Gimmal Records

Gimmal Records

Exported on 10/05/2022

Table of Contents

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

Search

1 Featured Pages

- (4.7) Getting started[1]
- (5.0) Getting started[2]
- (5.1) Getting started[3]
- Getting started(see page 21)
- Power BI(see page 446)
- Record Manager Guide(see page 91)
- User Guide(see page 38)

[1] https://gimmal.atlassian.net/wiki/spaces/GR/pages/18777765/%284.7%29+Getting+started
[2] https://gimmal.atlassian.net/wiki/spaces/GR/pages/18778915/%285.0%29+Getting+started
[3] https://gimmal.atlassian.net/wiki/spaces/GR/pages/18779539/%285.1%29+Getting+started

2 Recently Updated

- (5.21) Release Notes(see page 468)
  Sep 29, 2022 • contributed by Jonathan Starr[4]
- (5.20) Release Notes(see page 470)
  Sep 29, 2022 • contributed by Jonathan Starr[5]
- (5.0) Rule Builder[6]
  Sep 27, 2022 • contributed by Jonathan Starr[7]
- (5.1) Rule Builder[8]
  Sep 27, 2022 • contributed by Jonathan Starr[9]
- (5.1) SharePoint Online Connector Configuration[10]
  Sep 08, 2022 • contributed by Jonathan Starr[11]

[4] https://gimmal.atlassian.net/wiki/display/~620e9c4c1d088700694fa31e
[5] https://gimmal.atlassian.net/wiki/display/~620e9c4c1d088700694fa31e
[6] https://gimmal.atlassian.net/wiki/spaces/GR/pages/18778651/%285.0%29+Rule+Builder
[7] https://gimmal.atlassian.net/wiki/display/~620e9c4c1d088700694fa31e
[8] https://gimmal.atlassian.net/wiki/spaces/GR/pages/18779273/%285.1%29+Rule+Builder
[9] https://gimmal.atlassian.net/wiki/display/~620e9c4c1d088700694fa31e
[10] https://gimmal.atlassian.net/wiki/spaces/GR/pages/18778707/%285.1%29+SharePoint+Online+Connector+Configuration
[11] https://gimmal.atlassian.net/wiki/display/~620e9c4c1d088700694fa31e

3 Getting started

First of all, thank you for being a client. We appreciate that you trusted Gimmal 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.

- Administrator Guide(see page 219)
- Global Record Manager Guide(see page 217)
- Record Manager Guide(see page 91)
- User Guide(see page 38)
- Developer Guide(see page 423)

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.

3.1 1. Deployment

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

Plan Your Deployment(see page 219)

3.1.1 Connector Deployment

To deploy connectors on your own services, start with the Connector Deployment(see page 233) topic.

3.1.2 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.You will also need to configure the Physical Records Management extension, start with the Physical Records Management Configuration(see page 393) topic to learn more.

3.2 2. First time setup

If this is the first time you are personally using Gimmal 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.

First time setup(see page 27)

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

3.3 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 Building Your File Plan(see page 91).

3.4 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.

Classification[12]

3.5 5. Adding policies to Record Classes

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

Lifecycles and Record Classes(see page 114)

3.6 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.

Inbox(see page 39)

3.7 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 25).

Term	Description
Unclassified Document	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. If an Unclassified Document cannot be assigned to a Record Class, it remains unclassified and is assigned to the Undefined Record Class.
Record (Classified Document)	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.
Declared Record (Immutable)	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".

[12] https://gimmal.atlassian.net/wiki/spaces/ALT/pages/12812302/Classification

Term	Description
Administration Records	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.
Case Records	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.
Vital Records	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".
Classification	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.
Rules	A set of simple expressions that define how an action will take place. Rules are used for Classification, Rule Triggers, and Legal Holds.
Rule Sets	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.
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.

Term	Description
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	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. 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.
Inbox	There are several Inbox types: An Action Item Inbox and a Requests Inbox. • **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.
Retention Schedule	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. 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.
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.

Term	Description
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.

3.7.1 Physical Records Management Terminology

Term	**Description**
Container	A container is an entity that represents an organizational hierarchy for physical records repositories. It serves as a holding place for physical assets. There are two types of containers: **Location** and **Logical** 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. 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. You can create and use both location-based and logical-based containers.
Create Request	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.

Term	Description
Create Return	If you are a user, you will perform this task when you want to return a physical asset back to its Home location.
Direct Hold	A direct hold is a legal hold that you apply manually (directly) to an asset/record.
Indirect Hold	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.
Location	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: • **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. • 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	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.

Term	Description
Physical Asset	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). 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.
Processing an Extension	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.
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).

3.8 First time setup

This is where you should start if you are signing in or setting up Gimmal 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.

3.8.1 Admin

3.8.2 Users and Record Managers

3.8.3 Admin

3.8.3.1 Creating the Master Account

3.8.3.2 Assign System Admin Users

3.8.3.3 Global Preferences and Theme

3.8.3.4 Email Settings

3.8.3.5 Creating the Master Account

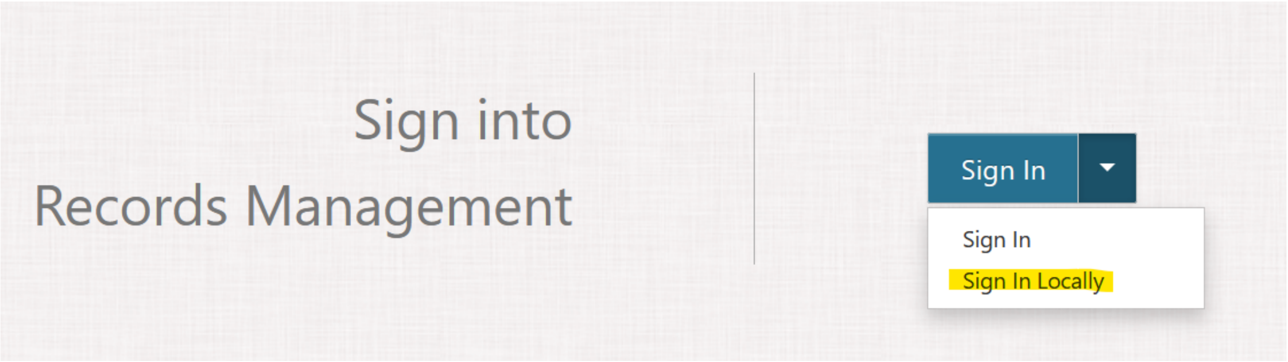
To begin using Records Management for the first time, the first thing you must do is Sign In Locally using the Master Account, so that you can provision other users in the system. To sign in locally, enter the username **administrator** and then enter any password you desire.

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.

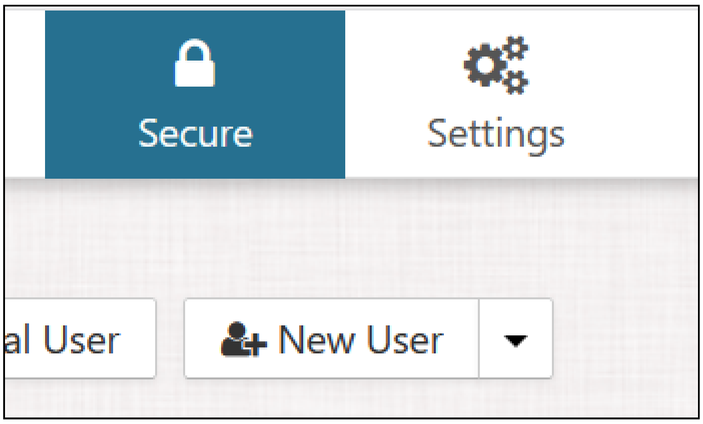


ⓘ The password entered here will automatically become the password of the Master Account. After the first sign in, to re-sign in with the Master Account, enter the username **administrator** and the password that you provided.

ⓘ 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!

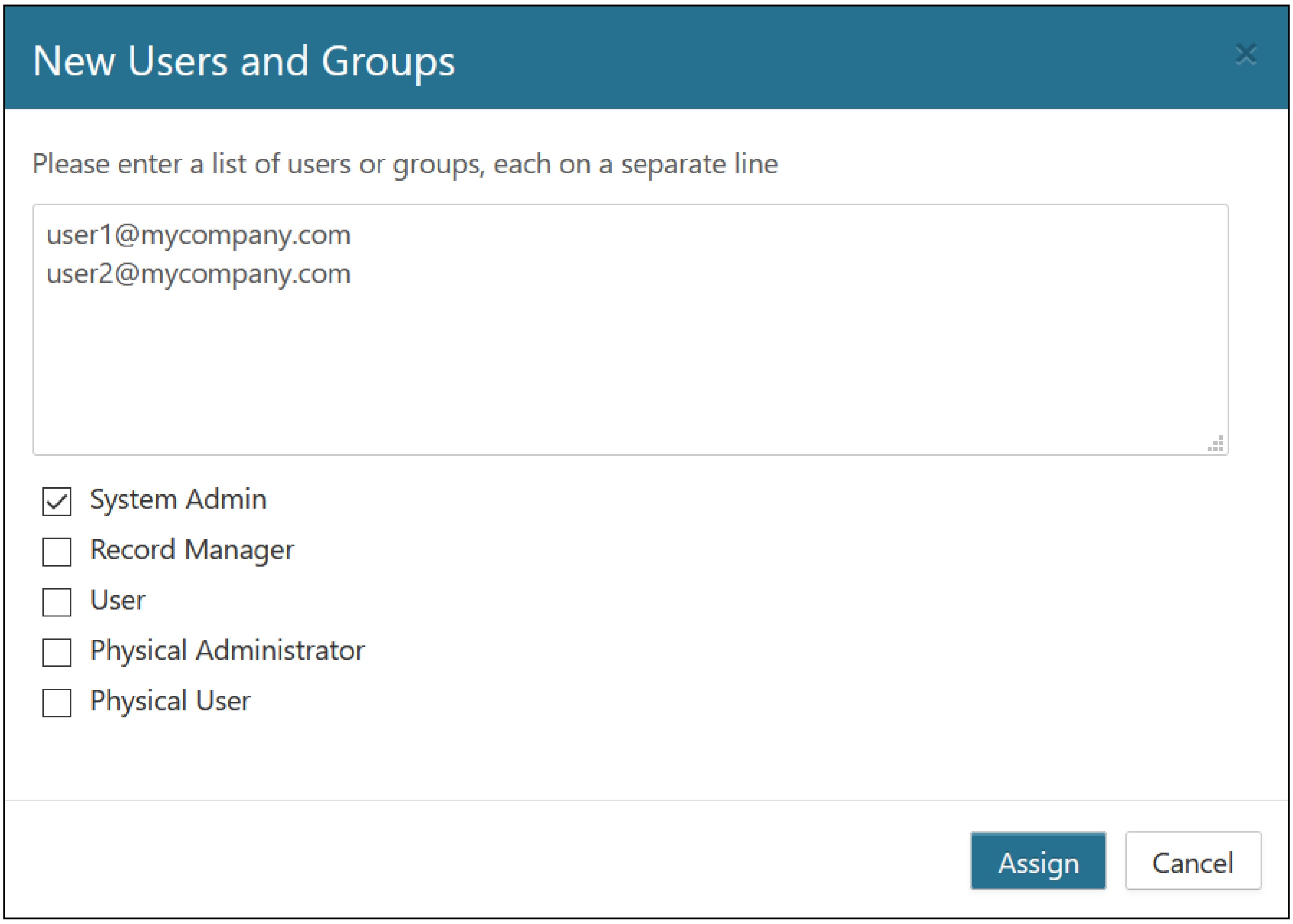
3.8.3.6 Assign System Admin Users

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

3.8.3.7 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.

3.8.3.8 Email Settings

Email Server

If you are a Gimmal Records Cloud customer - you have the option to use either the built-in Gimmal Email Service or you may specify to use your own e-mail server settings.

Gimmal Email Service

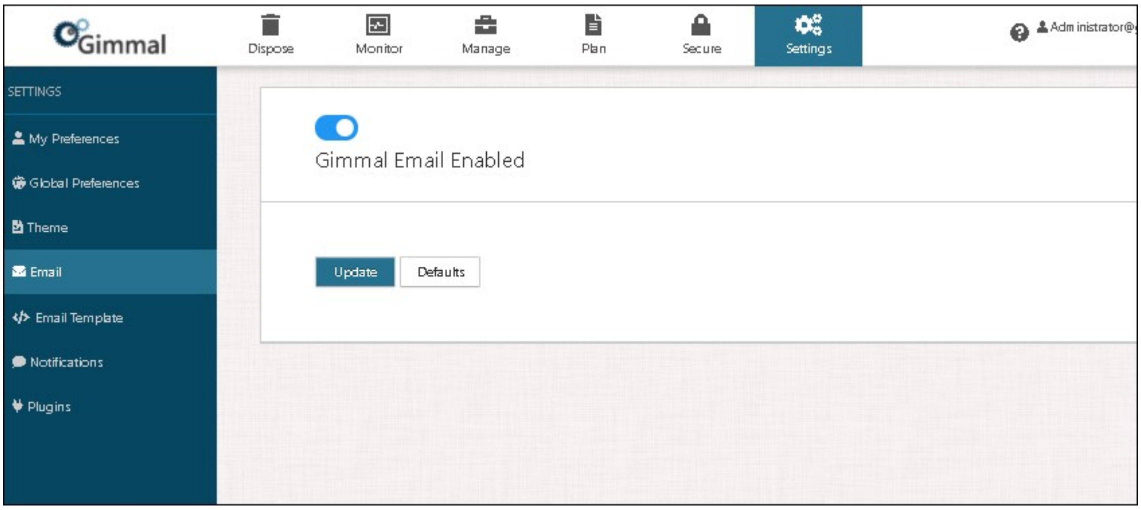
The Gimmal Email Service is hosted in the Gimmal Cloud and is only available to Gimmal Cloud customers.

It is not available to on-premise installations. Gimmal Email will be automatically enabled for new Cloud customers and existing Cloud customers with email that has not yet been configured.
Existing Gimmal Cloud customers may chose to continue to use their specified email configuration or enable the Gimmal Email service.
Emails sent by the Gimmal Email Service are from no-reply@gimmal.com[13]. This is a global setting for all tenants

[13] mailto:no-reply@gimmal.com

and is not configurable. Please ensure that if your organization has any email security settings for spam or junk notifications that you need to whitelist "no-reply@gimmal.com[14]".

1. Select **Settings** from the Main Menu.
2. Select **Email** from the left navigation menu.
3. Ensure the slider is set to on for **Gimmal Email Enabled** setting.
4. Click **Update**.



