communications security for client/server applications. To enable TLS 1.2, you must add the following Windows registry settings to the Records Management Core server(s) and the servers of any Records Management connectors you are using (if applicable), and then reboot your system.

- HKLM:\SOFTWARE\Microsoft\.NETFramework\v4.0.30319 "SchUseStrongCrypto"= dword:00000001
- HKLM:\SOFTWARE\Microsoft\.NETFramework\v4.0.30319 "SystemDefaultTlsVersions"= dword:00000001
- HKLM:\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319 "SchUseStrongCrypto"= dword:00000001
- HKLM:\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319 "SystemDefaultTlsVersions"= dword:00000001

Note that some operating systems require additional steps to enable TLS 1.2. For more information, see [Microsoft's TLS documentation](#)⁷⁵ To verify that your operating system supports TLS 1.2, read the [Support for TLS 1.2 section of Microsoft's documentation](#)⁷⁶.

Database Server

- SQL Server 2016 or greater
- 100 MB for FileNet Database

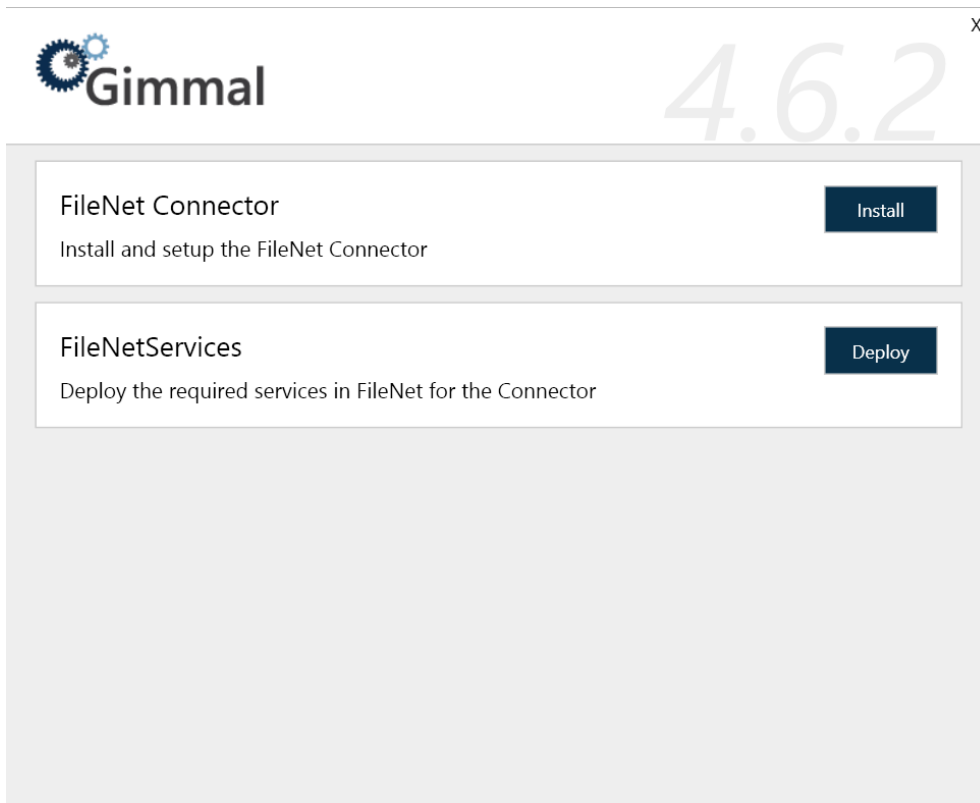
6.14.9.8 FileNet Connector Installation

 Ensure that you run the installer as the Local Administrator.

Upon launching the FileNet Connector installer, the following screen displays:

⁷⁵ <https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls#systemdefaulttlsversions>

⁷⁶ <https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls#support-for-tls-12>



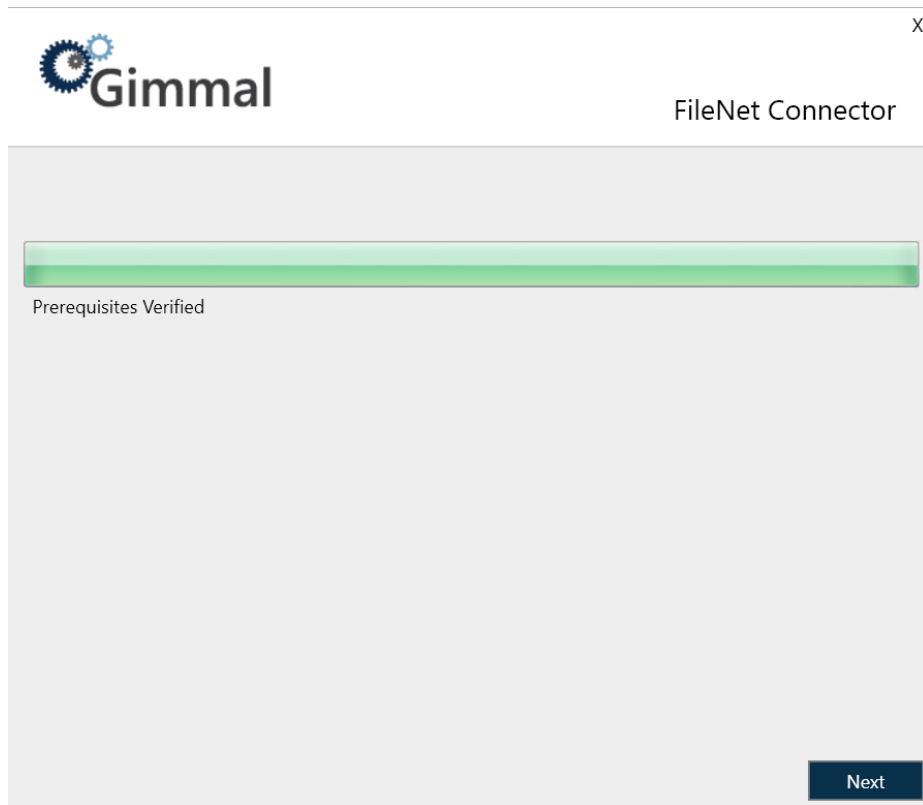
Installing the FileNet Connector

Before you install the FileNet Connector, verify the Connector [system requirements](#).(see page 325) This installation section assumes that you have already installed the Records Management Core platform.

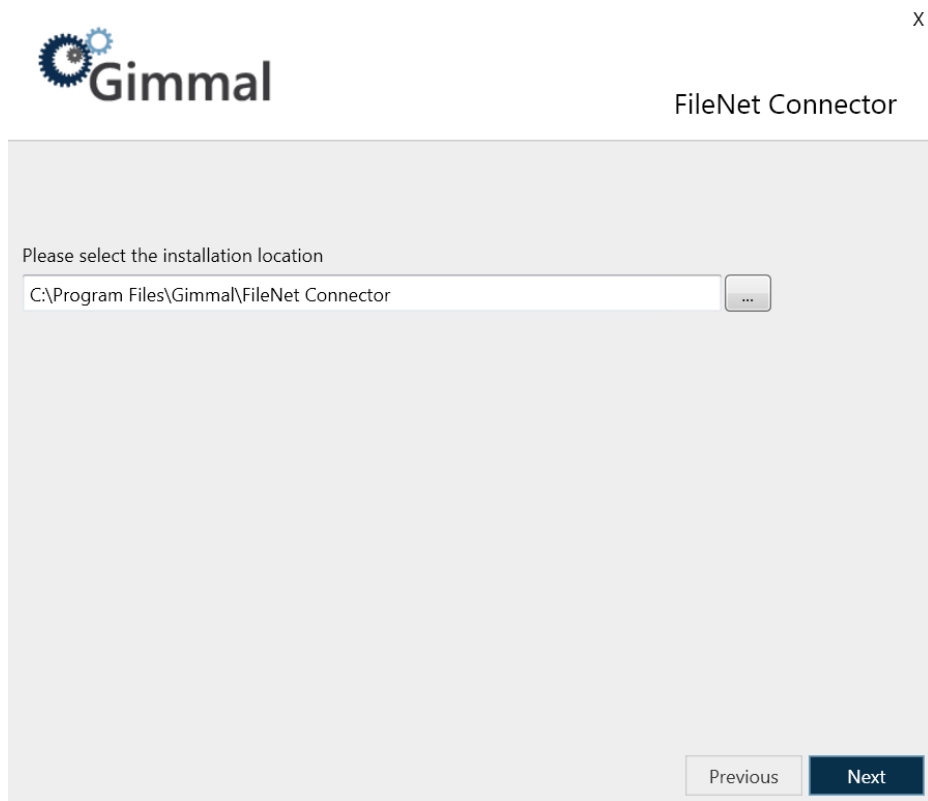
i When you install the FileNet Connector, a Configuration Application and two Records Management Windows Services are installed automatically as part of this process.

To install the FileNet Connector, perform the following steps:

1. From the Records Management splash screen, click the **Install FileNet Connector** link. The User Account Control window opens.
2. Click Yes to allow the installer to make changes to your computer. The FileNet Connector installation screen displays.
3. On the FileNet Connector installation screen, click **Install** to the right of the FileNet Connector option. The first screen that displays is the check for prerequisites. This screen validates the following information before allowing the installation to proceed:
 - The current user is Local Administrator
 - You have installed .NET Framework 4.5



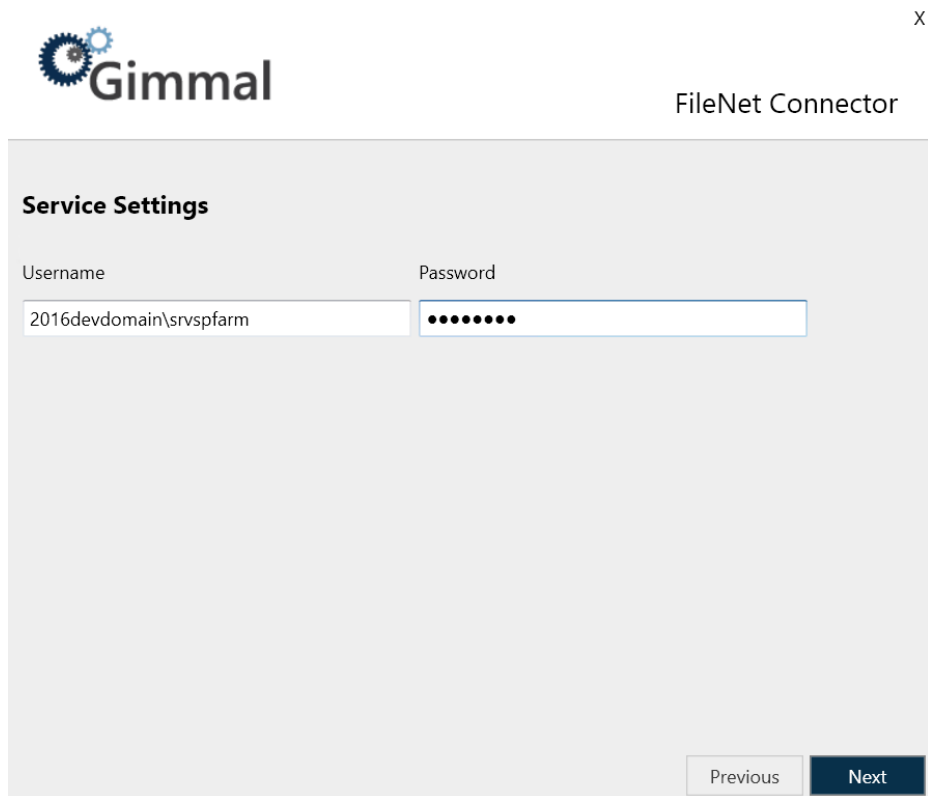
4. Click **Next**. The installation location screen displays, which determines where the connector will be installed.



5. Leave the installation path as the default, or to change it, click the ... icon next to the installation location field, select the desired installation location, and then click **Next**. The Service Settings screen displays.

 You must have at least 100MB of disk space available.

X



Gimmel FileNet Connector

Service Settings

Username Password

2016devdomain\srvspfarm ●●●●●●●●

Previous Next

6. Enter the following required information to specify which user account to use when you run the Windows Services:

- **Username** (Ex. DOMAIN\Username)
- **Password**

The user account can be a domain account (DOMAIN\username) or a computer account if it has access to the SQL Server database (COMPUTERNAME\username). The account must have the following file system permissions:

- Read/Write: %Install path%\Logs

7. Click Next. The Database Settings screen displays.


X



FileNet Connector

Database Settings

Database Server	Database Name
<input type="text" value="2016SVR"/>	<input type="text" value="FileNetConnector"/>
<input checked="" type="checkbox"/> Automatically Create Database	<input type="checkbox"/> Use SQL Authentication
Username	Password
<input type="text"/>	<input type="text"/>

 The "Database Server" and the "Database Name" settings, and the "Automatically Create Database" checkbox, will be populated automatically, however, you can change these settings. For information on the settings, see below.

8. Enter/select the following database settings to determine the connection information that will be used by the FileNet Connector to connect to SQL Server:
- **Database Server:** The name of the SQL Server Install (ex. SERVERNAME\InstanceName)
 - **Database Name:** The name of the actual SQL Server Database (The default name for the database is "FileNetConnector", but you can change it here.)
 - **Automatically Create Database:** See description below
 - **Use SQL Authentication:** Specifies that the connection information should use SQL Authentication with the Username and Password indicated below
 - **Username:** The SQL Server username to use if SQL Authentication is specified
 - **Password:** The SQL Server password to use if SQL Authentication is specified

If **SQL Authentication** is not specified, the connection information will use Windows Authentication by specifying a trusted connection. This means that the Service account will be used to connect to SQL Server, therefore, this account will need the following database permissions. If SQL Authentication is specified, the SQL user will also require the following permissions.

- **db_datareader**
- **db_datawriter**
- **GRANT EXECUTE** on all Stored Procedures
- **GRANT EXECUTE** on all Scalar User Defined Functions
- **GRANT SELECT** on all Table and Inline User Defined Functions

If **Automatically Create Database** is specified, the installation will automatically attempt to create the database using the Database Server and Database Name indicated. The appropriate account will also be


automatically granted the appropriate rights to this database. This option requires that the current user has permission to create databases and manage security in the SQL Server instance indicated.

If **Automatically Create Database** is not specified, the installation will configure connection information but will not attempt to create the database. In this case, you will need to leverage the SQL Script at the following location to manually create the database in the SQL Server instance indicated. You will also need to manually configure security as indicated above.

- %Install Path%\Configuration\Sql\RecordLion.RecordsManager.FileNet.sql
9. Click **Next** to perform the final installation using the database settings you specified above. The progress bar indicates the state of the installation.
 10. When the application finishes installing, click **Next** to continue to the Finish screen. This screen indicates that everything installed successfully.
 11. Click **Finish** to return to the main Setup screen, which should now indicate that the FileNet Connector was installed successfully.
 12. After you have finished installing the FileNet Connector, you must perform the following steps to run the newly installed Windows Services. (For information on how to run Windows Services, see Microsoft's online documentation.)
 - Open the Windows Services Manager.
 - In the Services window, verify that the **Gimmel FileNet Classification Service** and the **Gimmel FileNet Retention Services** are listed.
 - Start both services. When the services begin, the Status column will display "Running".
 - Using the SQL Server Management Studio, connect to the SQL database and navigate to the Databases folder. The database you applied settings to in step 9 is located under this Databases folder.
 - Verify that **FileNetConnector** is listed.
 - Expand the nodes: **FileNetConnector > Security > Users**, and then verify that the Service/User account that was created during the installation steps above is listed and has the correct permissions.
 13. Continue the installation process by installing the FileNet Services component. For information, see [Installing FileNet Services](#)⁷⁷.

6.14.9.9 FileNet Services Installation

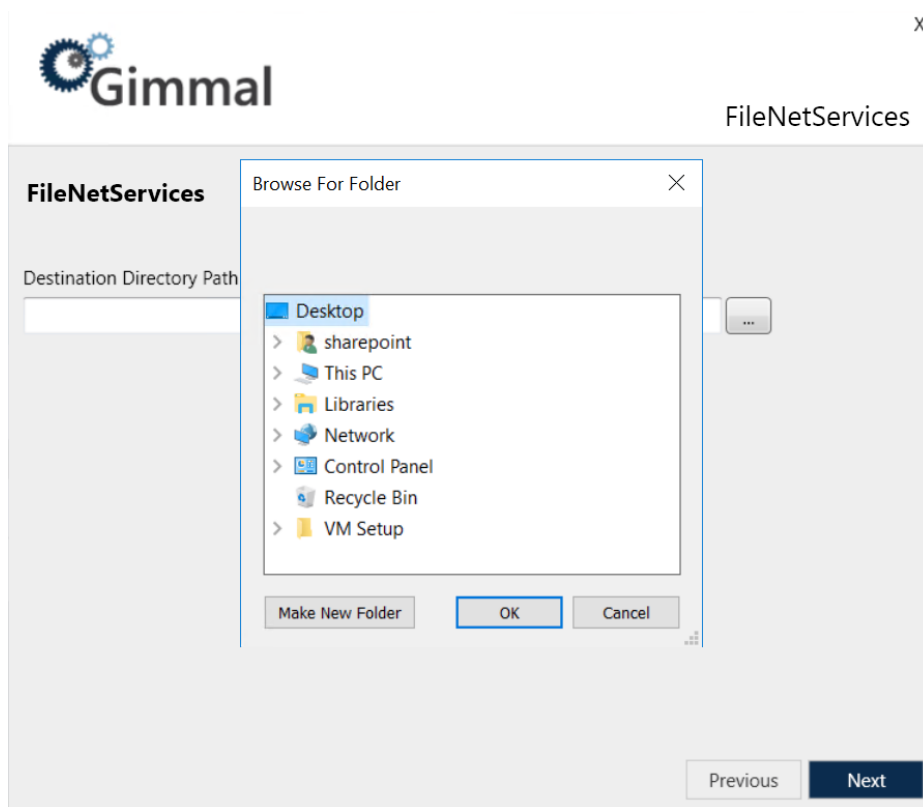
The FileNet Services component deploys required services and components into the FileNet Server, which the FileNet Connector will leverage to communicate with FileNet. Additionally, a .WAR file*, which contains the services that are deployed to the FileNet farm, is deployed. The FileNet Connector uses these services to manage documents inside of FileNet.

 The .WAR file that is installed as part of the FileNet Connector is deployed only to Apache Tomcat. Tomcat must be version 8.x or higher.

To install FileNet Services, perform these steps on the same machine where the FileNet app server is installed:

1. On the FileNet Connector installation screen, click Deploy to the right of the FileNet Services option. The Destination Directory Path screen displays.
2. Click the ... icon next to the Destination Directory Path field. The Browse For Folder dialog opens.

⁷⁷ <http://docs.gimmel.com/en/14452-installing-filenet-services.html>



3. Select the webapps folder of the Java web server that hosts FileNet, and then click **Next**. The installation begins, with a progress bar indicating the state of the installation. Upon deployment, the following screen displays:
4. Click **Next**. The Finish screen displays, indicating the component was installed successfully.
5. Click **Finish** to close the installer.

Deploying .WAR File to a FileNet Server

Perform the following steps to deploy the FileNet Connector .WAR file to a FileNet server.

1. From the Records Management splash screen, click the **Install FileNet Connector** link. The User Account Control window opens.
2. Click **Yes** to allow the installer to make changes to your computer. The FileNet Connector installation screen displays.
3. On the FileNet Connector installation screen, click **Install** to the right of the **FileNet Services** option.
4. Perform the steps described in [Installing FileNet Services](#)⁷⁸. When you get to step three, choose a temporary folder location (on current server or safe network location) where you want to deploy the .WAR file. This file enables you to configure the FileNet server so that it interfaces with the FileNet Connector server.
5. Take the .WAR file from the temporary folder location and copy it to the “webapps” folder of the Java web server that hosts FileNet.
6. Complete the remaining steps of the installation.
7. Start the FileNet Retention and Classification Windows services on the FileNet Connector server.

⁷⁸ <http://docs.gimmel.com/en/14452-installing-filenet-services.html>

6.14.9.10 Applying FileNet Property Settings

When you install FileNet Services, a WAR file is deployed as part of the process. Additionally, an "application.properties" file is included as part of the deployment process. The "application.properties" file provides property settings for the FileNet runtime. The FileNet Connector requires these property settings. To update the settings in this file, navigate to the "application.properties" file located at <TOMCAT INSTALLATION DIRECTORY>\webapps\filenet-rest\WEB-INF\classes, and edit the file. The following section lists the properties and values.

Application.Properties File Properties and Values

The "application.properties file" includes critical settings that are required for FileNet Services to reach a FileNet server. The following table includes the properties available in the "application.properties" file and a description of the values:

Property	Value
filenet.connection.uri	The link to the FileNet web services instance
server.servlet.contextPath	The location of the FileNet Connector web services (This value needs to be entered as-is.)
server.port	The preferred port number (Default is 8888.)

6.14.9.11 FileNet Connector Configuration

The FileNet Connector Configuration component is a desktop application that is installed along with the FileNet Connector. The Configuration dialog provides three "tabs" that enable you to configure your FileNet connection settings, select your FileNet Libraries, view the available jobs in the connector, and schedule the job intervals.


The screenshot shows the 'FileNet Connector' configuration window with the 'Connection' tab selected. The window title is 'FileNet Connector' with a close button 'X'. The navigation bar includes 'Connection' (active), 'Global Configuration', and 'Job Configuration'. The main area is titled 'Connection' and contains the following fields:

- Manager Web URL: A text input field with a 'Test' button to its right.
- Username: A text input field.
- Password: A text input field.
- FileNet Web Services URL: A text input field.
- FileNet Username: A text input field.
- FileNet Password: A text input field.

A 'Save' button is located at the bottom left of the configuration area.

Configuring the FileNet Connection Settings

The Connection tab enables you to enter the required credentials so you can access the FileNet server.

 Before you begin these configuration steps, ensure that you have created the Manager Web account username and password.

To configure the Connection settings, perform these steps on the same machine where you are running the Records Management FileNet Connector. Launch the Gimmel

1. Launch the Gimmel FileNet Connector Configuration application. The application should be found in the installation location you specified during the FileNet Connector installation process, or you can launch the application from the Windows Start menu. The FileNet Connector dialog opens on the Connection page.
2. Enter the following information
 - **Manager Web URL:** The URL to the Manager Web (i.e., where Records Management is installed)
 - **Username:** The username of the Service Account created in Records Management
 - **Password:** The password of the Service Account created in Records Management
 - **FileNet Web Services URL:** The URL to the FileNet Web Services URL (note that multiple FileNet instances are not supported)
 - **FileNet Username:** The FileNet user ID; ID is used to carry out all Connector activities within FileNet
 - FileNet Password: **The FileNet password**
3. Click **Save**.
4. Continue with the next section.

Configuring the FileNet Global Configuration

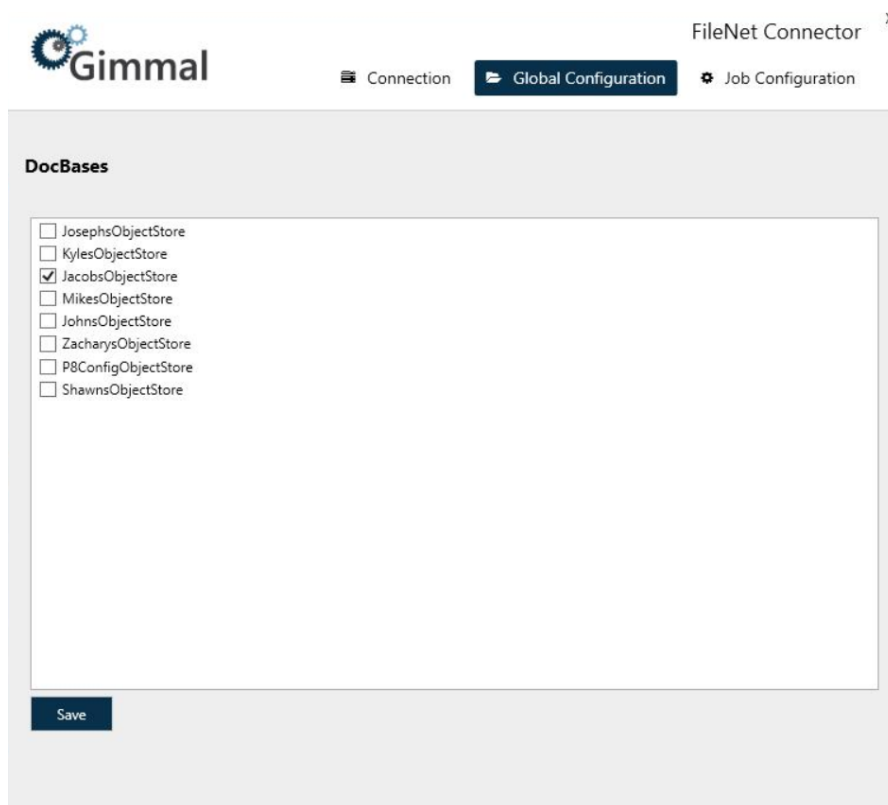
The Global Configuration dialog enables you to select which Libraries you would like to classify and apply retention actions to. Different Libraries support different users, departments, operations, etc.

! One or more Libraries, containing content (documents), must exist. They must share a common user ID for the Records Management FileNet Connector to use when carrying out its tasks. (You configured this FileNet user on the Connection screen. You must configure a user first, or you will not be able to access the Global Configuration dialog.)

i To ensure that all documents are entered into Records Management accurately, ensure that the Libraries you selected on this tab have already been crawled by the Custom Classification job described in Configuring the FileNet Job Configuration.

To select your Libraries, perform the following steps:


1. On the FileNet Connector Configuration dialog, click **Global Configuration**. The Global Configuration page opens, showing a list of available Libraries in FileNet.




2. Select the desired Library(s).
3. Click **Save**.
4. Continue with the next section

Configuring the FileNet Job Configuration

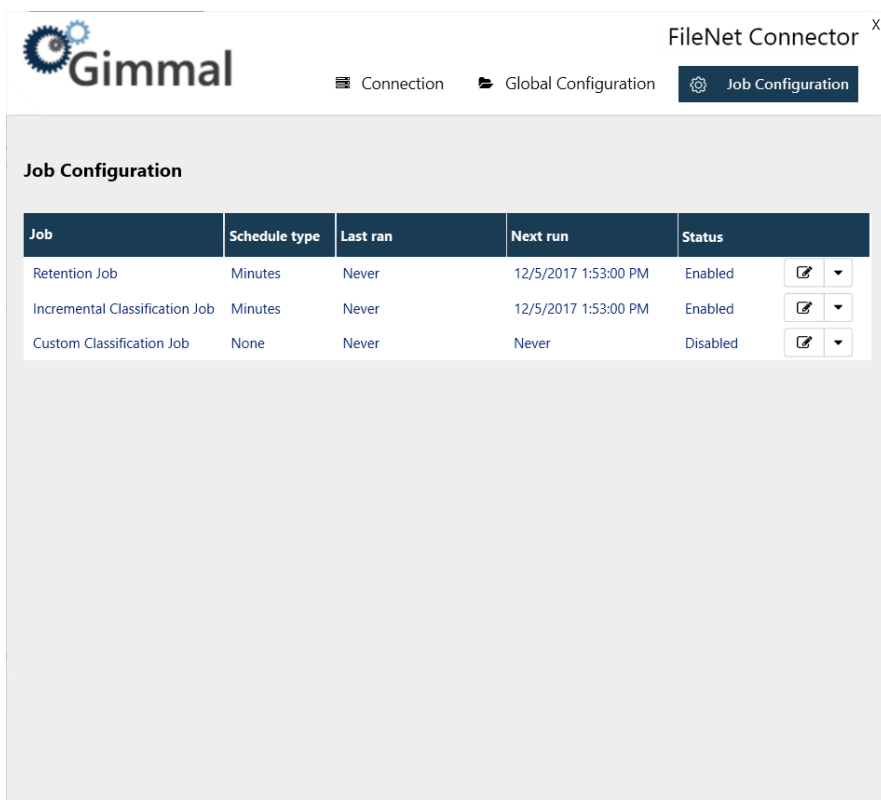
The Job Configuration dialog displays the retention and classification jobs included in the FileNet Connector, and enables you to either run the jobs immediately, or schedule how often you want the jobs to run. The jobs default to running every five minutes.

 The only way to schedule the retention and classification jobs is through the Connector configuration application.







 Also listed in the Job Configuration dialog is the Custom Classification Job. The Custom Classification Job is essential to configure the client for the first time. The Edit icon opens a separate dialog that displays all of the Libraries, along with DocTypes that are available in that Library. This dialog enables you to select which DocTypes under each Library you want to be included in the initial classification of a FileNet Server.

To ensure that all documents will be entered into Records Management accurately, ensure that the Libraries you selected on the Global Configuration tab have already been crawled by the Custom Classification job. To configure your retention and classification jobs, perform the following steps:

1. Ensure that you have started both the FileNet Retention Service and the FileNet Classification Service either manually or from the Windows Services dialog.
2. On the FileNet Connector Configuration screen, click Job Configuration. The Job Configuration dialog opens, showing a list of retention and classification jobs.



The screenshot shows the 'FileNet Connector' window with the 'Job Configuration' tab selected. The 'Job Configuration' section contains a table with the following data:

Job	Schedule type	Last ran	Next run	Status	
Retention Job	Minutes	Never	12/5/2017 1:53:00 PM	Enabled	 
Incremental Classification Job	Minutes	Never	12/5/2017 1:53:00 PM	Enabled	 
Custom Classification Job	None	Never	Never	Disabled	 

3. Perform either of the following steps:
To run a job immediately, click the drop-down arrow to the right of the desired job and then click **Run Now**.

To schedule how often a job is to be run, click the **Edit** icon to the right of the desired job and set the Schedule Type (Minutes, Hourly, Daily), and the Time Interval; then click **Save**. The Next Run column will update with the time when the job is to be run next.

Windows Services

When you install the FileNet Connector, two Windows Services are added during the installation process. These Services enable Records Management to manage the lifecycle of records and information stored in FileNet. A description of the Services follows:

Service Type	Description
Gimmel FileNet Classification Service	<p>The Classification Service is responsible for discovering the content that exists in FileNet and notifying Records Management of its existence, including any updates and removals of this content.</p> <p>NOTE: Because the Classification Service is limited by Windows Operating System Disk Notifications, it is possible that the buffer used to notify the Classification Service of file changes may overflow. This occurs if a large number of files are created or updated within a very short amount of time resulting in files not being classified. The service executes a full crawl daily, allowing the items that were not classified, to be classified appropriately.</p>
Gimmel FileNet Retention Service	<p>The Retention Service is responsible for executing the lifecycle actions, as indicated by Records Management at various points in time according to the specified File Plan.</p>

6.14.9.12 Uninstall FileNet Connector

To uninstall the FileNet Connector, perform the following steps:

1. On the server that hosts the FileNet Connector, navigate to the Windows Control Panel and select **Uninstall a Program** from the Programs section.
2. On the “Uninstall or change a program screen”, locate the **Gimmel FileNet Connector** and double-click it. (You can also select Gimmel FileNet Connector and then click the **Uninstall** option above the program list.) A dialog displays, asking you to confirm the uninstallation.
3. Click **Yes** to confirm the uninstallation. The User Account Control dialog displays, asking you to confirm the uninstallation.
4. Click **Yes** to begin the uninstallation process. When the uninstallation has completed, the Records Management FileNet Connector program will be removed from the Programs list.
5. If desired, you can remove the .WAR file and the web app from the Apache Tomcat server.
6. Verify that the Gimmel FileNet Classification Service and the Gimmel FileNet Retention Service no longer display in the Windows Services list.

After uninstalling, the FileNet Connector database will remain intact on the database server. You may keep this database in case you will be reinstalling the connector, or you can delete the database manually if it is no longer needed.

6.14.10 SharePoint Online Connector

The SharePoint Online Connector enables content in your SharePoint Online tenant to be managed by Gimmel Records Management. The topics below walk you through the deployment of this connector.


- [SharePoint Online Requirements](#)(see page 339)
- [Prepare to use the SharePoint Online Connector](#)(see page 341)
- [SharePoint Online Connector On-Premise Only](#)(see page 344)
- [Uploading SharePoint Online Connector App Package](#)(see page 355)
- [SharePoint Online Connector Configuration](#)(see page 356)
- [Renewing a Client Secret](#)(see page 362)
- [Unregistering a SharePoint App from an Individual Web](#)(see page 363)

6.14.10.1 SharePoint Online Requirements

Microsoft 365

The SharePoint Online Connector supports the following Microsoft 365 environments:

- E5
- E3
- G3
- G5

 The SharePoint Online Connector may work with other Microsoft 365 environments, but they may not be supported by Gimmel.


SharePoint Online


SharePoint Online Sites (also known as Site Collections)

- Communication Site
- Team Site (no Office 365 group)
- Team Site (connected to Office 365 group) has limited support outline in the topic [Managing Team Sites with Office 365 Groups](#)(see page 340)
- Document Center

SharePoint Online Subsites

- Team Site (no Office 365 Groups)
- Team Site (classic experience)
- Document Center
- Records Center

 The SharePoint Online Connector may work with other types of sites, however, they have not been tested and you may experience varying results.

 The “In Place Records Management” feature in SharePoint must be enabled for any Sites you wish to use with the SharePoint Online Connector and Gimmel Records. You would want to enable this feature for your Site prior to registering and configuring the SharePoint Online Connector. Please contact your SharePoint system administrator for help enabling the “In Place Records Management” feature.


Managing Team Sites with Office 365 Groups

Microsoft Teams stores content to a specific Team Site in SharePoint Online. However, these sites are pre-configured differently than typical SharePoint Sites. The sites are connected to Office 365 Groups when a new Team is created, or when a new Team Site connected to an Office 365 Group is created from SharePoint.

For any site in SharePoint to work correctly with Gimmel Records Management, the “In Place Records Management” feature in SharePoint must be enabled. This feature is not turned on by default with Team Sites connected to Office 365 Groups. Please contact your SharePoint system administrator for help enabling the “In Place Records Management” feature.

Channels may also be created within Microsoft Teams and a corresponding folder will be created in the document library for each Channel. When a user shares content to these channels there is specific behavior to consider. The following table lists the known issues when using Gimmel with channels within Microsoft Teams:

<p>Declaring content as a record or adding content to a legal hold in a Teams channel folder</p>	<p>The content will be successfully locked but Gimmel Records Management will not be able to delete it at the end of the lifecycle due to the Channel folder behavior.</p> <p>Workaround: Manually un-declare the record within SharePoint before the disposition phase.</p>
<p>Declaring a record using In Place Record Management</p>	<p>Gimmel strongly discourages you from using the user interface in SharePoint to declare a record using "In Place Records Management" while using Gimmel Records Management. If content is declared using "In Place Records Management", Gimmel Records Management will not be able to delete it at the end of the lifecycle due to the separate hold.</p> <p>Workaround: If a record is declared via the SharePoint interface for these folders it is necessary to manually un-declare the record within SharePoint before the disposition phase.</p>

 Gimmel recommends that when using Records Management with Microsoft Teams to not declare records or create legal holds on items within Microsoft Team channels.

6.14.10.2 Prepare to use the SharePoint Online Connector

i These instructions are provided for convenience. Registering the SharePoint App and creating the catalog are out of scope for Gimmel Support. Please contact your SharePoint Online or Microsoft 365 administrator for help completing these tasks.

! You cannot configure the SharePoint Online Connector app (effectively the same O365 tenant) to work with two different instances of Records Management. You must provide distinct Microsoft 365 tenants to accomplish this requirement. For example, <https://test-company.sharepoint.com> is registered to <https://records.gimmel.build> and <https://company.sharepoint.com> is registered to <https://records.gimmel.cloud>

Registering the SharePoint App

For the SharePoint Online Connector (SPOC) to be able to connect to SharePoint Online using OAuth, the app identity needs to be registered with Microsoft Azure Access Control Service (ACS) and the SharePoint App Management Service of the tenancy. To register the app, perform the following steps:

1. Navigate to the following location: http://{your_sponline_url_to_any_sitecollection}/_layouts/15/appregnew.aspx

The following page displays, where you will provide the necessary configuration information described below.

The screenshot shows the 'Register an App' page in a SharePoint Online environment. The browser address bar displays the URL: https://rlion.sharepoint.com/sites/appdev4/_layouts/15/appregnew.aspx. The page title is 'Register an App'. The main content area is titled 'App Dev 4' and contains a form for creating a new app. The form includes the following fields and buttons:


- Client Id:** A text input field with a 'Generate' button.
- Client Secret:** A text input field with a 'Generate' button.
- Title:** A text input field.
- App Domain:** A text input field with an example: "www.contoso.com".
- Redirect URI:** A text input field with an example: "https://www.contoso.com/default.aspx".


At the bottom of the form, there are 'Create' and 'Cancel' buttons. The left sidebar shows navigation options: Home, Notebook, Documents, Documents2, Documents3, Apps in Testing, Samples, Developer Center, Recent, SharePoint Online Connector, and Site Contents.

- **Client ID:** Click **Generate** to automatically populate this value.
- **Client Secret:** Click **Generate** to automatically populate this value.
- **Title:** Enter the value of “SharePoint Online Connector”.
- **App Domain:** Enter the authority and port number portions of the exact URL to where the SharePoint Online Connector Web will be accessed; for example, spoc.domain.com⁷⁹:8084. If you are using the default HTTPS port (443) for your connector web, then you can omit it from the App Domain; for example, spoc.domain.com⁸⁰.

Redirect URL: Enter the exact, full URL to where the SharePoint Online Connector Web will be accessed; for example, <https://spoc.domain.com:8084>. If you are using the default port for HTTPS (443) for your connector web, then you can omit it from the Redirect URL; for example, <https://spoc.domain.com>.

 SharePoint Online requires the Redirect URL to be secured via HTTPS or you will not be able to successfully register the app. Unsecured (HTTP) redirect URLs are not supported.