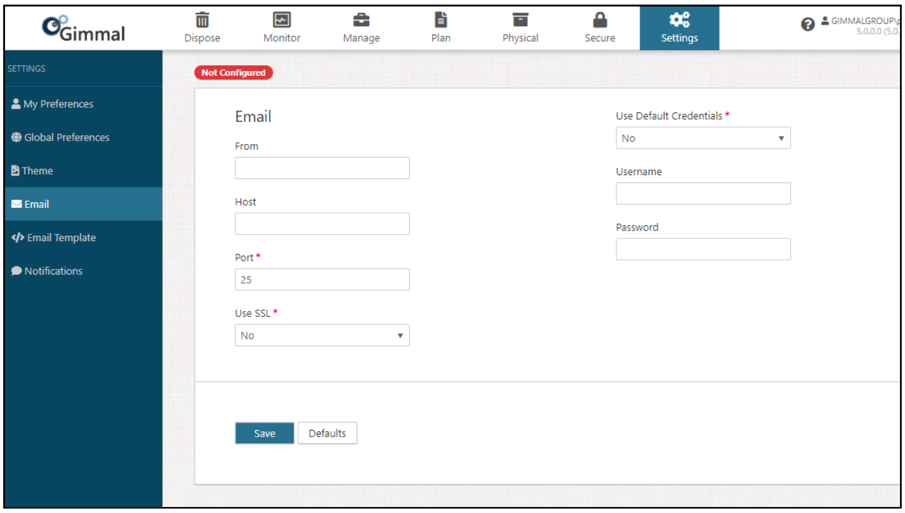
Specify Your Own Email Server Settings

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.

[14] mailto:no-reply@gimmal.com

8. Click **Save**.



Email

From

Host

Port * 25

Use SSL * No

Use Default Credentials * No

Username

Password

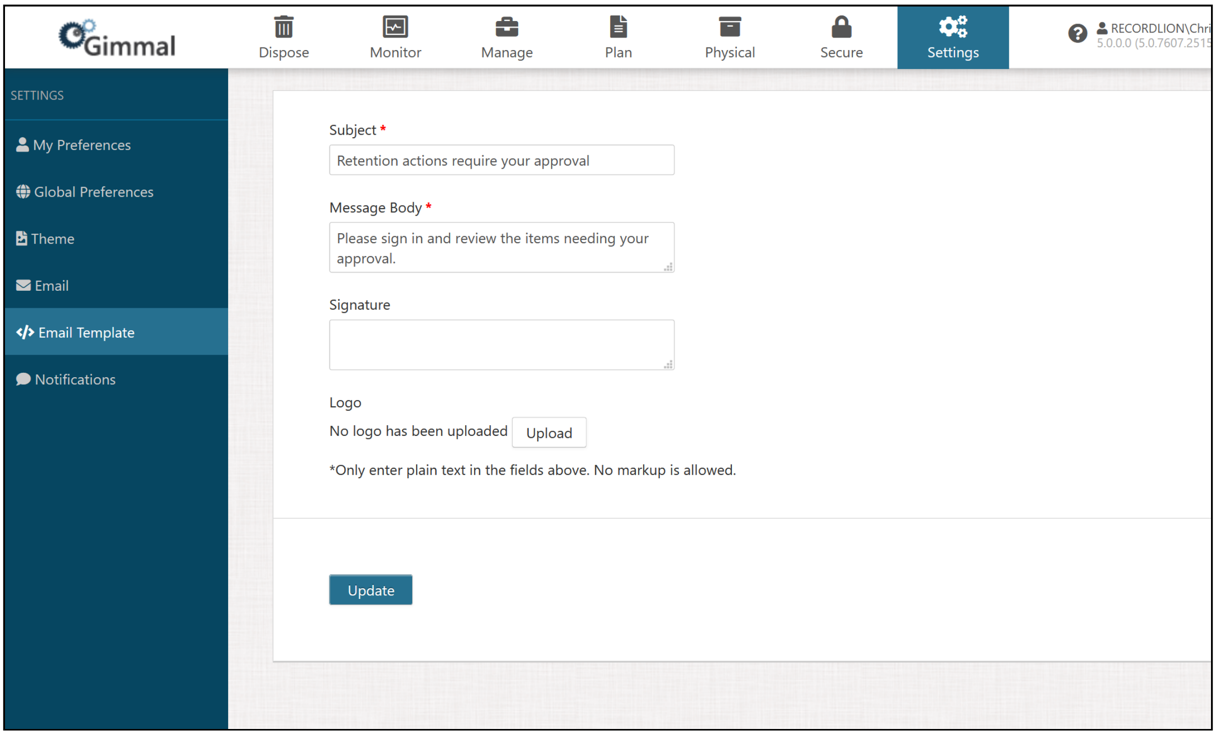
Email Template

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**.



Subject *
Retention actions require your approval

Message Body *
Please sign in and review the items needing your approval.

Signature

Logo
No logo has been uploaded

*Only enter plain text in the fields above. No markup is allowed.

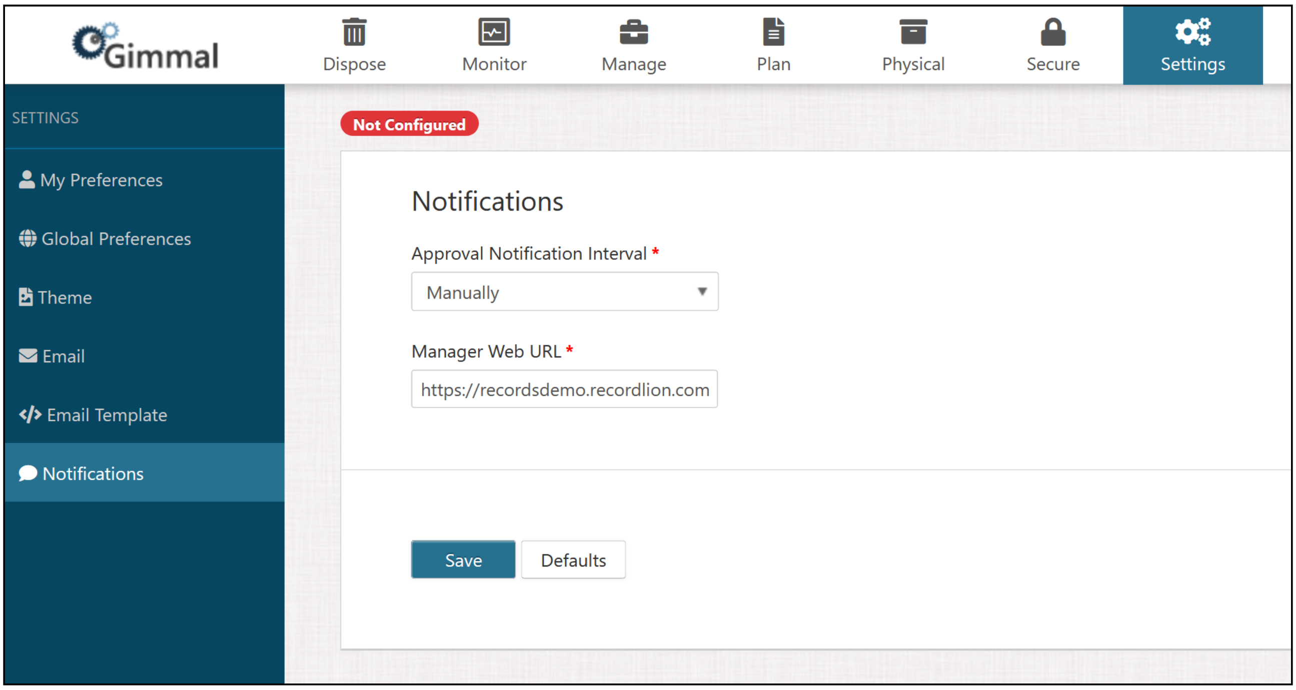
Notifications

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.



Notifications

Approval Notification Interval *

Manually

Manager Web URL *

https://recordsdemo.recordlion.com

3.8.4 Users and Record Managers

- Requirements(see page 35)
- Signing In(see page 35)
- User Preferences(see page 36)

3.8.4.1 Requirements

Browser Requirements

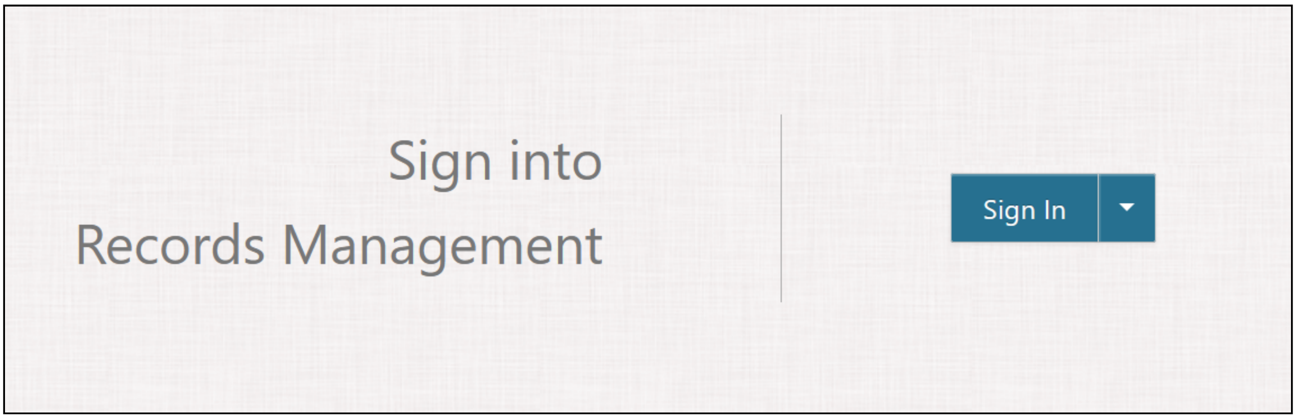
Unless otherwise noted for a specific connector, extension, or other related application, Gimmal Records Management is compatible with the following browsers.

- Mozilla Firefox (latest)
- Google Chrome (latest)
- Microsoft Edge (latest)

3.8.4.2 Signing In

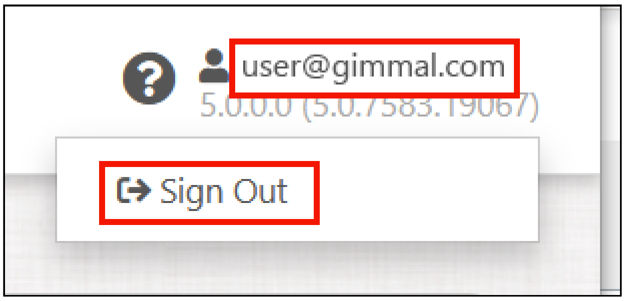
Sign In

To access Records Management, use a web browser to navigate to https://records.gimmal.cloud.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.

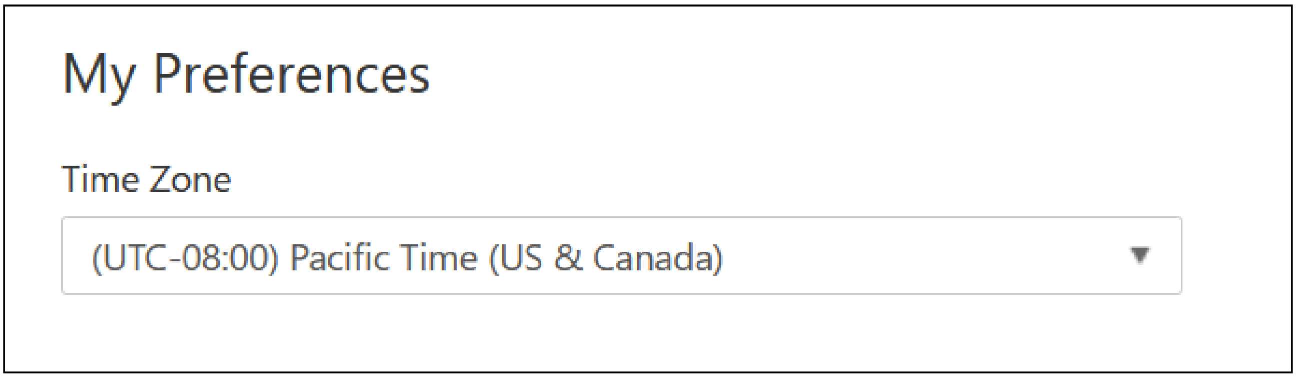


3.8.4.3 User Preferences

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.



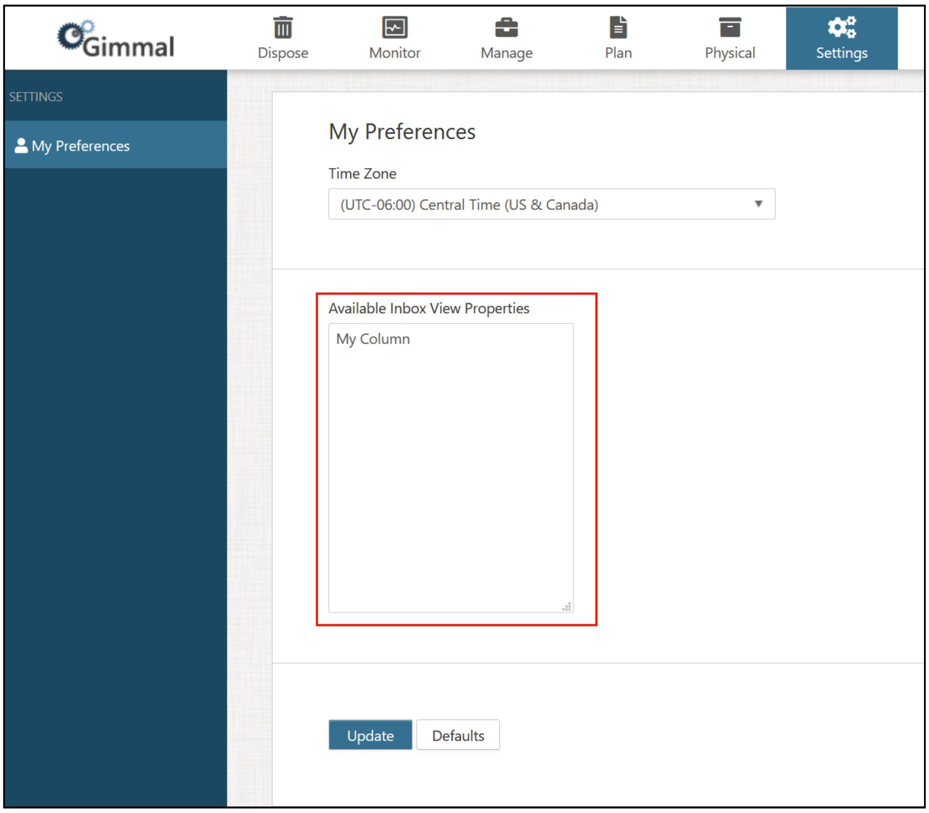
My Preferences

Time Zone

(UTC-08:00) Pacific Time (US & Canada)

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.



My Preferences

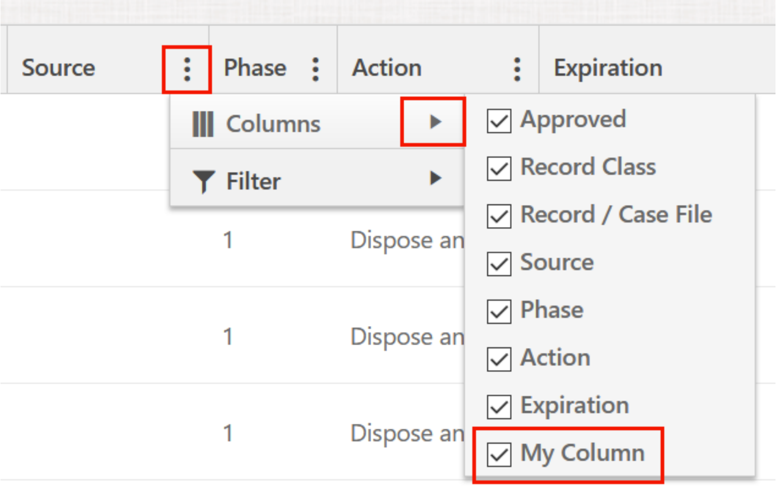
Time Zone: (UTC-06:00) Central Time (US & Canada)

Available Inbox View Properties

My Column

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.