 **Existing** Gimmel Cloud service customers (pre-Feb. 27th, 2021) should continue to use the existing URLs. **New** Gimmel Cloud service customers (post-Feb. 27th, 2021) should use the new URLs. Note: Existing customers already using the existing URL should not change to the new URLs as this may cause issues. See special instructions below...

 **EXISTING CUSTOMERS - SPECIAL INSTRUCTIONS IF YOU SUBSCRIBE TO OUR CLOUD SERVICE AND YOUR CONNECTOR IS HOSTED IN THE GIMMAL CLOUD**

- Your SharePoint Online Connector app should be configured in O365 exactly as follows for a TEST tenant (<https://test.recordlion.net>⁸¹):
App Domain: test-conn-spo.recordlion.net⁸²
Redirect URL: <https://test-conn-spo.recordlion.net>⁸³
- Your SPOC app should be configured in O365 exactly as follows for a PRODUCTION tenant (<https://app.recordlion.net>⁸⁴):
App Domain: app-conn-spo.recordlion.net⁸⁵
Redirect URL: <https://app-conn-spo.recordlion.net>⁸⁶

 **EXISTING CUSTOMERS - SPECIAL INSTRUCTIONS FOR UNITED KINGDOM CLIENTS WHO SUBSCRIBE TO OUR CLOUD SERVICE AND YOUR CONNECTOR IS HOSTED IN THE GIMMAL CLOUD**

- Your SharePoint Online Connector app should be configured in O365 exactly as follows for a TEST tenant (<https://testuk.recordlion.net>⁸⁷):

⁷⁹ <http://spoc.domain.com>

⁸⁰ <http://spoc.domain.com>

⁸¹ <https://testuk.recordlion.net>

⁸² <http://testuk-conn-spo.recordlion.net>

⁸³ <https://testuk-conn-spo.recordlion.net>

⁸⁴ <https://uk.recordlion.net>

⁸⁵ <http://uk-conn-spo.recordlion.net>

⁸⁶ <https://uk-conn-spo.recordlion.net>

⁸⁷ <https://test.recordlion.net>

App Domain: testuk-conn-spo.recordlion.net⁸⁸

Redirect URL: <https://testuk-conn-spo.recordlion.net>⁸⁹

- Your SPOC app should be configured in O365 exactly as follows for a PRODUCTION tenant (<https://uk.recordlion.net>⁹⁰):

App Domain: uk-conn-spo.recordlion.net⁹¹

Redirect URL: <https://uk-conn-spo.recordlion.net>⁹²

! NEW CUSTOMERS - SPECIAL INSTRUCTIONS IF YOU SUBSCRIBE TO OUR CLOUD SERVICE AND YOUR CONNECTOR IS HOSTED IN THE GIMMAL CLOUD

- Your SharePoint Online Connector app should be configured in O365 exactly as follows for a TEST tenant (<https://records.gimmel.build>):

App Domain: spo-records.gimmel.build⁹³

Redirect URL: <https://spo-records.gimmel.build>

- Your SPOC app should be configured in O365 exactly as follows for a PRODUCTION tenant (<https://records.gimmel.cloud>):

App Domain: spo-records.gimmel.cloud⁹⁴

Redirect URL: <https://spo-records.gimmel.cloud>

! NEW CUSTOMERS - SPECIAL INSTRUCTIONS FOR UNITED KINGDOM CLIENTS WHO SUBSCRIBE TO OUR CLOUD SERVICE AND YOUR CONNECTOR IS HOSTED IN THE GIMMAL CLOUD

- Your SharePoint Online Connector app should be configured in O365 exactly as follows for a TEST tenant (<https://records.uk.gimmel.build>):

App Domain: spo-records.uk.gimmel.build⁹⁵

Redirect URL: <https://spo-records.uk.gimmel.build>

- Your SPOC app should be configured in O365 exactly as follows for a PRODUCTION tenant (<https://records.uk.gimmel.cloud>):

App Domain: spo-records.uk.gimmel.cloud⁹⁶

Redirect URL: <https://spo-records.uk.gimmel.cloud>

! NEW CUSTOMERS - SPECIAL INSTRUCTIONS FOR CANADIAN CLIENTS WHO SUBSCRIBE TO OUR CLOUD SERVICE AND YOUR CONNECTOR IS HOSTED IN THE GIMMAL CLOUD

- Your SPOC app should be configured in O365 exactly as follows for a PRODUCTION tenant (<https://records-ca.gimmel.cloud>):

App Domain: spo-records-ca.gimmel.cloud⁹⁷

Redirect URL: <https://spo-records-ca.gimmel.cloud>

⁸⁸ <http://test-conn-spo.recordlion.net>

⁸⁹ <https://test-conn-spo.recordlion.net>

⁹⁰ <https://app.recordlion.net>

⁹¹ <http://app-conn-spo.recordlion.net>

⁹² <https://app-conn-spo.recordlion.net>

⁹³ <https://spo-records.gimmel.build>

⁹⁴ <https://spo-records.gimmel.cloud>


⁹⁵ <https://spo-records.uk.gimmel.build>

⁹⁶ <https://spo-records.uk.gimmel.cloud>


⁹⁷ <https://spo-records-ca.gimmel.cloud>

Prior to clicking **Create** in the next step, copy the Client ID and Client Secret to a file because they will be used when installing the Web and Services components of the SharePoint Online Connector. This file **must** be stored in a secure location so it can be referenced for future upgrades.

2. Make note of the Client ID and Client Secret in a secure location as they will be used when installing the Web and Services components of the SharePoint Online Connector.

 Failure to make note of the Client ID and Client Secret will require you to regenerate them before installing the connector.

3. Click Create to complete the registration process.


 Following the registration process, the Client Secret that is generated is only good for **one year**, and will need to be replaced by generating a new Client Secret for the corresponding Client ID. For information on how to renew a client secret, see [Renewing a Client Secret](#)

Creating the SharePoint App Catalog

To enable an App Package to be deployed to SharePoint Online, you must create the App Catalog where App Packages will be hosted and made available to each SharePoint Online Web. If this has not already been done for your tenancy, perform the following steps:

1. Open the SharePoint Online Admin Center.
2. Select “apps” from the left menu.
3. Click **App Catalog**, then click **OK** to accept the default option.
4. On the Create App Catalog Site Collection page, specify the Title and Address for your App Catalog, as well as any other options indicated.
5. Click **OK** to create the App Catalog.

6.14.10.3 SharePoint Online Connector On-Premise Only

 If you are setting up the SharePoint Online Connector using the Gimmel Cloud platform, skip the topics for SharePoint Online Connector On-Premise.

The SharePoint Online Connector enables Gimmel Records Management to manage the lifecycle of documents stored in SharePoint Online. It consists of the following components:

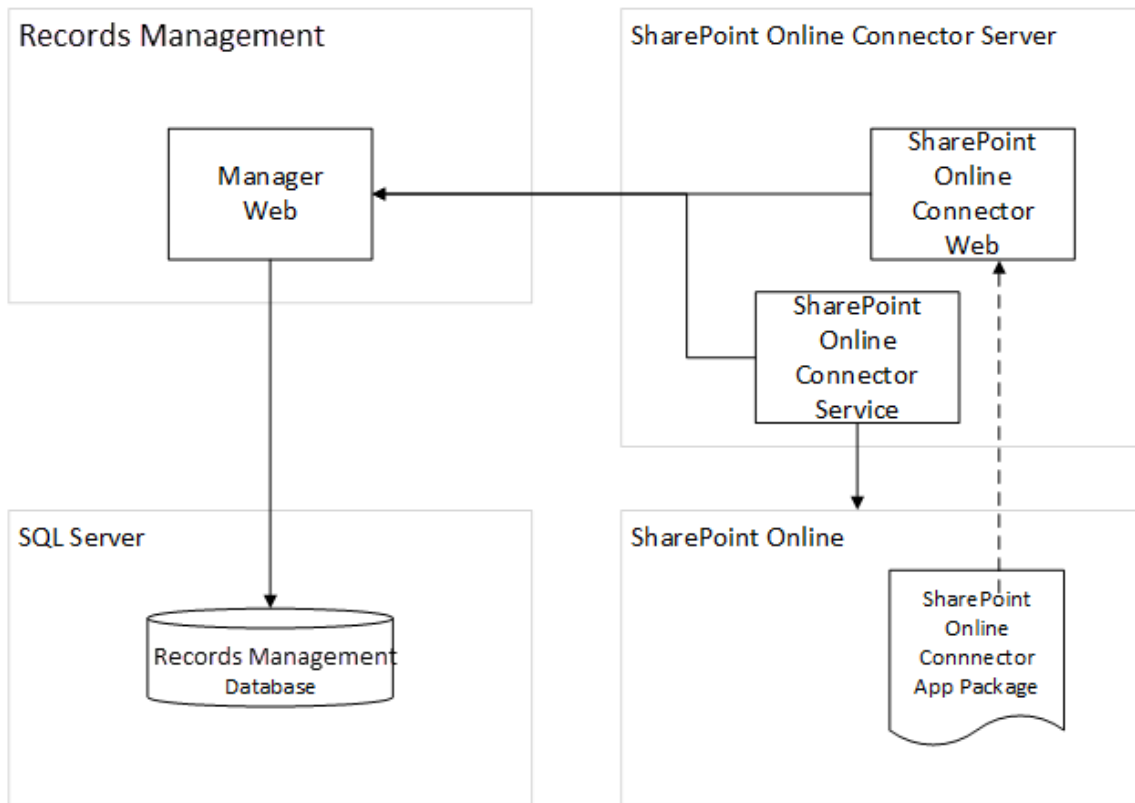
SharePoint Online Connector Web

When you install the SharePoint Online Connector (on-premises only), a Web Application is created, which provides the interface for registering a SharePoint Web with the SharePoint Online Connector as well as configuring the SharePoint Online Connector to communicate with Records Management.

SharePoint Online Connector Service

When you install the SharePoint Online Connector (on-premises only), a Windows Services called the SharePoint Online Connector Service is set up in Windows to perform the actions necessary to enable Records Management to manage the lifecycle of records and information stored in SharePoint Online.

SharePoint Online Architecture



Scalability

SharePoint Online Connector Web	
What comprises the solution...	<ul style="list-style-type: none"> • SharePoint App model <ul style="list-style-type: none"> • Provider-Hosted architecture • App redirects SharePoint Online to SharePoint Online Connector Web for configuration and registration • SharePoint Online Connector Service executes retention actions on items stored in SharePoint Online according to each item’s lifecycle • User interface components added to SharePoint Online are hosted by SharePoint Online Connector Web
How scaling works...	<ul style="list-style-type: none"> • App package is registered on every individual site, within the site collection • Once installed, every app must be registered with the Connector before it can "manage" the site
When to scale...	<ul style="list-style-type: none"> • When CPU utilization is consistently above 90% for extended durations, more cores should be added or new servers should be added to the load balancer • When Memory Pressure is consistently above 80% for extended durations, more memory should be added or new servers should be added to the load balancer

SharePoint Online Connector Web

General Sizing Guidelines...

- Should have at least 2 servers for failover

SharePoint Online Connect On-Premise Requirements

Before you install the Records Management SharePoint Online Connector (on-premises), verify that your system meets or exceeds the following requirements.

SharePoint Online Connector Server

	Core	Memory (MB)
Minimum	2	4096
Recommended	4	8192

- Windows Server 2012 or later (x64)
- Windows Server 2012 R2 or later (x64)
- .NET Framework 4.5 (x64)
- IIS 7+



Windows Server 2012 and later have TLS 1.2 installed and enabled by default.

On the server(s) hosting the SharePoint Online Connector, [several registry entries must be created](#)⁹⁸.

As a security best practice when using the .NET Framework, Gimmel recommends that you enable Transport Layer Security (TLS) 1.2, which provides communications security for client/server applications. To enable TLS 1.2, you must add the following Windows registry settings to the Records Management Core server(s) and the servers of any Records Management connectors you are using (if applicable), and then reboot your system.

- HKLM:\SOFTWARE\Microsoft\.NETFramework\v4.0.30319 "SchUseStrongCrypto"= dword:00000001
- HKLM:\SOFTWARE\Microsoft\.NETFramework\v4.0.30319 "SystemDefaultTlsVersions"= dword:00000001
- HKLM:\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319 "SchUseStrongCrypto"= dword:00000001
- HKLM:\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319 "SystemDefaultTlsVersions"= dword:00000001

Note that some operating systems require additional steps to enable TLS 1.2. For more information, see [Microsoft's TLS documentation](#)⁹⁹ To verify that your operating system supports TLS 1.2, read the [Support for TLS 1.2 section of Microsoft's documentation](#)¹⁰⁰.

Database Server

- SQL Server 2016 or greater

⁹⁸ <https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls#systemdefaulttlsversions>

⁹⁹ <https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls#systemdefaulttlsversions>

¹⁰⁰ <https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls#support-for-tls-12>


SharePoint Online Connector On-Premise Installation

Pre-Installation

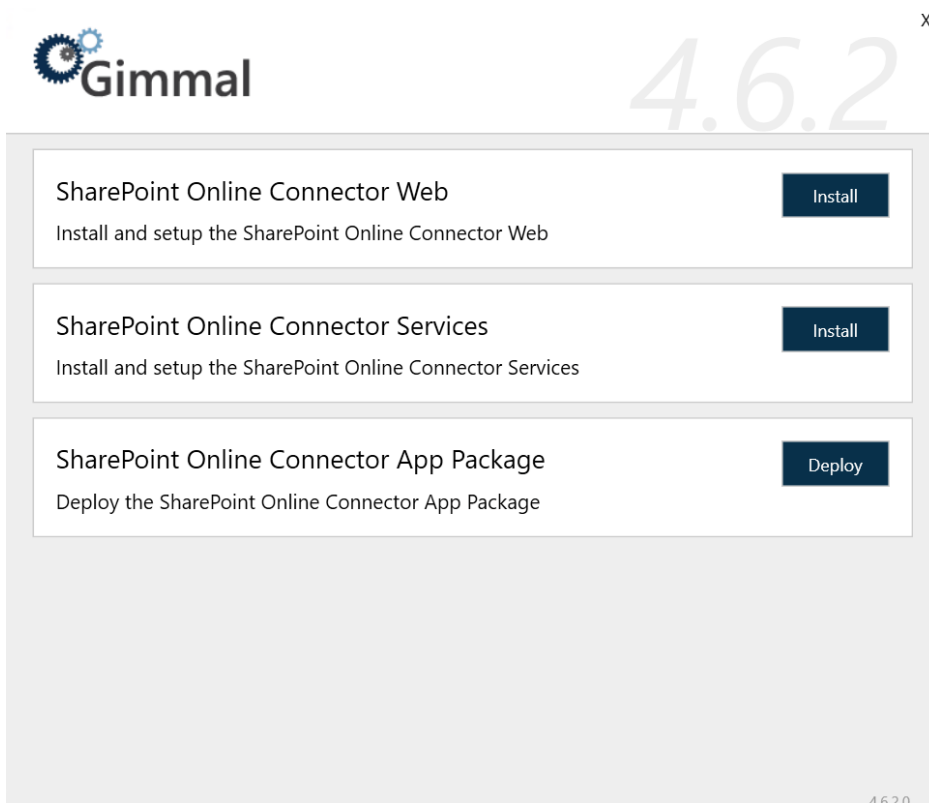
Configure Windows Roles and Features as follows:

- Role: Web Server
 - Role Services:
 - Static Content
 - Static Content Compression
 - Http Logging
 - Windows Authentication
 - ASP.NET 4.5
 - Management Tools

Installation

 Ensure that you run the installer as the Local Administrator. Each of these components can be installed on the same machine or on a separate machine for scale out scenarios.

Upon launching the SharePoint Online Connector installer, the following screen displays:

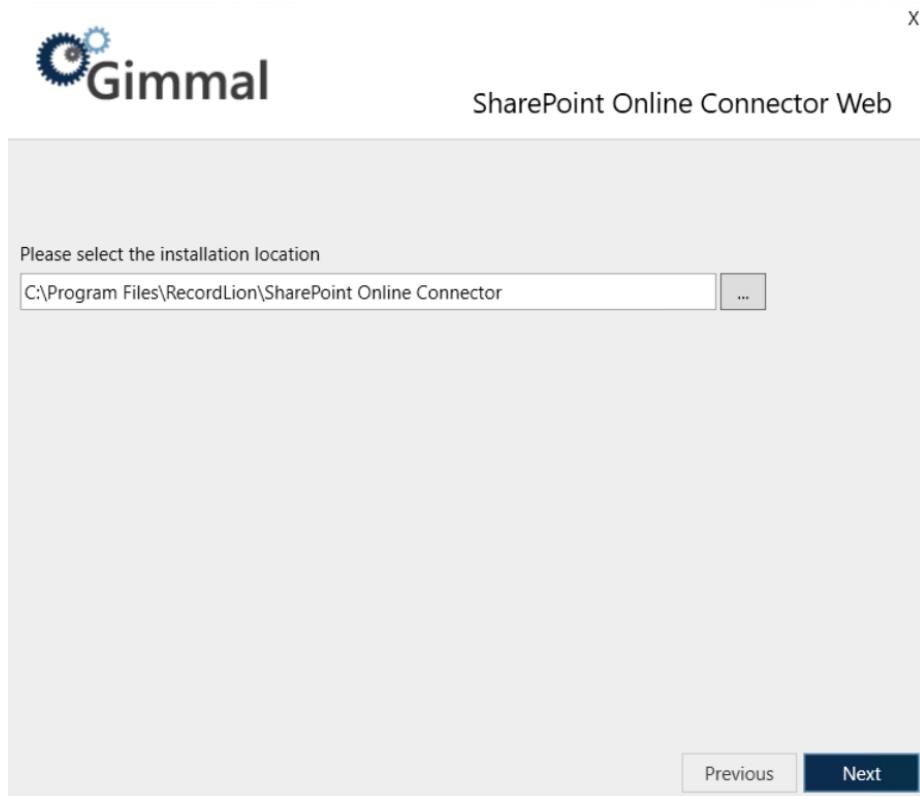


This screen presents each installable component that is a part of the SharePoint Online Connector. Click **Install** next to the component that you want to install. This will launch the specific installation wizard for that component.

Installing the SharePoint Online Connector Web

To install the SharePoint Online Web Connector, perform these steps:

1. On the SharePoint Online Connector installer, click **Install** to the right of the SharePoint Online Connector Web option. The first screen that displays is the Check for Prerequisites. This screen validates the following information before allowing the installation to proceed:
 - Current User is Local Administrator
 - IIS 7+ is Installed
2. Click **Next**. The installation location screen displays, which determines where the connector will be installed.



3. Leave the installation path as the default, or to change it, click the ... icon next to the installation location field, select the desired installation location and then click **Next**. The IIS Settings screen displays, where you will configure the IIS settings for the SharePoint Online Connector Web.

X

Gimmel SharePoint Online Connector Web

IIS Settings

Web Application Name: Web Application Port:

SSL Certificate:

Application Pool Account

Username: Password:

4. Enter the following information:

- **Web Application Name:** Determines what the respective site will be named in IIS
- **Web Application Port:** Determine what port the respective site will use in IIS
- **SSL Certificate:** Determines whether to create IIS bindings using SSL (*highly recommended) or without SSL

When you install the SharePoint Online Connector Web, a new Application Pool will be created that is used by the created web application. The following options specify which user account to use for this Application Pool. This should be a domain account.

- Username (ex. DOMAIN\Username)
- Password

5. Click **Next** to go the Database Settings screen, where you will configure the Database that will be used by the SharePoint Online Connector.



X

SharePoint Online Connector Web

Database Settings

Database Server	Database Name
<input type="text" value="2016SVR"/>	<input type="text" value="SPOnlineConnector"/>
<input checked="" type="checkbox"/> Automatically Create Database	<input type="checkbox"/> Use SQL Authentication
Username	Password
<input type="text"/>	<input type="text"/>

6. Enter the following information to determine the connection information that will be used by the SharePoint Online Connector to connect to SQL Server:

- **Database Server:** The name of the SQL Server Install (ex. SERVERNAME\InstanceName)
- **Database Name:** The name of the actual SQL Server Database
- **Use SQL Authentication:** Specifies that the connection information should use SQL Authentication with the Username and Password indicated below
- **Username:** The SQL Server username to use if SQL Authentication is specified
- **Password:** The SQL Server password to use if SQL Authentication is specified

If SQL Authentication is not specified, the connection information will use Windows Authentication by specifying a trusted connection. This means that the Application Pool account will be used to connect to SQL Server, therefore, this account will need the following database permissions. If SQL Authentication is specified, the SQL user will also require the following permissions.

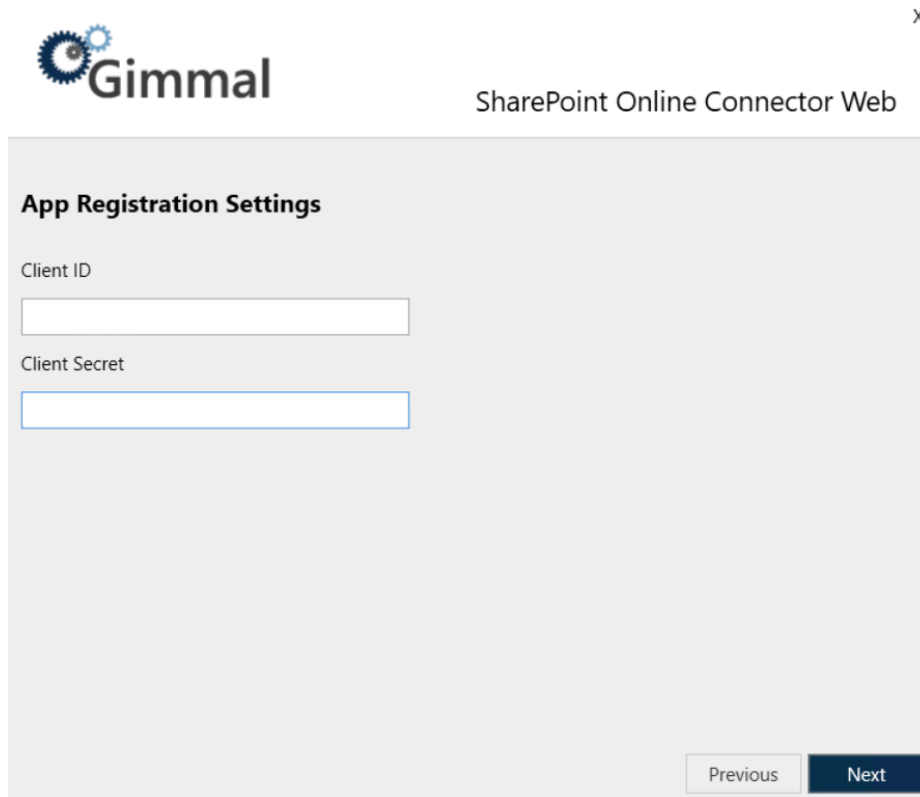
- **db_datareader**
- **db_datawriter**
- **GRANT EXECUTE** on all Stored Procedures
- **GRANT EXECUTE** on all Scalar User Defined Functions
- **GRANT SELECT** on all Table and Inline User Defined Functions

If Automatically Create Database is specified, the installation will automatically attempt to create the database using the Database Server and Database Name indicated. The appropriate account will also be automatically granted the appropriate rights to this database. **This option requires that the current user has permission to create databases and manage security in the SQL Server instance indicated.**

If Automatically Create Database is not specified, the installation will configure connection information but will not attempt to create the database. In this case, you will need to leverage the SQL Scripts at the following location (in the order listed) to manually create the database in the SQL Server instance indicated. You will also need to manually configure security as indicated above.

- %Install Path%\Web\Sql\RecordLion.RecordsManager.SPOnline.sql

- Click **Next** to go to the App Registration Settings screen, where you will enter the **Client ID** and **Client Secret** that were generated during [App Registration](#)(see page 341).



X

Gimmel

SharePoint Online Connector Web

App Registration Settings

Client ID

Client Secret

Previous Next

- Open the file where you saved the **Client ID** and **Client Secret** when you registered the SharePoint App and copy each value into the corresponding text fields.
- Click **Next**. The Installation screen displays. The progress bar indicates the current state of the installation.
- When the application is finished installing, click **Next**. The Finish screen indicates that everything installed successfully.
- Click **Finish** to close the installer.

Continue to the next topic to install the SharePoint Online Connector Service:

[Installing SharePoint Online Connector Services](#)(see page 351)

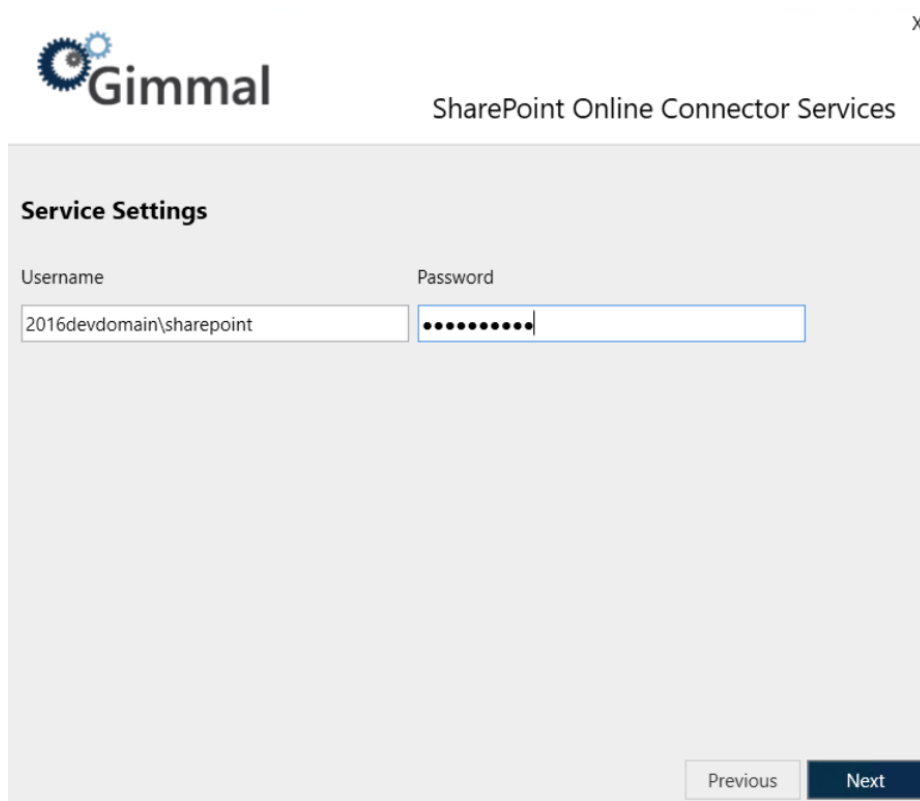
Installing SharePoint Online Connector Services

The SharePoint Online Connector Services is a Windows Service that manages the lifecycle of files for any SharePoint Online Site that has been registered from the SharePoint Online Connector Web. Without this component, files contained within a Site cannot be managed by Records Management. To install SharePoint Online Connector Services, perform these steps:

- On the SharePoint Online Connector installer, click **Install** to the right of the SharePoint Online Connector Services option. The first screen that displays is the Check for Prerequisites. This screen validates the following information before allowing the installation to proceed:
- Click **Next**. The installation location screen displays, which determines where the connector will be installed.



3. Leave the installation path as the default, or to change it, click the ... icon next to the installation location field, select the desired installation location and then click **Next**. The Service Settings screen displays, where you will configure the settings for the SharePoint Online Connector Services.



The screenshot shows a window titled "SharePoint Online Connector Services" with the Gimmel logo in the top left. Below the title bar is a "Service Settings" section. It contains two input fields: "Username" with the text "2016devdomain\sharepoint" and "Password" with masked characters. At the bottom right of the settings area are two buttons: "Previous" and "Next".

When SharePoint Online Connector Services is installed, a Windows Service is created. The following settings specify which user account to use to execute this Windows Service.

- **Username** (Ex. DOMAIN\Username)
- **Password**

The user account should be a domain account and must have the following file system permissions, which are granted during installation:

- Read/Write: %Install Path%\Logs

4. Click **Next** to continue to the Database Settings screen, where you will configure database settings for the SharePoint Online Connector Services.

X



SharePoint Online Connector Services

Database Settings

<p>Database Server</p> <input style="width: 90%;" type="text" value="2016SVR"/>	<p>Database Name</p> <input style="width: 90%;" type="text" value="SPOneConnector"/>
<input checked="" type="checkbox"/> Automatically Create Database	<input type="checkbox"/> Use SQL Authentication
<p>Username</p> <input style="width: 90%;" type="text"/>	<p>Password</p> <input style="width: 90%;" type="text"/>

5. Enter your settings based on the descriptions below. You should use the same options you used when configuring the SharePoint Online Connector Web

The following options determine the connection information that will be used by the SharePoint Online Connector to connect to SQL Server.

- **Database Server:** The name of the SQL Server Install (ex. SERVERNAME\InstanceName)
- **Database Name:** The name of the actual SQL Server Database
- **Use SQL Authentication:** Specifies that the connection information should use SQL Authentication with the Username and Password indicated below
- **Username:** The SQL Server username to use if SQL Authentication is specified
- **Password:** The SQL Server password to use if SQL Authentication is specified

If SQL Authentication is not specified, the connection information will use Windows Authentication by specifying a trusted connection. This means that the Service account will be used to connect to SQL Server, therefore, this account will need the following database permissions. If SQL Authentication is specified, the SQL user will also require the following permissions.

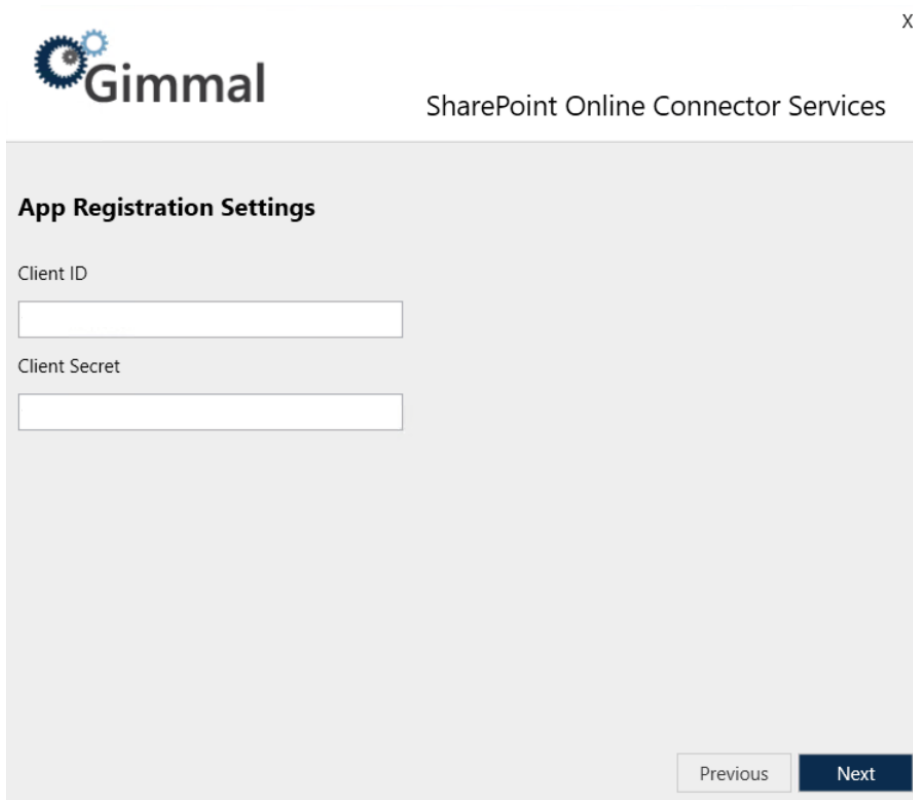
- **db_datareader**
- **db_datawriter**
- **GRANT EXECUTE** on all Stored Procedures
- **GRANT EXECUTE** on all Scalar User Defined Functions
- **GRANT SELECT** on all Table and Inline User Defined Functions

If **Automatically Create Database** is specified, the installation will automatically attempt to create the database using the Database Server and Database Name indicated. The appropriate account will also be automatically granted the appropriate rights to this database. This option requires that the current user has permission to create databases and manage security in the SQL Server instance indicated.

If **Automatically Create Database** is **not** specified, the installation will configure connection information but will not attempt to create the database. In this case, you will need to leverage the SQL Scripts at the

following location (in the order listed) to manually create the database in the SQL Server instance indicated. You will also need to manually configure security as indicated above.


- %Install Path%\Service\Sql\RecordLion.RecordsManager.SPOnline.sql
6. Click **Next** to go to the App Registration Settings screen, where you will enter the **Client ID** and **Client Secret** that were generated during App Registration.




The screenshot shows a window titled "Gimmel SharePoint Online Connector Services". Inside the window, the heading "App Registration Settings" is displayed. Below the heading, there are two text input fields: "Client ID" and "Client Secret". At the bottom right of the window, there are two buttons: "Previous" and "Next".

7. Open the file where you saved the **Client ID** and **Client Secret** when you registered the SharePoint App and copy each value into the corresponding text fields.
8. Click **Next**. The Installation screen displays. The progress bar indicates the current state of the installation.
9. When the application finishes installing, click **Next** to continue to the Finish screen. This screen indicates that the application installed successfully.
10. Click **Finish** to close the installer screen.

6.14.10.4 Uploading SharePoint Online Connector App Package

 Ensure that the account used to connect to the SharePoint Online App Catalog does **NOT** use multi-factor authentication. If you upload the SharePoint Online Connector App Package using multi-factor authentication, the upload will fail.

 The installer, which deploys the app package, needs to be run from a machine where TLS 1.2 is enabled.

To install the SharePoint Online Connector to a specific SharePoint Web, you need to upload the App Package to the SharePoint Online App Catalog, which makes it available to the Web for installation.

1. To upload the SharePoint Online Connector App Package, enter the necessary deployment settings, and then click **Next**.

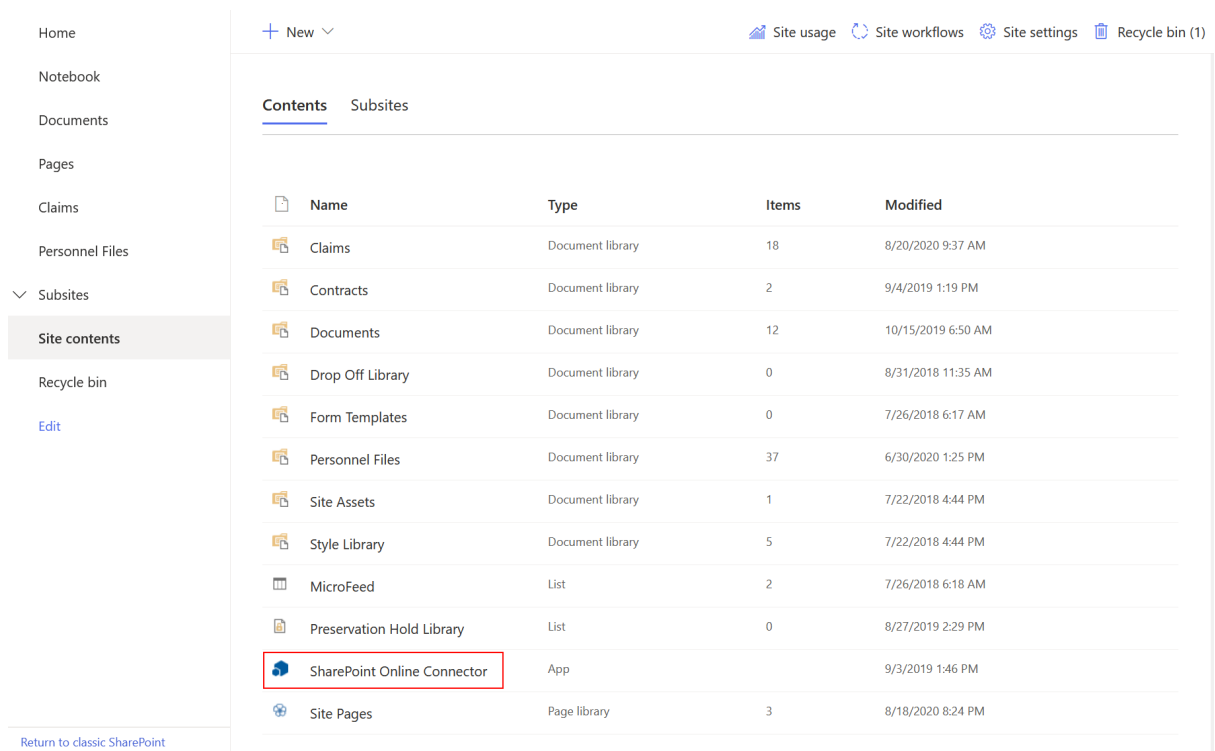
- **Connector Web URL:** The URL to the SharePoint Online Connector Web
 - **App Catalog URL:** The URL to the SharePoint Online App Catalog
 - **Client ID:** The Client ID that was generated during section 5.1.1
 - **SharePoint Online Username:** Used to connect to SharePoint Online
 - **SharePoint Online Password:** Used to connect to SharePoint Online
2. Click **Next**. The App Package will be uploaded to the SharePoint Online App Catalog you specified above.

6.14.10.5 SharePoint Online Connector Configuration

Connection

Once you install the SharePoint Online Connector, you must direct the Connector to the location of Records Management. To do so, perform the following steps:

1. Browse to a SharePoint Site that has the connector installed and open the Site Contents page.



2. Select the SharePoint Online Connector to open the SharePoint Online Connector Web and ensure that you're on the **Connection** tab.

SharePoint Online Connector

Connection Jobs Transfers Workflows Unregister

Return to SharePoint

Connection Configuration


Manager Web URL Test

Username

Password

Save

3. Enter the URL to the Manager Web.
4. Enter the Username* of the [Service Account](#)(see page 248) created in Records Management.
5. Enter Password of the [Service Account](#)(see page 248) created in Records Management. (The password has a maximum length of 18 characters)
6. Click **Save**.

 The Service Account username format depends on whether or not you are connecting to the Gimmal Cloud for Records Management. If the Gimmal Cloud is being used, the username format is: {service account name}@{tenant domain} (e.g. spocservice@gimmal.com¹⁰¹, or fscservice@companyname.com¹⁰²), otherwise, the format is just: {service account name}.