4 User Guide

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

4.1 Signing In and Out

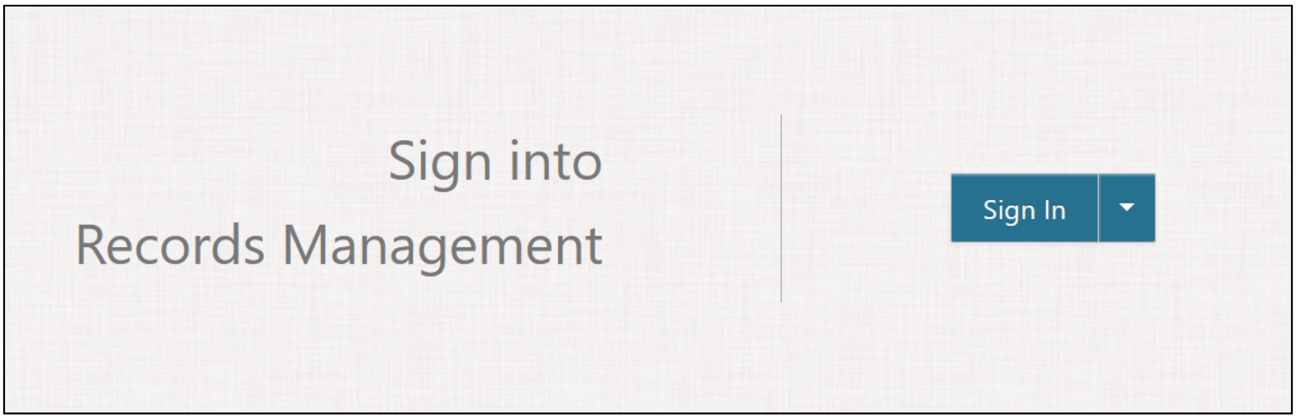
4.2 Inbox

4.3 Physical Assets

4.4 Signing In and Out

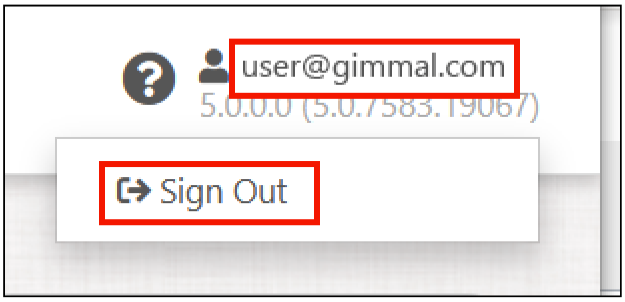
4.4.1 Sign In

To access Records Management, use a web browser to navigate to https://records.gimmal.cloud.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.



4.4.2 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.



4.5 Inbox

4.5.1 Overview

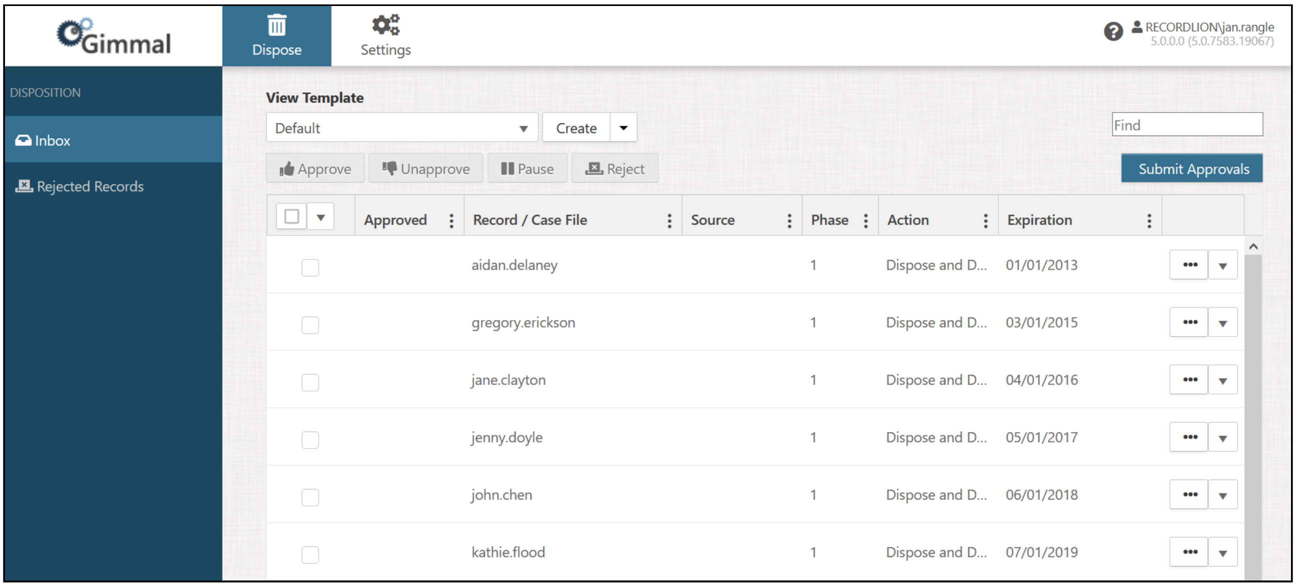
You have created Lifecycles, associated them with Record Classes, and created Event Occurrences. Now, you are ready to approve items that are waiting at the end of the retention period of a specific Lifecycle Phase, typically known as disposition. The Inbox is where you approve and submit items to either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

4.5.2 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 115) 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**.

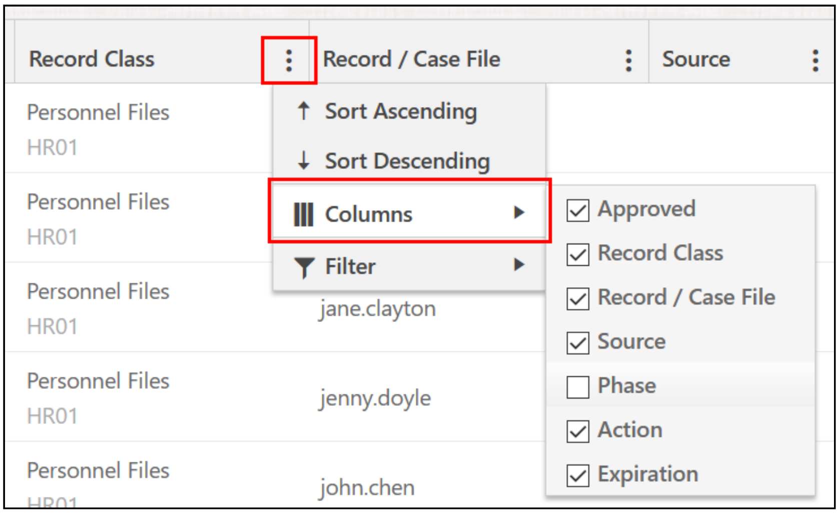


□	Approved	Record / Case File	Source	Phase	Action	Expiration
□		aidan.delaney		1	Dispose and D...	01/01/2013
□		gregory.erickson		1	Dispose and D...	03/01/2015
□		jane.clayton		1	Dispose and D...	04/01/2016
□		jenny.doyle		1	Dispose and D...	05/01/2017
□		john.chen		1	Dispose and D...	06/01/2018
□		kathie.flood		1	Dispose and D...	07/01/2019

4.5.3 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.

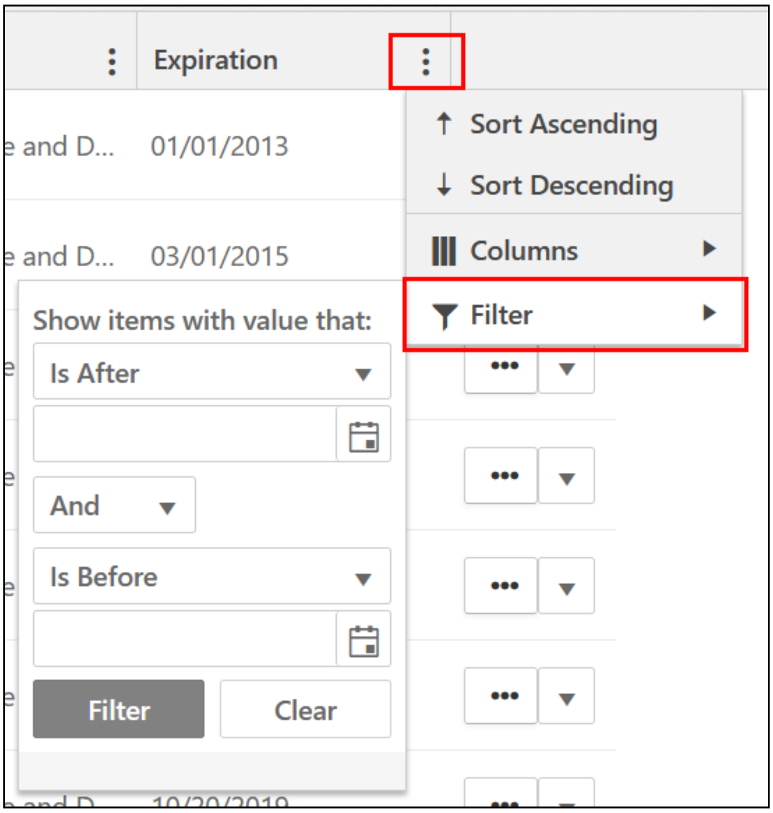
Turn the checkboxes on and off to make a column visible or to hide it.



For information on how to make a new column available, view the Adding Columns to Your Inbox Views(see page 53) topic.

4.5.4 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.

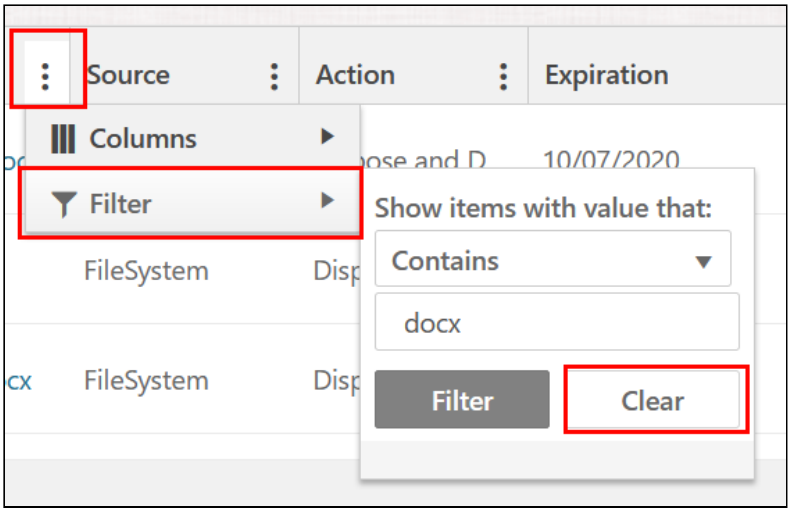


e and D... 01/01/2013

e and D... 03/01/2015

Show items with value that:
Is After
And
Is Before

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.



FileSystem Disp

FileSystem Disp

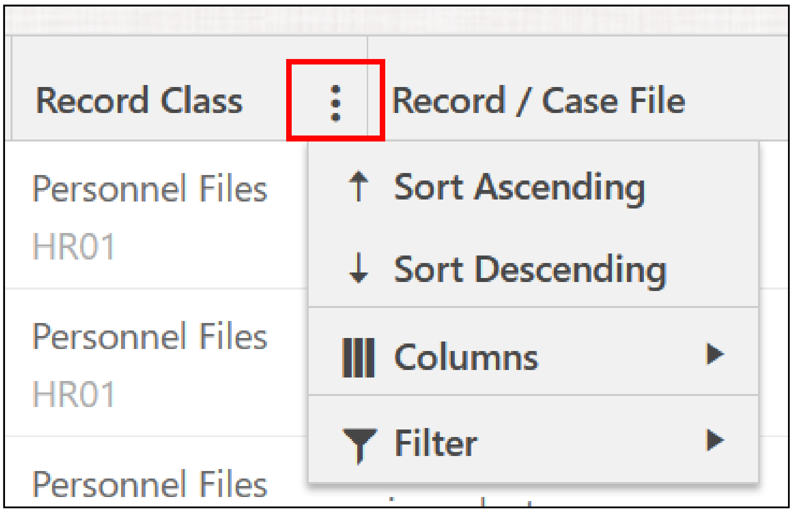
Show items with value that:
Contains
docx

4.5.5 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:

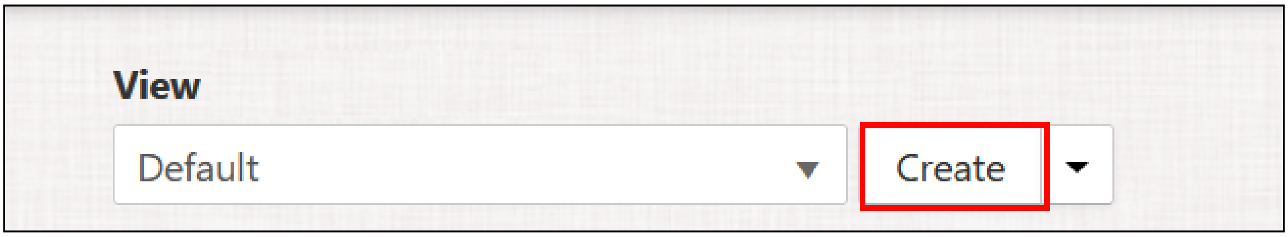
- Record Class
- Expiration Date

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



4.5.6 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 Inbox View(see page 117) topic. Personal views are created by clicking the Create button next to the Inbox views list.



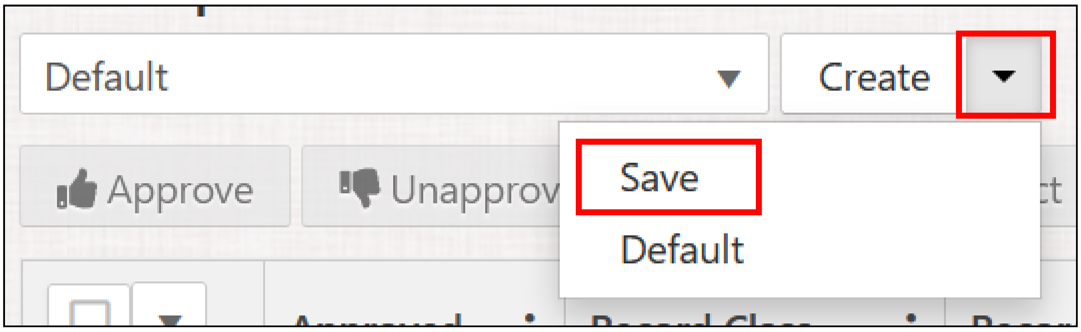
All your settings related to the current layout of the Inbox are saved including visible columns, column order, column width, filters, and any sorting.