Timer Jobs

When you install the SharePoint Online Connector, there are a number of Timer Jobs that are created. These are necessary for the SharePoint Online Connector to perform its duties. These Timer Jobs are registered with and executed by the SharePoint Online Connector Service. See the following table for a list of the timer jobs and a description.

¹⁰¹ <mailto:spocservice@gimmal.com>

¹⁰² <mailto:fscservice@companyname.com>

Timer Job Type	Description
Gimmel Full Classification Job	<p>The Full Classification job crawls every file contained within SharePoint Online sites, or Webs, enabled for Records Management, and notifies Records Management of their existence.</p> <p>This job is typically executed upon initial setup of the SharePoint Online Connector. Although it can be scheduled to run on a regular basis, note that it can put considerable strain on the SharePoint servers.</p> <p>When enabling a new Web for Records Management, or if full crawls need to be more granular due to farm size, at these times you would respectively manually run or schedule the Full Classification job.</p>
Gimmel Incremental Classification Job	<p>The Incremental Classification job synchronizes all file changes that have occurred within SharePoint Online Webs enabled for Records Management. Keeping the schedule on this job as small as possible will reduce the amount of work that must be performed on each execution and will ultimately put less strain on the SharePoint servers.</p>

Timer Job Type	Description
Gimmal Retention Job	<p>The Retention job processes approved retention actions for SharePoint Online items after they have been approved from Records Management. As the Retention job completes the processing of retention actions, it notifies Records Management of the completion status. The job's status is shown in the Pending Automation section.</p> <div data-bbox="347 566 1385 1361" style="border: 1px solid black; padding: 10px;"> <p>Edit Job Schedule</p> <p>Retention</p> <p> <input checked="" type="radio"/> Minutes Every <input type="text" value="10"/> minute(s) <input type="radio"/> Hourly <input type="radio"/> Daily <input type="radio"/> Weekly <input type="radio"/> Monthly <input type="radio"/> Monthly by Day </p> <hr/> <p><input type="checkbox"/> Disabled</p> <hr/> <p><input type="checkbox"/> Discard check-outs when deleting documents</p> <hr/> <p style="text-align: right;"> <input type="button" value="Save"/> <input type="button" value="Cancel"/> </p> </div> <p><i>Discard Check-outs When Deleting Documents</i></p> <p>This is a tenant level setting, configurable by the administrator for the Retention Job Schedule. You must enable this feature in order to discard check-outs when deleting documents. This option is off by default.</p>

Default Timer Job Schedules

These job schedules are the optimized intervals for this timer job, and changing them could affect the overall performance of Gimmal Records Management functions.


Job	Schedule
Gimmal Full Classification Job	Monthly
Gimmal Incremental Classification Job	Every 5 Minutes

Job	Schedule
Gimmel Retention Job	Every 5 Minutes

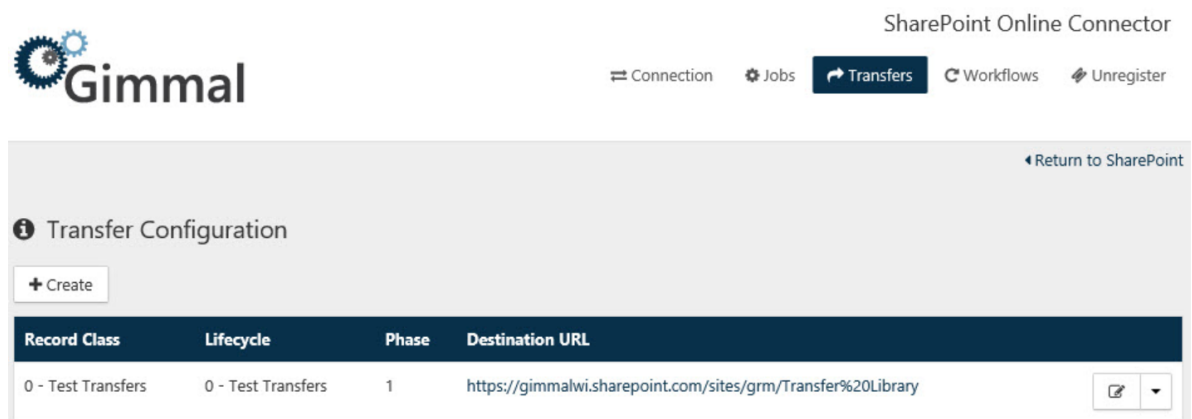
Transfer

When a lifecycle in Records Management contains a Transfer Action, the SharePoint Online Connector requires that an Administrator configure the repository-specific destination of the transfer for items contained within the repository. This tells the Connector where to put the files when it sees that it needs to execute a Transfer Action for an item. This step is optional unless you have configured a Transfer Action (Transfer or Dispose and Transfer) in your File Plan. To set up a transfer destination, perform the following steps:

1. Open the SharePoint Online Connector app by navigating to the site contents of the site where it is deployed.

 The site collection you launch the SharePoint Online Connector app from is the context for the SharePoint Online Connector. Changes you make to the Transfer Configuration will only apply to the site collection in context.

2. Click **Transfers**



SharePoint Online Connector

Connection Jobs **Transfers** Workflows Unregister

Return to SharePoint

Transfer Configuration

+ Create

Record Class	Lifecycle	Phase	Destination URL
0 - Test Transfers	0 - Test Transfers	1	https://gimmelwi.sharepoint.com/sites/grm/Transfer%20Library

3. Click **+ Create** on the Transfer Configuration page. The Create Transfer Configuration dialog opens.

Create Transfer Configuration
✕

Record Class ▼

Lifecycle

Phase ▼

Destination URL

Retain Directory Structure ▼

Create
Cancel

4. Select the Record Class and Retention Phase for which you would like to configure the transfer destination.
5. Provide the destination URL for the Site Collection location in SharePoint.
6. Choose whether to "Retain Directory Structure".
7. Click **Create**

i When configuring a transfer destination, in the rare circumstance that a Drop-Off Library is used as the destination and there are no matching Routing Rules for the document, the document will remain in the Drop-Off Library but will only be visible to the Farm Account due to the way that Drop-Off Libraries were designed. Cross-site collection transfers are not currently supported by the SharePoint Online Connector. This means you cannot transfer an item from one site collection to another. Only transfers within the same site collection are supported.

⚠ The transfers you have configured here only apply to the site collection in context. This site collection in context is determined from which site collection the SharePoint Online Connector app was launched.

Workflow


! Workflow Actions are not supported in SharePoint Online. They are supported in SharePoint on-premises only.

Register

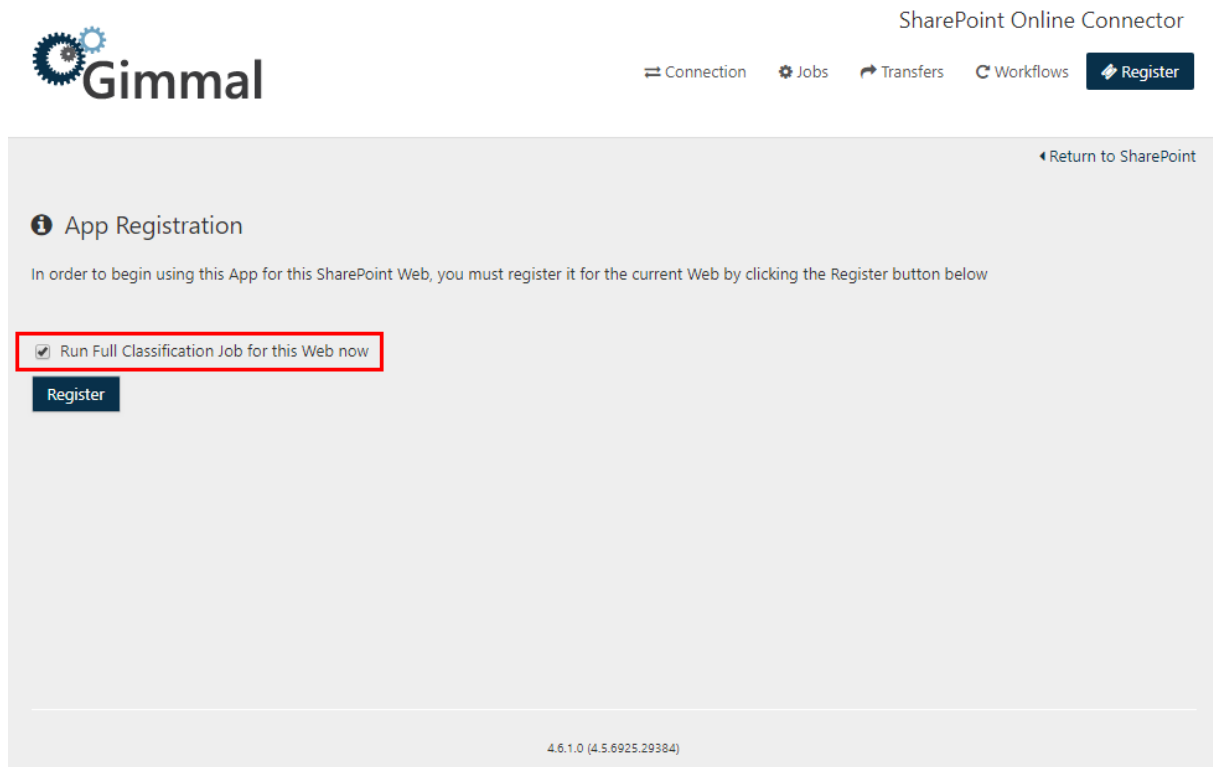
To register an app with a SharePoint Online Web (Site) perform the following steps:


1. Select Register on the top menu

2. Check to run Full Classification job for this web now

 Selecting the "Run Full Classification Job for this Web now" checkbox to limit the full classification job so that it runs for **just** this individual Web (instead of running the job for all Webs). This will improve processing performance.

3. Click the **Register** button. This notifies the SharePoint Online Service that this Web is being managed, and enables you to begin using this app for this SharePoint Web.



 If you need to unregister or rename the URL of a Web (SharePoint site), follow the directions on the topic [\(5.2.3\) Unregistering a SharePoint App from an Individual Web](#) (see page 363).

6.14.10.6 Renewing a Client Secret

Microsoft provides [documentation for replacing an expiring or expired client secret in a SharePoint Add-ins](#)¹⁰³, and it should always be the primary source of instructions for updating a client secret. This help page will serve as a guide to updating the client secret but we rely mainly on [Microsoft's Client secret documentation](#)¹⁰⁴ since this

¹⁰³ <https://docs.microsoft.com/en-us/sharepoint/dev/sp-add-ins/replace-an-expiring-client-secret-in-a-sharepoint-add-in>

¹⁰⁴ <https://docs.microsoft.com/en-us/sharepoint/dev/sp-add-ins/replace-an-expiring-client-secret-in-a-sharepoint-add-in>

entire process is controlled by Microsoft and Gimmel is not responsible for the validity and accuracy of instructions over its lifetime.

See the following sections to renew your client secret for the on-premises and Gimmel Cloud versions of the SharePoint Online Connector.

On-Premises


To renew a client secret for SharePoint Online Connector.on-premises, you must execute the following PowerShell Command on the SharePoint Online Connector Server, as shown below:

```
$secret = New-SPOClientSecret
Set-ServicePrincipalClientSecret -ClientId { Your Client Id} -ClientSecret $secret
Set-SPOConnectorService -ClientId { Your Client Id} -ClientSecret $secret
Set-SPOConnectorWeb -SiteName "SPOnline Connector Web" -ClientId { Your Client Id} -
ClientSecret $secret
```

Gimmel Cloud

To renew a client secret for SharePoint Online Connector in the Gimmel Cloud, there are some steps you must perform in addition to the steps listed in Microsoft's documentation.

1. Perform the steps in [Microsoft's client secret documentation](#)¹⁰⁵ to renew the client secret. Note the important sections on how to find out a client secret's expiration date, and how to create a client secret that is valid for three years.
2. Make note of your Client Secret value.
3. Submit a [Gimmel Support ticket](#)¹⁰⁶, providing the Client Secret value that you generated in step 1. (Gimmel Support must perform some additional steps to complete the renewal of your client secret.)

 For additional information on renewing a client secret, including how to create a new client secret, how to extend an existing client secret, and how to use the Gimmel Extend Client Secret Script, see the following [Knowledge Base article](#)¹⁰⁷ located at the Gimmel Support site.

6.14.10.7 Unregistering a SharePoint App from an Individual Web

If you plan on removing a SharePoint app from an individual Web, Gimmel recommends that you first unregister the SharePoint app from the Web. If you don't unregister, the app will remain in the list of apps for this Web, and the Incremental and Full Classification jobs will include this app in their crawls, and populate the SharePoint Online Connector logs with errors.

To unregister an app, perform these steps:

1. Navigate to the Web, and open the app from Site Contents. The SharePoint Online Connector configuration screen displays.

¹⁰⁵ <https://docs.microsoft.com/en-us/sharepoint/dev/sp-add-ins/replace-an-expiring-client-secret-in-a-sharepoint-add-in>

¹⁰⁶ <https://support.gimmel.com/hc/en-us>

¹⁰⁷ <https://support.gimmel.com/hc/en-us/articles/360022551712-Extending-Expired-Client-Secret-for-SharePoint-Online-Add-Ins>

SharePoint Online Connector

Connection Configuration

Manager Web URL Test

Username

Password

Save

Return to SharePoint

2. Click **Unregister**. The app is now unregistered from the Web

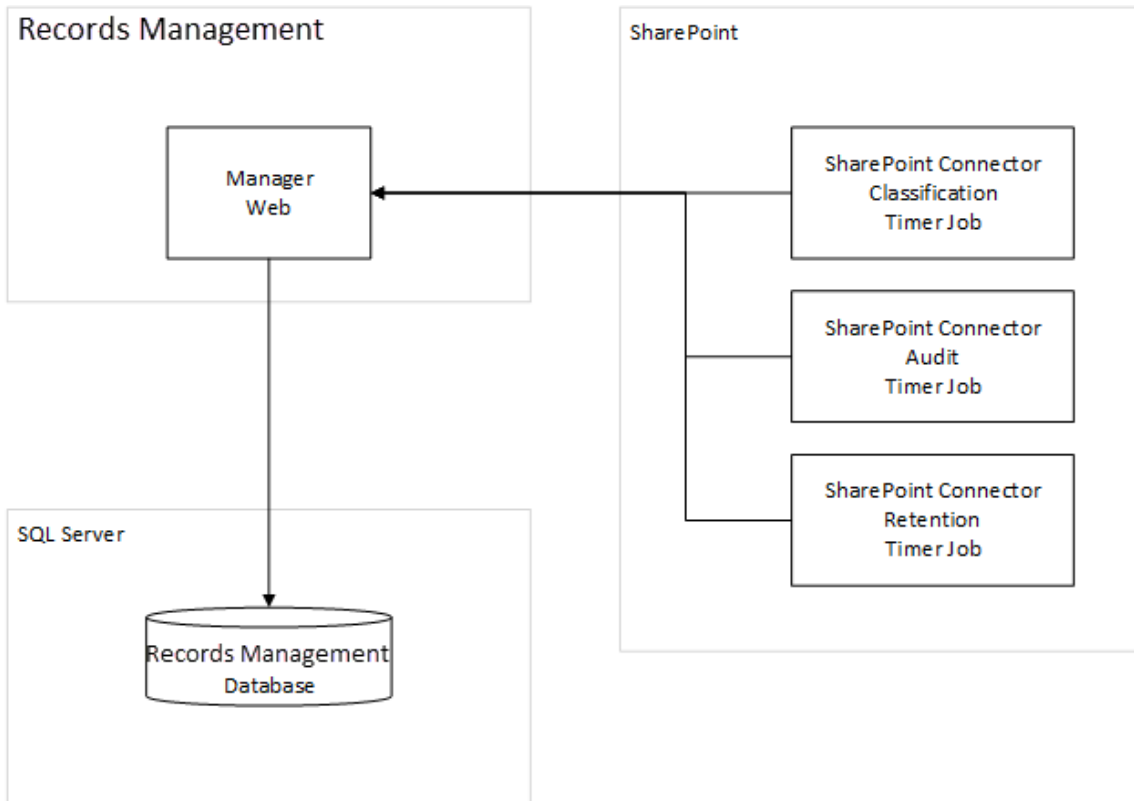
6.14.11 SharePoint Server Connector

The SharePoint Connector enables Records Management to manage the lifecycle of documents stored in on-premise SharePoint 2016 and SharePoint 2019.

This section describes how to install and configure the SharePoint Connector.

! If your SharePoint environment makes use of Alternate Access Mappings, please note that the SharePoint Connector uses the Default Zone Url to locate documents. Changes to the SharePoint Default Zone Url after deployment of the SharePoint Connector are not supported.

6.14.11.1 Architecture



6.14.11.2 Scalability

What comprises the solution...	<ul style="list-style-type: none"> • .NET-based SharePoint Solution Package • Solution installs multiple SharePoint timer jobs • Timer jobs synchronize metadata and audit log information with items stored in SharePoint with Core Platform • Timer jobs execute retention action items stored in SharePoint according to each item’s lifecycle • User interface components added to SharePoint Layouts directory to support integration
How scaling works...	<ul style="list-style-type: none"> • Multiple instances of SharePoint can be load balanced • Will scale in accordance with the scaling of the SharePoint farm
When to scale...	<ul style="list-style-type: none"> • Scale SharePoint farm according to Microsoft Recommended Guidelines and your unique environment needs
General Sizing Guidelines...	<ul style="list-style-type: none"> • Follow Microsoft capacity planning guidelines for SharePoint https://technet.microsoft.com/en-us/library/ff758645(v=office.15).aspx

6.14.11.3 Additional Topics

[SharePoint Server Connector Installation](#)

[Configure SharePoint Server](#)

[SharePoint Server Connector Configuration](#)

[SharePoint Server Connector Requirements](#)

6.14.11.4 SharePoint Server Connector Installation

Launching the SharePoint Connector Installer


The SharePoint Server Connector must be installed on a SharePoint Application Server, the same server that hosts Central Administration.

Installing the SharePoint Connector

The SharePoint Connector component enables Records Management to manage the lifecycle of documents stored within SharePoint 2016 or SharePoint 2019. The Connector also integrates with the SharePoint user interface to allow direct interaction with Records Management as though it were a part of SharePoint.

To install the SharePoint Connector, perform these steps:

1. From the Records Management splash screen, click the **Install SharePoint Connector** link. The SharePoint Connector installation screen displays.
2. Click **Install** to the right of the SharePoint Connector option. The first screen that displays is the check for prerequisites. This screen validates the following information before allowing the installation to proceed:
 - SharePoint is installed
 - Current user is Local Administrator
 - Current user is a SharePoint Farm Administrator
3. Click **Next**. The Installed screen displays.
4. Click **Next** to complete the installation.
5. When the application finishes installing, the Finish screen displays. This indicates that everything installed successfully.

 If you experience any errors during the installation process, refer to the installer log in your Windows Temp folder.

6. Click Finish to close the installer screen.
7. After the installation has completed and the solution has been deployed to SharePoint, you must perform the following steps within SharePoint:
 - Open **Central Administration**.
 - Navigate to **Central Administration > System Settings > Manage Farm Solutions**.
 - Select the solution: .recordsmanager.sharepoint.wsp.
 - Click **Deploy Solution**.
 - Specify When and Where to Deploy the Solution.
 - Default settings of Now and All Content Web Applications should suffice.

- Click **OK**.
 - When the solution is finished deploying, its status will be indicated in **Central Administration > System Settings > Manage Farm Solutions**.

Deploy Solution

Solution Information

Information on the solution you have chosen to deploy.

Name: recordlion.recordsmanager.sharepoint.wsp

Locale: 0

Deployed To: None

Deployment Status: Not Deployed

Deploy When?

A timer job is created to deploy this solution. Please specify the time at which you want this solution to be deployed.

Choose when to deploy the solution:

Now

At a specified time:

11/26/2013  2 PM  00 

Deploy To?

The solution contains Web application scoped resources and should be deployed to specific Web applications. Please choose the Web application where you want the solution to be deployed.

Choose a Web application to deploy this solution:

All content Web applications 

Warning: Deploying this solution will place assemblies in the global assembly cache. This will grant the solution assemblies full trust. Do not proceed unless you trust the solution provider.

OK

Cancel

Important Note for Least Privileged Installations

The Records Management installation is designed to automatically configure SharePoint during the solution deployment. This design has the benefit of requiring little intervention by the setup user across a large farm. However, this design does require that you perform additional steps in a least privileged installation of SharePoint.

In a least privileged installation of SharePoint, the farm account is typically not a local machine administrator. The farm account is the Windows user account running the SharePoint timer service (SPTimerV4) and the SharePoint Central Administration IIS application pool. **Note:** The farm account is also known as the database account.

If the farm account is not a local machine administrator when deploying the solution, then the farm account will not be able to copy files needed for the Central Administration web site. This can result in an error message similar to,

“Could not find any resources appropriate for the specified culture or the neutral culture” when accessing the Records Management pages in Central Administration.

The **first workaround** is to grant the farm account membership to the local machine administrators group for each Central Administration or web front end server in the farm. This workaround is only necessary during the deployment phase of the installation. The **second workaround** requires the use of the STSADM utility. The utility is typically located in the following directory:

- %ProgramFiles%\Common Files\Microsoft Shared\Web Server Extensions\15\Bin

From an elevated command prompt, execute the following STSADM command:

- STSADM.exe -o CopyAppBinContent

You will be notified that one of these workarounds is required if you receive the following error when attempting to access the SharePoint Connector pages within Central Administration:

Sorry, something went wrong

Could not find any resources appropriate for the specified culture or the neutral culture. Make sure "Resources.RLGlobalization.SPResources.resources" was correctly embedded or linked into assembly "App_GlobalResources.olenbgrt" at compile time, or that all the satellite assemblies required are loadable and fully signed.

[TECHNICAL DETAILS](#)

[GO BACK TO SITE](#)

In order for the SharePoint Server connector to work, you will need to configure SharePoint Server and the SharePoint Server connector. The following topics will walk you through those steps:

[\(5.2.4\) Configure SharePoint Server](#)(see page 368)

[\(5.2.4\) SharePoint Server Connector Configuration](#)(see page 371)

6.14.11.5 Configure SharePoint Server

Configure for SharePoint 2016 or 2019

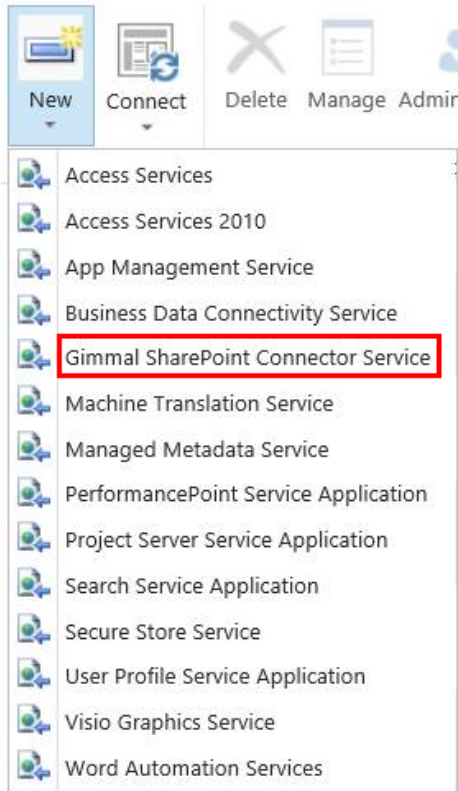
To finish installing the SharePoint Connector, you must perform the following steps:

1. After the solution has been deployed, you must activate SharePoint Connector Farm Feature by performing the following steps:
 - **Open Central Administration.**
 - Navigate to **Central Administration > System Settings > Manage Farm Features.**
 - Find the SharePoint Connector Feature and click **Activate.**

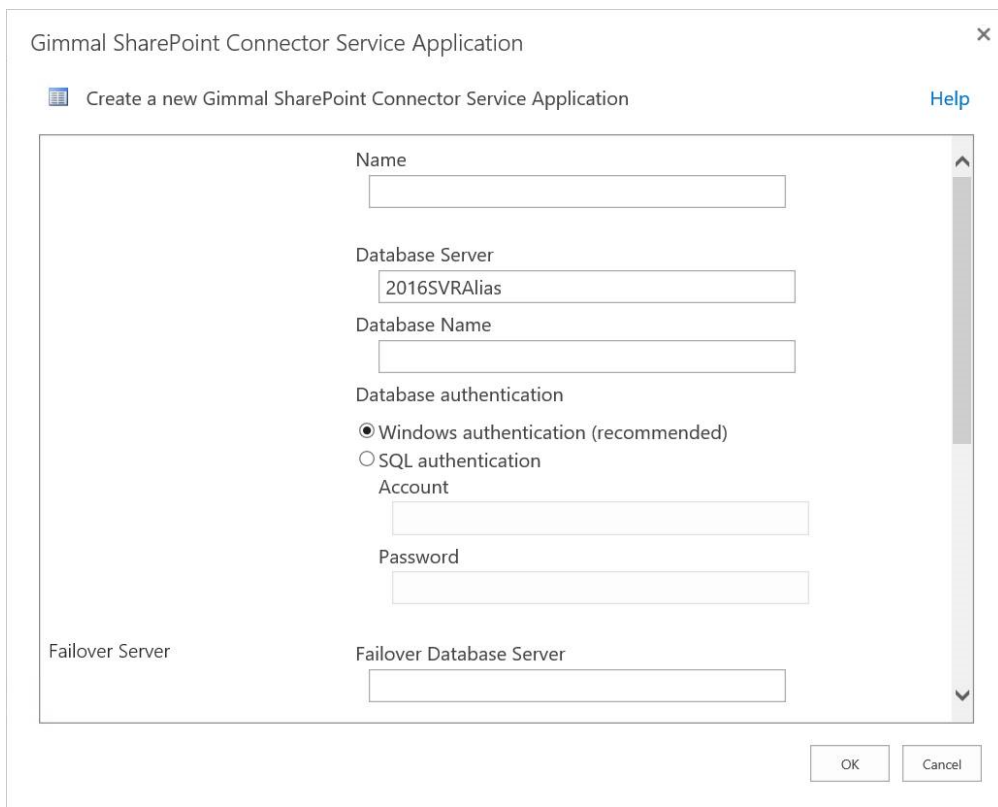


2. Next, you must create a Gimmel SharePoint Connector Service Application. To do this, perform the following steps:

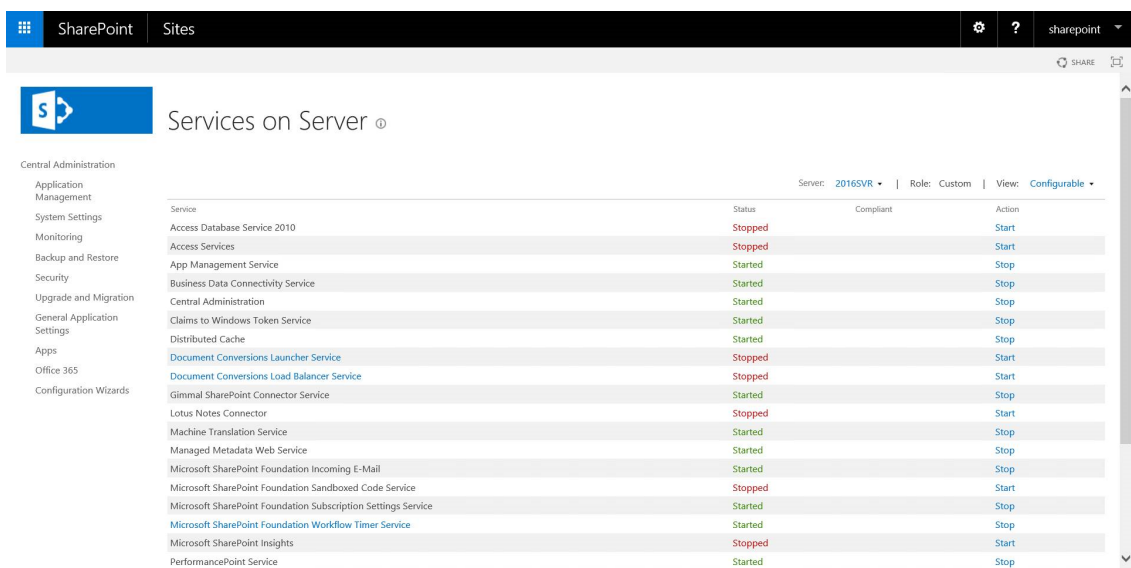
- **Open Central Administration.**
- Navigate to **Central Administration > Application Management > Manage Service Applications.**
- From the **New** option in the ribbon, choose **Gimmel SharePoint Connector Service.**



- Provide the requested information to create the Service Application. (**Important!** A unique name is required for the **Database Name** setting.)



- Click **OK**.
- 3. After you create the Gimmel SharePoint Connector Service Application, you must start the Gimmel SharePoint Connector Service on each SharePoint Server that should process Gimmel SharePoint Connector Timer Jobs. To do this, perform the following steps:
 - **Open Central Administration.**
 - Navigate to **Central Administration > System Settings > Manage Services on Server.**
 - Select the Server in which you want to start the service.
 - Click **Start** on the row provider for the Gimmel SharePoint Connector Service.



4. After starting the Gimmal SharePoint Connector Service, you must configure the Connector to communicate with Information Lifecycle. To do this, perform the following steps:
 - **Open Central Administration.**
 - Navigate to **Central Administration > Application Management > Manage Service Applications.**
 - Select the **Gimmal SharePoint Connector Service Application.**
 - From the Ribbon, click **Manage.**
 - Click **Configure Connection.**
 - Enter the following information:
 - URL to Information Lifecycle (ex. https://server:8080)
 - Records Management Service Account ([Service accounts are created in Records Management Core](#)(see page 258))
 - Password for Service Account
 - Click **OK.**

6.14.11.6 SharePoint Server Connector Configuration

The first step in configuring the SharePoint Connector involves enabling Site Collections for Records Management. The SharePoint Connector works by monitoring files within SharePoint and reporting those changes back to Records Management. Only Site Collections that have been enabled will be managed by Records Management.

To enable a Site Collection, perform the following actions in SharePoint:

1. Open the root site of a SharePoint Site Collection.
2. Navigate to **Site Settings > Site Collection Administration > Site Collection Features.**
3. Activate the SharePoint Connector Integration feat



! Using the built-in SharePoint Records Management Features when the Records Management Site Collection Integration Feature is enabled is NOT SUPPORTED. These Features must be deactivated to ensure that Records Management can effectively manage the records and information in the Site Collection.

The following search configurations must be made to allow Records Management the ability to manage content:

- Within Site Settings - 'Allow this site to appear in search results' must be set to **'Yes'**.
- Within Library Settings - 'Allow items from this document library to appear in search results' must be set to **'Yes'**.

SharePoint Server Timer Jobs

When you install the SharePoint Connector, there are a number of Timer Jobs that are created. These are necessary for the SharePoint Connector to perform its duties. See the following table for a list of the timer jobs and a description.

Timer Job Type	Description
Records Management Audit Job	The Records Management Audit Job synchronizes the SharePoint audit log with the Records Management audit log. For each type of SharePoint audit enabled, this job will send any captured audits from SharePoint to Records Management to provide a single audit log for a managed file.
Records Management Farm Deployment Job	The Records Management Farm Deployment Job pushes required program files to servers in the SharePoint Farm. When a new server is added to the Farm, this job will ensure that all program files are added to the new server.
Records Management Full Classification Job	<p>The Records Management Full Classification Job crawls every file contained within SharePoint site collections enabled for Records Management and notifies Information Lifecycle of their existence.</p> <p>This job is typically executed upon initial setup of the SharePoint Connector. Although it can be enabled to run on a regular basis, it is disabled by default as it can put a considerable load on the SharePoint Farm.</p> <p>When enabling a new site for Records Management, at that time you will want to run the Full Classification Job.</p>
Records Management Incremental Classification Job	The Records Management Incremental Classification Job synchronizes all file changes that have occurred within SharePoint site collections enabled for Records Management.
Records Management Retention Job	The Records Management Retention Job processes approved retention actions for SharePoint items after they have been approved from Records Management. As the Retention Job completes the processing of retention actions, it notifies Records Management of the completion status. The job's status is shown in the Pending Automation section.
Records Management System Job	The Records Management System Job processes lock and unlock actions for SharePoint items as directed by Records Management. As the System Job completes the processing of retention actions, it notifies Records Management of the completion status.

Default Timer Job Schedules


These job schedules are the optimized intervals for this timer job, and changing them could affect the overall performance of Gimmel Records Management functions. The following table lists the default Timer Job schedules.

Job	Schedule
Records Management Audit Job	Every 5 Minutes
Records Management Farm Deployment Job	Daily between 00:30:00 and 00:30:00

Job	Schedule
Records Management Full Classification Job	Disabled (Monthly - 1st Monday at 00:00:00)
Records Management Incremental Classification Job	Every 2 Minutes
Records Management Retention Job	Daily between 20:00:00 and 23:59:00
Records Management System Job	Every 2 Minutes

SharePoint Server UI Integration

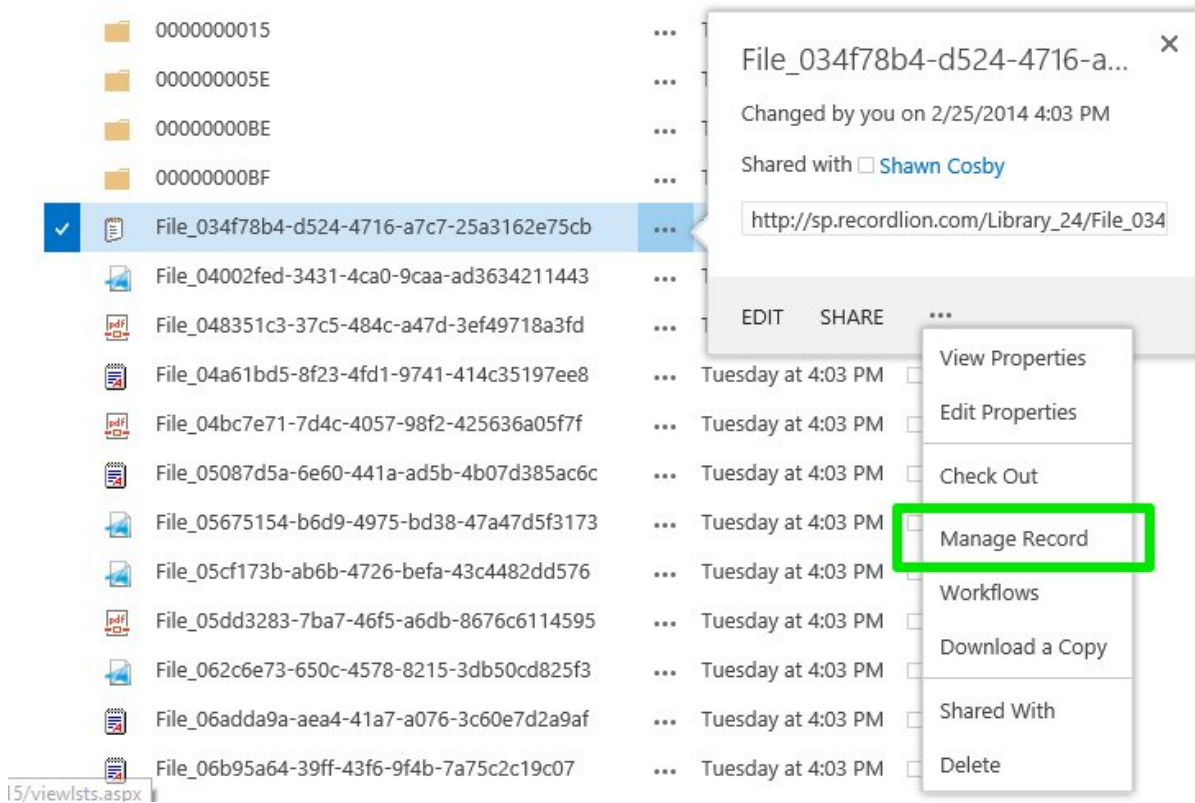
Enabling UI Integration with Records Management

 Activating SharePoint Connector UI Integration will remove the Compliance Details option from SharePoint. Deactivate this Site Collection Feature to bring back the Compliance Details button.

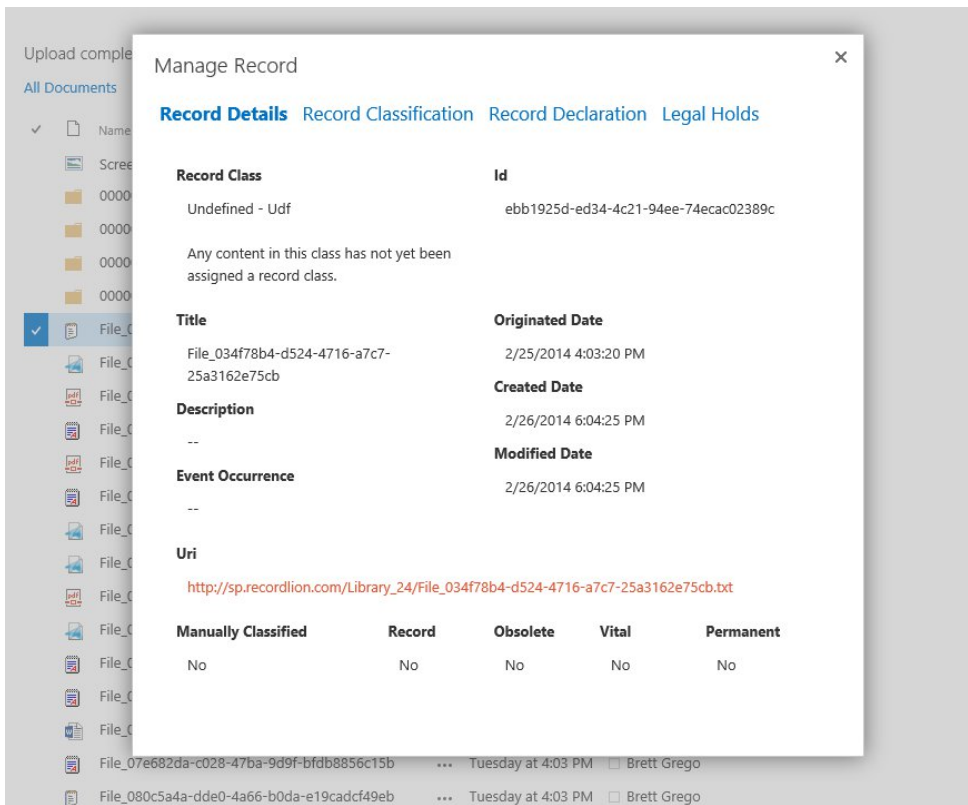
After enabling a Site Collection for Records Management, the lifecycle for all of the documents contained within the Site Collection will be managed by Records Management. However, there will not be any way to interact with Records Management from SharePoint without activating the SharePoint Connector UI Integration Feature within SharePoint. To enable user interface integration with Records Management from a SharePoint Site Collection, perform the following steps in SharePoint:

1. Open the root site of a SharePoint Site Collection.
2. Navigate to Site Settings->Site Collection Administration->Site Collection Features.
3. Activate the SharePoint Connector UI Integration feature.