4.5.6.1 Using a View

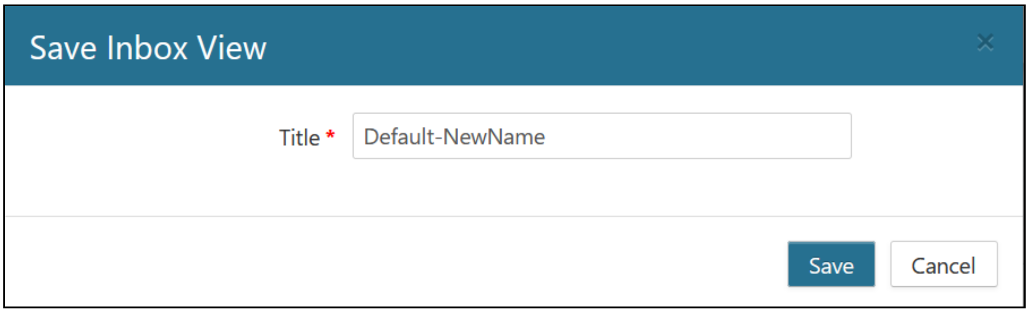
To use a saved view, simply select it from the list of views.

4.5.6.2 Saving existing View

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



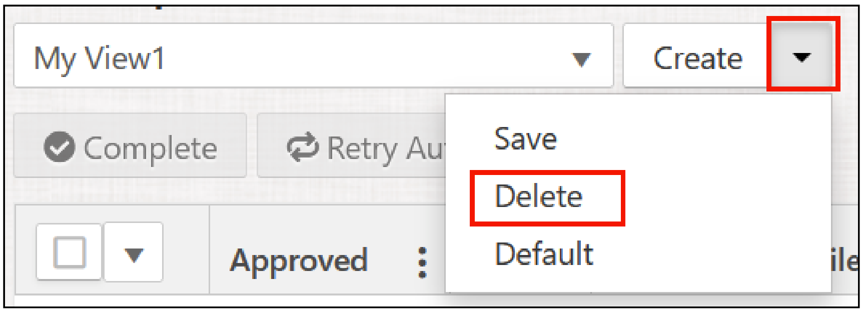
After selecting Save a window will be displayed allowing you to change the name of the view before saving it.



Title * Default-NewName

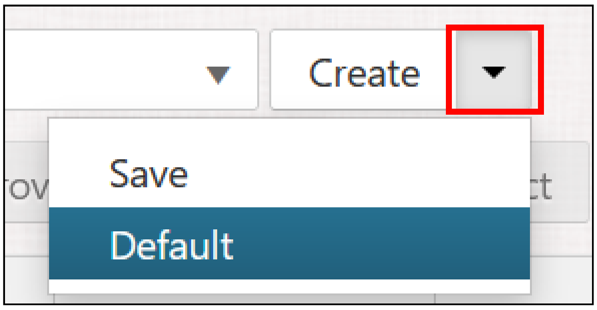
4.5.6.3 Deleting a View

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.

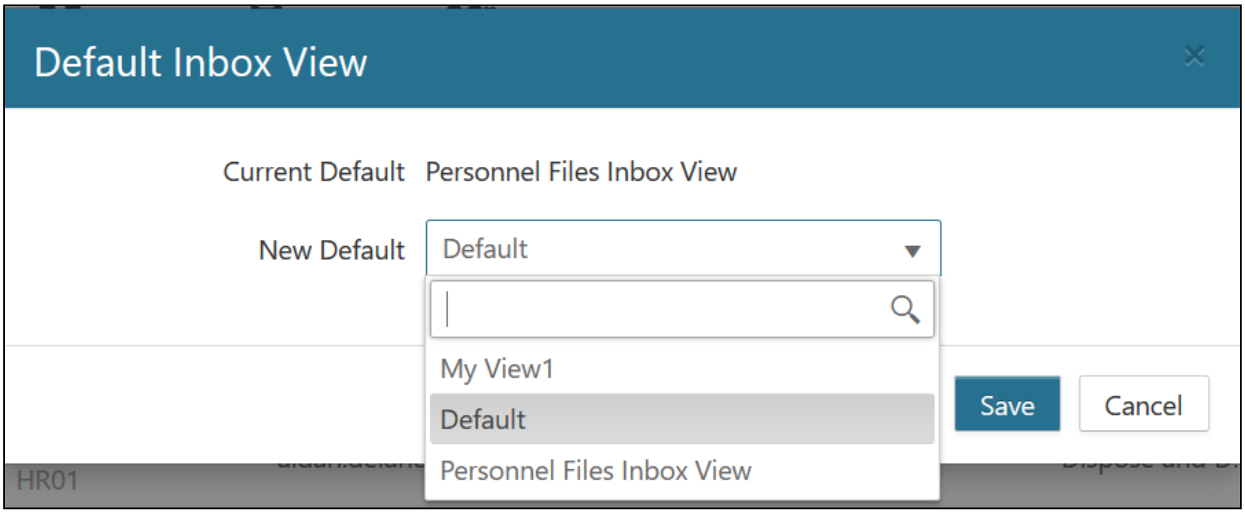


4.5.6.4 Changing the Default View

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.



4.5.7 Disposition Actions

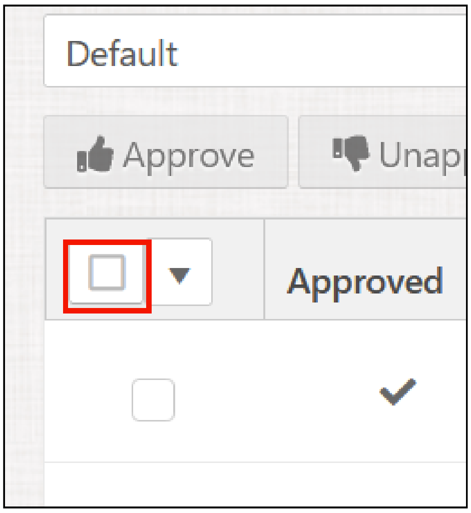
There are several actions that can be taken on records in the Inbox. These actions can be executed on one record at a time, or on any number of selected records. Each action is detailed in the following topics:

- Approving Records(see page 45)
- Unapprove(see page 47)
- Pause(see page 48)
- Reject(see page 50)
- Submitting Approvals(see page 51)
- Adding Columns to Your Inbox Views(see page 53)

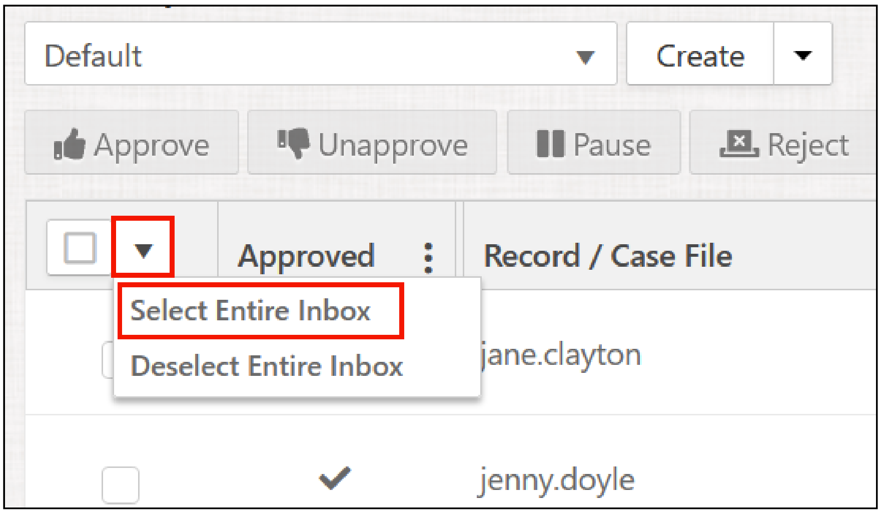
4.5.7.1 Selecting Records

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.



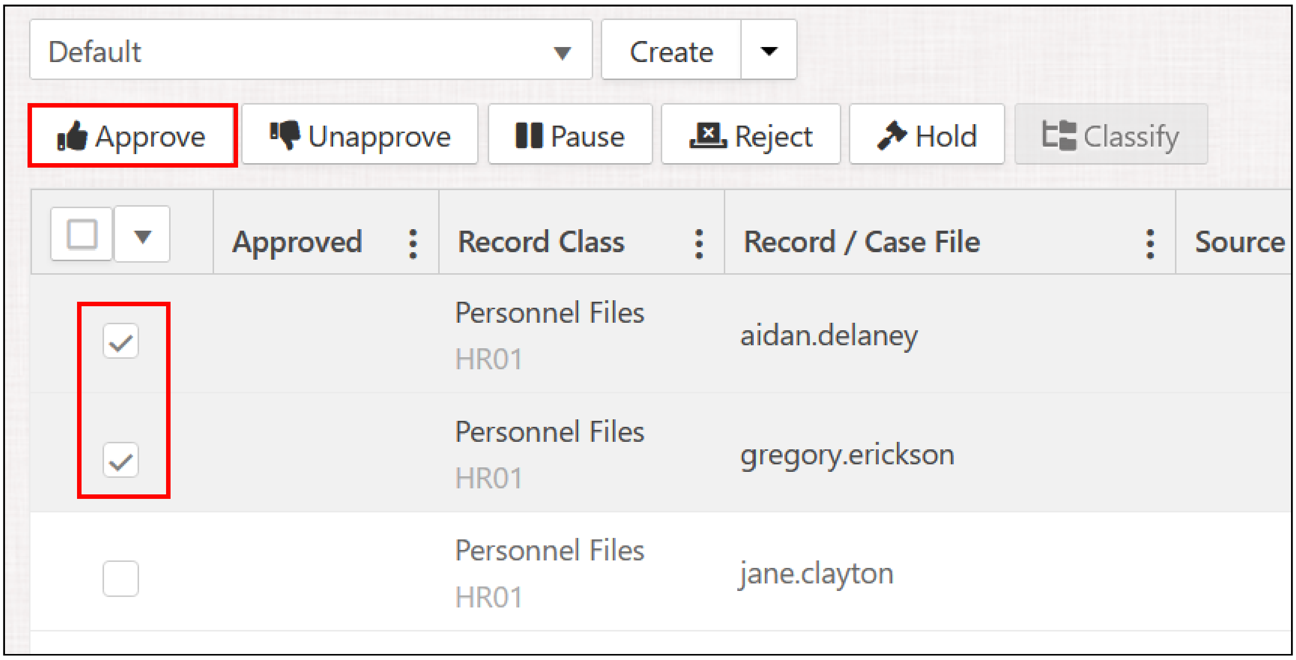
To select records on all pages, select the pulldown on the leftmost column header, and then Select Entire Inbox. You can also deselect the entire Inbox. Records on all pages except the current page will also get deselected if you deselect any one item after selecting the entire Inbox.



4.5.8 Approving Records

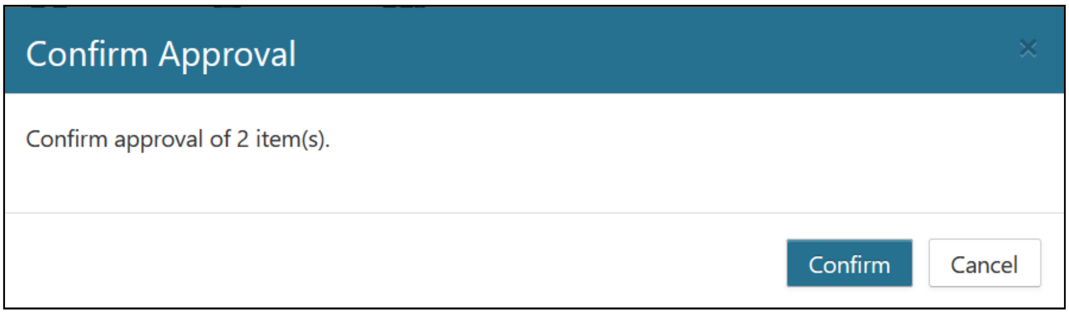
When records have expired and are ready to be approved, they will appear in the Inbox of the user who is set to approve those items.

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



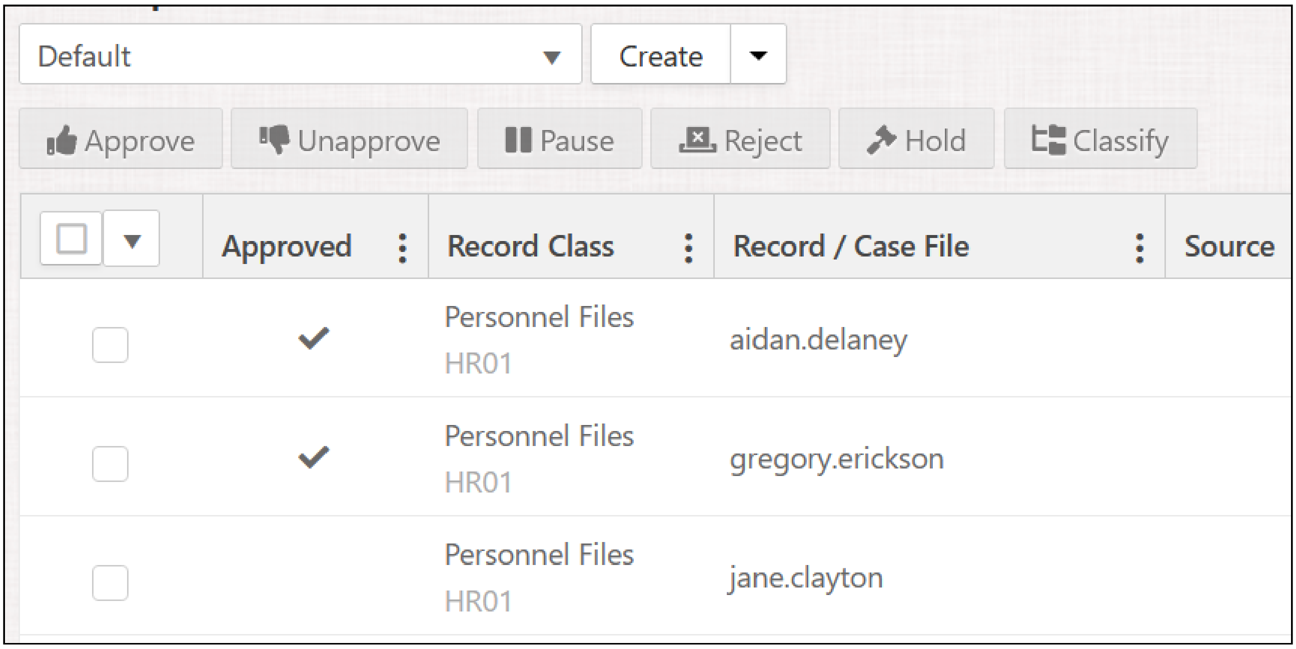
	Approved	Record Class	Record / Case File	Source
☑		Personnel Files HR01	aidan.delaney	
☑		Personnel Files HR01	gregory.erickson	
□		Personnel Files HR01	jane.clayton	

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



Confirm approval of 2 item(s).