Once you enable this feature, each Document Library within the Site Collection will have the **Manage Record** option added to its Edit Control Block.



The **Manage Record** option enables you to perform many of the functions that are provided by Information Lifecycle for an individual file directly from the SharePoint interface. For more information, see (Link) Connector Integration Overview.



Directing the SharePoint Server Connector to Records Management

After you install the SharePoint Connector, you must direct the Connector to the location of Records Management. To do so, perform the following steps:

- Open SharePoint Central Administration.
- Go to **Manage Service Applications > Gimmel SharePoint Connector**.
- Select Configure Connection.

SharePoint Sites

SharePoint Connector ⓘ

Central Administration

- Application Management
- System Settings
- Monitoring
- Backup and Restore
- Security
- Upgrade and Migration
- General Application Settings
- Apps
- Office 365
- Configuration Wizards

Server URL

http://server:8080

Credentials

Service

••••••••••

Advanced

Batch Size

50

Client Timeout (Minutes)

10

Max Queue Length

5

Job Scope

WebApplication ▼

Cancel OK

- Enter the following information:
 - Server URL to Information Lifecycle Manager Web (ex. <http://server:8080>)
 - Username* for the [Service Account](#)¹⁰⁸ (Service Account is created in Records Management)
 - Password for the [Service Account](#)¹⁰⁹
 - Batch Size
 - Client Timeout in minutes.
 - Max Queue Length
 - Job Scope
- Click OK. (Credentials will be validated.)

¹⁰⁸ <http://docs.gimmel.com/en/3517-creating-a-service-account.html>

¹⁰⁹ <http://docs.gimmel.com/en/3517-creating-a-service-account.html>

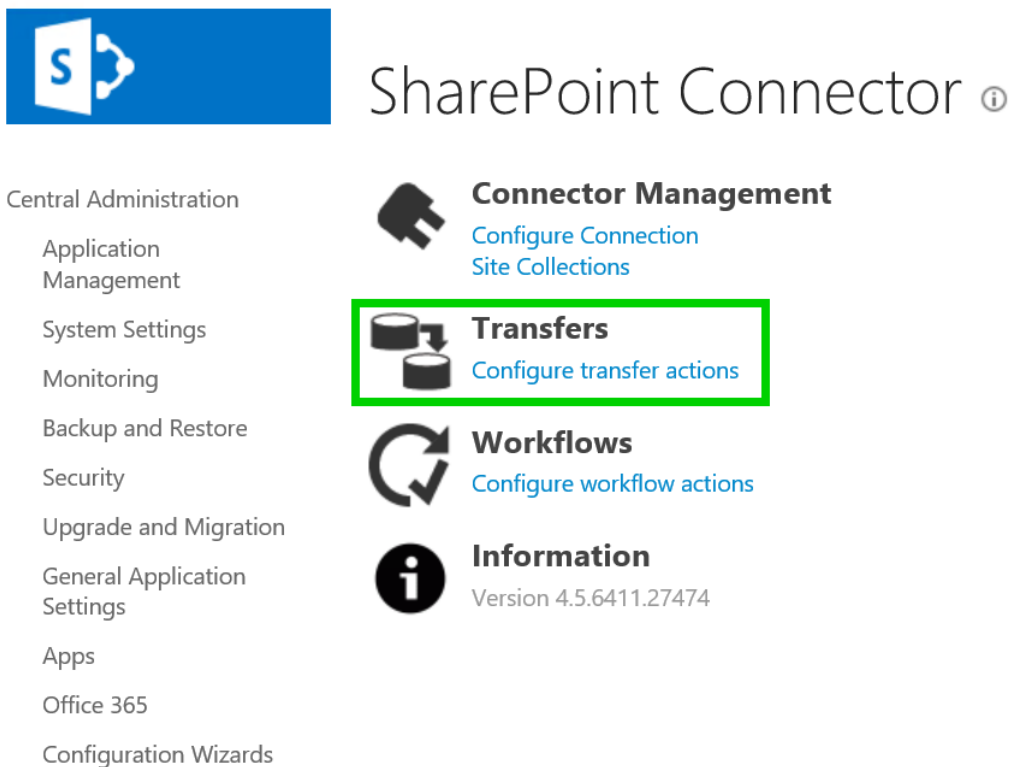
i The Service Account username format depends on whether or not you are connecting to the Gimmel Cloud for Records Management. If the Gimmel Cloud is being used, the username format is: {service account name}@{tenant domain} (e.g. spocservice@gimmel.com¹¹⁰, or fscservice@companyname.com¹¹¹), otherwise, the format is just: {service account name}.

Creating Transfer and Workflow Actions

Configuring Transfer Actions

When a lifecycle in Records Management contains a Transfer Action, the Connector requires that an Administrator configure the repository-specific destination of the transfer for items contained within the repository. This tells the Connector where to put the files when it sees that it needs to execute a Transfer Action for an item. This step is optional unless you have configured a Transfer Action (Transfer or Dispose and Transfer) in your File Plan. To set up a transfer destination, perform the following steps:

1. Open SharePoint Central Administration.
2. From the Application Management section, click **Manage Service Applications > Gimmel SharePoint Connector**.
3. On the SharePoint Connector page, click **Configure transfer actions** from the Transfers section.

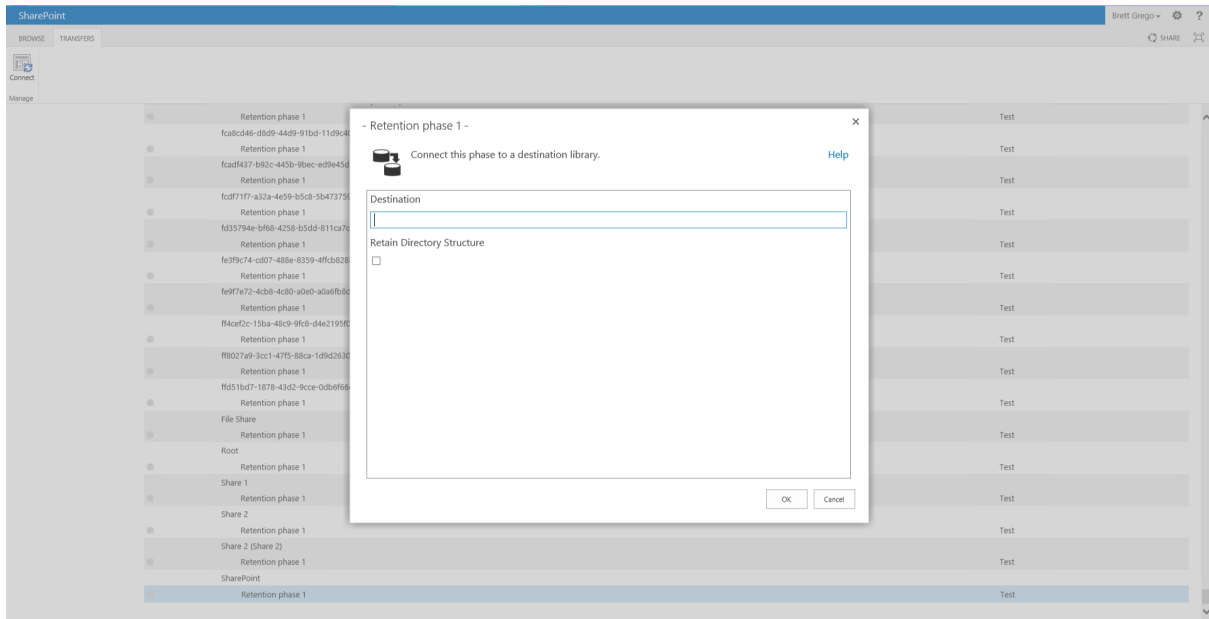


4. Select the Retention Phase for the Record Class in which you would like to configure the transfer destination.

¹¹⁰ <mailto:spocservice@gimmel.com>

¹¹¹ <mailto:fscservice@companyname.com>

5. Click **Connect** from the ribbon.



6. Provide the destination URL for Site Collection location in SharePoint.

7. Choose whether to "Retain Directory Structure".

8. Click **OK**

! When configuring a transfer destination, in the rare circumstance that a Drop-Off Library is used as the destination and there are no matching Routing Rules for the document, the document will remain in the Drop-Off Library but will only be visible to the Farm Account due to the way that Drop-Off Libraries were designed.

Configuring Workflow Actions

When a lifecycle in Records Management contains a Workflow Action, the Connector requires that an Administrator configure the repository-specific Workflow to initiate items contained within the repository. This tells the Connector which Workflow to initiate for files when it sees that it needs to execute a Workflow Action for an item.


i Workflow Actions work in SharePoint on-premises only; they are not supported in SharePoint Online.

This step is optional unless you have configured a Workflow Action in your File Plan. To set up a Workflow to initiate, perform the following steps:

1. Open SharePoint Central Administration.
2. Select the **Gimmel Records Management** menu option.
3. Select **Configure Workflow Actions** from the Workflows section.



4. Select the Retention Phase for the Record Class in which you would like to configure the Workflow to initiate.
5. Click **Connect** from the Ribbon.
6. Choose the appropriate Workflow Association Type.
7. Enter the name of your SharePoint Workflow Association.
8. Click **OK**

 To start a Workflow Action, the Connector must be able to find the SharePoint Workflow Association as configured. For example, if a SharePoint Web's Workflow Association Collection does not have a Workflow Association matching the configured name, then no Workflow Action can be started.

Workflow Association Types

Association Type	Description
Web	Workflow Name should refer to a Workflow associated with the File's parent Web
List	Workflow Name should refer to a Workflow associated with the File's parent Library
Content Type	Workflow Name should refer to a Workflow associated with the File's assigned Content Type
Custom	Allows a custom Workflow Initiator to be selected. Workflow Name should refer to a Workflow that the Custom Workflow initiator understands

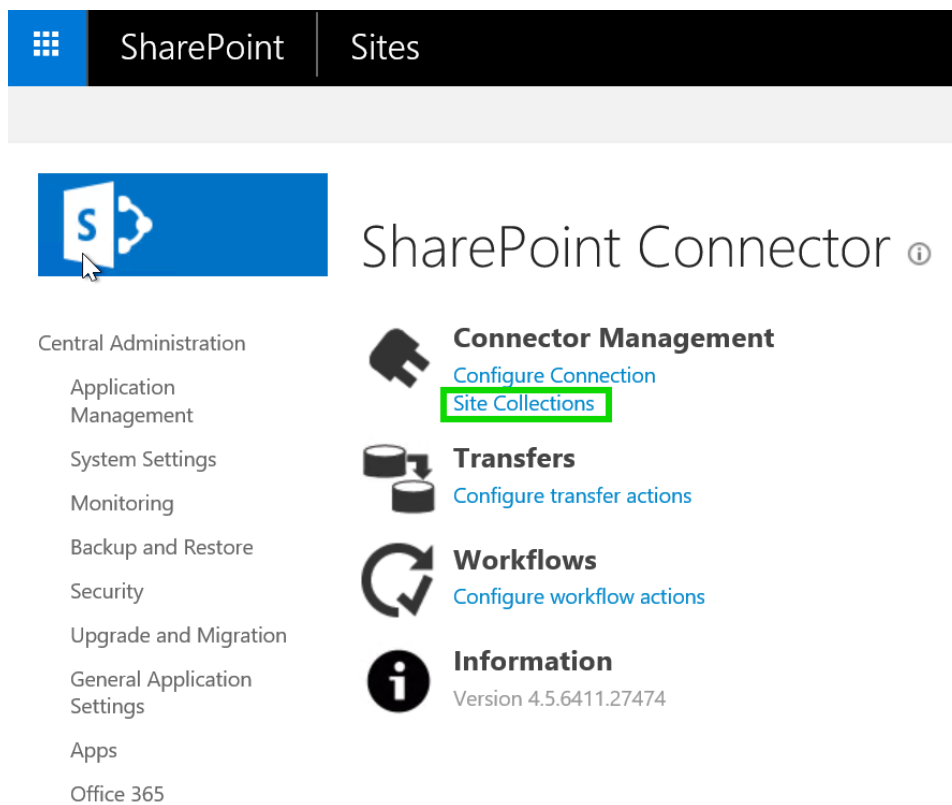
Configuring a New Site Collection

Every enabled site collection must be crawled, whether fully or incrementally. However, because there is only one Full Classification timer job, one Incremental Classification timer job, and one Retention timer job serving the Farm, each newly enabled site collection rolls up under, and becomes managed by, those singular timer jobs. It is important that each time a new site collection is enabled that a Full Classification be manually run.

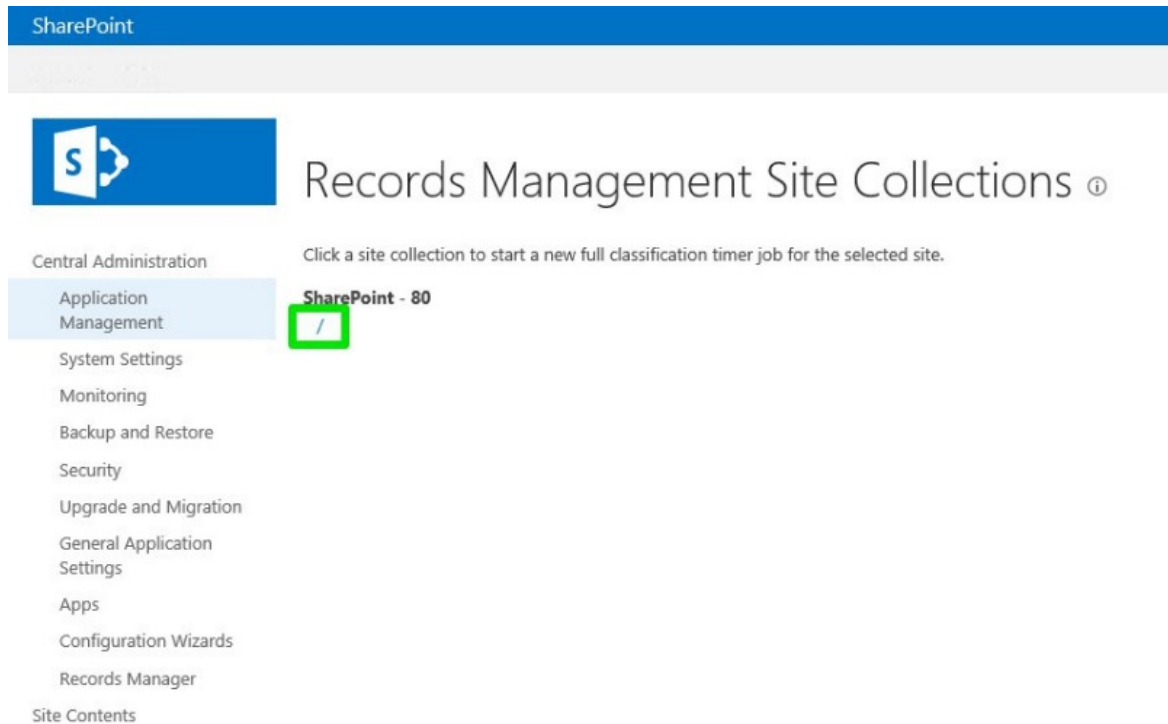
 Manually running any of these timer jobs does not affect the run schedule already set.

To do a full crawl on a newly enabled site collection, perform the following steps:

1. Open SharePoint Central Administration.
2. Go to **Manage Service Applications > Gimmel SharePoint Connector**.
3. Select Site Collections from the Connector Management section.



- Click the Site Collection that you would like to submit to the full crawl.



Uninstall SharePoint Server Connector

To ensure a clean uninstall of the SharePoint Connector, perform the following steps:

SharePoint 2016 and above

- Open SharePoint Management Shell.
- Import the Gimmel SharePoint Connector PowerShell Module (see PowerShell Section).
- Execute `Remove-RecordsManagerServices` to delete and unregister any Gimmel SharePoint Connector Service Applications.
- Open **Central Administration**.
- Navigate to **Central Administration > System Settings > Manage Farm Features**.
- Deactivate the **Gimmel SharePoint Connector** feature.
- Navigate to **Central Administration > System Settings > Manage Farm Solutions**.
- Click `recordsmanager.sharepoint.wsp`.
- Select **Retract Solution** and click **OK**.
- Click `recordsmanager.sharepoint.wsp`.
- Select **Remove Solution** and click **OK**.
- Open Services MMC.
- Right-click **SharePoint Timer Service** and choose **Restart**.
- Right-click **App Fabric Caching Service** and choose **Restart**.
- Open a command prompt.
- Execute command `IIS Reset`.
- Open directory `%windir%\assembly`.

18. Delete any assemblies beginning with RecordLion.RecordsManager...”.
19. Open directory %windir%\Microsoft.NET\assembly.
20. Delete any assemblies beginning with RecordLion.RecordsManager...”.

6.14.11.7 SharePoint Server Connector Requirements

Below are the system requirements for installing the SharePoint Server Connector in your environment. Note that the requirements are specifically **for the server that will have the Connector installed**. Please verify that the server in question meets these requirements.

SharePoint

- SharePoint Server 2016 + .NET 4.8
- SharePoint Server 2019 + .NET 4.8
- 100 MB Disk Space for Software

Database Server


- SQL Server 2016 or greater

6.14.12 Universal File Share Connector

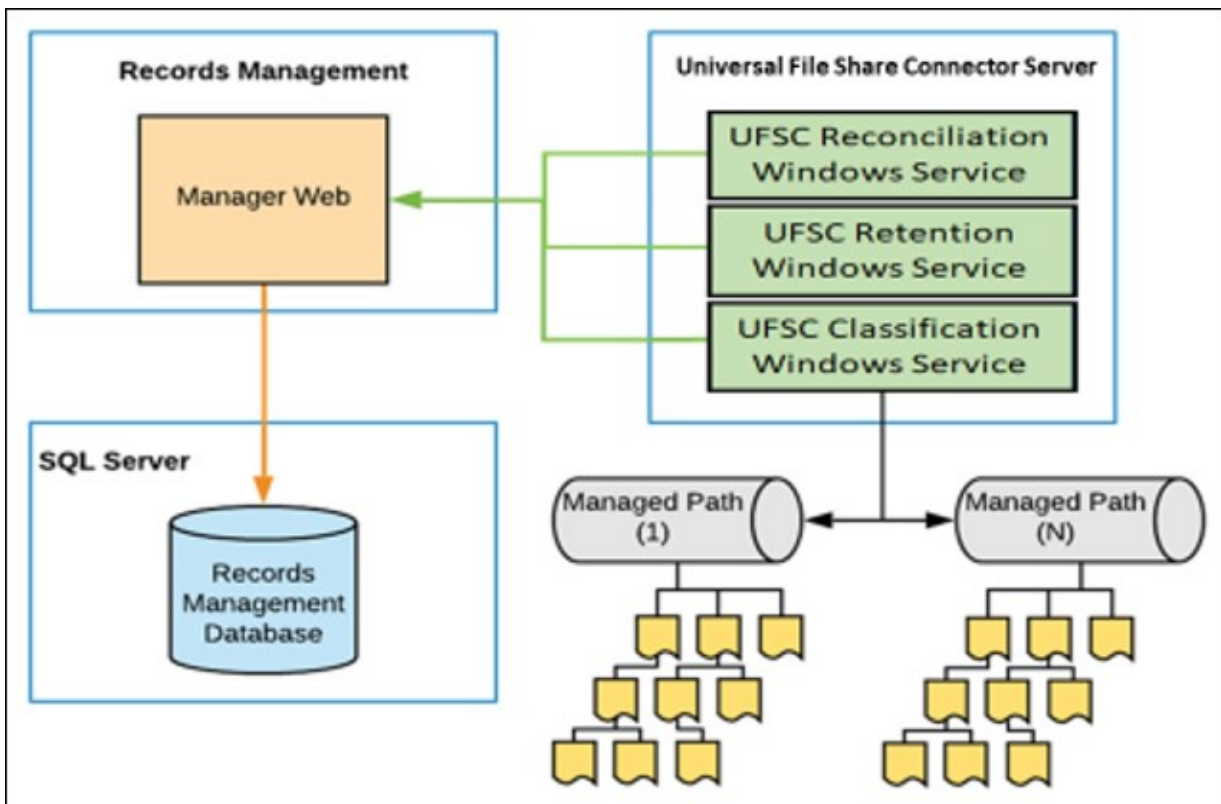
The Universal File Share Connector enables Records Management to manage the lifecycle of documents stored on network file shares.

For the Universal File Share Connector to be able to effectively manage network file shares, the file shares should be located within the same Local Area Network and, if possible, on the same machine where the Universal File Share Connector is installed.

The Universal File Share Connector can be used to crawl network file shares directly or network file shares from Gimmel Altitude. For more details.

 It is strongly recommended to discontinue the use of deprecated File Share Connector. Concurrent use of both the Universal File Share Connector and the original File Share Connector is not supported.

6.14.12.1 Universal File Share Connector Architecture




6.14.12.2 Scalability

<p>What comprises the solution...</p>	<ul style="list-style-type: none"> • .NET-based Windows Service for crawling and classification • .NET-based Windows Server for retention action execution • Services are configured by adding a list of file share paths to be managed
<p>How scaling works...</p>	<ul style="list-style-type: none"> • Each managed path represent a single application thread • Managed paths must not overlap • Application can be installed to multiple servers to form a cluster • Application supports fail-over, not load distribution • Managed paths can be divided among multiple clusters
<p>When to scale...</p>	<ul style="list-style-type: none"> • When CPU Utilization is consistently above 90% for extended periods, a new cluster should be created and managed paths should be divided among the available clusters • When Memory Pressure is consistently above 80% for extended periods, a new cluster should be created and managed paths should be divided among the available clusters

General Sizing Guidelines...	<ul style="list-style-type: none"> • $(\text{Total \# Files} / 10,000,000) = \text{\# Managed Paths}$ • $\text{Ceiling}(\text{\# Managed Paths} / 10) = \text{\# Servers}$
------------------------------	--

6.14.12.3 Universal File Share System Requirements

 The maximum number of characters allowed for a file path (file name + directory route) is **445**. For example "\\servername\root\childpath\filename.txt" is consider a file path.

Universal File Share Connector Server


Before you install the Records Management Universal File Share Connector, verify that your system meets or exceeds the following requirements.

	Cores	Memory (MB)
Minimum	4	4096
Recommended	8	8192

- Windows Server 2012 or later (x64)
- Windows Server 2012 R2 or later (x64)
- Windows Server 2016
- .NET Framework 4.5** (x64)
- .NET Desktop Runtime 3.1.x
- 100 MB Disk Space for Software

Database Server

- SQL Server 2016 or greater
- 100 MB for File Share Connector Database

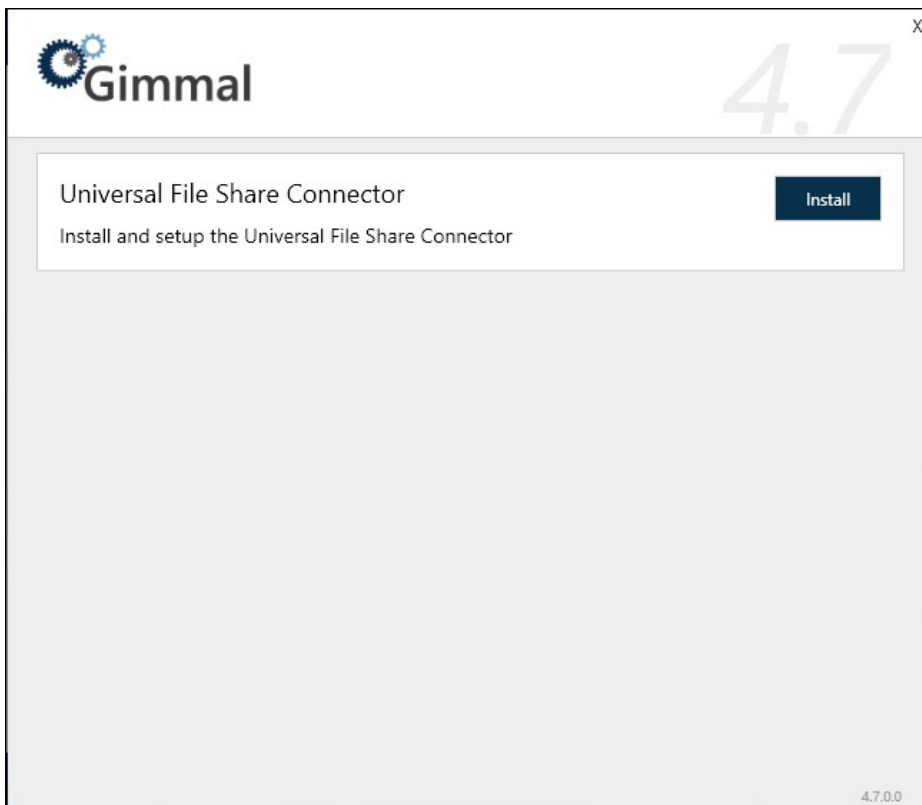
 As a security best practice when using the .NET Framework, Gimmel recommends that you enable Transport Layer Security (TLS) 1.2, which provides communications security for client/server applications. To enable TLS 1.2, you must add the following Windows registry settings to the Records Management Core server(s) and the servers of any Records Management connectors you are using (if applicable), and then reboot your system.

- HKLM:\SOFTWARE\Microsoft\.NETFramework\v4.0.30319 "SchUseStrongCrypto"= dword:00000001
- HKLM:\SOFTWARE\Microsoft\.NETFramework\v4.0.30319 "SystemDefaultTlsVersions"= dword:00000001
- HKLM:\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319 "SchUseStrongCrypto"= dword:00000001
- HKLM:\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319 "SystemDefaultTlsVersions"= dword:00000001

Note that some operating systems require additional steps to enable TLS 1.2. For more information, see [Microsoft's TLS documentation](#)¹¹² To verify that your operating system supports TLS 1.2, read the [Support for TLS 1.2 section of Microsoft's documentation](#)¹¹³.

6.14.12.4 Universal File Share Connector Installation

Upon starting the Universal File Share Connector, the following screen displays:



Click **Install**. The installation wizard will launch.

Installing the Universal File Share Connector

The Universal File Share Connector component installs a Desktop Configuration Application and a group of Windows Services that work with Records Management to manage the lifecycle of files on any File Share that is configured.

To install the Universal File Share Connector, perform the following steps:

1. From the Records Management splash screen, click the **Install Universal File Share Connector** link. The Universal File Share Connector installation screen displays.
2. Click **Install** to the right of the Universal File Share Connector option. The first screen that displays is the check for prerequisites. This screen validates that .NET Desktop Runtime 3.1.x is installed and the Current User is Local Administrator before allowing the installation to proceed.

¹¹² <https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls#systemdefaulttlsversions>

¹¹³ <https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls#support-for-tls-12>

⚠ The Universal File Share Connector requires that .NET Desktop Runtime is installed. If for some reason both .NET Core Desktop Runtime 5.0 and 3.1 are both installed, the installer will fail with the message ".Net Core 3.1 is not installed". To rectify - please uninstall both .NET Core Desktop Runtime 5.0 and .NET Core Desktop Runtime 3.1 and re-install only .NET Desktop Runtime 3.1.

3. Click **Next**. The installation location screen displays, which determines where the connector will be installed.
4. Leave the installation path as the default, or to change it to the desired installation location, and click **Next**. The Service Settings screen displays, where you will configure the settings for the Universal File Share Connector Services.

The screenshot shows a window titled "Gimmel Universal File Share Connector". The window has a header with the Gimmel logo and the title. Below the header, the main content area is titled "Service Settings". Under "Service Settings", there are two input fields: "Username" and "Password". At the bottom right of the window, there are two buttons: "Previous" and "Next".

When the Universal File Share Connector Service is installed, Windows Services are created. The following options specify which user account to use to execute these services.

Username (ex. DOMAIN\Username)

Password

The user account should be a domain account and must have the following file system permissions:

Read/Write: %Install Path%\Logs

Full Control: Managed file share locations to be configured (Recursive)

⚠ When assigning permissions to the account for the managed file share locations, assign them directly to the user rather than to a group in which the user is a member.

5. Click **Next**. The Data Provider screen displays, which enables you to configure the data provider used by the Universal File Share Connector. This stores Universal File Share Connector data in the configured database.

The following options determine the connection information that the Universal File Share Connector will use to connect to SQL Server:

- **Database Server:** The name of the SQL Server Install (ex. SERVERNAME\InstanceName)
- **Database Name:** The name of the actual SQL Server Database
- **Use SQL Authentication:** Specifies that the connection information should use SQL Authentication with the Username and Password indicated below
- **Username:** The SQL Server username to use if SQL Authentication is specified
- **Password:** The SQL Server password to use if SQL Authentication is specified

If SQL Authentication is not specified, the connection information will use Windows Authentication by specifying a trusted connection. This means that the Service account will be used to connect to SQL Server, therefore, this account will need the following database permissions. If SQL Authentication is specified, the SQL user will also require the following permissions.

- **db_datareader**
- **db_datawriter**

If Automatically Create Database is specified, the installation will automatically attempt to create the database using the Database Server and Database Name indicated. The appropriate account will also be automatically granted the appropriate rights to this database. This option requires that the current user has permission to create databases and manage security in the SQL Server instance indicated.

If Automatically Create Database is not specified, the installation will configure connection information but will not attempt to create the database. In this case, you will need to leverage the SQL Scripts at the following location to manually create the database in the SQL Server instance indicated. You will also need to manually configure security as indicated above.

%Install Path%\Configuration\Sql\RecordLion.RecordsManager.UniversalFileShare.sql

6. Click **Next** and then Finish to continue through the remaining screens and complete the installation.

6.14.12.5 Universal File Share Connector Configuration

After you install the Universal File Share Connector, you must configure it using the **Universal File Share Connector Configuration** application, using the following steps. The Gimmal Universal File Share Connector Classification Service will not start unless the connector is configured.

Configuring the Connector


Connection

The screenshot shows the 'Universal File Share Connector' configuration window. It has a title bar with the Gimmal logo and the text 'Universal File Share Connector'. Below the title bar are three tabs: 'Connection' (selected), 'Servers', and 'Transfers'. The 'Connection' tab contains the following fields and buttons:

- Manager Web URL:** A text input field with a 'Test' button to its right.
- Username:** A text input field.
- Password:** A text input field.
- Save:** A blue button at the bottom left.

The version number '4.7.0.0' is displayed in the bottom right corner of the window.

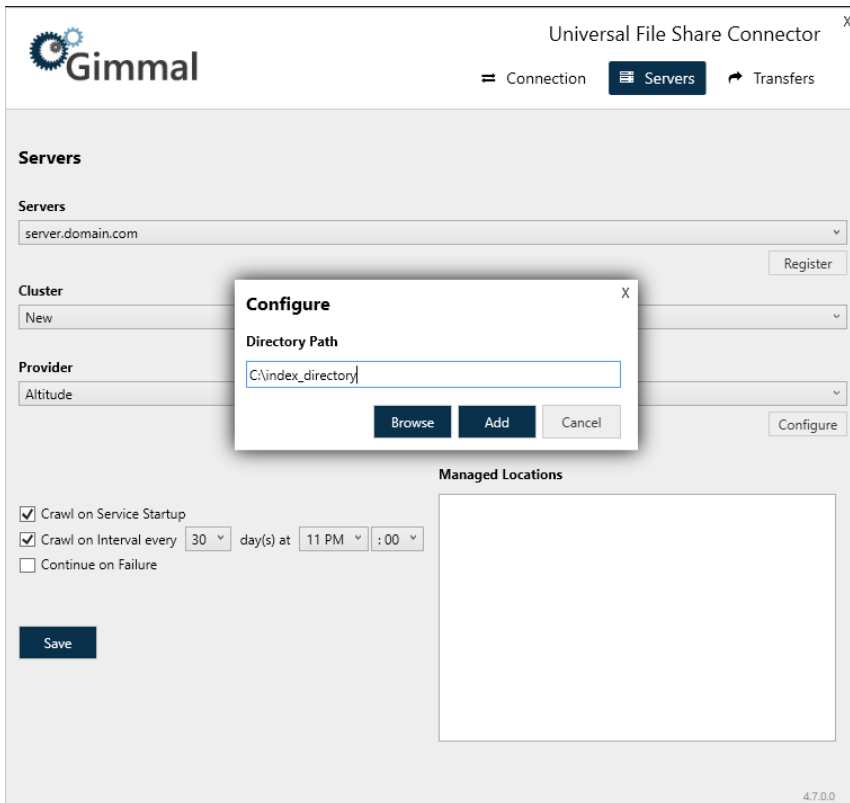
1. Enter the URL to the Records Management Manager Web.
2. Enter the Username* of the Universal File Share Connector Service Account created in Records Management Manager Web.
3. Enter the Password of the Universal File Share Connector Service Account created in Records Management Manager Web.

 The Service Account username format depends on whether you are connecting to the Gimmal Cloud for Records Management. If the Gimmal Cloud is being used, the username format is: {service account name}@{tenant domain} (e.g. spocservice@gimmal.com¹¹⁴, or fscservice@companyname.com¹¹⁵), otherwise, the format is just: {service account name}.


¹¹⁴ <mailto:spocservice@gimmal.com>

¹¹⁵ <mailto:fscservice@companyname.com>


Servers




1. Register the server where the Universal File Share Connector is installed.
2. The value in the **Cluster** field is automatically generated.
3. Select the **Provider**: File System or Altitude. If you need to manage both the File System and Altitude, you will need to install separate Universal File Share Connectors.

 To configure for Altitude: **Browse** to the location of the Gimmal Altitude index file. Click **Add** to populate the selection into the **Directory Path** field. (The index files are generated in Gimmal Altitude).

4. Enter the UNC path to file shares to be managed by Records Management (one per line) in the **Managed Locations** field.

 The account running the Universal File Share Connector needs to have full control access to the managed paths.

5. Choose whether to initiate a Full Crawl of managed paths on service startup.
6. Choose whether to perform a Full Crawl of managed paths on a specified interval.
7. Choose whether to continue Full Crawl when an error/failure occurs (e.g. permissions issue).

 If the **Continue on Failure** box is checked, the Full Crawl will complete even if there are errors during the crawl. You would need to examine the log file to discover these errors.

8. Click **Save**.

Transfers

1. Create a Transfer Configuration by selecting a cluster from the drop-down list.
2. Click **+Create** to assign a Record Class, select a Lifecycle Phase, enter the Destination Directory Path, and indicate if you want to retain the directory structure.
3. Click **Save**.

Transfers using the Gimmel Altitude Connector

If records are to be managed by Gimmel Records Management after they have been transferred, the index must be regenerated in Gimmel Altitude.

For a successful transfer, the destination path must be entered in the Managed Locations of the Universal File Share Configuration application.

Changing the Cluster

The Cluster field specifies a unique set of configuration options. If two Universal File Share Connector servers share the same Cluster ID, they will form a failover cluster. A failover cluster works in an active/passive failover model. One of the servers in the cluster will be designated automatically as the active service. If something happens to the active machine that prevents it from processing, one of the passive machines will be selected automatically as the active server and will take over-processing. Perform the following steps on the Servers tab:

1. On the **Servers** tab, select an existing cluster from the **Cluster** drop-down list or choose new to create a form a new cluster.
2. Click **Save**.



Configuring the Failover Cluster for the Altitude Connector

When configuring a failover cluster for use with Gimmel Altitude IG, a new index must be created for the failover server. Afterward the Universal File Share Configuration application must be re-configured to point to the new index.

Windows Services

When you install the Universal File Share Connector, there are three Windows Services that are set up in Windows to perform the actions necessary to enable Records Management to manage the lifecycle of records and information stored on network file shares.

Whether File System or Altitude are selected as the Provider, the same windows services are used.

Service Type	Description
Gimmel Universal File Share Classification Service	This service is responsible for discovering the content that exists in the configured file shares and notifying Records Management of its existence and any updates and removals of this content.
Gimmel Universal File Share Reconciliation Service	This service is responsible for performing reconciliation actions for records in Records Management.

Gimmel Universal File Share Retention Service

This service is responsible for executing the lifecycle actions as indicated by Records Management at various points in time according to the specified File Plan.

i The time is saved to the database in UTC format. The next crawl time is calculated based upon the time that the "Save" button is pressed. For example, the interval is set to be every 1 day at 7:00 AM. At the time "Save" is pressed, the local time is 6:05 PM CST Wednesday which is 12:05 UTC Thursday. The connector calculates the next crawl will be Friday.

6.14.12.6 Uninstall Universal File Share Connector

To uninstall the Universal File Share Connector, perform the following steps:

1. Open **Add/Remove Programs** on servers hosting the Universal File Share Connector.
2. Double-click **Universal File Share Connector**.
3. Choose **Uninstall**.

After uninstalling, the **UniversalFileShare** database will remain intact on the database server. You may keep this database in case you will be reinstalling or you can delete the database manually if it is no longer needed.