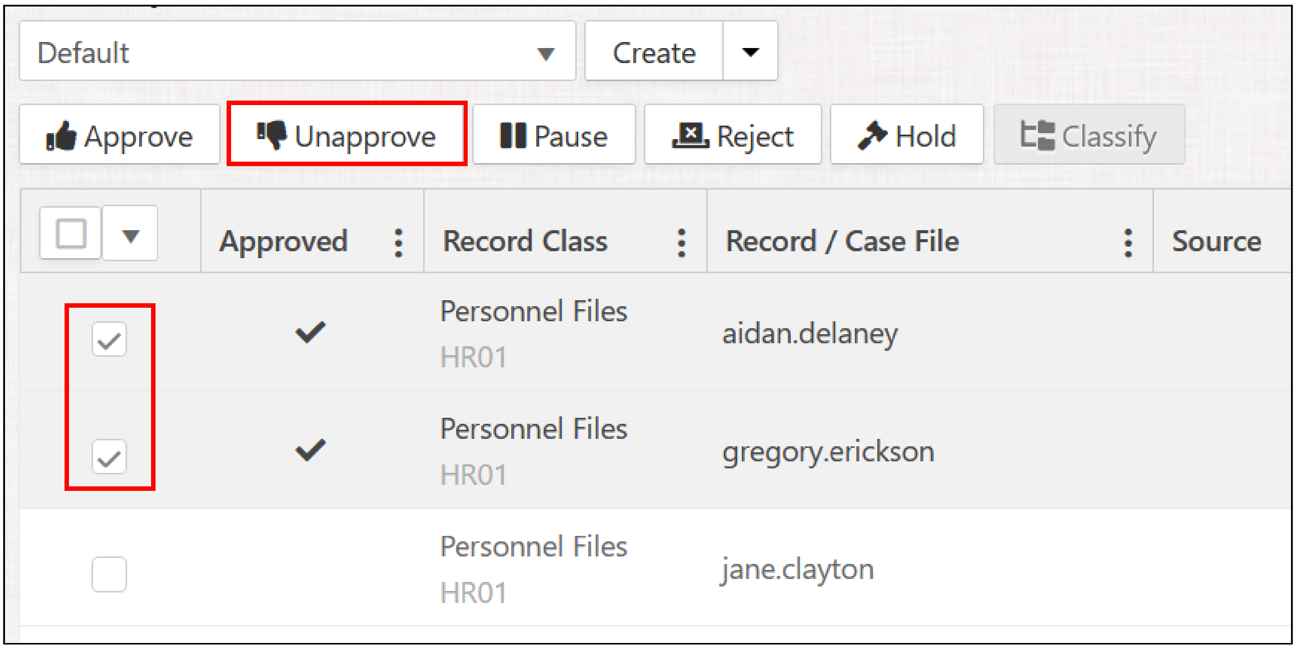
Once the records are approved a check will show up in the Approved column for that item.



□ ▾	Approved	Record Class	Record / Case File	Source
□	✓	Personnel Files HR01	aidan.delaney	
□	✓	Personnel Files HR01	gregory.erickson	
□		Personnel Files HR01	jane.clayton	

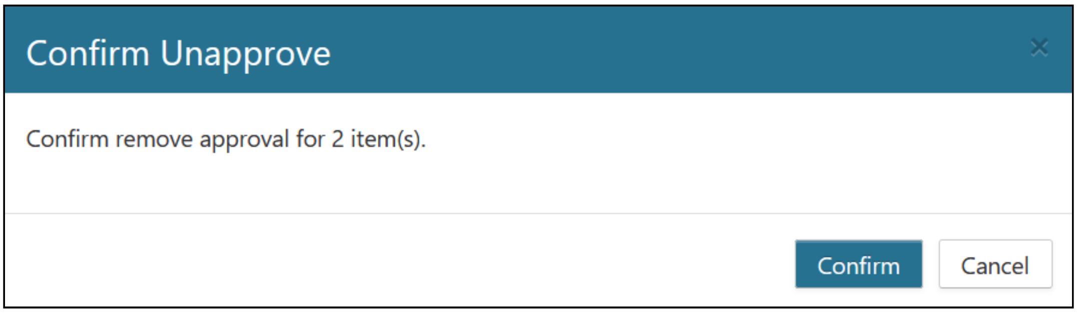
4.5.9 Unapprove

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



□ ▾	Approved	Record Class	Record / Case File	Source
☑	✓	Personnel Files HR01	aidan.delaney	
☑	✓	Personnel Files HR01	gregory.erickson	
□		Personnel Files HR01	jane.clayton	

You will be asked to confirm the unapproval action.



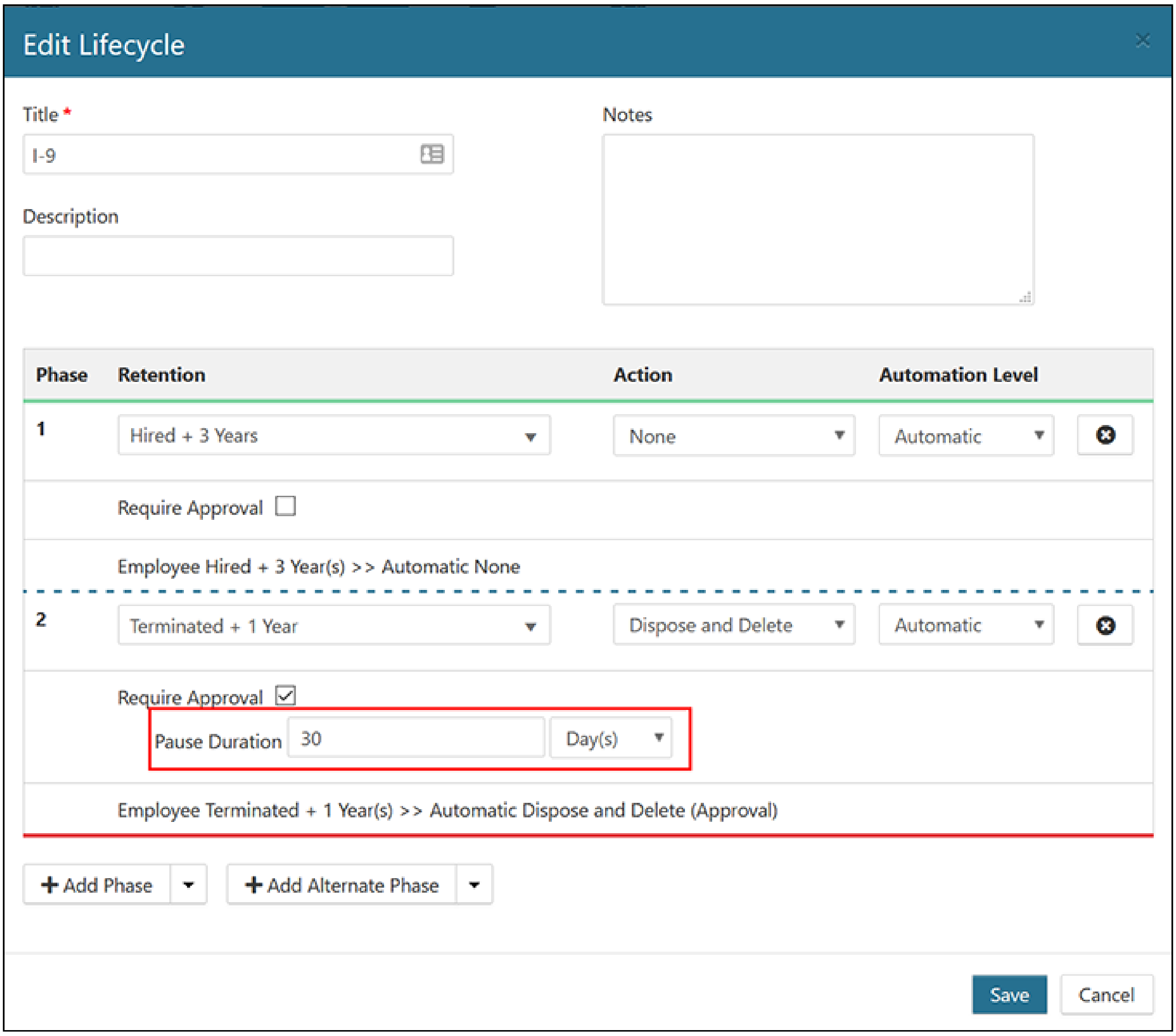
Confirm Unapprove

Confirm remove approval for 2 item(s).

4.5.10 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 *: I-9

Notes:

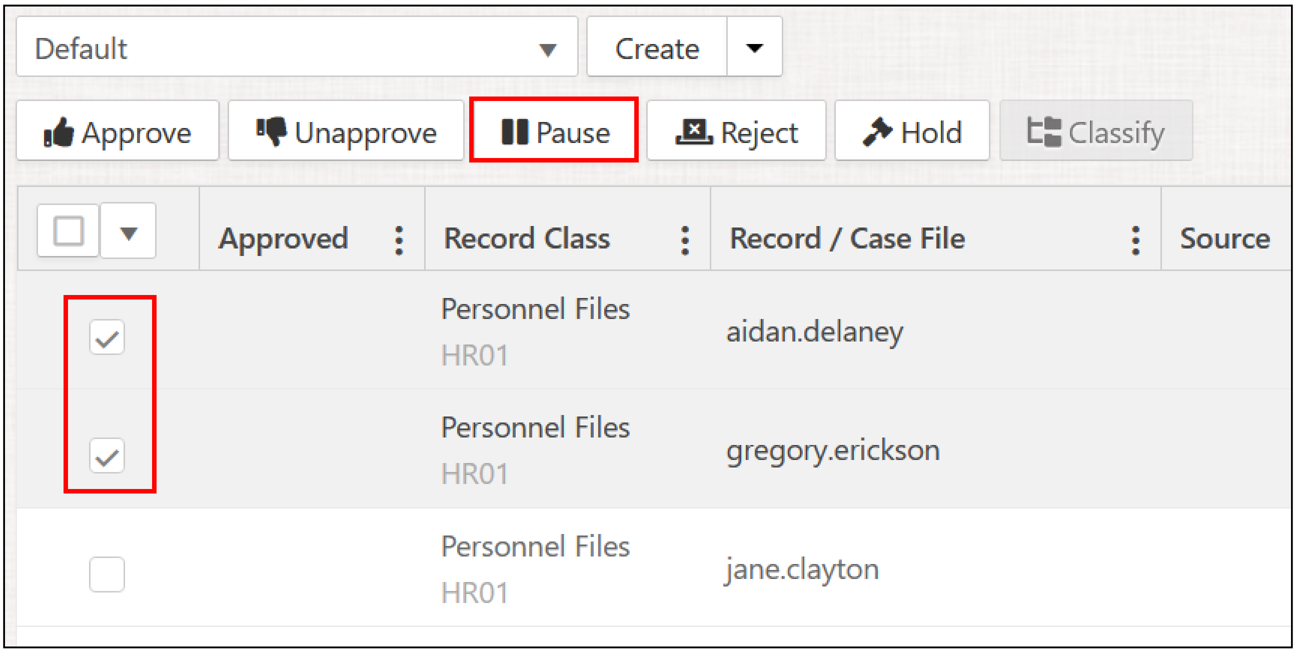
Description:

Phase	Retention	Action	Automation Level
1	Hired + 3 Years	None	Automatic
	Require Approval □		
	Employee Hired + 3 Year(s) >> Automatic None		
2	Terminated + 1 Year	Dispose and Delete	Automatic
	Require Approval ☑		
	Pause Duration 30 Day(s)		
	Employee Terminated + 1 Year(s) >> Automatic Dispose and Delete (Approval)		

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.

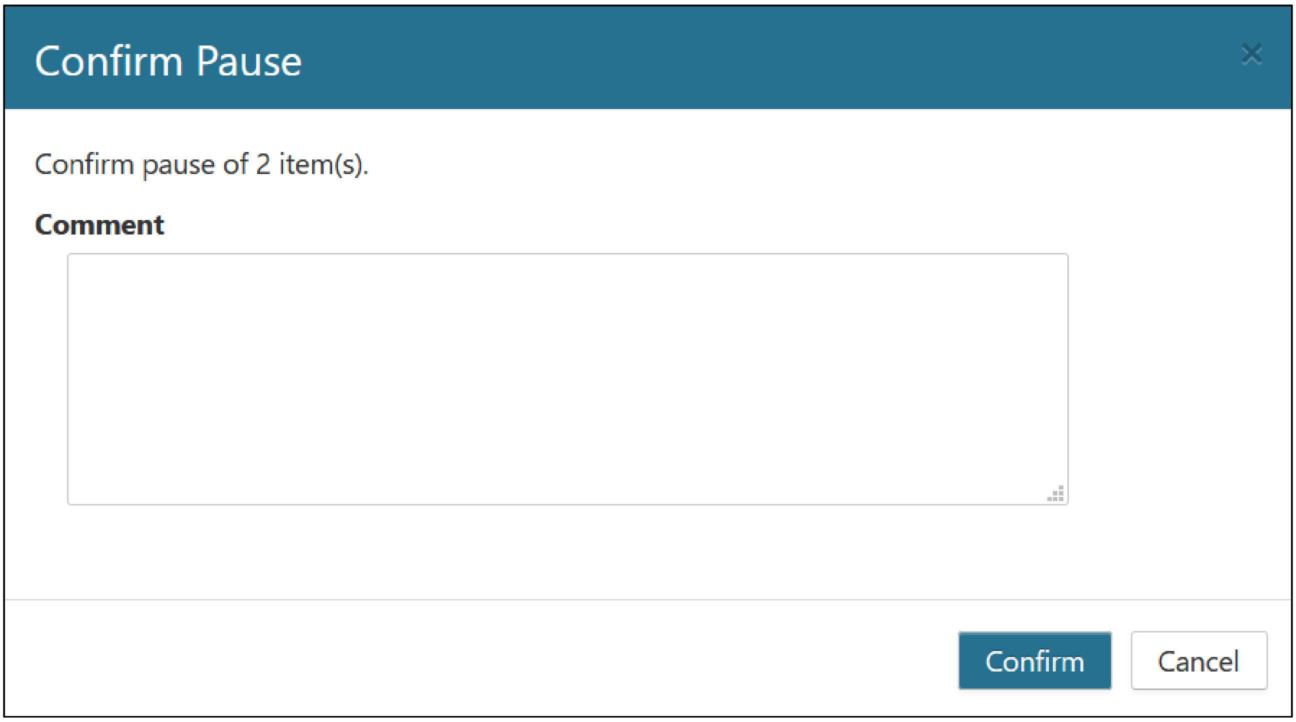
Your records manager will still be able to see Paused records when they are looking at all the records that have expired.

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



☐	Approved	Record Class	Record / Case File	Source
☑		Personnel Files HR01	aidan.delaney	
☑		Personnel Files HR01	gregory.erickson	
☐		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.