6.15 Physical Records Management Deployment

6.15.1 Physical Records Management Server Deployment

6.15.2 Physical Records Management Configuration

6.15.3 Physical Records Management Server Deployment

6.15.3.1 Physical Records Management Requirements

6.15.3.2 Physical Records Management Installation

6.15.3.3 Starting Gimmel Records Management Service

6.15.3.4 Physical Records Management Plugin Configuration

6.15.3.5 Uninstall Physical Records Management

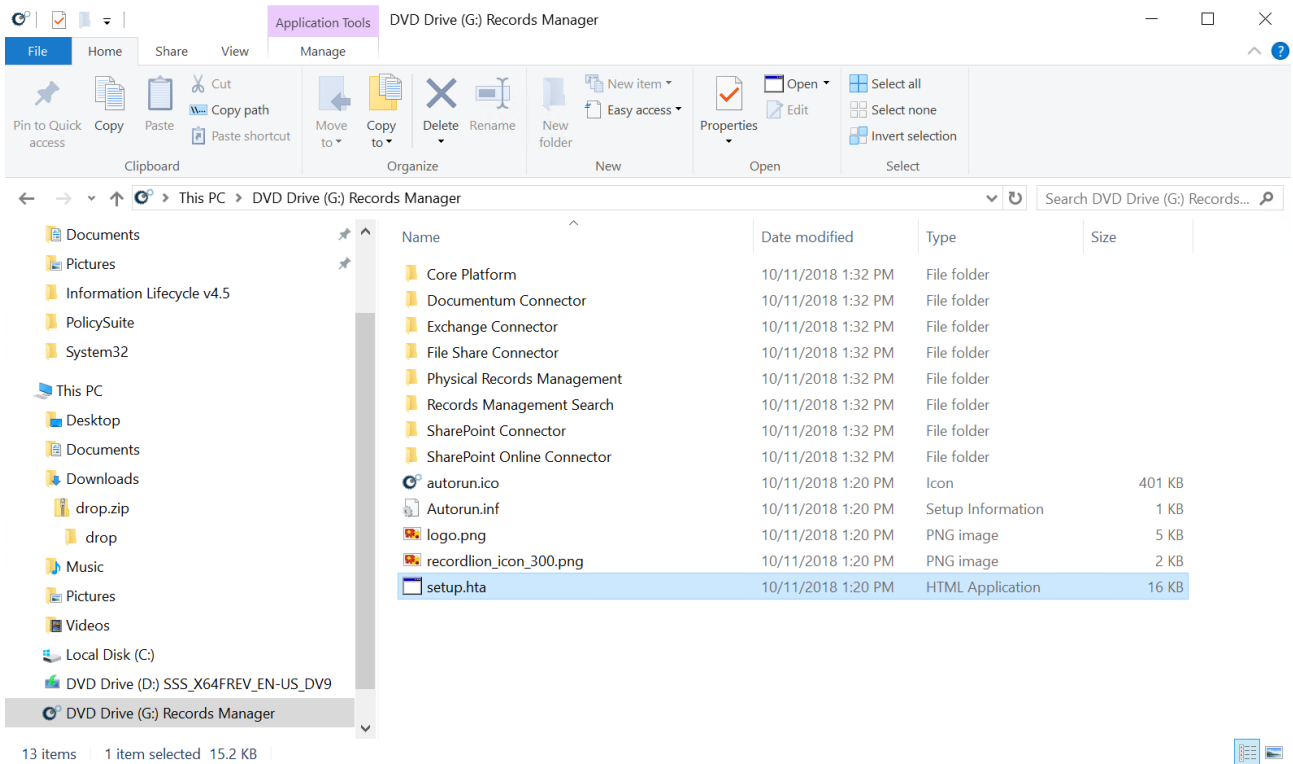
6.15.3.6 Physical Records Management Requirements


- Records Management Core must be deployed and configured.
- .NET Framework 4.8

6.15.3.7 Physical Records Management Installation

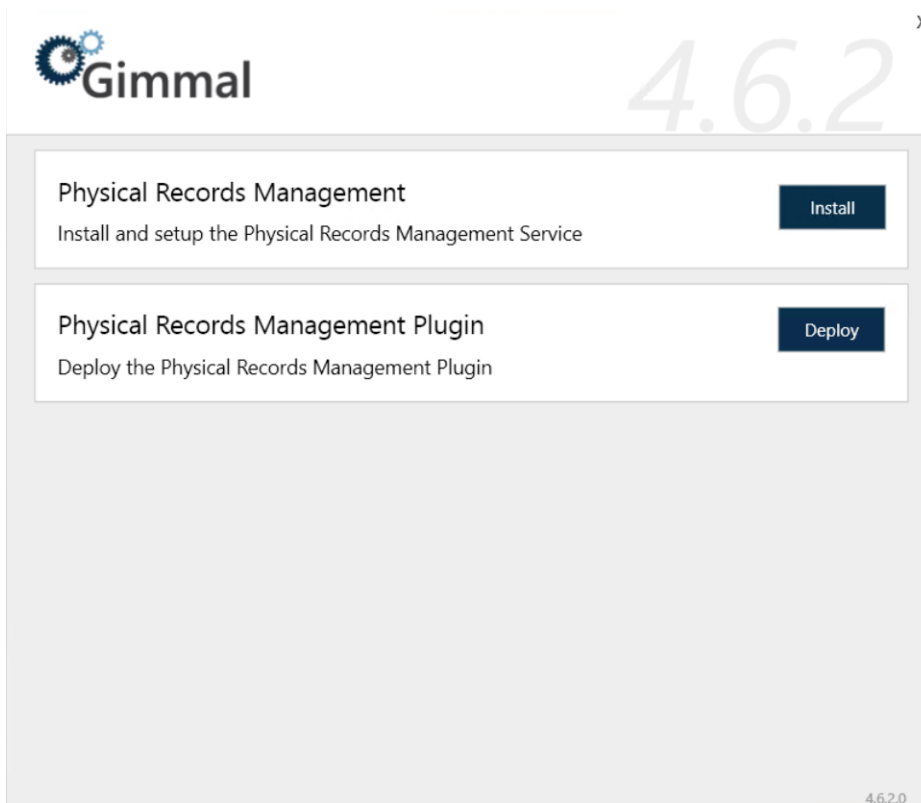
Installation Media

The installation media consists of a single ISO that contains everything necessary to install and set up Physical Records Management and other Records Management components. To initiate the setup process, regardless of the component, double-click the **setup.hta** file in the root folder of the ISO.



 Ensure that you run the installer as the Local Administrator.

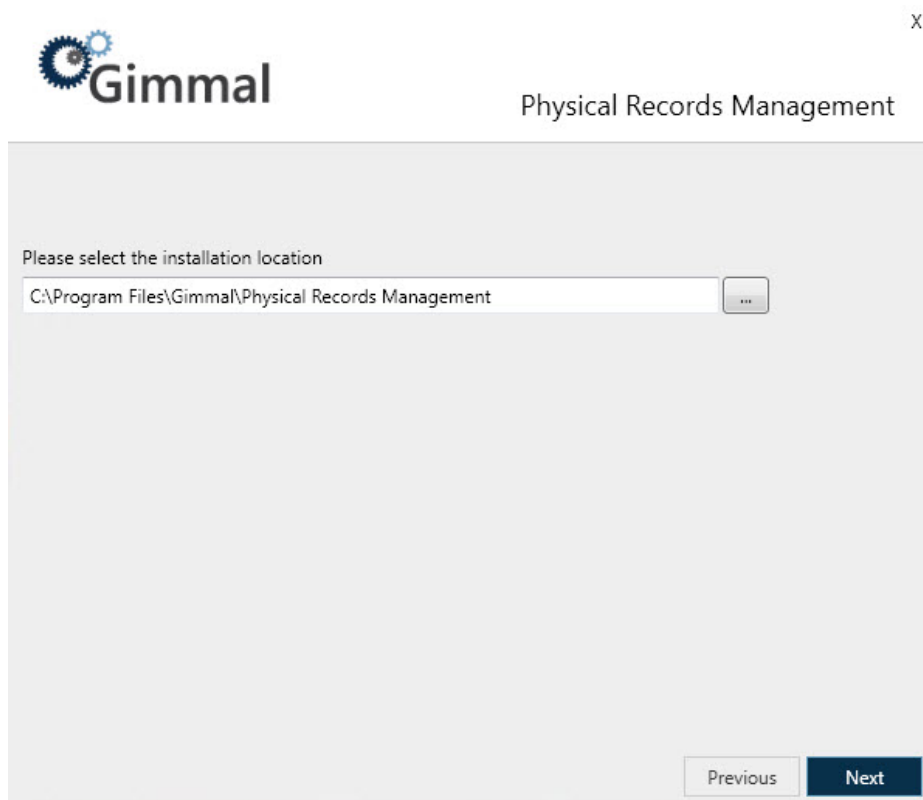
Upon initiating setup, the Records Management splash screen launches, which provides links to the Physical Records Management installation modules.



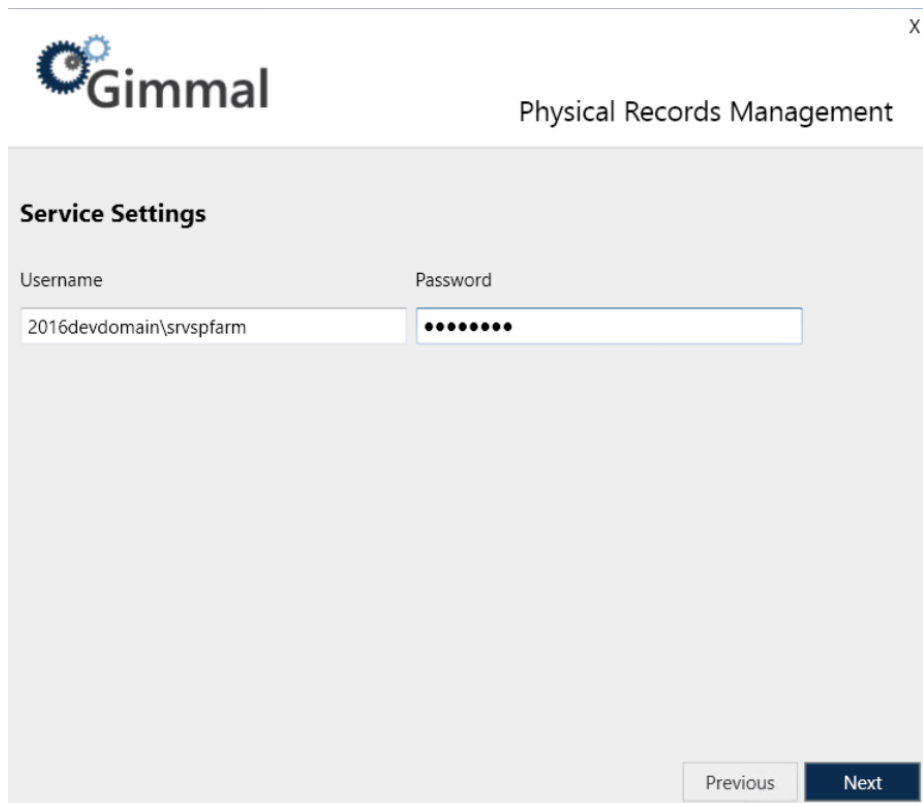
Installing Physical Records Management

To install Physical Records Management, perform the following steps:

1. From the Records Management splash screen, click the Install **Physical Records Management** link. The User Account Control window opens.
2. Click **Yes** to allow the installer to make changes to your computer. The Physical Records Management installation screen displays.
3. On the Physical Records Management installation screen, click **Install** to the right of the Physical Records Management option. The first screen that displays is the check for prerequisites. This screen validates the following information before allowing the installation to proceed:
 - The current user is Local Administrator
 - You have installed the required version of .NET
4. Click **Next**. The installation location screen displays, which determines where Physical Records Management will be installed.



5. Leave the installation path as the default, or to change it, click the ... icon next to the installation location field, select the desired installation location, and then click **Next**. The Service Settings screen displays.



The screenshot shows the Gimmel Physical Records Management interface. At the top left is the Gimmel logo, and at the top right is a close button (X). The main title is "Physical Records Management". Below this is a "Service Settings" section. It contains two input fields: "Username" with the value "2016devdomain\srvspfarm" and "Password" with a masked password of ten dots. At the bottom right of the dialog are two buttons: "Previous" and "Next".

6. Enter the following required information to specify which user account to use when you run the Windows Services:
- **Username** (Ex. DOMAIN\Username)
 - **Password**
- The user account must be a domain account and must have the following file system permissions:
- **Read/Write:** %Install path%\Logs

7. Click Next. The Database Settings screen displays.

The screenshot shows a web-based configuration window titled "Physical Records Management" with the Gimmel logo in the top left. The main content area is titled "Database Settings" and contains the following fields and options:

- Database Server:** A text input field containing "2016SVR".
- Database Name:** A text input field containing "PhysicalRecordsManagement".
- Automatically Create Database:** A checked checkbox.
- Use SQL Authentication:** An unchecked checkbox.
- Username:** An empty text input field.
- Password:** An empty text input field.

At the bottom right of the form, there are two buttons: "Previous" (disabled) and "Next" (active).

8. Enter/select the following database settings to determine the connection information that will be used by Physical Records Management to connect to SQL Server:
- **Database Server:** The name of the SQL Server Install (ex. SERVERNAME\InstanceName)
 - **Database Name:** The name of the actual SQL Server Database (The default name for the database is “PhysicalRecordsManagement”, but you can change it here.)
 - **Automatically Create Database:** See description below
 - **Use SQL Authentication:** Specifies that the connection information should use SQL Authentication with the Username and Password indicated below
 - **Username:** The SQL Server username to use if SQL Authentication is specified
 - **Password:** The SQL Server password to use if SQL Authentication is specified

If **SQL Authentication** is not specified, the connection information will use Windows Authentication by specifying a trusted connection. This means that the Service account will be used to connect to SQL Server, therefore, this account will need the following database permissions. If **SQL Authentication is specified**, the SQL user will also require the following permissions.

- **db_datareader**
- **db_datawriter**
- **GRANT EXECUTE** on all Stored Procedures
- **GRANT EXECUTE** on all Scalar User Defined Functions
- **GRANT SELECT** on all Table and Inline User Defined Functions


If **Automatically Create Database is specified**, the installation will automatically attempt to create the database using the Database Server and Database Name indicated. The appropriate account will also be automatically granted the appropriate rights to this database. This option requires that the current user has permission to create databases and manage security in the SQL Server instance indicated.

If **Automatically Create Database is not specified**, the installation will configure connection information but will not attempt to create the database. In this case, you will need to leverage the SQL Scripts at the

following location to manually create the database in the SQL Server instance indicated: %Install Path\Gimmel\Physical Records Management\Service\Sql\

Run the scripts, in the order listed below, as a user who has database creation privileges on the desired SQL Server. You must also manually configure security, as indicated above.

- RecordLion.RecordsManager.PhysicalAssets.sql
 - RecordLion.RecordsManager.PhysicalAssets.Optimize.sql
 - RecordLion.RecordsManager.PhysicalAssets.Seed.sql
9. Click **Next** to perform the final installation using the database settings you specified above. The progress bar indicates the state of the installation.
 10. When the application finishes installing, click **Next** to continue to the final screen. The final screen indicates that everything installed successfully.

 If you experience any errors during the installation process, refer to the installer log in your Windows Temp folder.

11. Click **Finish** to return to the main Setup screen, which should now indicate that Physical Records Management was installed successfully.
12. After you finish the installation, you must perform the following steps to run the newly installed Windows Services.
 - Open the Windows Services Manager.
 - In the Services window, verify that the **Gimmel Physical Records Management Service** is listed.
 - Right-click on the service and select **Start**. When the service begins, the Status column will display "Running".
 - Using the SQL Server Management Studio, connect to the SQL database and navigate to the **Databases** folder. (The database you applied settings to in step 8 is located under this Databases folder.)
 - Verify the **PhysicalRecordsManagement** (or the name you provided) database is listed.
 - Expand the nodes: **PhysicalRecordsManagement > Security > Users**, and verify that the Service/ User account that was created during the installation steps above is listed and has the correct permissions.
 - Exit out of the SQL Server Management Studio with saving anything.
13. Continue with the next topic, Installing the Physical Records Management Plugin.

Installing the Physical Records Management Plugin

To install the Physical Records Management plugin, perform the following steps:

1. On the Physical Records Management installation screen, click **Deploy** to the right of the Physical Records Management Plugin option. The first screen that displays is the check for prerequisites. This screen validates the following information before allowing the installation to proceed:
 - The current user is Local Administrator
 - You have installed .NET Framework 4.5
2. Click **Next** to perform the final deployment using the database settings you specified above. The progress bar indicates the state of the deployment.
3. When the application finishes deploying, click **Next** to continue to the Finish screen. This screen indicates that everything deployed successfully.

 If you experience any errors during the deployment process, refer to the installer log in your Windows Temp folder.

4. Click **Finish** to return to the Physical Records Management installation screen. (Note that the **Deploy** button will not be grayed out like the **Installed** button is.)

- Continue with the next section, Configuring Physical Records Management, to begin the configuration process.

6.15.3.8 Starting Gimmel Records Management Service

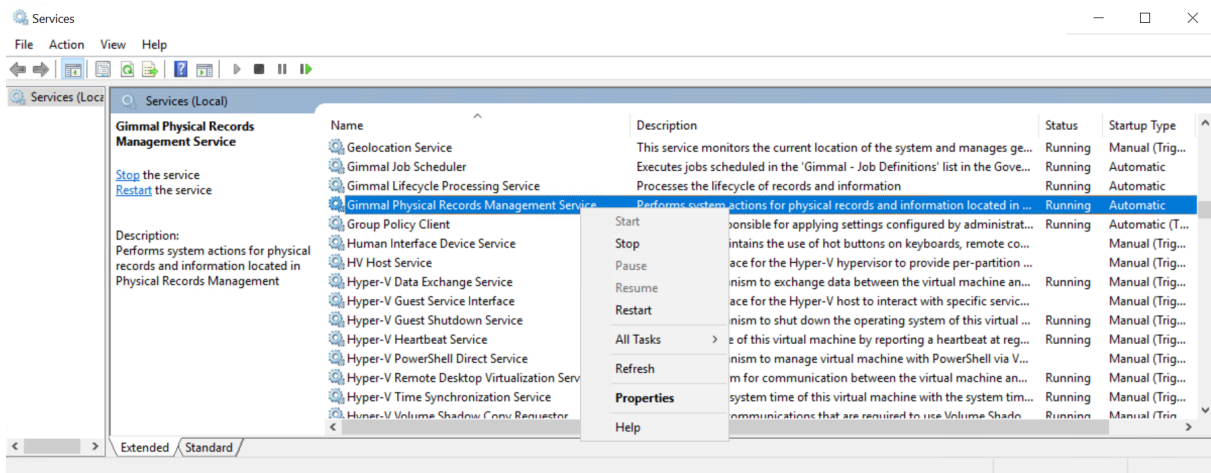
When you install Physical Records Management, a Windows Service is added during the installation process. A description of the Service follows. You must start this Service prior to using the Physical Records Management extension.

Service Type	Description
Gimmel Physical Records Management Service	Performs system actions for physical records and information located in Physical Records Management.

Starting and Stopping the Service

The Physical Records Management Service can be started and stopped from the Windows Services Control Panel. To do so, perform the following steps:

- Run Services.msc.
- Right-click **Gimmel Physical Records Management Service**.
- Click **Start** or **Stop**.




6.15.3.9 Physical Records Management Plugin Configuration

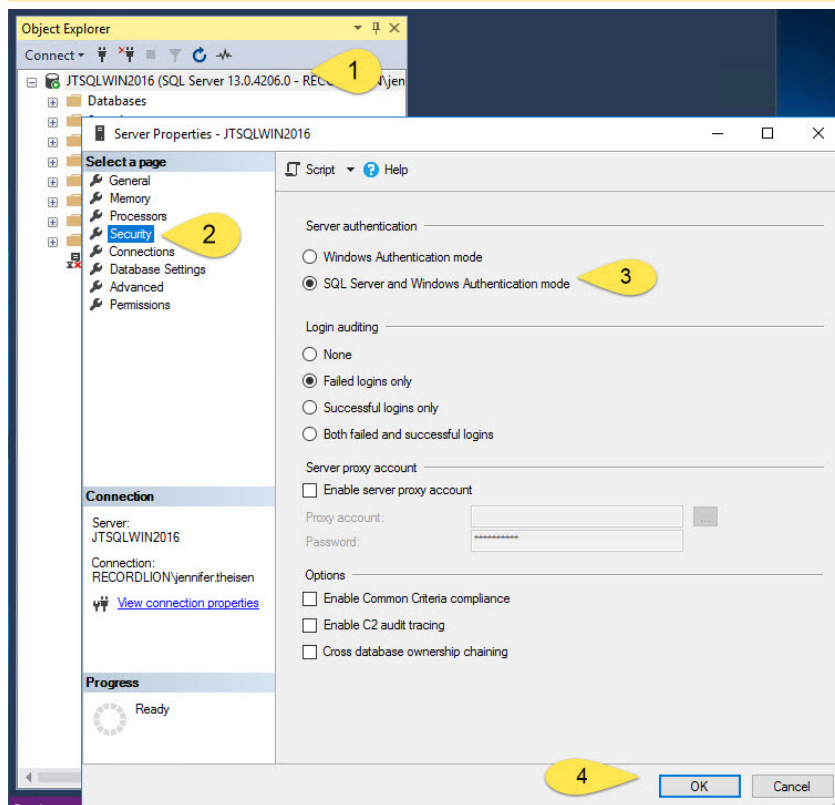
To set up Physical Records Management properly, you must configure the plugin first (using either SQL Authentication or Windows Authentication). This establishes your connection to the SQL database. Then, you can configure the Physical Records Management connection. Each authentication method is described below.

Setting Up the Plugin using SQL Authentication

- Open the SQL Server Management Studio.
- In Object Explorer, right-click your server name, and then click **Properties**. The Server Properties window opens.

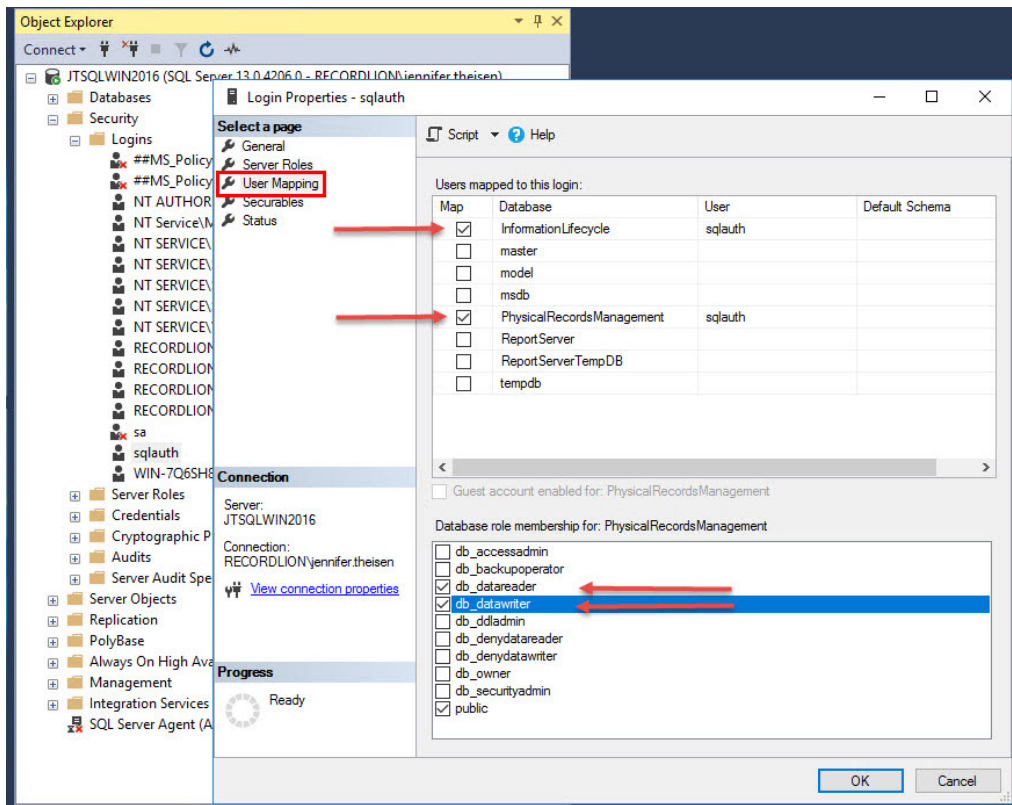
- From the left pane, click the **Security** page, and then select **SQL Server and Windows Authentication mode** in the Server authentication section. (**Note: Windows Authentication mode** is selected by default.)

 You can skip this step if the **SQL Server and Windows Authentication mode** setting has already been set on this server. (If this option has not already been set, a message displays telling you that the server will need to be restarted.)

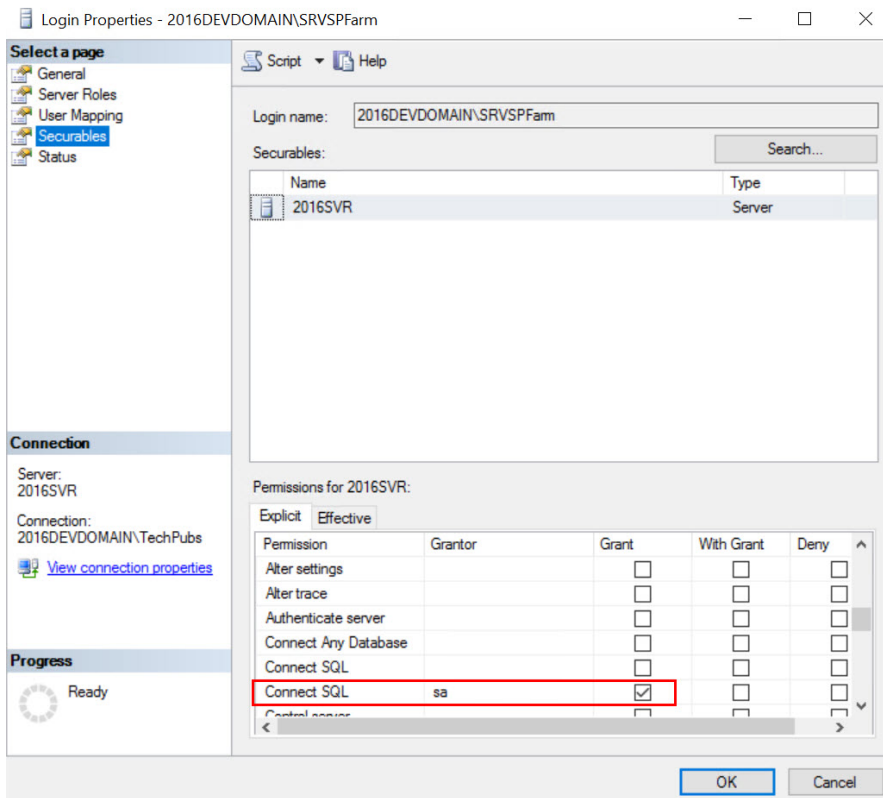


- Click **OK** to close the window.
- Return to Object Explorer, right-click your server name again, and select **Restart**.
- If the User Account Control window box appears, click **Yes**.
- When prompted if you want to perform the action, click **Yes**. The SQL Server Database Engine restarts.
- Return to Object Explorer and expand the **Security** folder.
- Right-click the **Logins** folder and select **New Login...** The Login - New window opens.
- Enter the credentials for a new **SQL Server Authentication** login. (For information on creating a new login, see [Microsoft's SQL documentation](#)¹¹⁶.)
- Note:** Ensure that you uncheck the box for "User must change password at next login".
- Click **OK** to create the new login.
- Under Select a page, click **User Mapping**. The User Mapping page displays.
- Give db_reader and db_writer access to any Manager Web databases, including the following SQL Server databases, for the new SQL login you just created.
 - InformationLifecycle**
 - PhysicalRecordsManagement** (or the database name you entered during the installation process)

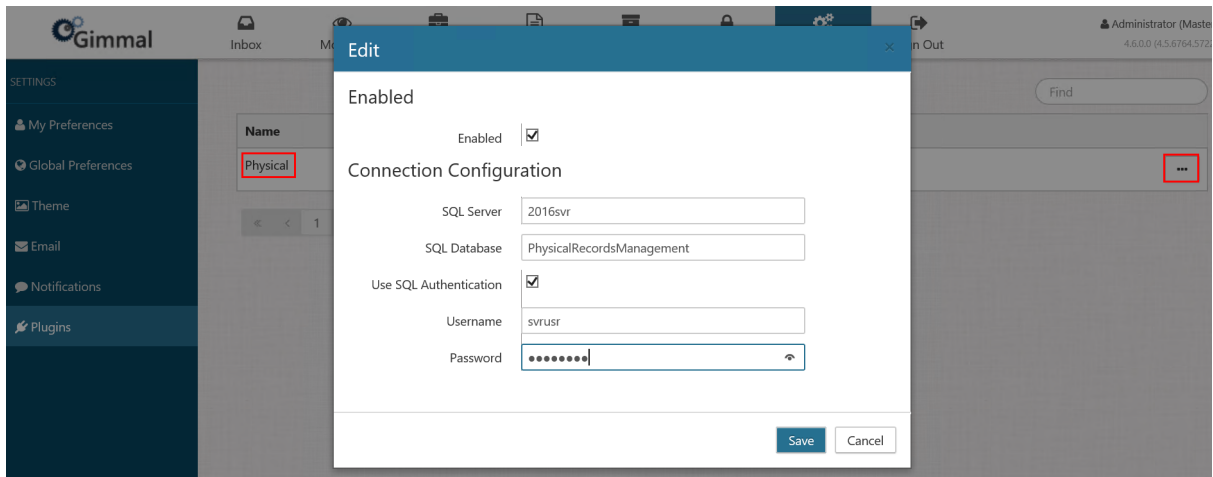
¹¹⁶ <https://docs.microsoft.com/en-us/sql/index?view=sql-server-2017>



14. Under Select a page, click **Securables**. The Securables/Permissions window displays.
15. Under the "Permissions for" section at the bottom, scroll down to **Connect SQL**, ensuring that under the Grantor column, the name of your new SQL Server authentication login is listed there.



16. Select the checkbox under the **Grant** column.
17. Click **OK**. This concludes the steps required in SQL Server Management Studio.
18. Next, sign in to Records Management's Manager Web as "Administrator" to create a Service account for the Physical Records Management plugin.



19. Click **Settings > Plugins**. The plugins list displays.
20. Click the ellipsis (...) to the right of the Physical plugin. The Edit window displays.
21. Click the **Enabled** checkbox.
22. Enter values for SQL Server and SQL Database.
23. Click the **Use SQL Authentication** checkbox.
24. Enter the Username and Password for the login you created in SQL Server Management Studio.

25. Click **Save**. The Edit window closes, and the following occurs:
 - The **Physical** tab displays at the top of the Manager Web Main Menu.
 - The following new roles appear on the **Secure** tab:
 - Physical Administrator
 - Physical User

Setting Up the Plugin using Windows Authentication

1. [Create a new service account](#)¹¹⁷ for the Physical Records Management user.
2. Click **Settings > Plugins** to see the list of available plugins by name.
3. Click the ellipsis (...) next to the desired plugin name to open the Edit window.

4. Check the **Enabled** box. (This activates the Physical tab on the Records Management main menu.)
5. Enter the name of your SQL Server and your SQL Database.
6. Click **Save**. The Edit window closes, and the following occurs:
 - The **Physical** tab displays at the top of the Manager Web Main Menu.
 - The following new roles appear on the **Secure** tab:
 - Physical Administrator
 - Physical User

6.15.3.10 Uninstall Physical Records Management

To uninstall Physical Records Management, perform the following steps:

¹¹⁷ <http://docs.gimmel.com/en/3517-creating-a-service-account.html>

1. On the server that hosts Physical Records Management, navigate to the Windows Control Panel and select **Uninstall a Program** from the Programs section.

2. On the “Uninstall or change a program screen”, locate **Gimmel Physical Records Management** and double-click it. (You can also select **Gimmel Physical Records Management** and then click the **Uninstall** option above the program list.) A dialog displays, asking you to confirm the uninstallation.
3. Click **Yes** to confirm the uninstallation. The User Account Control dialog displays, asking you to confirm the uninstallation.
4. Click **Yes** to begin the uninstallation process. When the uninstallation has completed, the **Gimmel Physical Records Management** program will be removed from the Programs list.
5. Verify that the **Gimmel Physical Records Management** Service no longer displays in the Windows Services list.

After uninstalling, the database will remain intact on the database server. You may keep this database in case you will be reinstalling Physical Records Management, or you can delete the database manually if it is no longer needed.

6.15.4 Physical Records Management Configuration

1. Log into Records Management Manager Web using your Master ("Administrator") account, and verify that the Physical Records Management Service Account has been created. (For more information, see [Creating a Service Account](#)¹¹⁸.)
2. Click **Physical** on the Main Menu, and then click **Connection** on the left Navigation Menu. The Connection Configuration page displays.

The screenshot shows the Gimmel Physical Records Management web interface. The top navigation bar includes 'Inbox', 'Monitor', 'Manage', 'Plan', 'Physical' (selected), 'Secure', 'Settings', 'Info/Help', and 'Sign Out'. The left navigation menu is divided into 'PHYSICAL' and 'ADMIN' sections. Under 'PHYSICAL', there are links for Containers, My Requests, Charge-Outs, Request Processing, Locations, and Barcodes. Under 'ADMIN', there are links for Connection (selected), Job Configuration, Audit, and Custom Metadata. The main content area is titled 'Connection Configuration' and contains three input fields: 'URL' with the value 'http://2016svr:8080', 'Username' with the value 'PhysicalRecordsManagement', and an empty 'Password' field. An 'Update' button is located below the fields.

3. Enter the connection URL
4. Enter the [Service Account](#)¹¹⁹ **Username** and the Service Account **Password**.

¹¹⁸ <http://docs.gimmel.com/en/3517-creating-a-service-account.html>

¹¹⁹ <http://docs.gimmel.com/en/3515-account-types---permission-overview.html>

5. Click **Update**. (This button will display **Save** if this is the first time configuring the connection)
6. Start the **Gimmel Physical Records Management Service** from the Windows Services dialog.
7. Return to Physical Records Management, and on the Main Menu, click **Monitor > Services**. A list of services displays.
8. Verify that **Physical Records Service** displays with the green heartbeat icon, as well as the "P" icon indicating that it's a Primary service.

Host	Source	Last Heartbeat	Status	Actions
2016SVR	Lifecycle Processing Service	6/25/2018 1:30:40 PM	Green Heartbeat, P	More, X
2016SVR	Physical Records Service	6/25/2018 10:07:53 AM	Red Heartbeat, P	X
2016SVR	SharePoint Audit Timer Job	6/25/2018 1:30:02 PM	Green Heartbeat	X
2016SVR	SharePoint Classification Timer Job	6/25/2018 1:30:17 PM	Green Heartbeat	X
2016SVR	SharePoint Retention Timer Job	6/24/2018 11:23:19 PM	Green Heartbeat	X
2016SVR	SharePoint System Timer Job	6/25/2018 1:30:02 PM	Green Heartbeat	X



Existing Gimmel Cloud service customers (pre-Feb. 27th, 2021) should continue to use the existing URLs.

- **US Test** - <https://test.recordlion.net>
- **US Production** - <https://app.recordlion.net>
- **UK Test** - <https://testuk.recordlion.net>
- **UK Production** - <https://uk.recordlion.net>

New Gimmel Cloud service customers (post-Feb. 27th, 2021) should use the new URLs.

- US Test - <https://records.gimmel.build>
- US Production - <https://records.gimmel.cloud>
- UK Test - <https://records.uk.gimmel.build>
- UK Production - <https://records.uk.gimmel.cloud>
- CAN Production - <https://records-ca.gimmel.cloud/>

NOTE: Existing customers already using the existing URL should not change to the new URLs as this may cause issues.

6.16 Monitoring Services

To verify that connectors and services are running appropriately, it is possible for System Admins to monitor the state of running services from the system.

The screenshot shows the Gimmal Monitor interface. The top navigation bar includes icons for Inbox, Monitor (selected), Manage, Plan, Physical, Secure, Settings, Info/Help, and Sign Out. The user is identified as Administrator (Master) with version 4.6.0.0 (4.5.6744.5701). The left sidebar shows a menu with sections: REPORTING (Dashboard, Reports, Destruction Certificates) and ACTIVITY (Audit, Event Occurrences, Pending Automation, Services). The main content area displays a table with the following data:

Host	Source	Last Heartbeat	Status Icon	Actions
2016SVR	Lifecycle Processing Service	6/25/2018 1:30:40 PM	Green Heartbeat	More options, Close
2016SVR	Physical Records Service	6/25/2018 10:07:53 AM	Red Heartbeat	Close
2016SVR	SharePoint Audit Timer Job	6/25/2018 1:30:02 PM	Green Heartbeat	Close
2016SVR	SharePoint Classification Timer Job	6/25/2018 1:30:17 PM	Green Heartbeat	Close
2016SVR	SharePoint Retention Timer Job	6/24/2018 11:23:19 PM	Green Heartbeat	Close
2016SVR	SharePoint System Timer Job	6/25/2018 1:30:02 PM	Green Heartbeat	Close

6.16.1 Heartbeat Icon Legend

The heartbeat icon to the right of the **Last Heartbeat** column in the preceding screenshot indicates the status of each service. See the following legend for the time thresholds corresponding to service status and icon color:

Icon Color	Service Status
Green	Connectors and services are running correctly.
Yellow	For non-clustered service, the difference between the current date time and the last heartbeat is larger than 24 hours . For clustered failover service, the difference between the current date time and last heartbeat is larger than 1 minute .
Red	For non-clustered service, the difference between the current date time and the last heartbeat is larger than 1 week . For clustered failover service, the difference between the current date time and last heartbeat is larger than 1 hour .

6.16.2 Lifecycle Processing Service

To view which activity the Lifecycle Processing Service is performing at the moment, click the three dots to the right of the Lifecycle Processing Service. The Details dialog opens, showing which processing activity is currently taking place. (If the Processing Activity displays "--", this means the Lifecycle Processing Service is idle.)