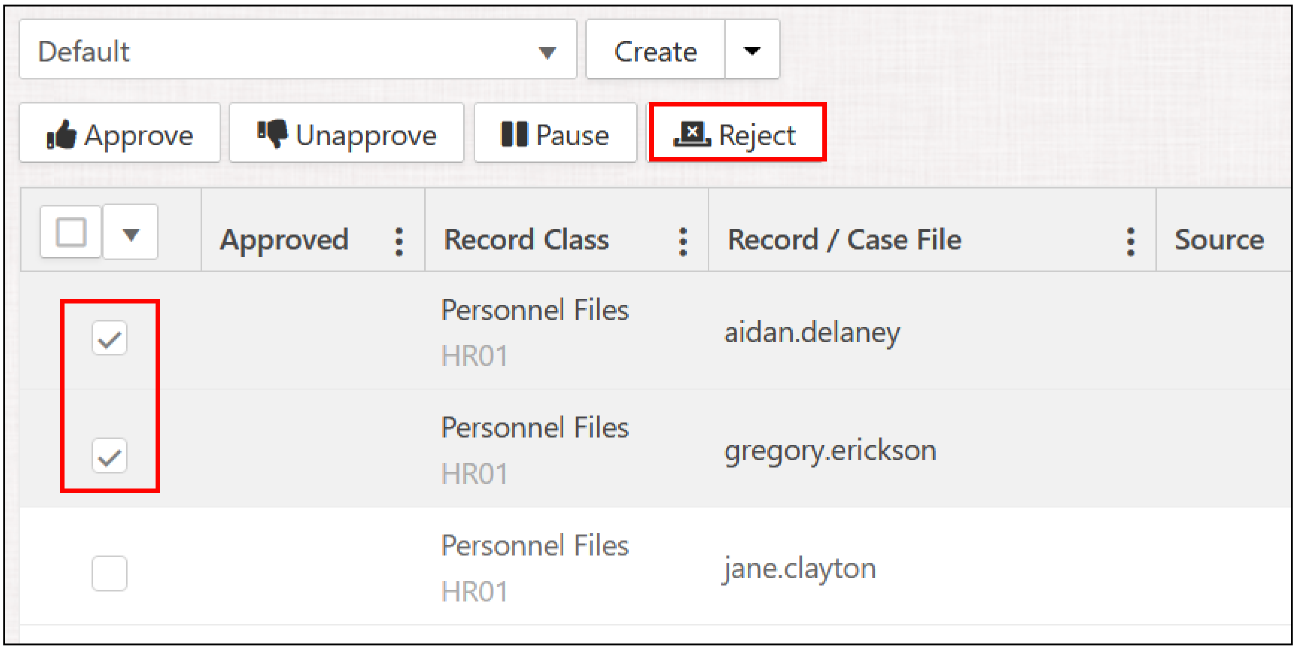
Confirm pause of 2 item(s).

4.5.11 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.

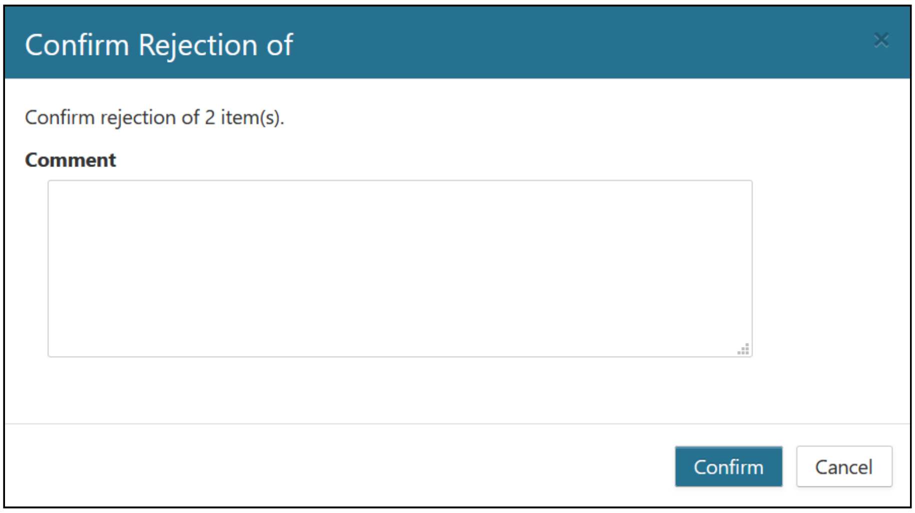
One advantage of using Reject is that the record will become visible to your records manager where they can make a decision to place it on legal hold, reclassify it, or perhaps reinstate it for you to approve again.

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



☐	Approved	Record Class	Record / Case File	Source
☑		Personnel Files HR01	aidan.delaney	
☑		Personnel Files HR01	gregory.erickson	
☐		Personnel Files HR01	jane.clayton	

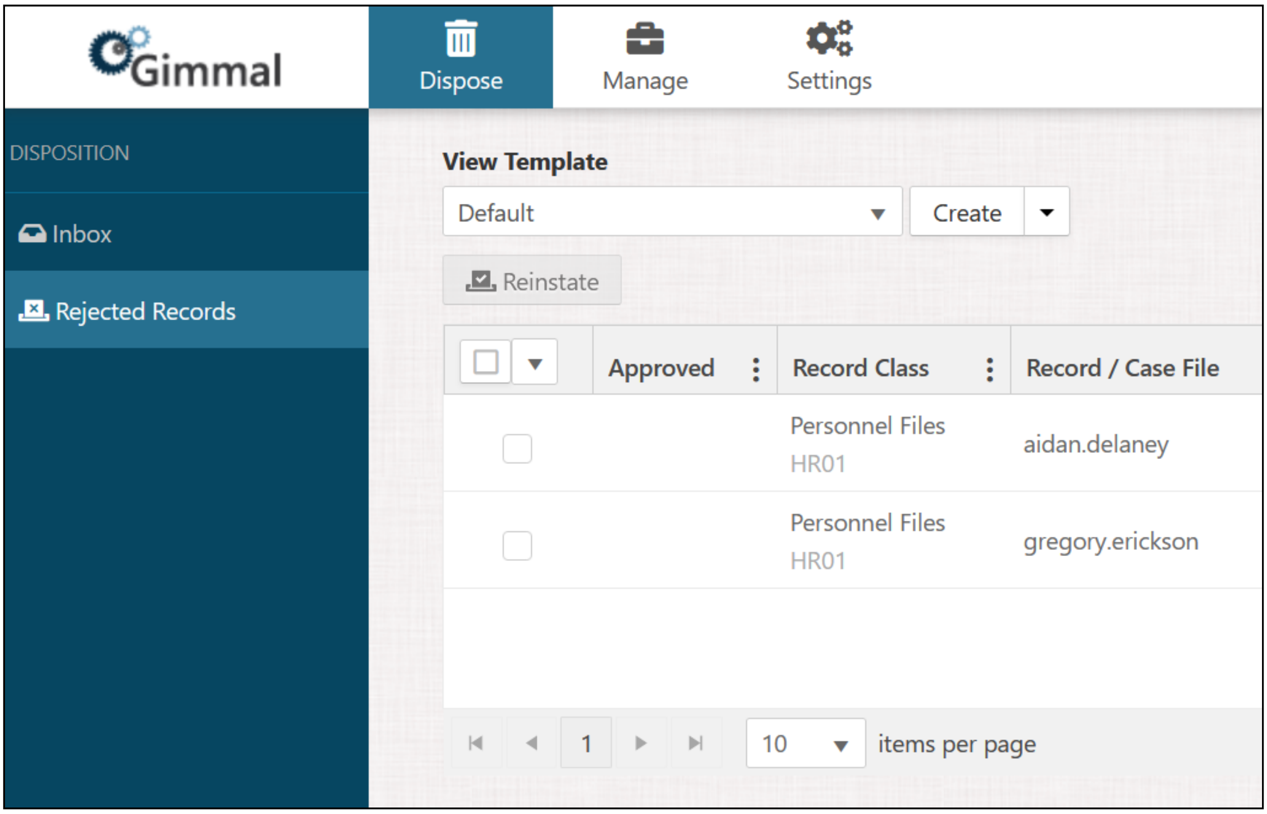
You will be asked to confirm and give a reason for rejecting the record. It is recommended that you explain in the Comment section why the record was rejected in order for you records manager to understand the reasoning.


Confirm Rejection of

Confirm rejection of 2 item(s).

Comment

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, the will have the option to place the record on legal hold or reclassify it.



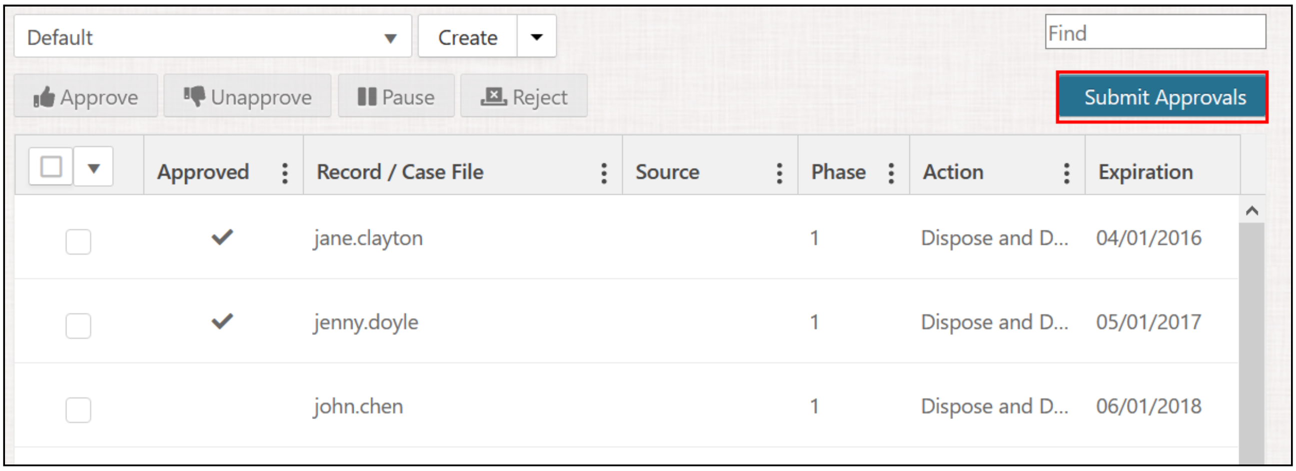
□	Approved	Record Class	Record / Case File
□		Personnel Files HR01	aidan.delaney
□		Personnel Files HR01	gregory.erickson

4.5.12 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.

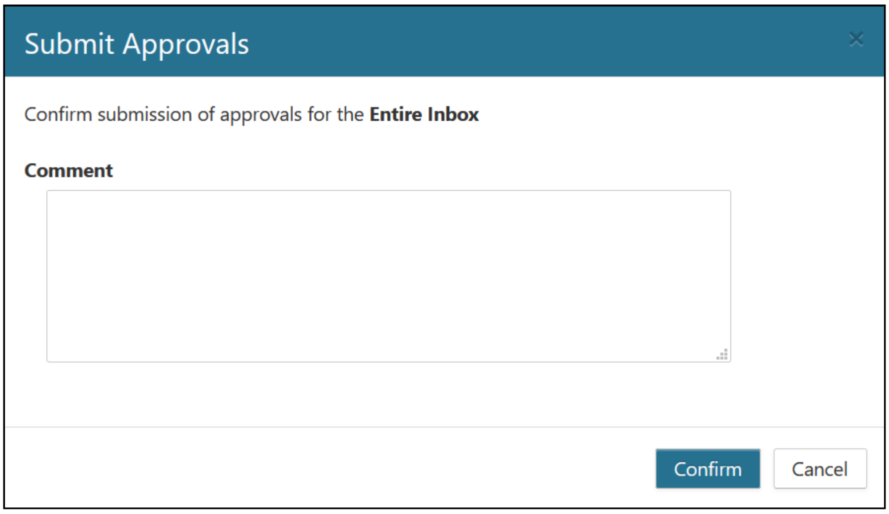
The primary reason to use to group many records into one submittal is to produce a single Destruction Certificate. When the final disposition action is taking place, all the records that had that action (typically delete) taken on the same day for their particular Record Class will be grouped into a 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.



□	Approved	Record / Case File	Source	Phase	Action	Expiration
□	✓	jane.clayton		1	Dispose and D...	04/01/2016
□	✓	jenny.doyle		1	Dispose and D...	05/01/2017
□		john.chen		1	Dispose and D...	06/01/2018

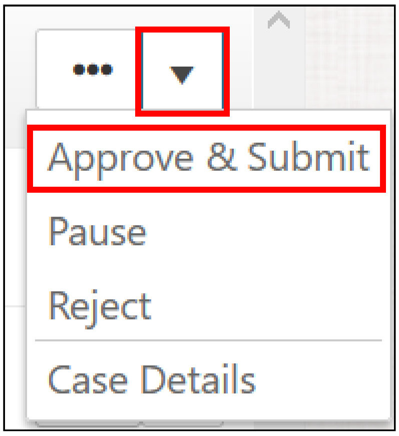
You will be asked to confirm the submittal and enter any comments necessary.



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

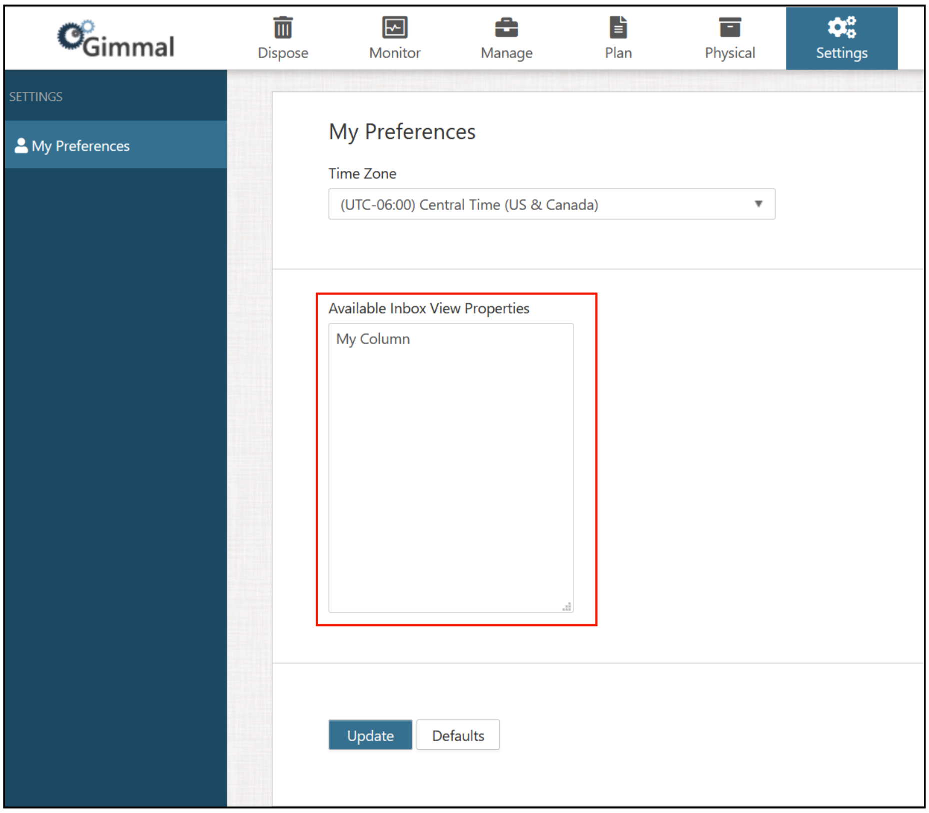
4.5.12.1 Approving and Submitting together

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.



4.5.13 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.



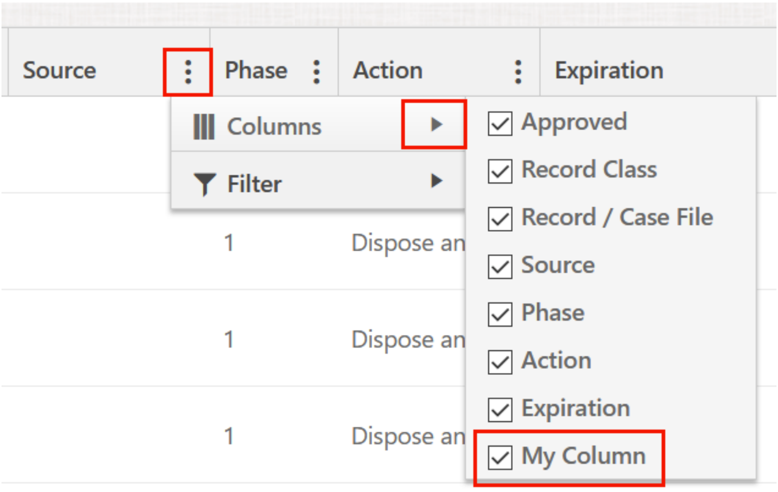
My Preferences

Time Zone: (UTC-06:00) Central Time (US & Canada)

Available Inbox View Properties: My Column

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.



☑ Approved
☑ Record Class
☑ Record / Case File
☑ Source
☑ Phase
☑ Action
☑ Expiration
☑ My Column

4.6 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.

4.6.1 Requesting an Asset

The following topics cover how to request an asset.

4.6.1.1 Creating a Request

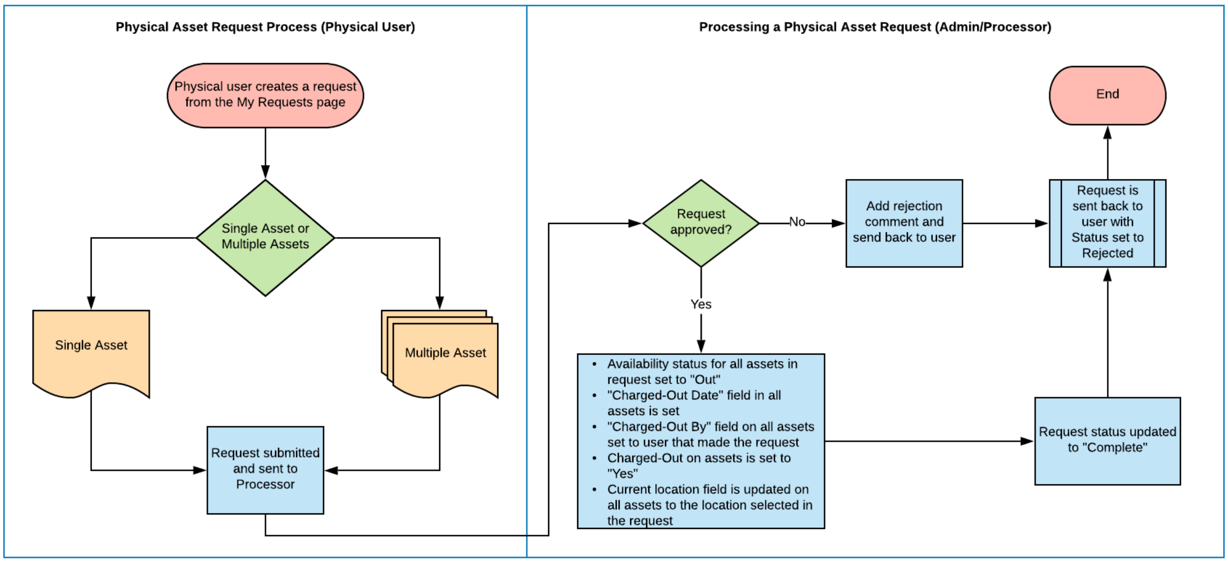
4.6.1.2 Adding and Removing Assets from a Request

4.6.1.3 Submitting a Request

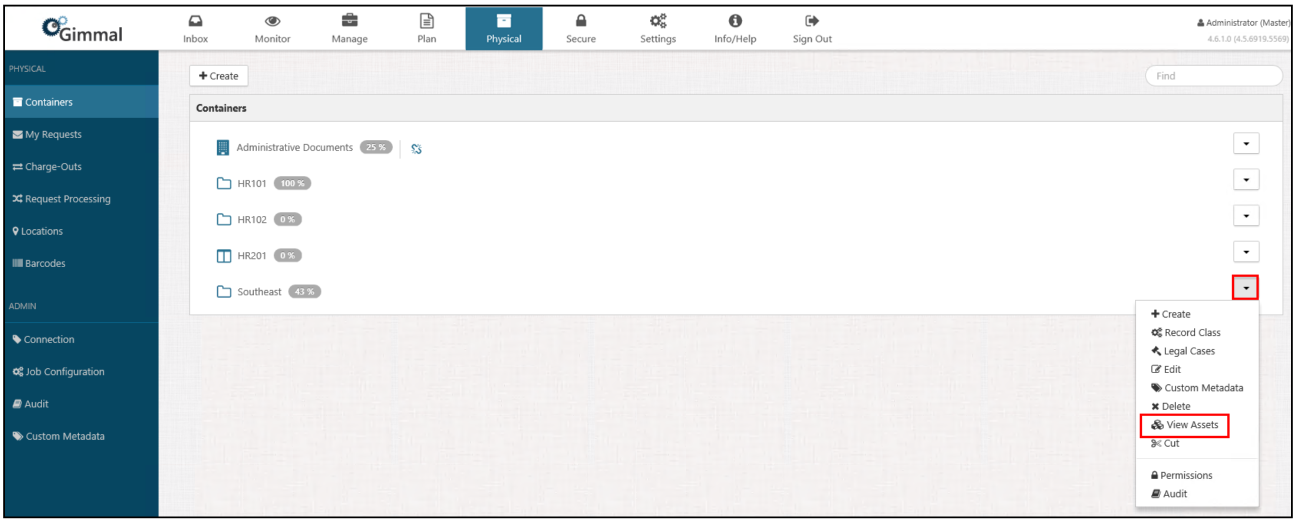
4.6.1.4 Request an Extension for a Charged Out Asset

4.6.1.5 Canceling and Deleting a Request

The following flowchart illustrates the request process.


Physical Asset Request Process (Physical User)
Physical user creates a request from the My Requests page
Single Asset or Multiple Assets
Single Asset
Multiple Asset
Request submitted and sent to Processor
Processing a Physical Asset Request (Admin/Processor)
Request approved?
No
Add rejection comment and send back to user
Request is sent back to user with Status set to Rejected
End
Yes
• Availability status for all assets in request set to "Out"
• "Charged-Out Date" field in all assets is set
• "Charged-Out By" field on all assets set to user that made the request
• Charged-Out on assets is set to "Yes"
• Current location field is updated on all assets to the location selected in the request
Request status updated to "Complete"

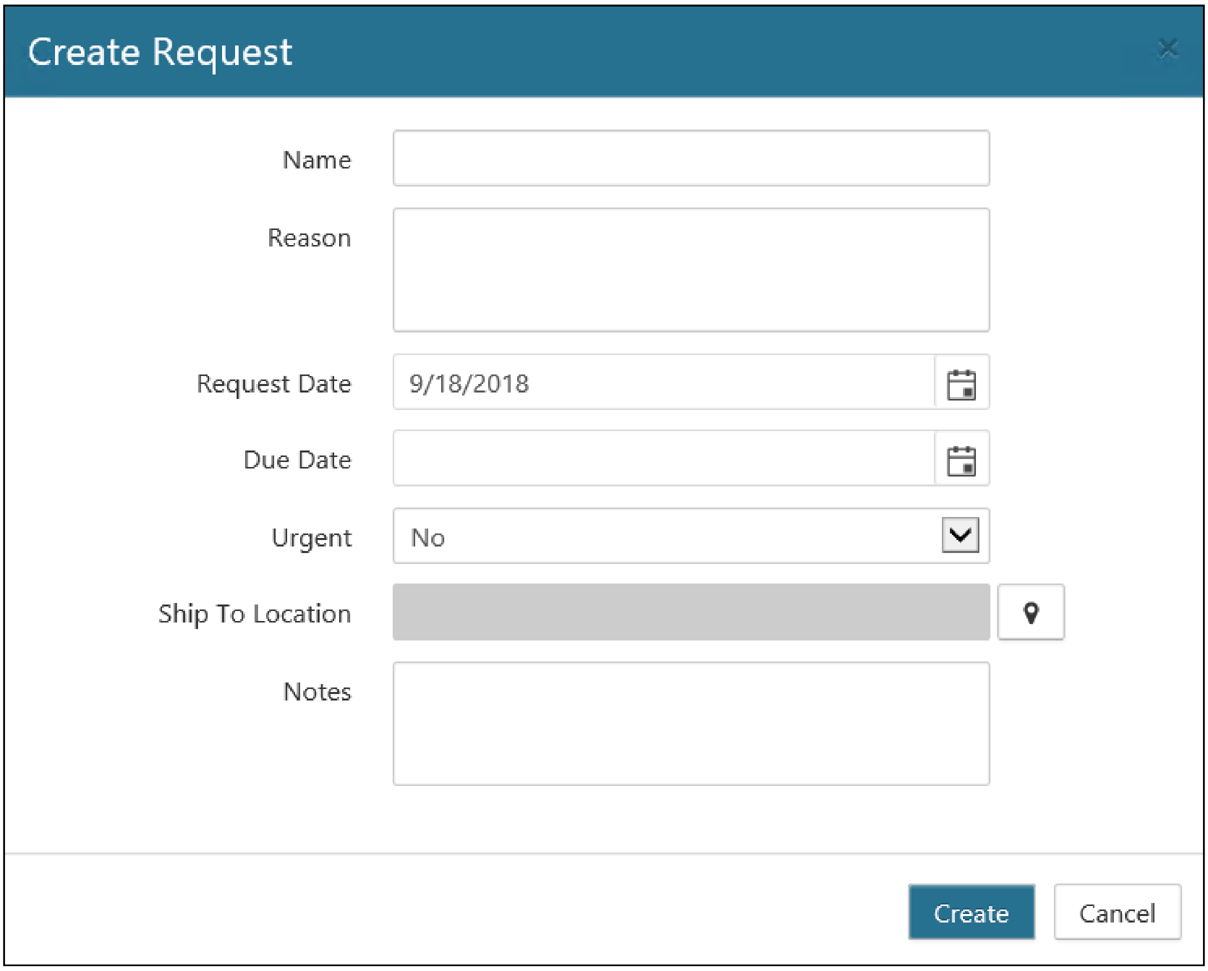
4.6.1.6 Creating a Request



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 9/18/2018

Due Date

Urgent No

Ship To Location

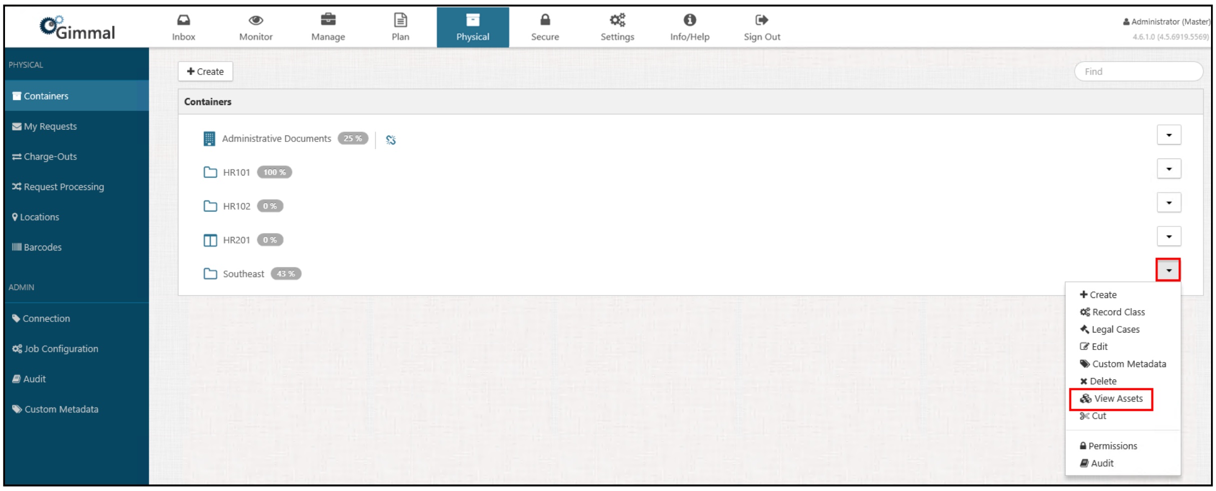
Notes

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[15]
    - **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[16].

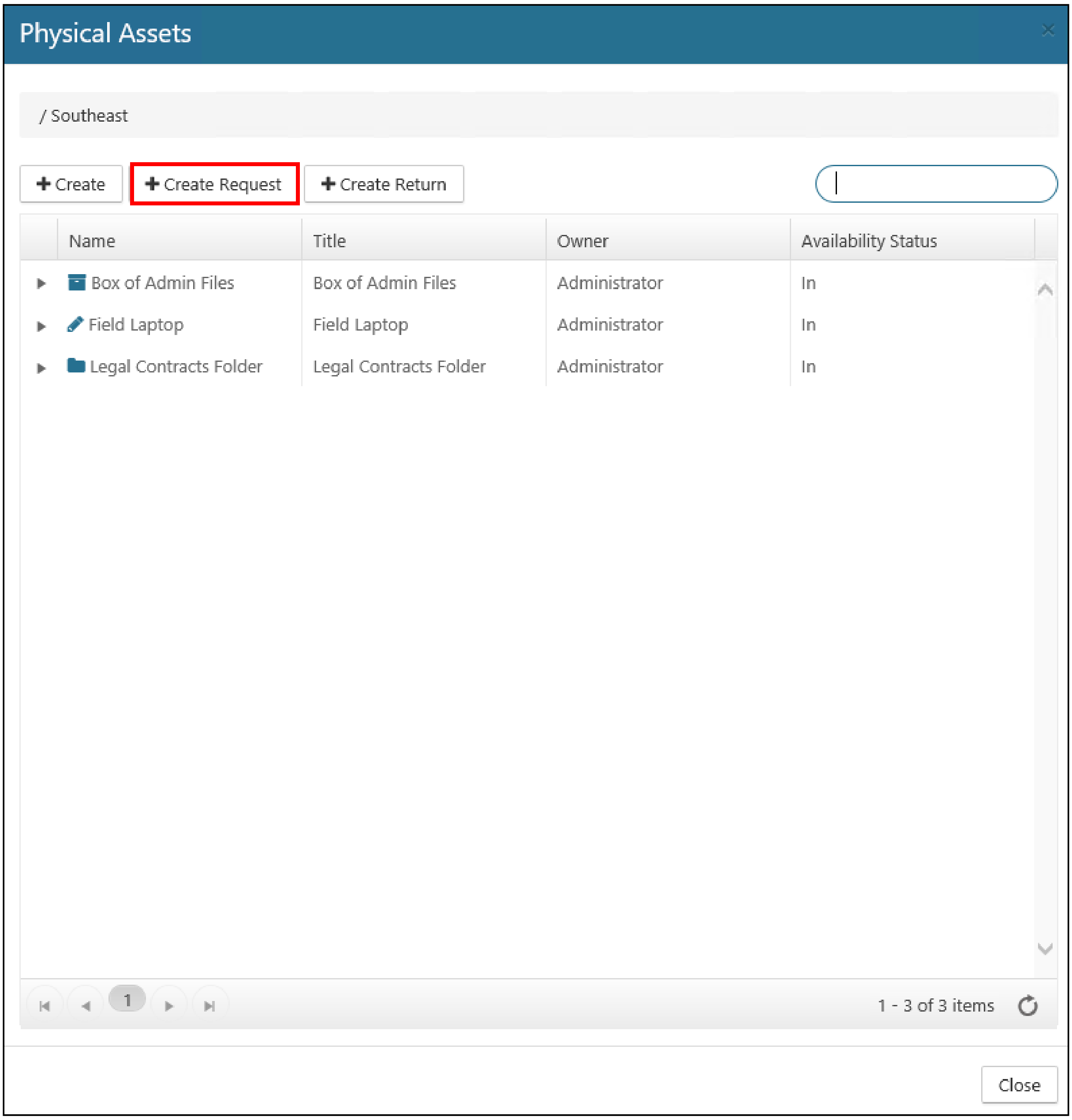
Creating a Return from the View Assets Dialog

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

[15] http://docs.gimmal.com/en/5905-managing-locations.html
[16] http://docs.gimmal.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

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

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.