✕
Details

Processing Scope
Items modified since 11/12/2018 7:37:54 PM

Processing Activity
Performing Classification

Force Processing of All Items

Close

 ***Do NOT** click the **Force Processing of All Items** button on the Details dialog unless directed to do so by a member of Gimmel's Client Success team. This action forces the processing of all items in Records Management, not just the items that have changed since the date/time shown under the Processing Scope heading above. This action can severely impact the time it takes for updates to be processed.

6.16.3 Deleting services no longer in use

If a service is no longer used, you can delete the row for the service by clicking the **X** next to the service you no longer want to monitor. Removing the service from this screen does not affect the service in any way. If the service is still running, the row representing that service instance will reappear.

6.17 Migration Utility

The Migration Utility for Records Management is used to perform the following Migrate and Import functions:

1. Migrate the following from one Records Management Server to another:
 - Classification rules
 - Record Classes
 - Lifecycles
 - Retentions
 - Triggers
 - Holds
2. Import the following from an Excel-based File Plan:
 - Record Classes
 - Lifecycles
 - Retentions
 - Triggers

 The migration utility does not support import/migration of Physical Records and containers.

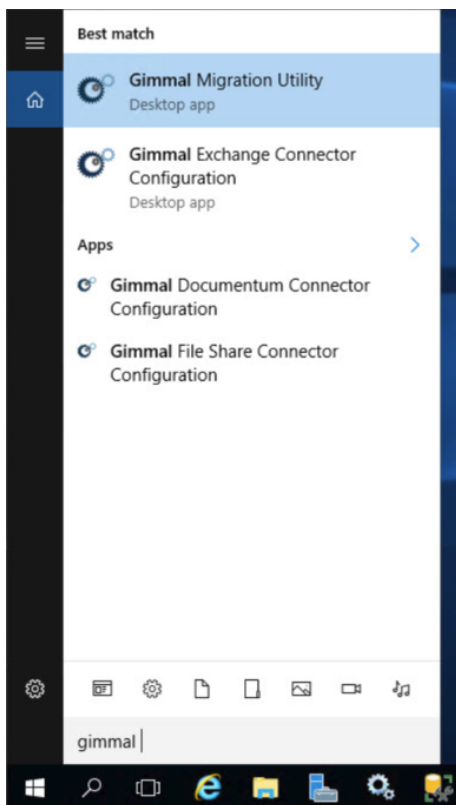
6.17.1 Running the Migration Utility

6.17.1.1 Open the Migration Utility

To open the Migration Utility, navigate to the directory selected during installation, and double-click `Gimmal.RecordsManager.Migrate.exe`. The default installation directory is:

`C:\Program Files\Gimmal\Records Management\Migration`

Conversely, you can open the Migration Utility from the Windows Start menu by selecting **Gimmal Migration Utility**.



6.17.1.2 Welcome Screen

When the application first opens, you will be presented with the Migration Utility Welcome screen. From here, you can select which function you would like to perform.

Select one of the following options, then select a Connection Type, and click Next.

1. [Migrate](#)(see page 417)
2. [Import](#)(see page 409)

Welcome

Would you like to perform a Gimmel Records Management import or migration?

Migrate Import

Migrate

You can copy Record Classes and Legal Cases between two installations.

Connection Type

Choose how you would like to connect to Records Management

Database Connection
 Web Service Connection


Next

6.17.2 Import

Select **Import** from the Welcome screen, this section will guide you through the wizard.

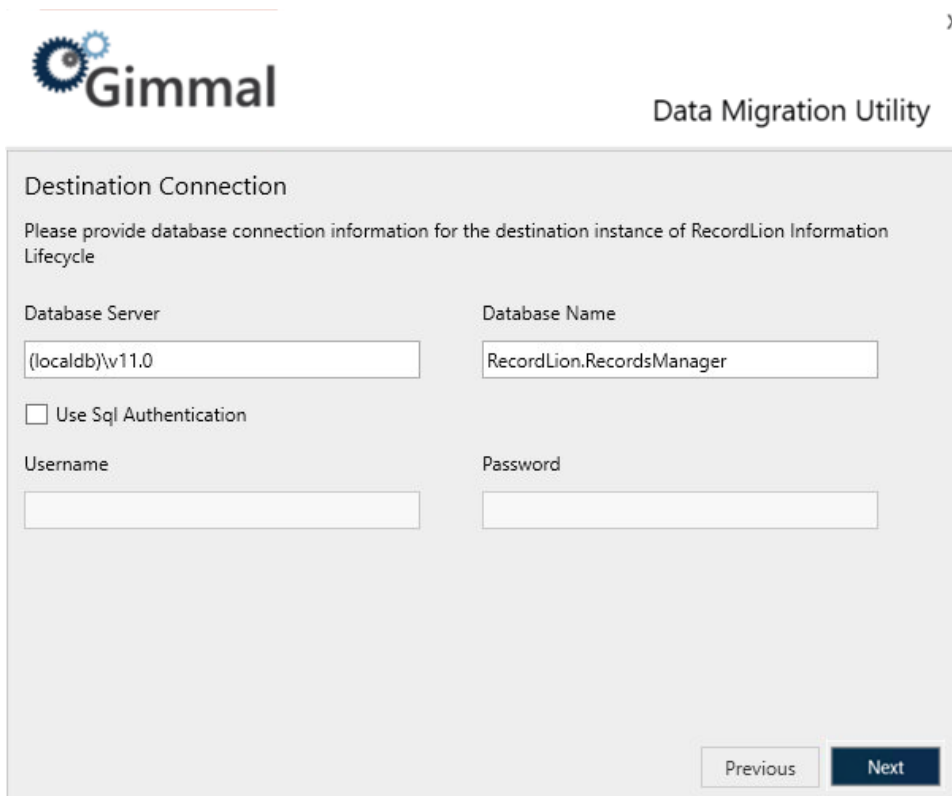
6.17.2.1 Import Configuration

The next screen you will be presented with is the Import Configuration Screen. In this screen, select the path to the Excel-based File Plan and corresponding Import Mapping File that will be used for performing the Import. Click **Next**.

 Select the option "Overwrite Existing Data" will result in the deletion of all existing File Plan configuration prior to executing the import. You will be prompted for confirmation before proceeding.

6.17.2.2 Destination Connection

The next screen you will be presented with is the Destination Connection Screen. In this screen, enter the connection information to the Information Lifecycle Server Database where data should be migrated to.



Destination Connection

Please provide database connection information for the destination instance of RecordLion Information Lifecycle

Database Server: (localdb)\v11.0

Database Name: RecordLion.RecordsManager

Use Sql Authentication

Username:

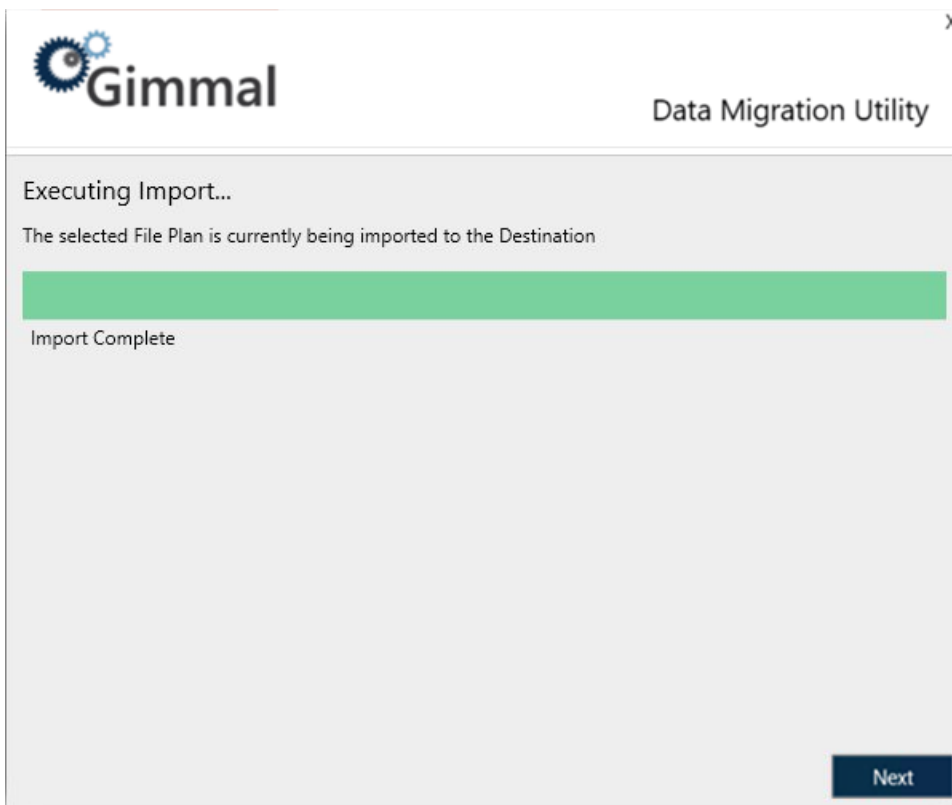
Password:

Previous Next

6.17.2.3 Executing Import

After kicking off the import, the next screen displayed is the Executing Import Screen. This screen displays the progress of the import while it is executing. Once the import has finished executing, click **Next**.

The final screen displayed is the **Import Complete Screen**. This screen simply notifies you that the import has been completed. Click **Finish** to exit the utility.



6.17.2.4 Import Mapping File

The Import Mapping File is an XML-based file that describes to the Data Migration Utility how to parse an Excel-based File Plan in order to import its content as Record Classes, Triggers, Retentions, and Lifecycles in Records Management. Because the Import Mapping File describes how the File Plan should be parsed, this allows the File Plan to remain unaltered and in the format of your choosing.

The Import Mapping File is validated during the import process and is required to adhere to the following format:

```
<?xml
version="1.0" encoding="UTF-8"?>
<import xmlns="http://www.gimmel.com/fileplan/import/v1">
  <recordClasses>
    <root title="Root Record Class Title" code="Root Record Class Code" /><!--
Optional: All Record Classes will be nested under
this node if provided -->
    <level>
      <mapping>
        <![CDATA[
          SELECT
            [Excel Column] AS [Record Class Property],
            ...
          FROM
            [Worksheet$]
          WHERE
```

```

                [Excel Column] some conditions
    ]]>
</mapping>
<levels>
  <level>
    <mapping>
      <![CDATA[
        SELECT
          [Excel Column] AS [Record Class Property],
          ...
        FROM
          [Worksheet$]
        WHERE
          [Excel Column] = '{Title}' AND
          [Excel Column] some conditions
      ]]>
    </mapping>
  <level>...
</levels>
</level>
<level>...
</levels>
</level>
<level>...
</recordClasses>
<lifecycles>
  <lifecycle>
    <mapping>
      <![CDATA[
        SELECT
          [Excel Column] AS [Lifecycle Property],
          ...
        FROM
          [Worksheet$]
        WHERE
          [Excel Column] some conditions
      ]]>
    </mapping>
  <phases>
    <mapping>
      <![CDATA[
        SELECT
          [Excel Column] AS [Lifecycle Phase Property],
          ...
        FROM
          [Worksheet$]
        WHERE
          [Excel Column] some conditions
      ]]>
    </mapping>
  </phases>
</lifecycle>
</lifecycles>
</recordClasses>
</mapping>
]]>

```



```

        </mapping>
    </phases>
</lifecycle>
<lifecycle>...
</lifecycles>
<retentions>
    <retention>
        <mapping>
            <![CDATA[
                SELECT
                    [Excel Column] AS [Retention Property],
                    [Excel Column] AS [TriggerTitle]
                ...
            FROM
                [Worksheet$]
            WHERE
                [Excel Column] some conditions
            ]]>
        </mapping>
    </retention>
<retention>...
</retentions>
<triggers>
    <eventTriggers>
        <eventTrigger>
            <mapping>
                <![CDATA[
                    SELECT
                        'Event Name' AS [Title],
                        2 AS [AssignmentPosition],
                        4 AS [Recurrence],
                        DateValue('12/31/2000') AS [NextEventDate]
                ]]>
            </mapping>
        </eventTrigger>
    <eventTrigger>...
</eventTriggers>
<datePropTriggers>
    <datePropTrigger>
        <mapping>
            <![CDATA[
                SELECT
                    'Created' AS [Title],
                    '@created' AS [PropertyName]
            ]]>
        </mapping>
    </datePropTrigger>
<datePropTrigger>...
</datePropTriggers>

```

```

<ruleTriggers>
  <ruleTrigger>
    <mapping>
      <![CDATA[
        SELECT
          [Excel Column] AS [Rule Trigger Property],
          ...
        FROM
          [Worksheet$]
        WHERE
          [Excel Column] some conditions
      ]]>
    </mapping>
    <rules>
      <mapping>
        <![CDATA[
          SELECT
            [Excel Column] AS [Rule Property],
            ...
          FROM
            [Worksheet$]
          WHERE
            [Excel Column] some conditions
        ]]>
      </mapping>
    </rules>
  </ruleTrigger>
</ruleTriggers>
</triggers>
</import>

```

6.17.2.5 Object Schema for Import Mapping

Record Class

Property Name	Mapping Name	Notes
Title	Title	
Description	Description	
Code	Code	
Organization	Organization	
Notes	Notes	
Priority	Priority	
Archive Records	ArchiveRecords	
Archive Record Properties	ArchiveRecordProperties	
Archive Record Audits	ArchiveRecordAudits	
Destruction Certificates	GenerateDestructionCerts	
Record Declaration Rule	RecordDeclarationRule	<ul style="list-style-type: none"> • 0 = Always • 1 = Never • 2 = Possible
Vital Rule	VitalRule	<ul style="list-style-type: none"> • 0 = Always • 1 = Never • 2 = Possible
Case Based	IsCaseBased	
Case File Rule	CaseFileRule	
Lifecycle	LifecycleTitle	(Relationship)

Lifecycle

Property Name	Mapping Name	Notes
Title	Title	
Description	Description	
Notes	Notes	
Phase [0..N]: Retention	RetentionTitlePhase[0..N]	(Relationship)
Phase [0..N]: Action	ActionPhase[0..N]	<ul style="list-style-type: none"> • 0 = None • 1 = Transfer • 2 = Workflow • 3 = Declare Record • 4 = Undeclare Record • 5 = Dispose and Delete • 6 = Dispose and Transfer • 7 = Permanent • 8 = Dispose and Recycle
Phase [0..N]: Automation Level	AutomationLevelPhase[0..N]	<ul style="list-style-type: none"> • 0 = Automatic • 1 = Manual
Phase [0..N]: Require Approval	RequireApprovalPhase[0..N]	
Phase [0..N]: Repeat Approval Interval	RepeatApprovalIntervalPhase[0..N]	
Phase [0..N]: Repeat Approval Time Period	RepeatApprovalTimePeriodPhase[0..N]	

Retention

Property Name	Mapping Name	Notes
Title	Title	
Description	Description	
Trigger	TriggerTitle	(Relationship)
Interval	Interval	
TimePeriod	TimePeriod	<ul style="list-style-type: none"> • 0 = Days • 1 = Months • 2 = Years

Event Trigger

Property Name	Mapping Name	Notes
Title	Title	
Description	Description	
Starting Event Date	NextEventDate	
Recurrence	Recurrence	<ul style="list-style-type: none"> • 0 = Manual • 1 = Once • 2 = Daily • 3 = Monthly • 4 = Yearly
Assignment Position	AssignmentPosition	<ul style="list-style-type: none"> • 0 = Nearest Occurrence to Record Origin • 1 = Nearest Occurrence Before Record Origin • 2 = Nearest Occurrence After Record Origin

Date Property Trigger

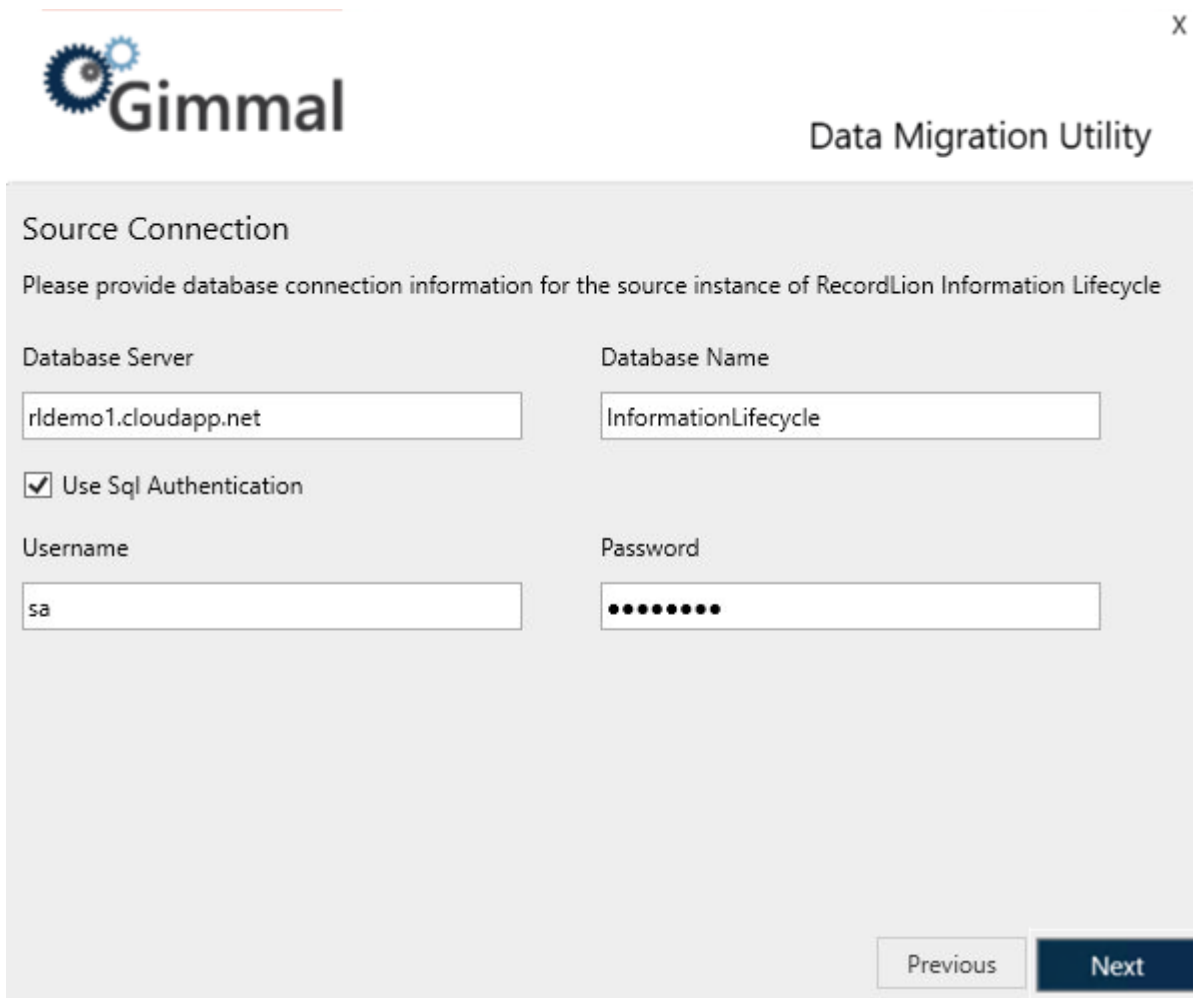
Property Name	Mapping Name	Notes
Title	Title	
Description	Description	
Property Name	PropertyName	

6.17.3 Migrate

If you selected Migrate from the Welcome screen, this section will guide you through the wizard.

6.17.3.1 Source Connection

The next screen you will be presented with is the Source Connection Screen. In this screen, enter the connection information to the Information Lifecycle Server Database for the source data. Click **Next**.



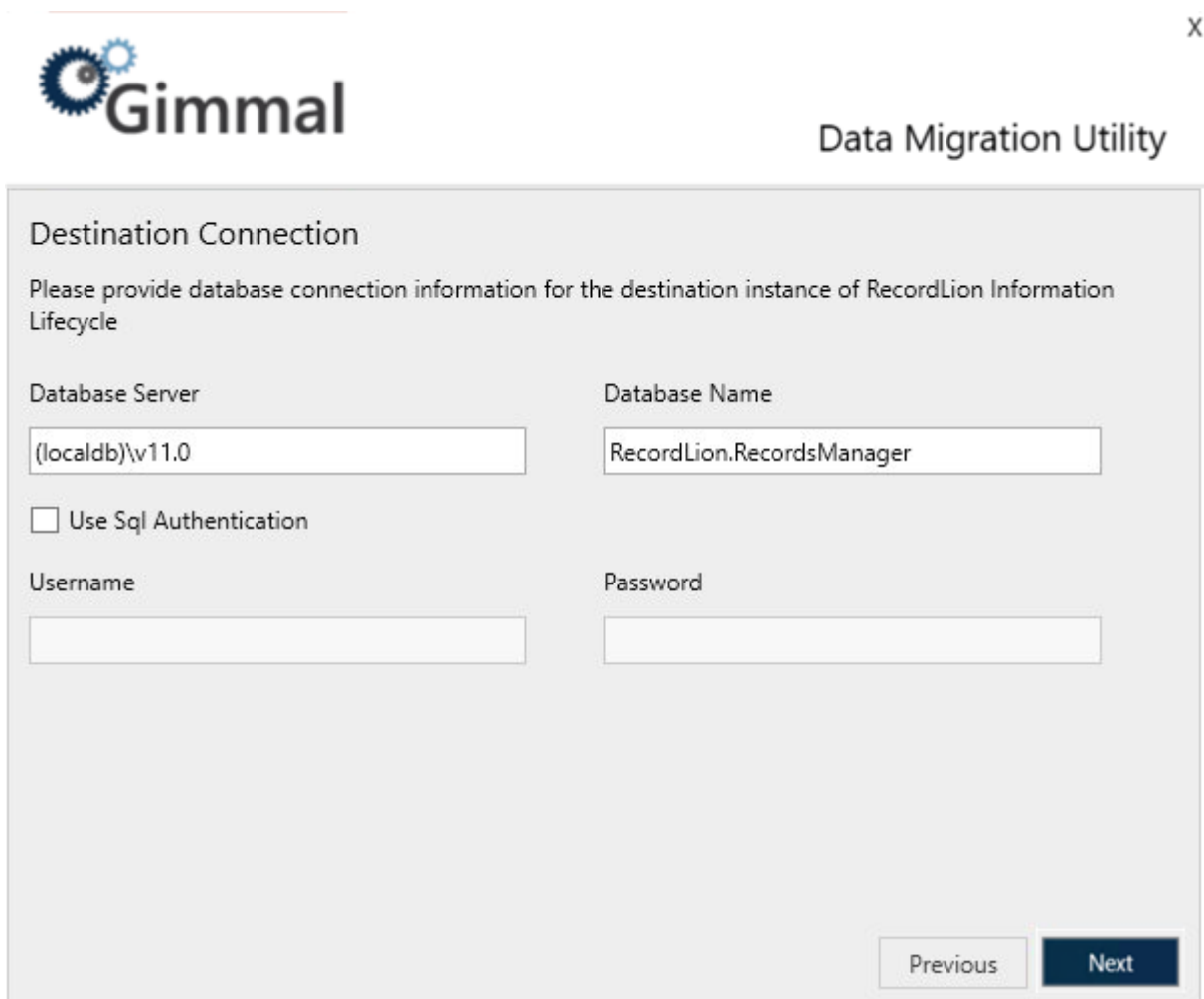
The screenshot shows a web application window titled "Data Migration Utility" with the Gimmel logo in the top left. The main content area is titled "Source Connection" and contains the following fields and controls:

- Database Server:** A text input field containing "rldemo1.cloudapp.net".
- Database Name:** A text input field containing "InformationLifecycle".
- Use Sql Authentication:** A checked checkbox.
- Username:** A text input field containing "sa".
- Password:** A password input field with 10 dots.

At the bottom right, there are two buttons: "Previous" (disabled) and "Next" (active).

6.17.3.2 Destination Connection

The next screen you will be presented with is the Destination Connection Screen. In this screen, enter the connection information to the Information Lifecycle Server Database where data should be migrated to.



Destination Connection

Please provide database connection information for the destination instance of RecordLion Information Lifecycle

Database Server: (localdb)\v11.0

Database Name: RecordLion.RecordsManager

Use Sql Authentication

Username: [Empty]

Password: [Empty]

Previous Next

6.17.3.3 Record Class Selection

The next screen you will be presented with is the Record Class Selection Screen. On this screen you choose the Record Classes that you want to migrate from the Source Connection to the Destination Connection. To select a Record Class, simply click on it. To select multiple Record Classes, hold **Shift** while clicking to select a range or **Control** to select multiple individual Record Classes. Once finished selecting, click **Next**.



X

Data Migration Utility

Record Class Selection

Please select the Record Classes that you would like migrated from the Source to the Destination

Reload

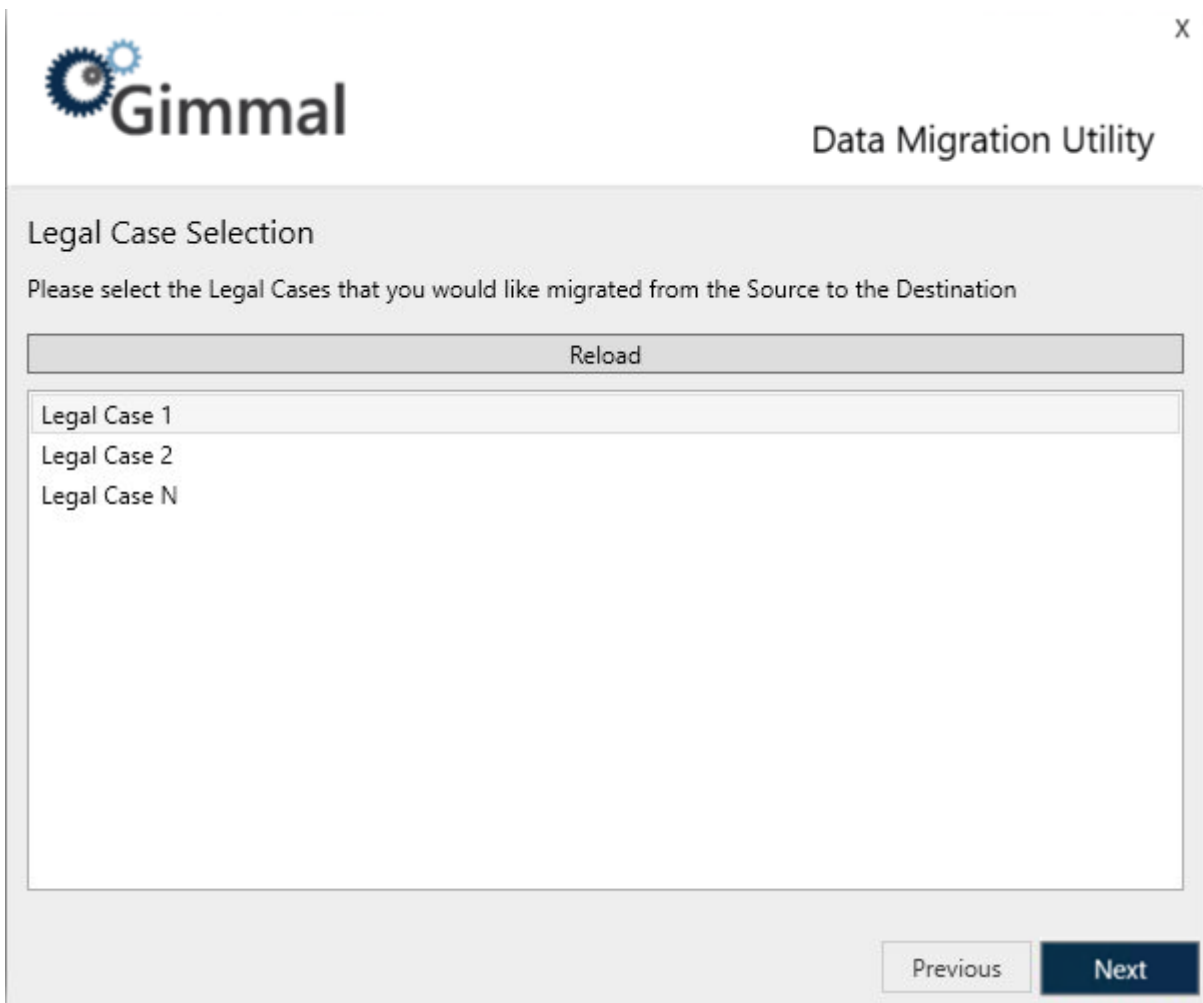
Accounting
Budget
Contracts
Finance
Government Contracts
Human Resources
Test 1
Third Party Contracts

Previous

Next

6.17.3.4 Legal Case Selection

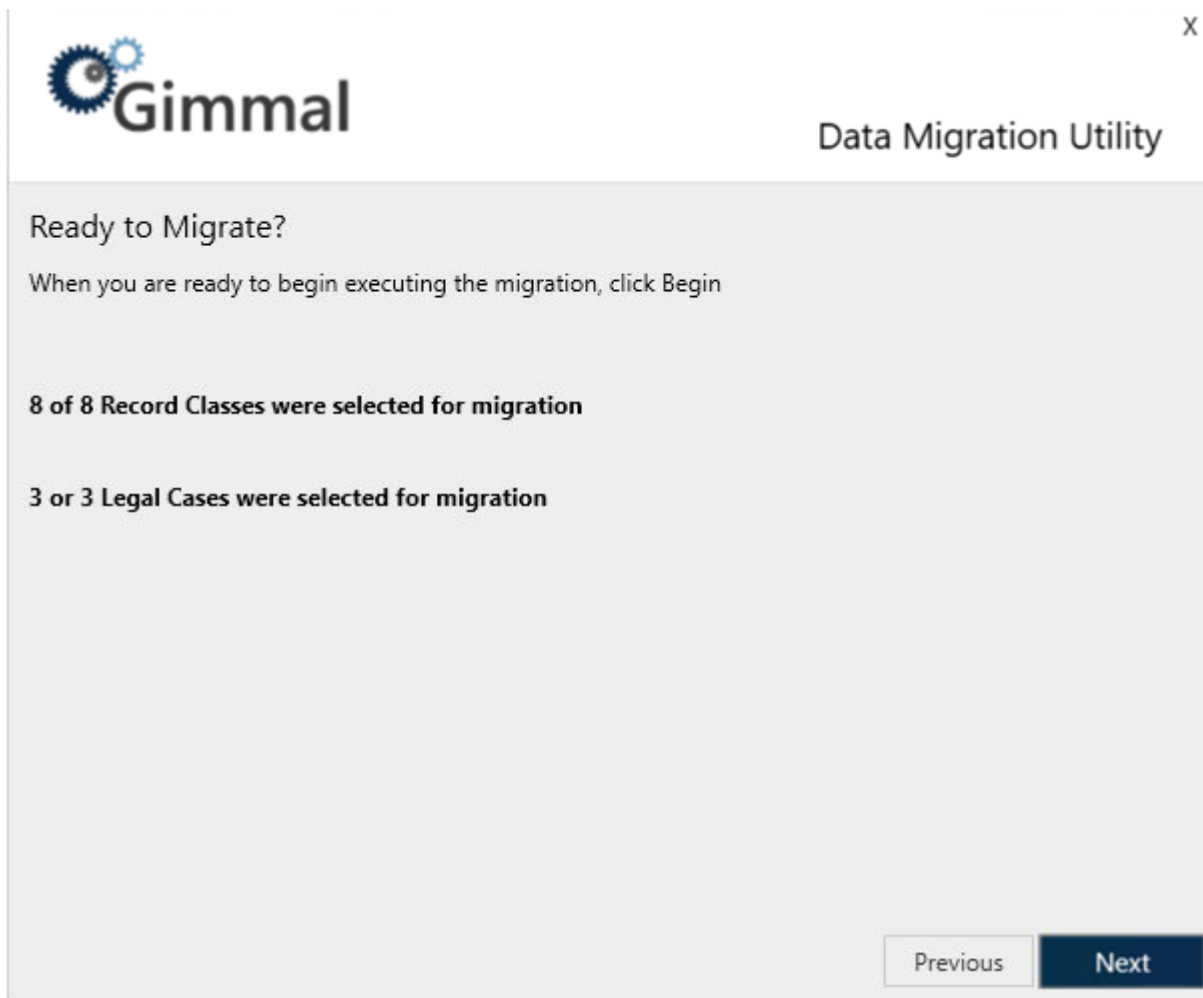
The next screen you will be presented with is the Legal Case Selection Screen. On this screen, you choose the Legal Cases that you want to migrate from the Source Connection to the Destination Connection. To select a Legal Case, simply click on it. To select multiple Legal Cases, hold **Shift** while clicking to select a range or **Control** to select multiple individual Legal Cases. Once finished selecting, click **Next**.



The screenshot shows a web application window titled "Data Migration Utility" with the Gimmel logo in the top left. The main heading is "Legal Case Selection". Below the heading is the instruction: "Please select the Legal Cases that you would like migrated from the Source to the Destination". A "Reload" button is centered above a list box containing three items: "Legal Case 1", "Legal Case 2", and "Legal Case N". At the bottom right, there are two buttons: "Previous" and "Next".

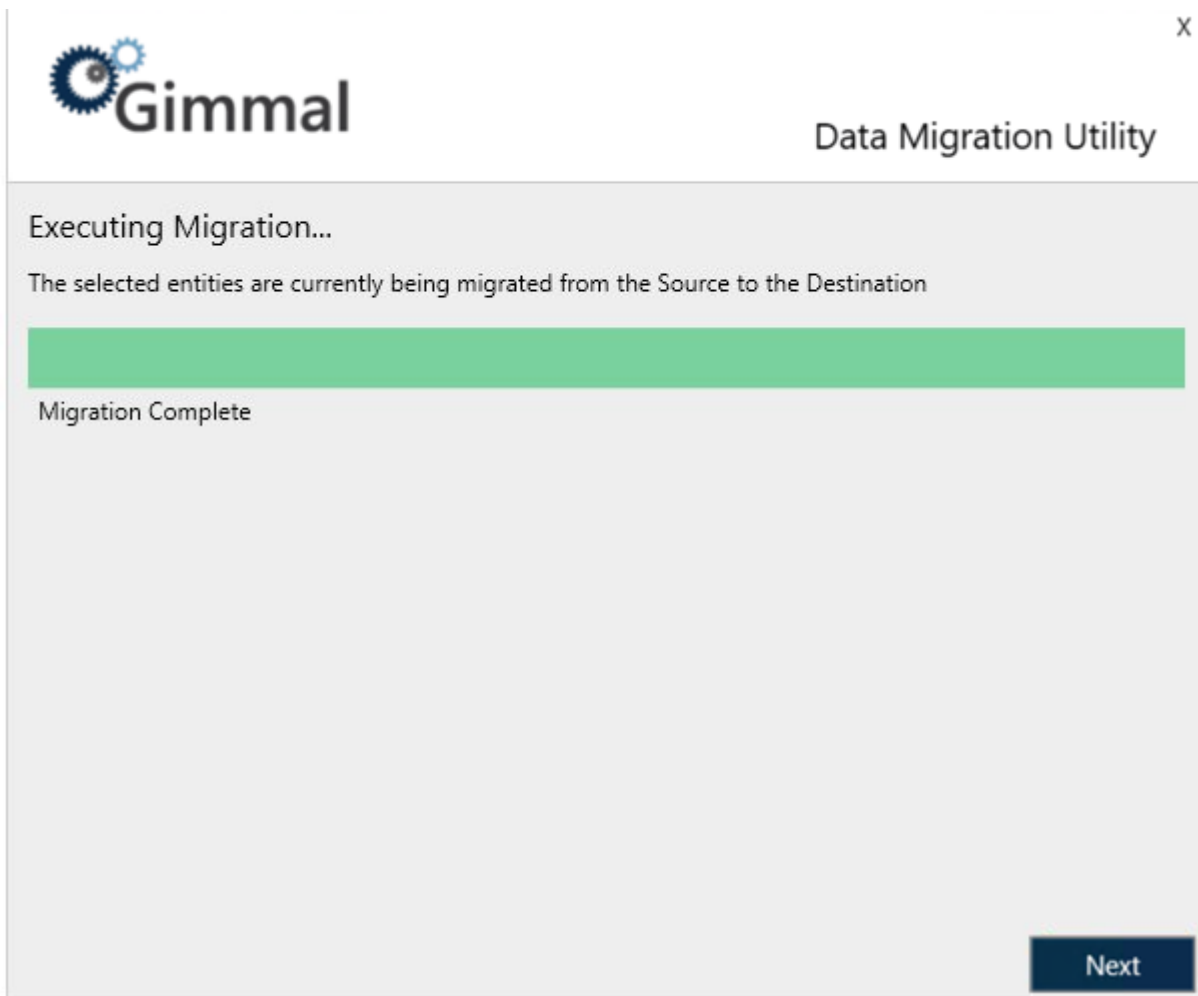
6.17.3.5 Ready to Migrate

The next screen displayed is the Record to Migrate Screen. This screen summarizes the number of Record Classes and Legal Cases selected and provides a button to kick off the migration. Click **Begin** to start the migration process.



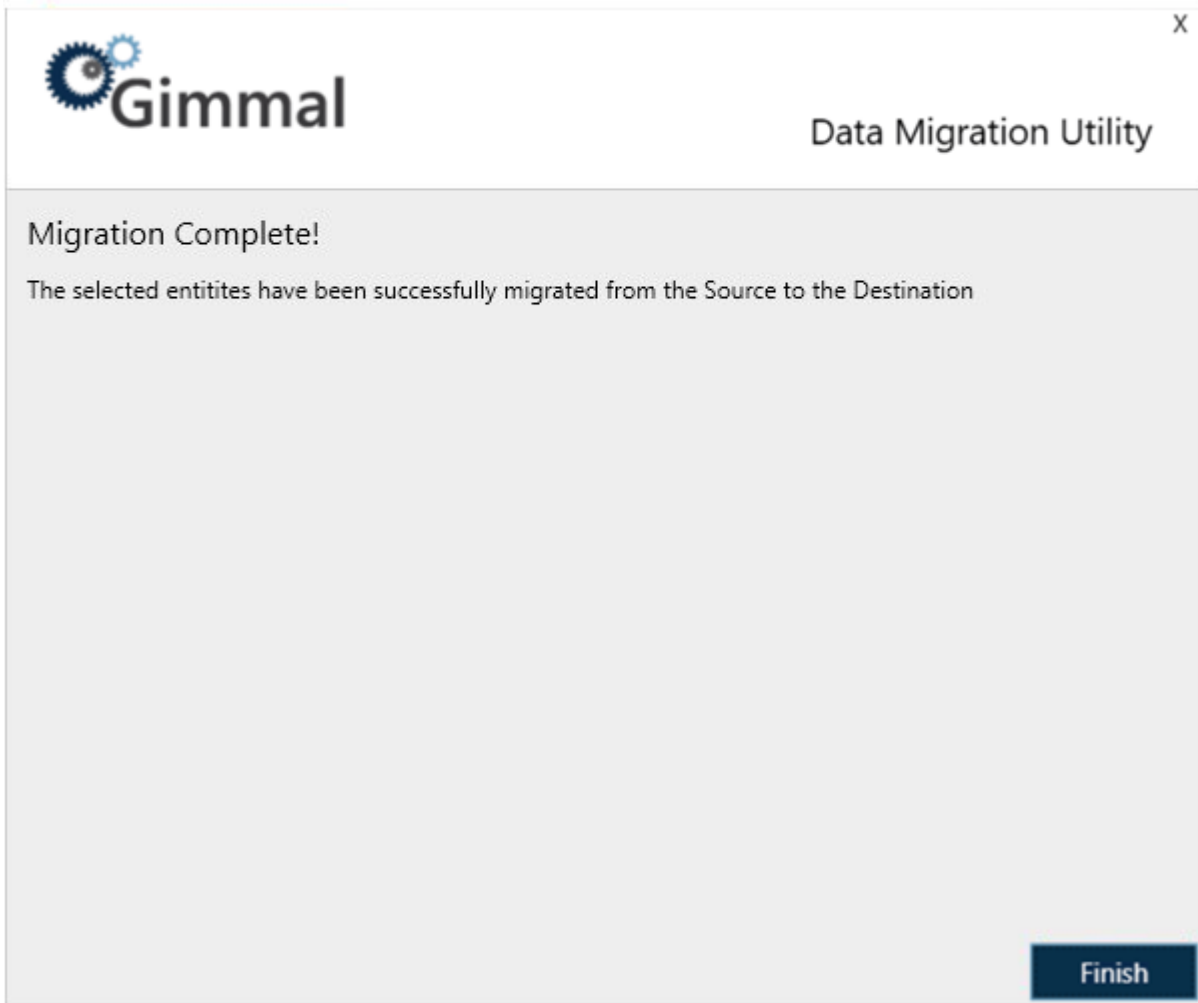
6.17.3.6 Executing Migration

After kicking off the migration, the next screen displayed is the Executing Migration Screen. This screen displays the progress of the migration while it is executing. Once the migration has finished executing, click **Next**.



6.17.3.7 Migration Complete

The final screen displayed is the Migration Complete Screen. This screen simply notifies you that the migration has been completed. Click **Finish** to exit the utility.



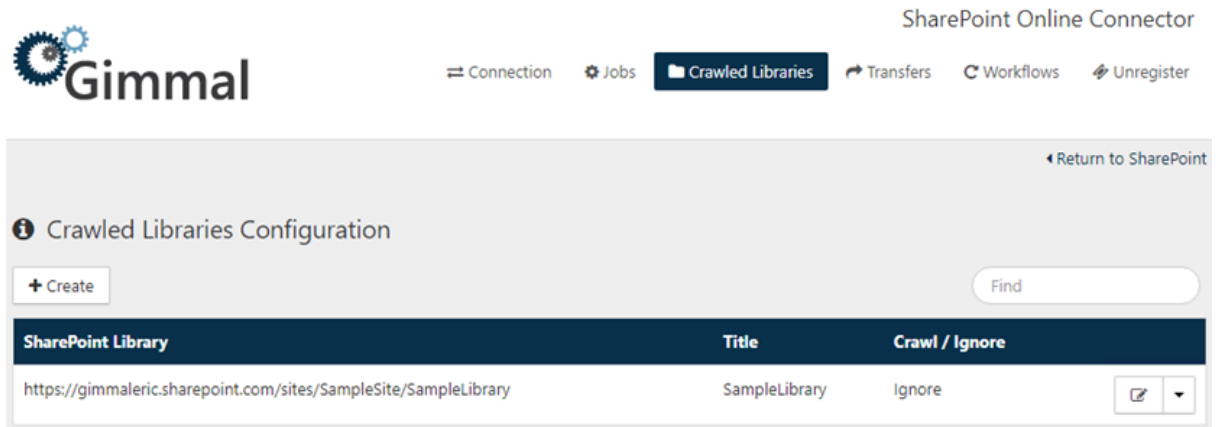
6.18 Setting Up Crawl Library Overrides

6.18.1 Background

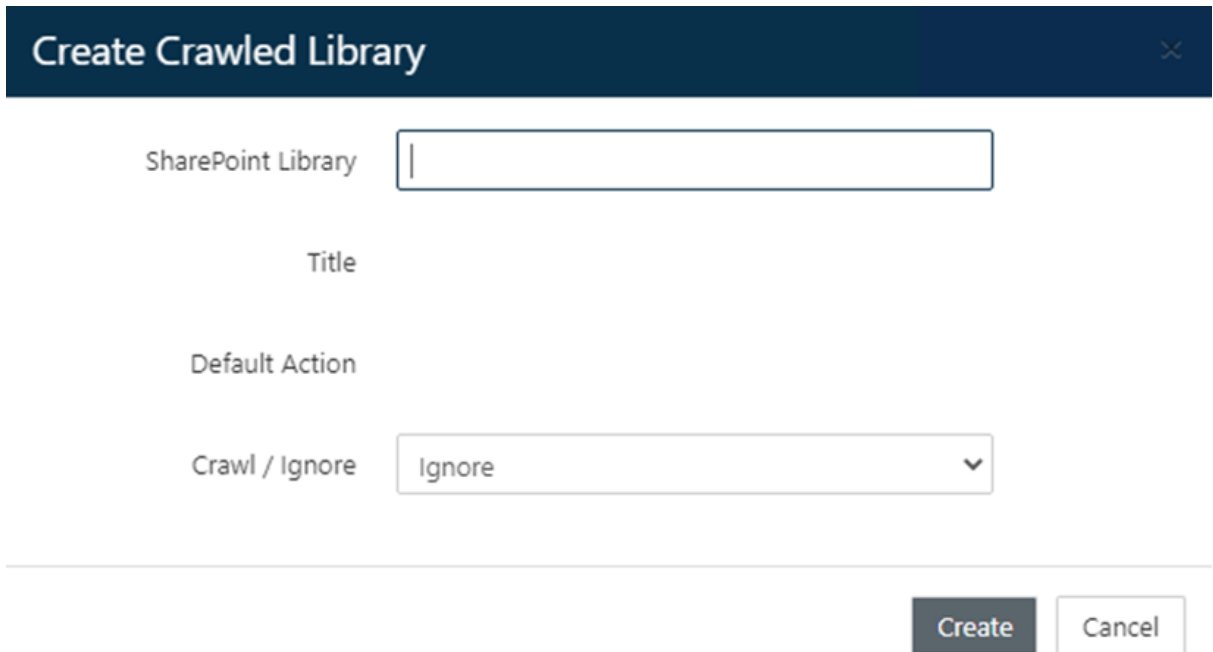
By default, the SharePoint Online Connector manages content in Document Libraries that are not hidden and are not excluded from a search. The Crawled Libraries tab allows for customized control of this behavior, allowing the creation of overrides to crawl content in hidden libraries or to ignore content in non-hidden libraries.

6.18.2 Creating a New Library Override

1. Open the SharePoint Online Connector app by navigating to the site contents of the site where it is deployed.
2. Click the link **Crawled Libraries** to view and manage all existing Library Overrides.



3. Click the button +Create on the Crawled Library page. The Create Crawled Library dialog opens.



4. In the **SharePoint** Library field, enter the URL to a SharePoint Document Library in the list of sites with which the SharePoint Online Connector is currently registered. Upon exiting the URL field, the URL will be validated. If it is valid the system will populate the Library’s Title and Default Action determining whether it would currently be Crawled or Ignored by the SharePoint Online Connector’s jobs.

Create Crawled Library
✕

SharePoint Library

Title HiddenLibrary

Default Action Ignore

Crawl / Ignore

5. Select an option from the dropdown **Crawl / Ignore** to specify whether the selected library will be crawled or ignored as an override. This override will supersede the default behavior for a library.

Create Crawled Library
✕

SharePoint Library

Title HiddenLibrary

Default Action Ignore

Crawl / Ignore

Ignore
Crawl
Ignore

6. If an override changes a Library's existing behavior from Crawl to Ignore or from Ignore to Crawl, a **Post-Override Action** field will appear. This will allow for a one-time, immediate action to be started by the Connector.

Create Crawled Library
✕

SharePoint Library

Title

Default Action

Crawl / Ignore

Post-Override Action

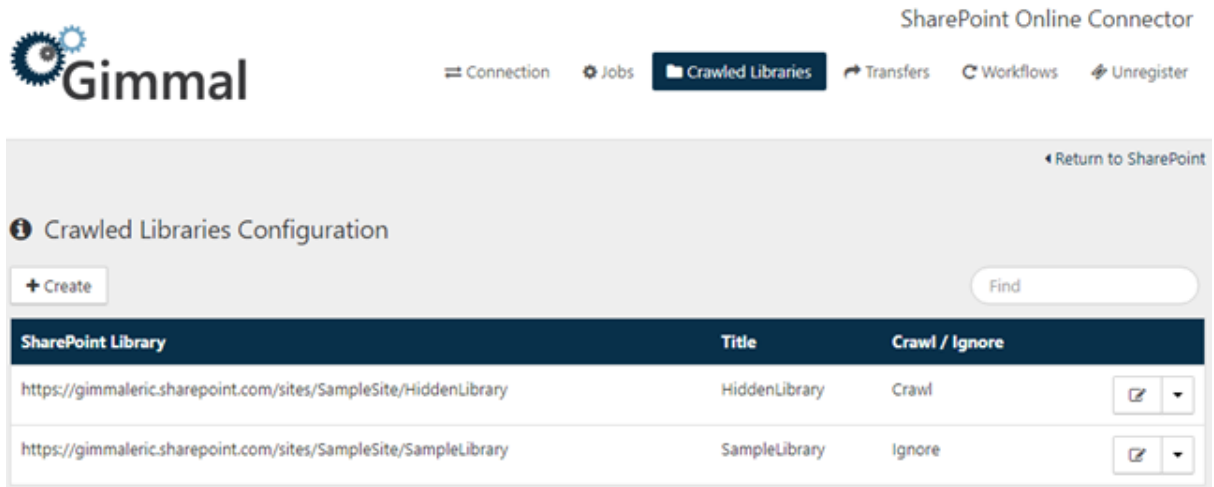
No Action

Run Classification

The Post-Override Actions are as follows:

Post-Override Action Type	Time Available	Description
No Action	Always (default).	No additional action is taken.
Run Classification	When a Library would go from being Ignored to Crawled.	Files in the newly crawled Library are queued to be ingested into Gimmel Records (along with any other new or modified files in that Library's overall Site).
Remove Records	When a Library would go from being Crawled to Ignored.	Records corresponding to the newly ignored Library's files are queued for removal in Gimmel Records. Note that without selecting this action, Records will not be removed from ignored Libraries unless the site is unregistered from the connector.

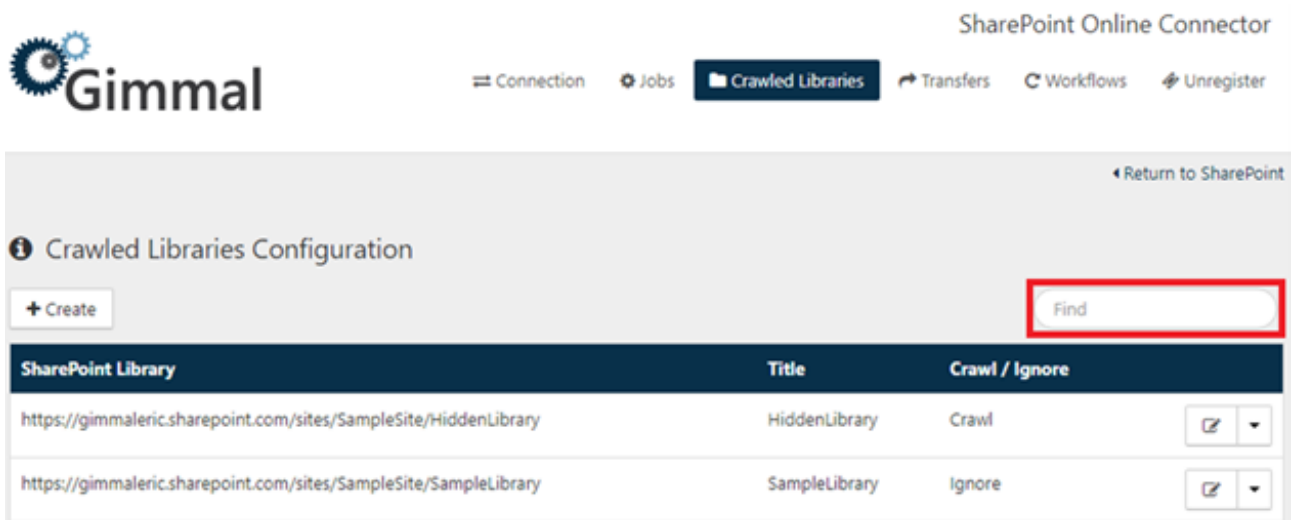
- Click **Create** to confirm the creation of the new override.



Overrides will automatically be applied to all future processing in the SharePoint Online Connector. This includes Classification Jobs (both Full and Incremental) which produces Records from managed SharePoint content, and Retention Jobs which apply lock and disposition actions onto managed SharePoint content.

6.18.2.1 Managing Existing Library Overrides

Existing overrides can be viewed and managed through the Crawled Libraries tab. The full list of overrides for all registered sites is shown and can be searched by Title or Url using the upper right Find search box (in the red rectangle pictured below).



6.18.2.2 Editing Existing Library Overrides

1. From the **Crawled Libraries** tab, click the **Edit Icon** on the right side of an individual override. This will open the Edit Crawled Library dialog. From this dialog, the current override behavior can be toggled between Crawl and Ignore. Nothing else is editable on this dialog.

Edit Crawled Library ✕

SharePoint Library `https://gimmaleric.sharepoint.com/sites/SampleSite/HiddenLibrary`

Title `HiddenLibrary`

Default Action `Ignore`

Crawl / Ignore `Crawl` ▼

- Crawl
- Ignore

Save

2. If the override behavior were to change the current Crawl/ Ignore state, a Post-Override Action Field will appear. This follows the same behavior as detailed above in the **Creating a New Library Override** section.

✕

Edit Crawled Library

SharePoint Library <https://gimmaleric.sharepoint.com/sites/SampleSite/HiddenLibrary>

Title HiddenLibrary

Default Action Ignore

Crawl / Ignore Ignore ▾


Post-Override Action
 No Action ▾
No Action
 Remove Records

Save
Cancel

- To save the new setting, click the **Save** button at the bottom of the dialog.

6.18.2.3 Deleting Existing Library Overrides

- From the **Crawled Libraries** tab, click **Delete** from an individual override’s dropdown menu.



SharePoint Online Connector
≡ Connection ⚙ Jobs 📁 Crawled Libraries ↔ Transfers 🔄 Workflows 🗑 Unregister

◀ Return to SharePoint

Crawled Libraries Configuration

+ Create

SharePoint Library	Title	Crawl / Ignore	
https://gimmaleric.sharepoint.com/sites/SampleSite/HiddenLibrary	HiddenLibrary	Ignore	✎ ▾
https://gimmaleric.sharepoint.com/sites/SampleSite/SampleLibrary	SampleLibrary	Ignore	✖ Delete

- If the deletion of an override were to change a Library’s Crawl/ Ignore state, a Post-Override Action Field will appear (as pictured below). This follows the same behavior as listed above in the **Creating a New Library Override** and the **Editing Existing Library Overrides** sections.

Delete Crawled Library ✕

SharePoint Library
https://gimmaleric.sharepoint.com/sites/SampleSite/SampleLibrary

Title
SampleLibrary

Default Action
Crawl

Crawl / Ignore
Ignore

Post-Override Action ▼

- No Action
- No Action**
- Run Classification

Delete

3. After clicking the Delete button, the override will be removed, and the system will revert the Library's Crawl / Ignore behavior to its default state.

7 Developer Guide

7.1 SDK

Gimmel Records Management has an SDK available at <https://github.com/recordlion>

7.2 PowerShell CmdLets

7.3 Reporting Tool

7.4 PowerShell CmdLets

The following topics provide the PowerShell Cmdlets supported by each Records Management component.

7.4.1 File Share Connector Web Cmdlets

7.4.2 File Share Connector Service Cmdlets

7.4.3 Lifecycle Services Cmdlets

7.4.4 SharePoint Connector Cmdlets

7.4.5 SharePoint Online Connector Web Cmdlets

7.4.6 SharePoint Online Connector Service Cmdlets

7.4.7 Manager Web Cmdlets


7.4.8 File Share Connector Web Cmdlets

File Share Connector Web supports configuration post installation by using a PowerShell Module installed to the following location:

```
%Install Path%\PowerShell\RecordLion.RecordsManager.FileShare.PowerShell.dll
```

When the File Share Connector Web is installed, the following Cmdlets are pre-registered with PowerShell and should be immediately available. However, if the Cmdlets are not available, simply execute the following command from a PowerShell Script to make the Cmdlets available.

```
Import-Module “%Install Path%
\PowerShell\RecordLion.RecordsManager.FileShare.PowerShell.dll”
```

 %Install Path% should be replaced with the absolute path to where installation was specified.

7.4.8.1 Cmdlets

Set-FileShareWeb

```
Set-FileShareWeb
-SiteName <lstring>
[-ConnectionString <string>]
[-DataProviderType <string>]
[-JsonProviderFileLocation <string>]
```

7.4.9 File Share Connector Service Cmdlets

File Share Connector Services supports configuration post-installation by using a PowerShell Module installed to the following location:

```
%Install Path%\PowerShell\RecordLion.RecordsManager.FileShare.PowerShell.dll
```

When the File Share Connector Services are installed, the following Cmdlets are pre-registered with PowerShell and should be immediately available. However, if the Cmdlets are not available, simply execute the following command from a PowerShell Script to make the Cmdlets available.

```
Import-Module “%Install Path%
\PowerShell\RecordLion.RecordsManager.FileShare.PowerShell.dll”
```

 %Install Path% should be replaced with the absolute path to where installation was specified.Cmdlets

7.4.9.1 Cmdlets

Remove-FileShareClassificationServicePermission

```
Remove-FileShareClassificationServicePermission  
[-ServiceIdentity <pscredential>]  
[-Stop]  
[-Start]  
[-ChangeLogon]  
[-GrantPermissionToServiceIdentity]
```

Remove-FileShareRetentionServicePermission

```
Remove-FileShareRetentionServicePermission  
[-ServiceIdentity <pscredential>]  
[-Stop]  
[-Start]  
[-ChangeLogon]  
[-GrantPermissionToServiceIdentity]
```

Remove-FileShareUnusedSettings

```
Remove-FileShareUnusedSettings
```

Reset-FileShareCrawlState

```
Reset-FileShareCrawlState  
[-DataProviderType <string>]  
[-ConnectionString <string>]  
[-JsonProviderFileLocation <string>]  
[-ManagedLocationPath <string>]
```

Set-FileShareClassificationService

```
Set-FileShareClassificationService  
[-ConnectionString <string>]  
[-ServiceIntervalInMS <int>]  
[-LoggingLevel <string>]  
[-DataProviderType <string>]  
[-JsonProviderFileLocation <string>]
```

```
[-ServiceIdentity <pscredential>]
[-Stop]
[-Start]
[-ChangeLogon]
[-GrantPermissionToServiceIdentity]
```

Set-FileShareConfiguration

```
Set-FileShareConfiguration
[-ConnectionString <string>]
[-DataProviderType <string>]
[-JsonProviderFileLocation <string>]
```

Set-FileShareRetentionService

```
Set-FileShareRetentionService
[-ConnectionString <string>]
[-ServiceIntervalInMS <int>]
[-LoggingLevel <string>]
[-DataProviderType <string>]
[-JsonProviderFileLocation <string>]
[-ServiceIdentity <pscredential>]
[-Stop]
[-Start]
[-ChangeLogon]
[-GrantPermissionToServiceIdentity]
```


7.4.10 Lifecycle Services Cmdlets

Records Management supports the post-installation configuration of Lifecycle Services by using a PowerShell Module installed to the following location:

```
%Install Path%\PowerShell\RecordLion.RecordsManager.PowerShell.dll
```

When Records Management Services are installed, the following Cmdlets are pre-registered with PowerShell and should be immediately available. However, if the Cmdlets are not available, simply execute the following command from a PowerShell Script to make the Cmdlets available.

```
Import-Module “%Install Path%\PowerShell\RecordLion.RecordsManager.PowerShell.dll”
```

 %Install Path% should be replaced with the absolute path to where installation was specified.

7.4.10.1 Cmdlets

Get-RetentionServiceStatus

```
Get-RetentionServiceStatus
[-SQLTimeout <int>]
```

Remove-RetentionServicePermission

```
Remove-RetentionServicePermission
[-ServiceIdentity <pscredential>]
[-Stop]
[-Start]
[-ChangeLogon]
[-GrantPermissionToServiceIdentity]
```

Set-IndexRebuildInterval

```
Set-IndexRebuildInterval
-Interval <IndexRebuildInterval> {None | Hourly | Daily | Weekly}
[-RebuildStartHour <int>]
[-SQLTimeout <int>]
```

Set-RetentionService

```
Set-RetentionService
[-ConnectionString <string>]
[-ServiceIntervalInMS <int>]
[-AuditLifespanInDays <int>]
[-LoggingLevel <string>]
[-ServiceIdentity <pscredential>]
[-Stop]
[-Start]
[-ChangeLogon]
[-GrantPermissionToServiceIdentity]
```

7.4.11 SharePoint Connector Cmdlets

SharePoint Connector supports configuration post-installation by using a PowerShell Module installed to the following location:


```
%GAC%\RecordLion.RecordsManager.SharePoint.PowerShell.dll
```

In order to use the Cmdlets contained within this module, simply execute the following command from a PowerShell Script.

```
[System.Reflection.Assembly]::LoadWithPartialName(
"RecordLion.RecordsManager.SharePoint.PowerShell") | Import-Module
```

7.4.11.1 Cmdlets

Get-ConnectorConfiguration

```
Get-ConnectorConfiguration
```

Set-ConnectorConfiguration

```
Set-ConnectorConfiguration
[-ServerUrl <string>]
[-Credentials <pscredential>]
[-ClassificationBatchSite <int>]
[-ClientTimeout <int>]
```

Start-SPConnectorFullCrawl

```
Start-SPConnectorFullCrawl
[-Confirm]
[-CrawlWebApp]
[-Folder <spfolder>]
[-Force]
[-List <splist>]
[-RelativeFolderUrl <string>]
[-RelativeListUrl <string>]
[-RelativeWebUrl string]
[-Site <spsite>]
[-SiteUrl <string>]
[-Web <spweb>]
[-WebAppJobScope]
[-WhatIf]
```


7.4.12 SharePoint Online Connector Web Cmdlets

SharePoint Online Connector Web supports the configuration post installation by using a PowerShell Module installed to the following location:

```
%Install Path%\PowerShell\RecordLion.RecordsManager.SPOnline.PowerShell.Web.dll
```

When the SharePoint Online Connector Web is installed, the following Cmdlets are pre-registered with PowerShell and should be immediately available. However, if the Cmdlets are not available, simply execute the following command from a PowerShell Script to make the Cmdlets available.

```
Import-Module “%Install Path%  
\PowerShell\RecordLion.RecordsManager.SPOnline.PowerShell.Web.dll”
```

 %Install Path% should be replaced with the absolute path to where installation was specified.

Cmdlets

7.4.12.1 Set-SPOConnectorWeb

```
Set-SPOConnectorWeb  
-SiteName <string>  
[-ClientId <string>]  
[-ClientSecret <string>]  
[-ConnectionString <string>]
```


7.4.13 SharePoint Online Connector Service Cmdlets

SharePoint Online Connector Service supports configuration post-installation by using a PowerShell Module installed to the following location:

```
%Install Path%\PowerShell\RecordLion.RecordsManager.SPOnline.PowerShell.Service.dll
```

When the SharePoint Online Connector Service is installed, the following Cmdlets are pre-registered with PowerShell and should be immediately available. However, if the Cmdlets are not available, execute the following command from a PowerShell Script to make the Cmdlets available.

```
Import-Module “%Install Path%  
\PowerShell\RecordLion.RecordsManager.SPOnline.PowerShell.Service.dll”
```

 %Install Path% should be replaced with the absolute path to where installation was specified.

7.4.13.1 Cmdlets

Get-SPOClientSecretEndDate

```
Get-SPOClientSecretEndDate
-ClientId <string>
-Credentials <pscredential>
```

Get-SPOJobSchedule

```
Get-SPOJobSchedule
-JobType <JobType> {Custom | FullClassification | IncrementalClassification |
Retention}
[-CustomJobId <guid>]
```

Invoke-SPOJobSchedule

```
Invoke-SPOJobSchedule
-JobSchedule <JobScheduleModel>
```

New-SPOClientSecret

```
New-SPOClientSecret
```

Register-SPAppSetting

```
Register-SPAppSetting
-SPHostUrl <string>
-SPSiteUrl <string>
-SPSiteId <guid>
-SPWebId <guid>
```

Set-ServicePrincipalClientSecret

```
Set-ServicePrincipalClientSecret
-ClientSecret <string>
-ClientId <string>
-Credentials <pscredential>
```

```
[-Duration <timespan>]
```

Set-SPOConnectorService

```
Set-SPOConnectorService  
[-ConnectionString <string>]  
[-ClientId <string>]  
[-ClientSecret <string>]  
[-ServiceIdentity <pscredential>]  
[-Stop]  
[-Start]  
[-ChangeLogon]  
[-GrantPermissionToServiceIdentity]
```

Set-SPOJobSchedule

```
Set-SPOJobSchedule  
-JobSchedule <JobScheduleModel>
```

Unblock-SPListItem

```
Unblock-SPListItem  
-ItemUrl <string>  
-SPOnlineCreds <pscredential>
```


7.4.14 Manager Web Cmdlets

The Manager Web supports configuration post installation by using a PowerShell Module installed to the following location:

- %Install Path%\PowerShell\RecordLion.RecordsManager.Web.PowerShell.dll

When the Manager Web is installed, the following Cmdlets are pre-registered with PowerShell and should be immediately available. However, if the Cmdlets are not available, simply execute the following command from a PowerShell Script to make the Cmdlets available.

```
Import-Module “%Install Path%  
\PowerShell\RecordLion.RecordsManager.Web.PowerShell.dll”
```

 %Install Path% should be replaced with the absolute path to where installation was specified. For an example on how to run several of these commands, see [\(Link\) Configuring Fully Qualified Domain Name \(FQDN\)](#).

7.4.14.1 Cmdlets

Get-Record

```
Get-Record  
[-RecordUri] <string>  
[-SQLTimeout] <int>
```

Remove-AuditEntries

```
Remove-AuditEntries  
[-Record] <RecordModel>  
[-SQLTimeout] <int>
```

Remove-Record

```
Remove-Record  
[-RecordUri] <string>  
[-PathUri] <string>  
[-SQLTimeout] <int>
```

Remove-UnresolvedAuditEntries

```
Remove-UnresolvedAuditEntries  
[-CreatedBefore] <datetime>  
[-SQLTimeout] <int>
```

Set-RecordsManagerSTSWeb

```
Set-RecordsManagerSTSWeb  
[-SiteName] <string>  
[-BaseUrl] <string>  
[-AllowHttp] <bool>  
[-CertificateIdentity] <string>  
[-IssuerName] <string>  
[-ExpectedAddress] <string>  
[-SigningCertificateSubjectName] <string>  
[-EncryptingCertificateSubjectName] <string>
```

Set-RecordsManagerWeb

```

Set-RecordsManagerWeb
[-SiteName] <string>
[-SiteUrl] <string>
[-AllowHttp] <bool>
[-PageSize] <int>
[-DialogPageSize] <int>
[-AudtPageSize] <int>
[-ConnectionString] <string>
[-WSFedMetaUrl] <string>
[-WSFedMetaRealm] <string>
[-WSFedMetaReply] <string>
[-WSFedMetaAudience] <string>
[-WSTrustUrl] <string>
[-SessionTimeout] <int>
[-ReportCacheDirectory] <string>
[-ReportDirectory] <string>
[-InitialRecordizationMode] <bool>
[-DaysUntilExpiration] <int>

```

Set-TemporaryAuditEntriesResolved

```

Set-TemporaryAuditEntriesResolved
[-SQLTimeout] <int>

```

Set-UserAccount

```

Set-UserAccount
-Credentials <pscredential>
-NewCredentials <pscredential>
[-SQLTimeout] <int>

```

7.5 Reporting Tool

Version: 1.0 and above (Not compatible with the cloud version)

7.5.1 Overview

Records Management contains a built-in report designer tool for use only with the Records Management SQL Server database. The reporting engine, user interface, and designer are licensed to you from a third-party tool called Telerik Reporting. You are free to use the designer on the server, or make a copy of the designer executable for use on client machines, as long as the reports are only used by Records Management by copying the custom reports to the appropriate server location defined in this documentation. See Reporting Licensing for more information.

While this section outlines the usage of the reporting tool, Telerik provides complete documentation on their reporting tool at:

- <http://docs.telerik.com/reporting/overview>
- <http://docs.telerik.com/reporting/standalone-report-designer>
- <http://docs.telerik.com/reporting/designing-reports>

In addition to the ability to create custom reports, there are 20+ standard reports that are included. Any user with the appropriate permission can run the standard reports or the custom reports. There are two report formats:

Report Format	Description
Compiled	These reports are built-in and will always show in the Reports section. These are pre-defined reports that are created with Visual Studio, compiled and DLL-based. They cannot be edited. There are 20+ compiled reports included.
Custom	These are reports that are created with the Report Designer Tool and are considered Declared Reports. They are XML-based (.trdx extension) and can be edited. There are not any custom reports included.

7.5.2 Reporting Licensing

In conformance with the End User License Agreement for Records Management, you are also licensed to use the Report Designer Program as part of Records Management. You can use the Report Designer with the following restrictions:

- You may not distribute or use the software for any purpose other than using the Records Management database as the data source.
- Users may only view reports using the Records Management web application; you may not disassemble the code, or attempt in any manner to reconstruct, discover, reuse or modify any source code or underlying algorithms of the Software. For avoidance of doubt, you are not permitted to use the Report Designer Program, or any portions thereof, for software development or application development purposes unless you also purchase a separate commercial license from Telerik for each of the users.

7.5.3 Report Life Cycle

Understanding the report life cycle is crucial to effectively using Telerik Reporting. See the link below for a detailed explanation on the life cycle.

<http://docs.telerik.com/reporting/designing-reports-life-cycle>

7.5.4 Report Deployment

To view a custom report within Records Management, the report needs to be deployed.

1. Deploy the report by copying the .trdx files to all Records Management servers in the farm. They should be deployed to the same location as the Telerik Report Designer executables.
 - %program files%/gimmel/information lifecycle/web/reports

2. Deploy the Report Descriptor File (Optional). By default, the report will display as the same name as the .trdx file. This is not very user friendly, so Records Management provides the ability to create a Report Descriptor File with additional report information. This is not part of the Telerik product; this is an added feature provided by Records Management.
 - The Report Descriptor File should have the same name as the .trdx file, except it will have an .xml extension.
 - It should be copied to the same location as the .trdx file.
 - The format of the Report Descriptor File is shown below:


```
<report> <name> Custom Report Name </name> <description> This is an example of a Custom Report created with the Standalone Report Designer </description> </report>
```

7.5.5 Database Schema for Reporting

When creating a custom report, you will need to define queries that go directly against the Information Lifecycle database. When defining these queries in a local installation, many of the tables and fields are self-evident. If assistance is needed in writing a custom report, please contact Gimmel to discuss a Premier Services engagement.

Please submit a [Support Ticket](#)¹²⁰ requesting this information if desired.

7.5.6 Creating Custom Reports

 Custom Reports can only be created when running an on-premise version of the Records Management Core.

These are the high-level steps required when creating a custom report. Each step is described in further detail below.

1. Open the Report Designer.
2. Select a Template.
3. Select a Data Source.
4. Build the report.
5. Preview the report.

Define a Data Source with a Connection String

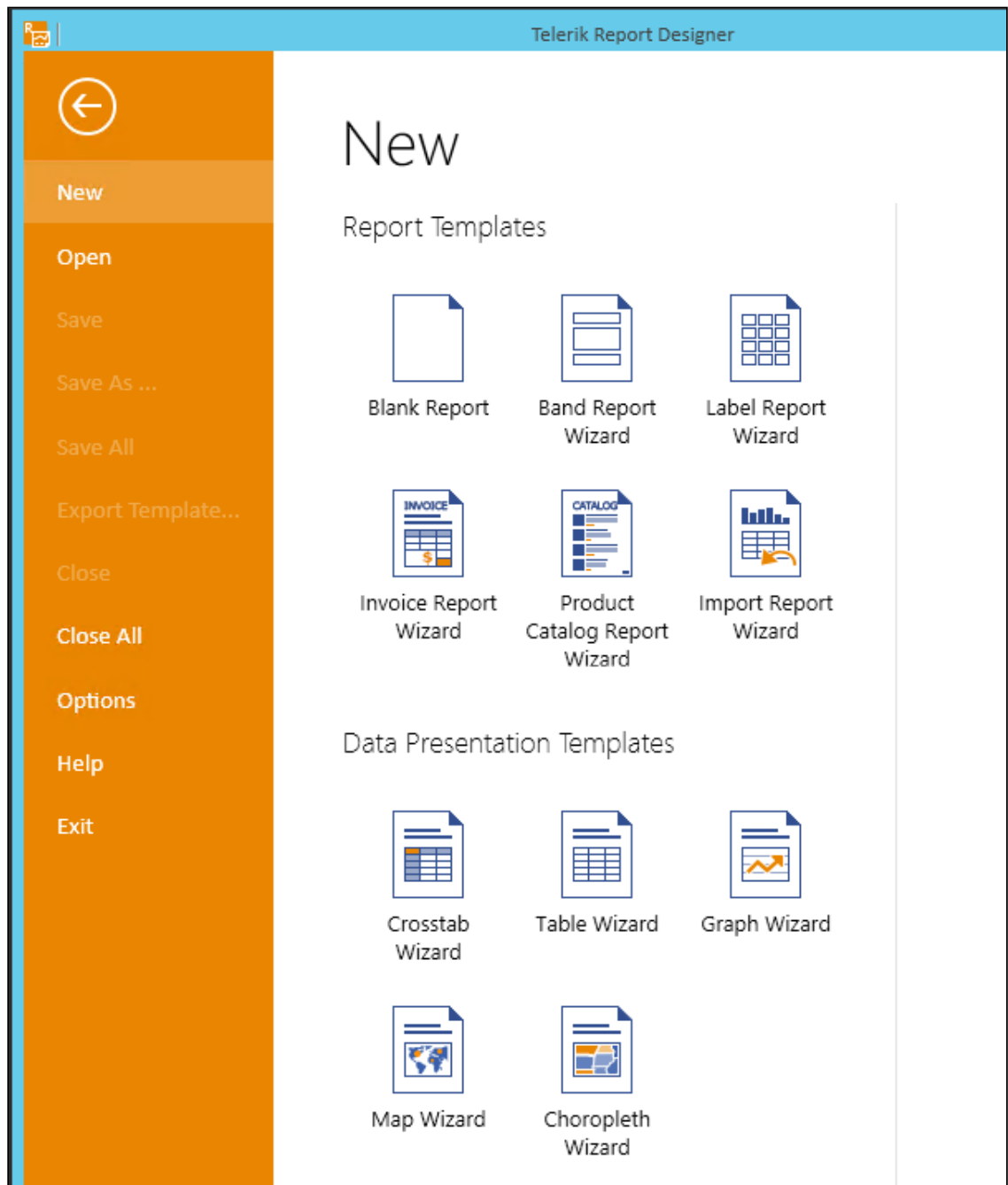
- **Local** - These are embedded inside of the report.
- **Shared** - These provide a connection string name in the file and this is a look-up value that will find the value in a configuration file. These are located in a user.config file that is in the App Data directory. The recommendation is to use the Shared Connection String "DefaultConnection". This is the same name that is used inside of Information Lifecycle.

1. Open the Report Designer
 - It is located at: C:\Program Files\Gimmel\Records Management\web\reports
 - There are two EXEs that are included; a 64-bit version and the x86 version. If you are developing these reports from the server, you will use the 64-bit version. If you are going to create the reports from your local desktop and you do not have a 64-bit desktop machine, then you will use the x86 version. In this case, you will copy the EXE and the Config file to your desktop computer.

¹²⁰ <https://support.gimmel.com/hc/en-us>

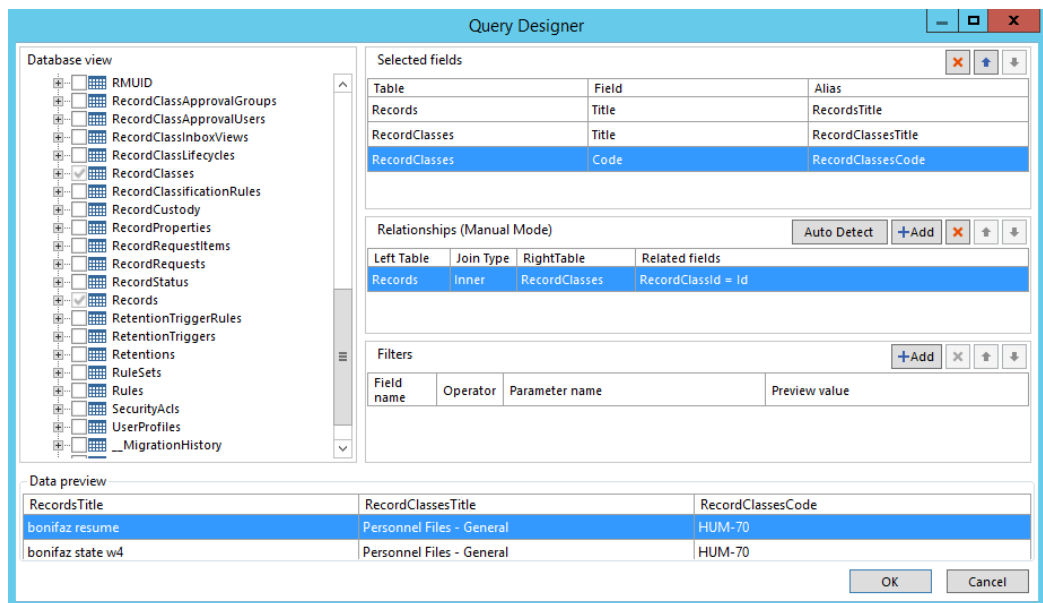
Name	Date modified	Type	Size
readme.txt	2/22/2016 9:58 AM	Text Document	1 KB
Telerik.ReportDesigner.exe	2/4/2016 6:54 PM	Application	13,938 KB
Telerik.ReportDesigner.exe.config	2/10/2016 4:18 PM	Visual Studio Code	3 KB
Telerik.ReportDesigner.x86.exe	2/4/2016 6:54 PM	Application	13,938 KB
Telerik.ReportDesigner.x86.exe.config	2/10/2016 4:18 PM	Visual Studio Code	3 KB

2. Select a Report Template
 - When you open the Report Designer, you can choose to open an existing report or a new report. If you select **New**, you will see a list of Wizards that can be used for creating a report. The wizards will guide you through the process for creating that specific type of report.



- For this example, the Table Wizard report template will be used. Select **Table Wizard**.
 - Select the location to save the report. For simplicity, you can save the report to the same directory where the Telerik EXEs are located. This will make deployment easier. You can save the reports to any directory and deploy them later.
 - Enter a name for your report. **Important:** Ensure the "Save as Type" file name extension is set to **.trdx**.
3. Choose a Data Source. If there is a Data Source already created that is the correct Data Source for the Records Management database, then you can use that Data Source. Otherwise, you will need to create one.
- Click **Add New Data Source...**

- Select **SQL Data Source**
- Enter a name in the **Data Source Name** field. You can use the default name or enter another name.
- Select **OK**
- Choose **Data Connection**. If you have created previous custom reports, you may already have a Connection String that can be used. Otherwise, you will need to create a new Connection String.
 - Select **Build new data connection**.
 - Select **SqlClient Data Provider** in the **Data provider** dropdown.
 - Connection String. You can manually enter or copy and paste a Connection String, or you can have the Wizard assist in creating the Connection String.
 - Select **Build** and the Connection Properties windows will be displayed.
 - Enter the name of the Server that is hosting your SQL Server.
 - Select **Windows Authentication**. When Records Management is installed, it is installed using Windows Integrated authentication. You will need Read rights to the database to be able to develop the reports. If you have SQL Authentication enabled on the server, you could use SQL Server Authentication.
 - Select or enter a database name. Click the drop-down and select "InformationLifecycle" or you may need to enter it manually.
 - Click **Test Connection**. This will validate that you can communication with the database. If this fails, then you may need to coordinate with your database administrator for troubleshooting.
 - Click **OK** and the Connection String will be formulated and copied to the Connection String field on the Configure SQL Data Source window.
 - Click **Next**
- Data Connection Options
 - Select **Use as shared connection**. This is the recommended option. If you select the "Embed" option, the Connection String will be embedded in the report and cannot be re-used. Enter an Alias. Enter "DefaultConnection". This sh
 - Enter an **Alias**. Enter "DefaultConnection". This should be used since this is the name that is used inside of the Records Management. This will enable you to easily move the reports between environments.
 - **Note:** You are only licensed to use the reporting designer with the Information Lifecycle database in accordance with Reporting Licensing.
 - Click **Next**
- Configure data source command. Enter a SQL statement that represents a base data source of the data to be used within the report. It is important to consider how much data you are pulling from the database and how you can optimize the data being pulled. You want to push as much of the work to the SQL Server as possible. You may need to collaborate with your database administrator to determine the best SQL statement.
 - If you need assistance building the SQL statement, you can use the Query Builder tool.
 - Click **Query Builder**
 - Open the Default Schema and you will see a list of all the tables within Records Management.
 - Select the table(s) that is needed for the SQL query. For this example, we are going to select the Records and RecordClasses tables.
 - Select the specific fields that you want to include in the query. For this example, we are going to select:
 - Records - Title
 - RecordClasses - Title, Code
 - The fields selected will be displayed in the Selected Fields section of the window. You can select an Alias for each field if desired. This can be helpful if you have fields that are named the same in two different tables. See the illustration below:

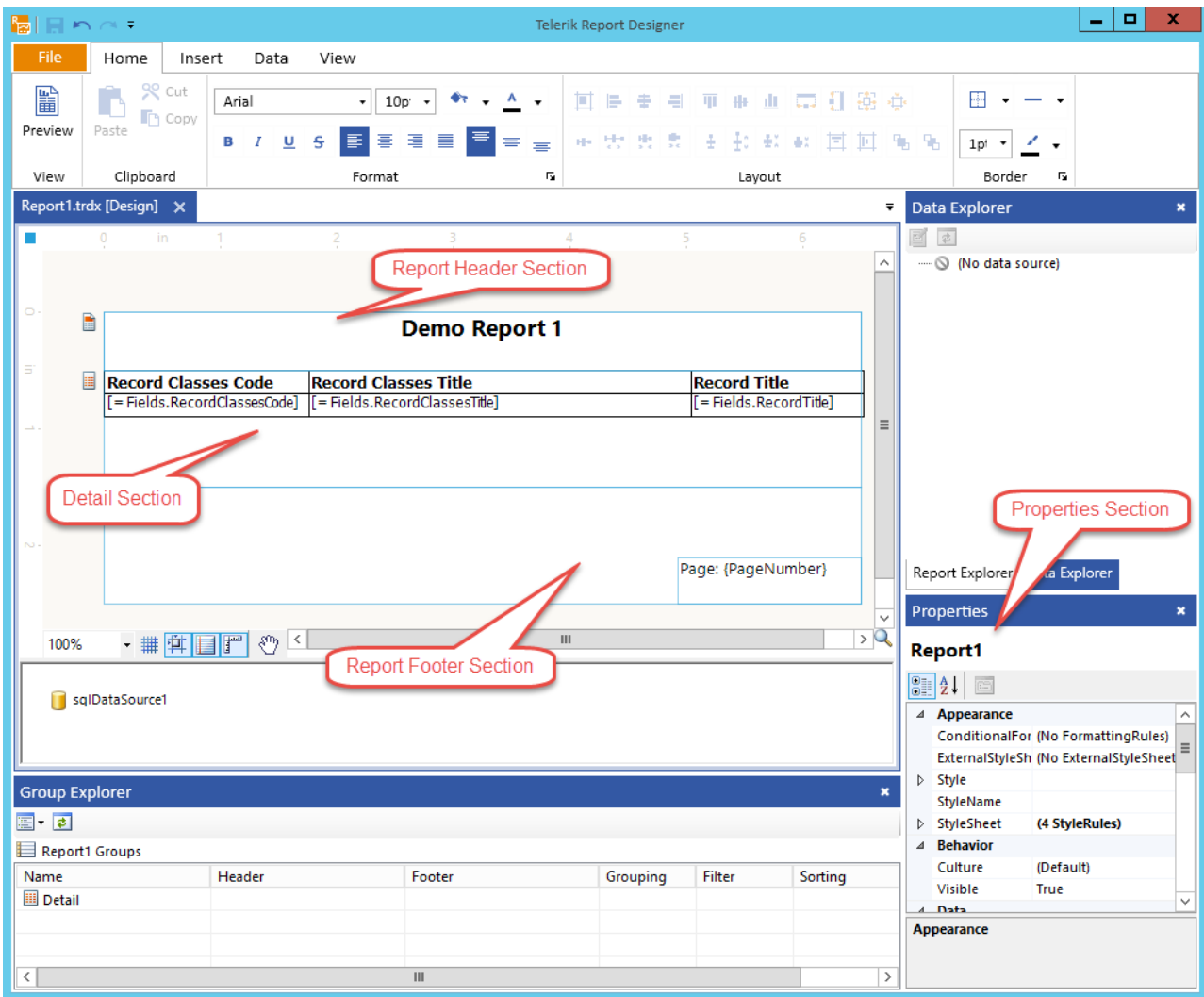


- Validate that the Relationships section contains the correct join for the tables you have selected.
 - Enter any Filters that may be needed.
 - Select **OK**
 - The SQL statement will be displayed in the Select Statement field in the Configure data source command dialog box. See below for an example
 - Select **Next**
4. Preview data source results. Click **Execute Query** to preview the data source results. You can go back and modify your query if the results are not correct.
 5. Click **Finish**.
 6. Select the name of the Data Source that you just created.
 7. Arrange Fields. Drag and drop the fields from the Data Source that you want to include on the report. Use the arrows to arrange the fields in the order you want them displayed.
 8. Click **Next**.
 9. Choose **Style**. Select a style to customize the appearance of the report.
 10. Click **Next**.
 11. Click **Finish** to generate the report.
 12. The Telerik Report Designer opens. See the Telerik Report Designer topic for more details on using the Designer.

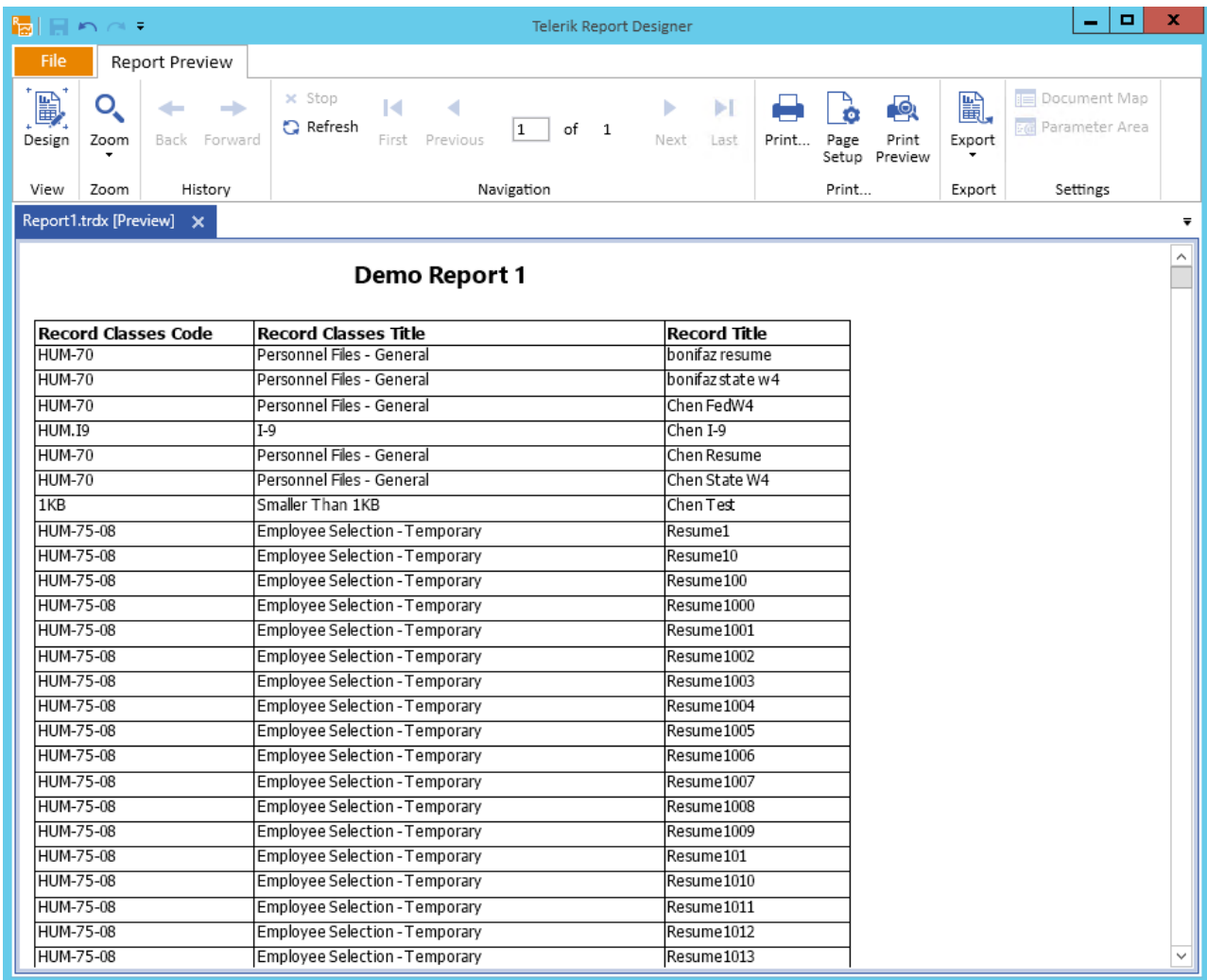
7.5.7 Telerik Report Designer

Complete documentation for the Telerik Report Designer can be found at: <http://docs.telerik.com/reporting/standalone-report-designer#standalone-report-designer-elements>

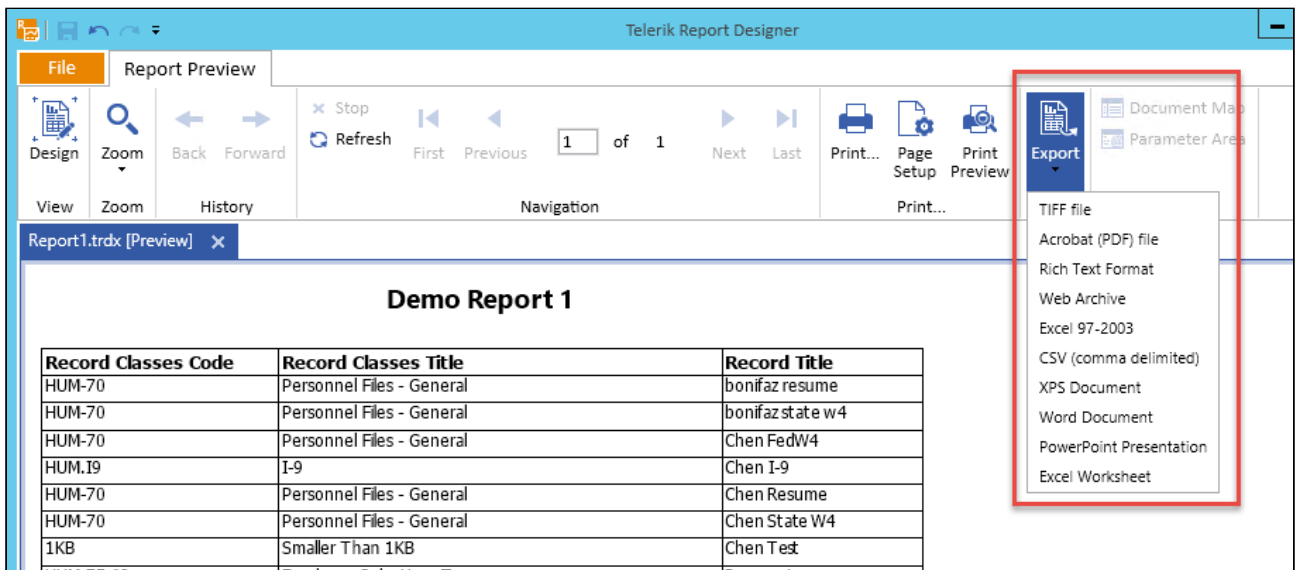
Below is an illustration of the Telerik Report Designer, with its main sections labeled.



Click **Preview** to go to Report Preview mode and see a preview of your report.



In **Report Preview** mode, you can Export the results of your report to a variety of different formats. This enables you to generate custom reports very quickly without deploying them to Records Management.



7.5.8 Creating Report Parameters

To create a report that will require the user to enter parameters/values, you will need to create Report Parameters in your SQL statement for the report. The example below shows a range being used for the OriginatedDate. The parameters in this example are @startRange and @endRange.

In addition, this sample SQL statement shows a report that will return the record metadata, record classes, and the associated disposition dates when the user selects a range of origination dates.

Configure SQL Data Source - sqlDataSource1

Configure data source command

Specify a select statement or a stored procedure to retrieve data for the data source.

Select Statement

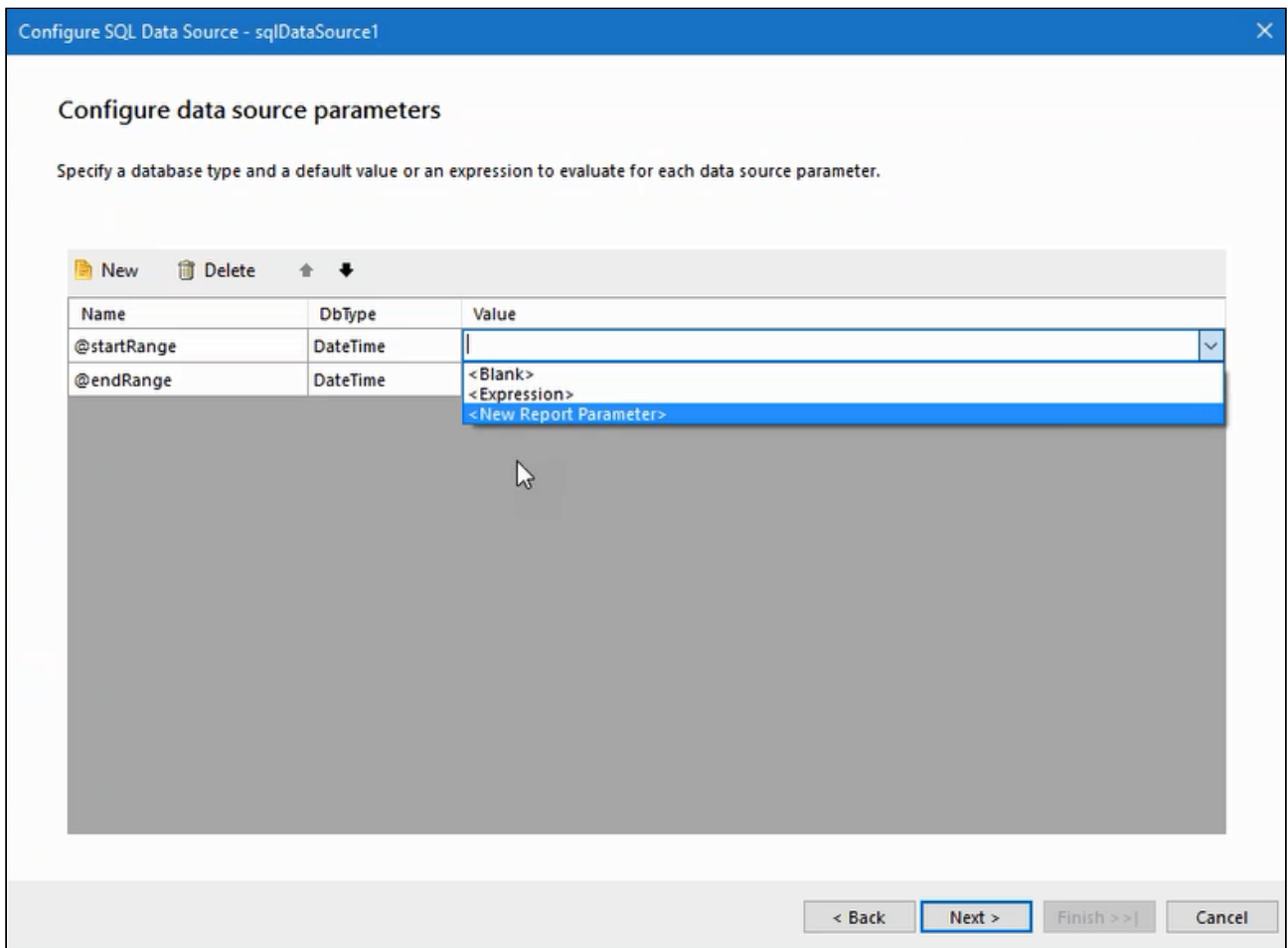
```
SELECT
  r.Title AS RecordTitle,
  r.Uri AS RecordUri,
  rc.Title AS RecordClassTitle,
  rc.Code AS RecordClassCode,
  rs.RetentionExpirationDate,
  rp.Name AS PropertyName,
  rp.Value AS PropertyValue
FROM Records r
JOIN RecordStatus rs ON r.Id = rs.Id
JOIN RecordClasses rc ON r.RecordClassId = rc.Id
JOIN RecordProperties rp ON r.Id = rp.RecordId
WHERE r.OriginatedDate >= @startRange AND r.OriginatedDate <= @endRange
ORDER BY r.OriginatedDate ASC
```

Stored Procedure

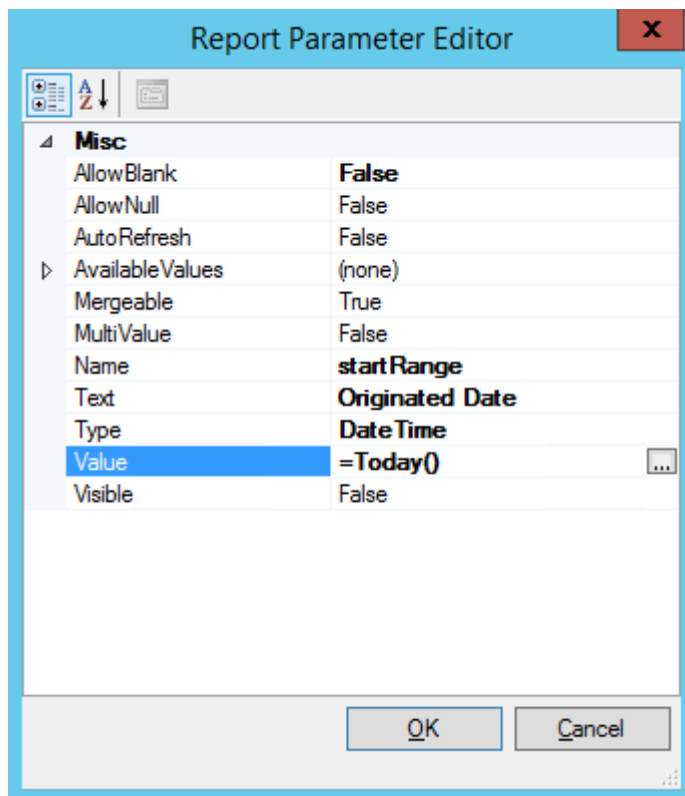
Query Builder...

< Back Next > Finish >> | Cancel

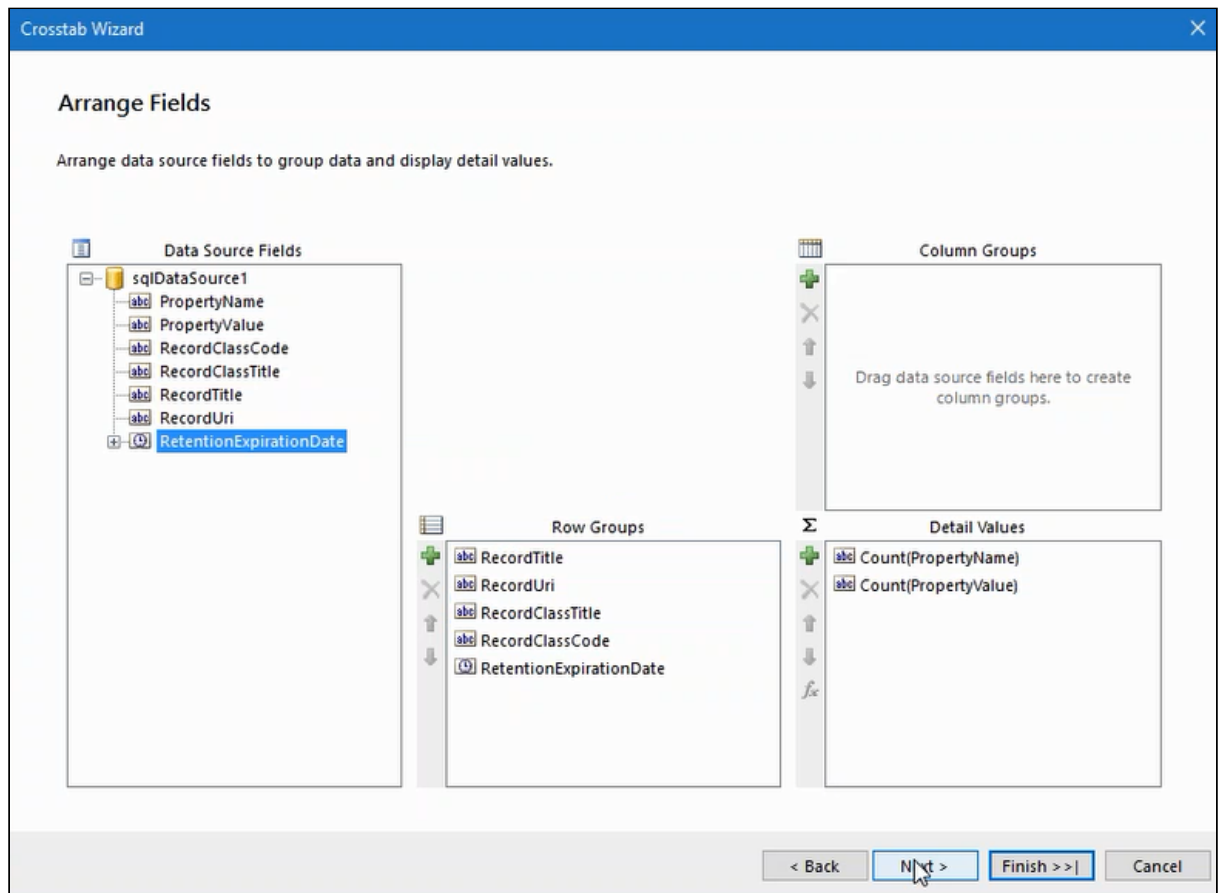
Click **Next** and the **Configure data source parameters** window will display.



1. Select DateTime for the DbType since the parameter is going to be a date.
2. For the **Value** field, you can hard code a value or expression, or you can define a New Report Parameter. The New Report Parameter will enable the user to enter values for the report parameters when the report is executed. In this example, the user will enter values for the Start Date and End Date.
3. Select **New Report Parameter**. This will open another dialog box titled Report Parameter Editor.



4. You can use the default settings, but depending upon the results desired, there may be some fields you want to modify.
 - **AllowBlank** - Change to False to force the user to enter a value.
 - **Text** - This is the label of the field that will be displayed to the user.
 - **Visible** - This shows the field to the user.
 - **Value** - This provides a default value for the field. This is not required. This example shows using a default value of Today's date. When you click the ellipses in the Value field an Edit Expression dialog box is displayed which enables you to enter an expression.
5. Click **Next**
6. The Configure design time parameters dialog box will be displayed. These values are not used in the final report, but they allow for testing of the data. Enter values for the Start and End Range fields.
7. Click **Next**
8. Click **Execute Query**.
9. The Preview data source results dialog box is displayed with the results of the query.
10. Click **Finish**
11. Click **Next**
12. The Arrange Fields dialog box displays. This enables you to arrange the fields to group data and display detail values.
 - **Detail Values** - Display these fields as detail values.
 - **Row Groups** - Display these fields as row groups.
13. Click **Next**



14. Choose **Layout**. Select whether to show subtotals and grand totals, and their placement.
15. Choose **Style**. Select a style to customize the appearance to the generated report.
16. Click **Finish**.

8 Release Notes

8.1 Release Date

June 5, 2023

This release comprises bug fixes to the SharePoint Server Connector.

8.2 Resolved Bugs and Issues

The following bugs and other issues have resolved

ID	Component	Description
86183	SharePoint Server Connector	Fixed an issue where on-premises SharePoint environments were unable to upgrade to the latest version of Gimmel Records if one or more servers were using the Search or Distributed Cache MinRoles.
86183	SharePoint Server Connector	Fixed an issue where on-premises SharePoint environments with one or more servers using the Search or Distributed Cache MinRole would cause the SharePoint Connector Service Application to be deleted when applying SharePoint Cumulative updates.
86183	SharePoint Server Connector	The Gimmel SharePoint Connector Incremental Classification Job now correctly processes its internal site change token incrementally.

8.3 Known Issues

In certain situations, when performing an upgrade to Gimmel Records 5.2.4, the SharePoint Connector Installer may appear to be frozen on the *Deploying Farm Solutions* step. To proceed, simply click the *Next* button and the installation upgrade should complete.

The Gimmel Records Core Service (and Manager Web) will incorrectly display version number 5.2.3. This will be resolved at a later date.

8.4 End-of-Life Update

No changes have been made to the Gimmel Records EOL dates with this release. For the full list of EOL dates, please see our [End-of-Life Notification Page](#)¹²¹.

With that in mind, Gimmel Records 5.2.4 and above will **no longer support SharePoint 2013**. Only versions 2016 and 2019 are currently supported in Gimmel Records 5.2.4 and above.

8.5 Upgrading

The installer for the updated version of all components can be found on our [software download site](#)¹²².

8.5.1 Core Service

The core service can only be upgraded from versions 5.0 and above. Any previously supported versions can and must first be upgraded to version 5.0. It is recommended to **stop all connectors** before upgrading the core service.

¹²¹ <https://gimmel1.sharepoint.com/sites/EXT-Software/SitePages/Upcoming-End-of-Life-Notification.aspx>

¹²² <https://gimmel1.sharepoint.com/sites/EXT-Software>

9 Certified Records Management

This topic and associated links are for version 4.14.0. Please contact support if you need earlier versions.

The Certified Records Management extension is a series of features that extend SharePoint's Records Center to give your organization a reliable and centralized repository for collaboration and records management that is compliant with both the Baseline and Classified standards of the Department of Defense (DoD) 5015.2 Records Management Program.

The Certified Records Management product consists of the following components:

- Compliance Suite
- Classified Records
- Enterprise Events

9.1 Compliance Suite

Gimmel's Compliance Suite combines with SharePoint 2019 to give your organization a reliable and centralized repository for collaboration and records management that is compliant with the standards of the Department of Defense (DoD) 5015.2 Records Management Program. The following links provide information on how to install/upgrade, configure, and use Compliance Suite.

- [Compliance Suite Release Notes](#)¹²³
- [Compliance Suite Installation Guide](#)¹²⁴
- [Compliance Suite Upgrade Guide](#)¹²⁵
- [Compliance Suite File Plan Builder Administration Guide](#)¹²⁶
- [Compliance Suite User Guide](#)¹²⁷

9.2 Classified Records

The Classified Records product is a separate, optional solution you install and use with Gimmel Compliance Suite (Cs). Organizations wanting to use this functionality must first install and configure Compliance Suite. Classified records extend the Compliance Suite's RMA Record and all functionality present in the latter is available for Classified Records. Classified Records has extended security controls that can be graded by an authorized user manually or automated by the system. The following links provide information on how to install/upgrade, configure, and use Classified Records.

¹²³ [https://gimmel.atlassian.net/wiki/download/attachments/178193806/Compliance_Suite_\(FA\)_Release_Notes_V4.14.0.pdf?api=v2&cacheVersion=1&modificationDate=1684799324659&version=1](https://gimmel.atlassian.net/wiki/download/attachments/178193806/Compliance_Suite_(FA)_Release_Notes_V4.14.0.pdf?api=v2&cacheVersion=1&modificationDate=1684799324659&version=1)

¹²⁴ [https://gimmel.atlassian.net/wiki/download/attachments/178193806/Compliance_Suite_\(FA\)_Installation_Guide_V4.14.0.pdf?api=v2&cacheVersion=1&modificationDate=1684799325023&version=1](https://gimmel.atlassian.net/wiki/download/attachments/178193806/Compliance_Suite_(FA)_Installation_Guide_V4.14.0.pdf?api=v2&cacheVersion=1&modificationDate=1684799325023&version=1)

¹²⁵ [https://gimmel.atlassian.net/wiki/download/attachments/178193806/Compliance_Suite_\(FA\)_Upgrade_Guide_V4.14.0.pdf?api=v2&cacheVersion=1&modificationDate=1684799324925&version=1](https://gimmel.atlassian.net/wiki/download/attachments/178193806/Compliance_Suite_(FA)_Upgrade_Guide_V4.14.0.pdf?api=v2&cacheVersion=1&modificationDate=1684799324925&version=1)

¹²⁶ [https://gimmel.atlassian.net/wiki/download/attachments/178193806/Compliance_Suite_File_Plan_Builder_\(FA\)_Administration_Guide_V4.14.0.pdf?api=v2&cacheVersion=1&modificationDate=1684799324854&version=1](https://gimmel.atlassian.net/wiki/download/attachments/178193806/Compliance_Suite_File_Plan_Builder_(FA)_Administration_Guide_V4.14.0.pdf?api=v2&cacheVersion=1&modificationDate=1684799324854&version=1)

¹²⁷ [https://gimmel.atlassian.net/wiki/download/attachments/178193806/Compliance_Suite_\(FA\)_User_Guide_V4.14.0.pdf?api=v2&cacheVersion=1&modificationDate=1684799324761&version=1](https://gimmel.atlassian.net/wiki/download/attachments/178193806/Compliance_Suite_(FA)_User_Guide_V4.14.0.pdf?api=v2&cacheVersion=1&modificationDate=1684799324761&version=1)

- [Classified Records Release Notes](#)¹²⁸
- [Classified Records Installation Guide](#)¹²⁹
- [Classified Records Admin Guide](#)¹³⁰
- [Classified Records User Guide](#)¹³¹

9.3 Enterprise Events

Enterprise Events (EE) provides a tool for conditional-based records management based on events, as opposed to cutoff or calendar dates. You can define events as any enterprise occurrence, such as the end of a contract or fiscal year. Enterprise Events allows you to create groups of event instances for which you can enter trigger dates at any time. The expiration date is automatically calculated from the trigger date you enter based upon the types, event instances, stages, and policies you put in place. Trigger dates can be in the past, present, or future. Enterprise Events can be used across multiple farms and works with Gimmel Compliance Suite's File Plan Builder. You can use Enterprise Events outside of a record center (i.e., team site), in a record center without Compliance Suite, and in a record center with Compliance Suite installed. SharePoint Administrators can use the Local Admin Mode to manage all configuration and administration for Enterprise Events. Accessing Enterprise Events through SharePoint's Site Settings allows you to edit types, permissions, and instances and produce the Enterprise Events report. The following links provide information on how to install/upgrade, configure, and use Enterprise Events.

- [Enterprise Events Release Notes](#)¹³²
- [Enterprise Events Install Guide](#)¹³³
- [Enterprise Events Admin Guide](#)¹³⁴
- [Enterprise Events API Guide](#)¹³⁵

¹²⁸[https://gimmel.atlassian.net/wiki/download/attachments/178193806/Classified_Records_\(FA\)_Release_Notes_V4.13.1.pdf?api=v2&cacheVersion=1&modificationDate=1684799325537&version=1](https://gimmel.atlassian.net/wiki/download/attachments/178193806/Classified_Records_(FA)_Release_Notes_V4.13.1.pdf?api=v2&cacheVersion=1&modificationDate=1684799325537&version=1)

¹²⁹[https://gimmel.atlassian.net/wiki/download/attachments/178193806/Classified_Records_\(FA\)_Installation_Guide_V4.13.1.pdf?api=v2&cacheVersion=1&modificationDate=1684799325613&version=1](https://gimmel.atlassian.net/wiki/download/attachments/178193806/Classified_Records_(FA)_Installation_Guide_V4.13.1.pdf?api=v2&cacheVersion=1&modificationDate=1684799325613&version=1)

¹³⁰[https://gimmel.atlassian.net/wiki/download/attachments/178193806/Classified_Records_\(FA\)_Admin_Guide_V4.13.1.pdf?api=v2&cacheVersion=1&modificationDate=1684799325708&version=1](https://gimmel.atlassian.net/wiki/download/attachments/178193806/Classified_Records_(FA)_Admin_Guide_V4.13.1.pdf?api=v2&cacheVersion=1&modificationDate=1684799325708&version=1)

¹³¹[https://gimmel.atlassian.net/wiki/download/attachments/178193806/Classified_Records_\(FA\)_User_Guide_V4.13.1.pdf?api=v2&cacheVersion=1&modificationDate=1684799325823&version=1](https://gimmel.atlassian.net/wiki/download/attachments/178193806/Classified_Records_(FA)_User_Guide_V4.13.1.pdf?api=v2&cacheVersion=1&modificationDate=1684799325823&version=1)

¹³²https://gimmel.atlassian.net/wiki/download/attachments/178193806/Enterprise_Events_Release_Notes_V4.13.1.pdf?api=v2&cacheVersion=1&modificationDate=1684799325901&version=1

¹³³https://gimmel.atlassian.net/wiki/download/attachments/178193806/Enterprise_Events_Install_Guide_V4.13.1.pdf?api=v2&cacheVersion=1&modificationDate=1684799325985&version=1

¹³⁴https://gimmel.atlassian.net/wiki/download/attachments/178193806/Enterprise_Events_Admin_Guide_V4.13.1.pdf?api=v2&cacheVersion=1&modificationDate=1684799326055&version=1

¹³⁵https://gimmel.atlassian.net/wiki/download/attachments/178193806/Enterprise_Events_API_Guide_V4.13.1.pdf?api=v2&cacheVersion=1&modificationDate=1684799326125&version=1