4.6.1.7 Adding and Removing Assets from a Request

Adding a Physical Asset to a Request

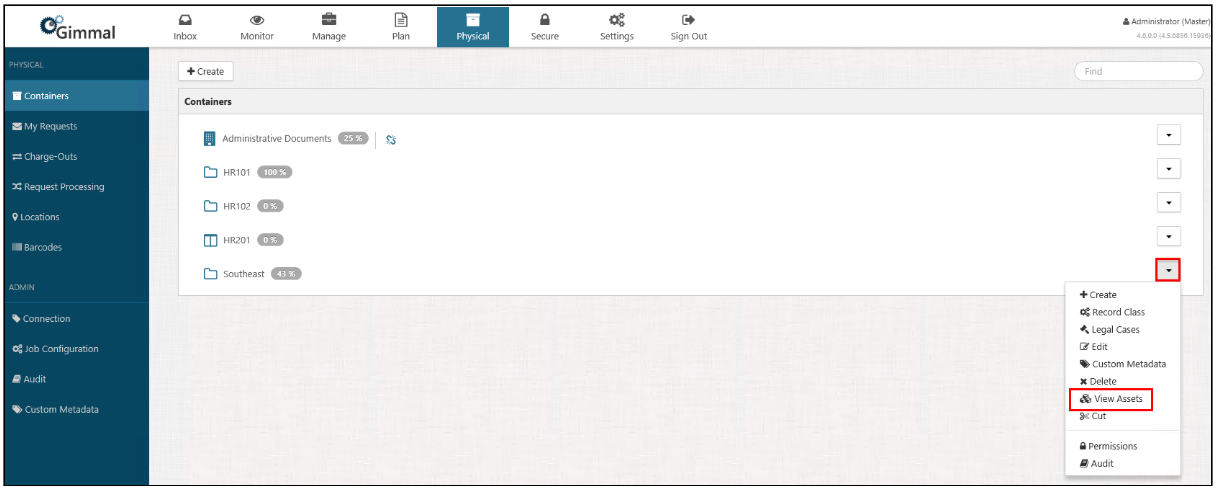
You can add one or more physical asset(s) to an existing request (one that has not yet been submitted) or you can create a new request and add it then. You must add an asset(s) to a request before you can submit it. If you do not, you an error message displays.

⚠ **Child Assets**

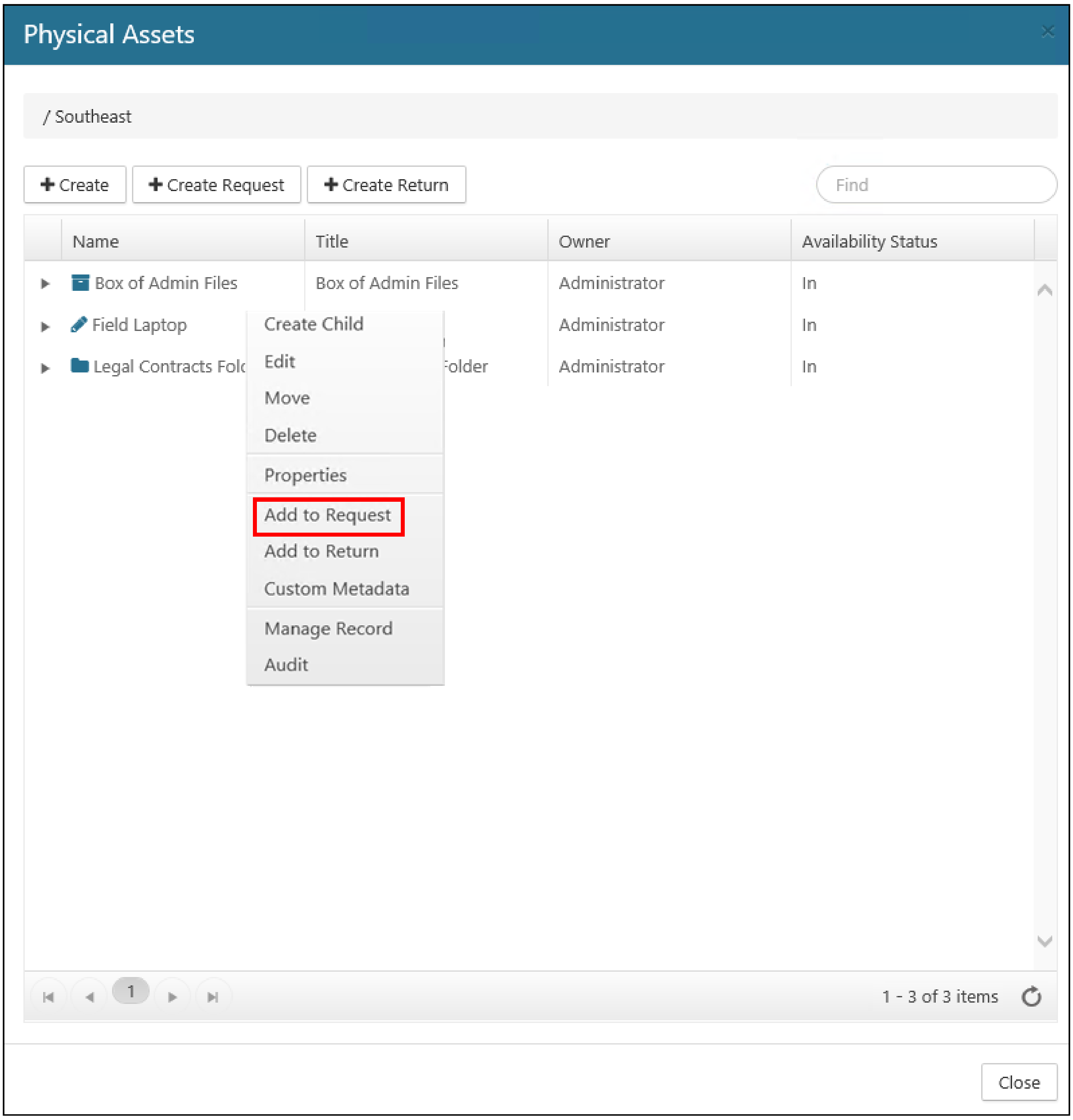
If you request a parent physical asset, all child assets will be included with the request. Conversely, you can request a child asset without requesting its parent asset.

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.)



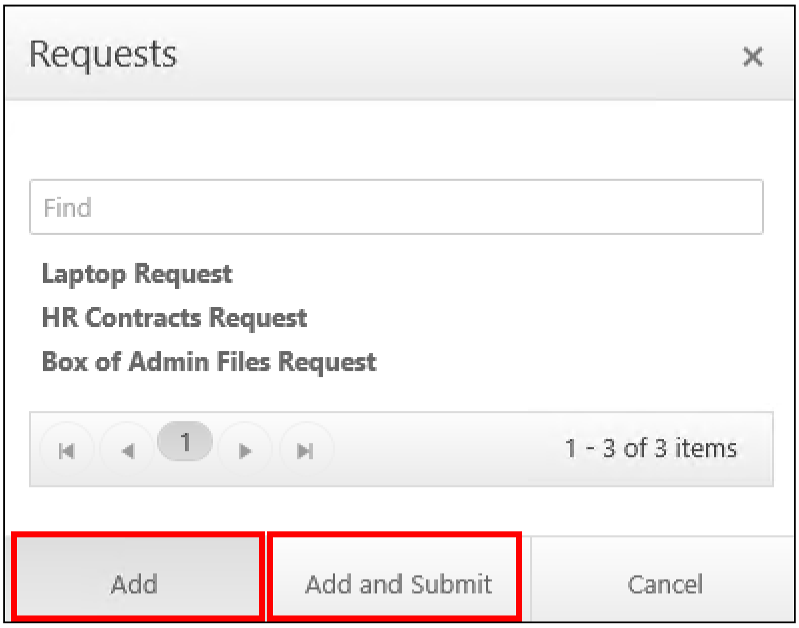
Physical Assets

/ Southeast

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

1 - 3 of 3 items

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



Requests

Find

Laptop Request

HR Contracts Request

Box of Admin Files Request

1 - 3 of 3 items

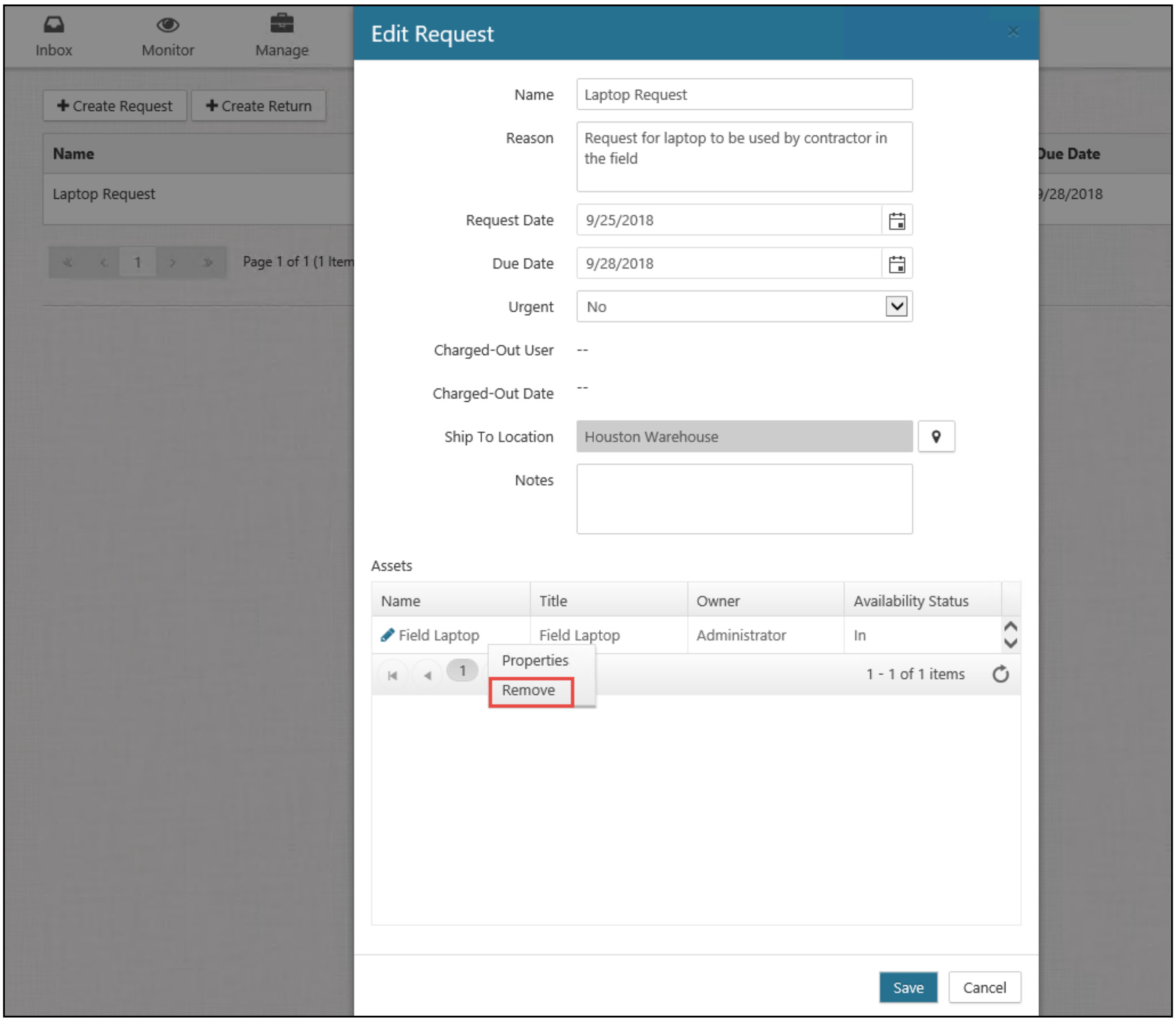
5. Perform either of the following steps:
   - Select the request you want to add the asset to, and then click **Add**. A green confirmation message displays in the upper right corner, indicating that the request was added. (You can verify the asset was added to the request by returning to the My Requests 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 clickEdit. (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**.



Edit Request

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:

Assets

Name	Title	Owner	Availability Status
Field Laptop	Field Laptop	Administrator	In

1 - 1 of 1 items

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.

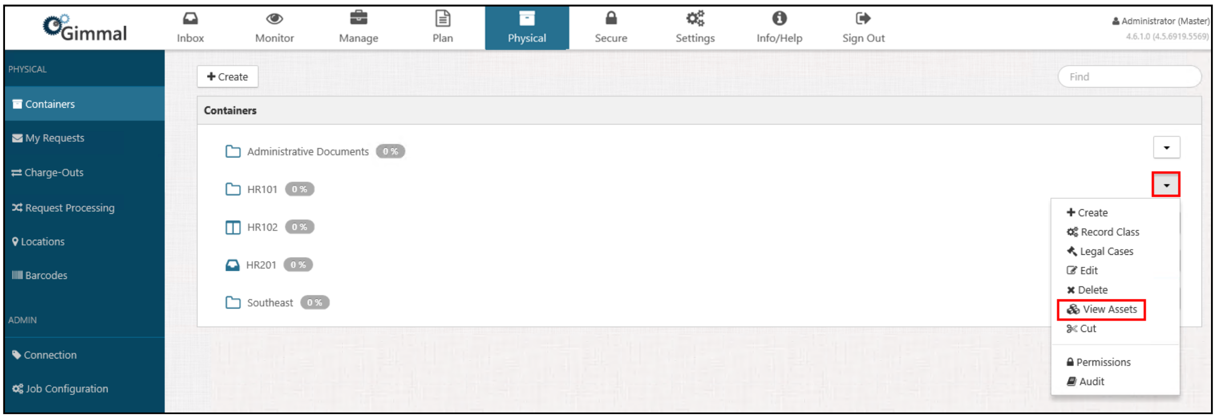
4.6.1.8 Submitting a Request

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:

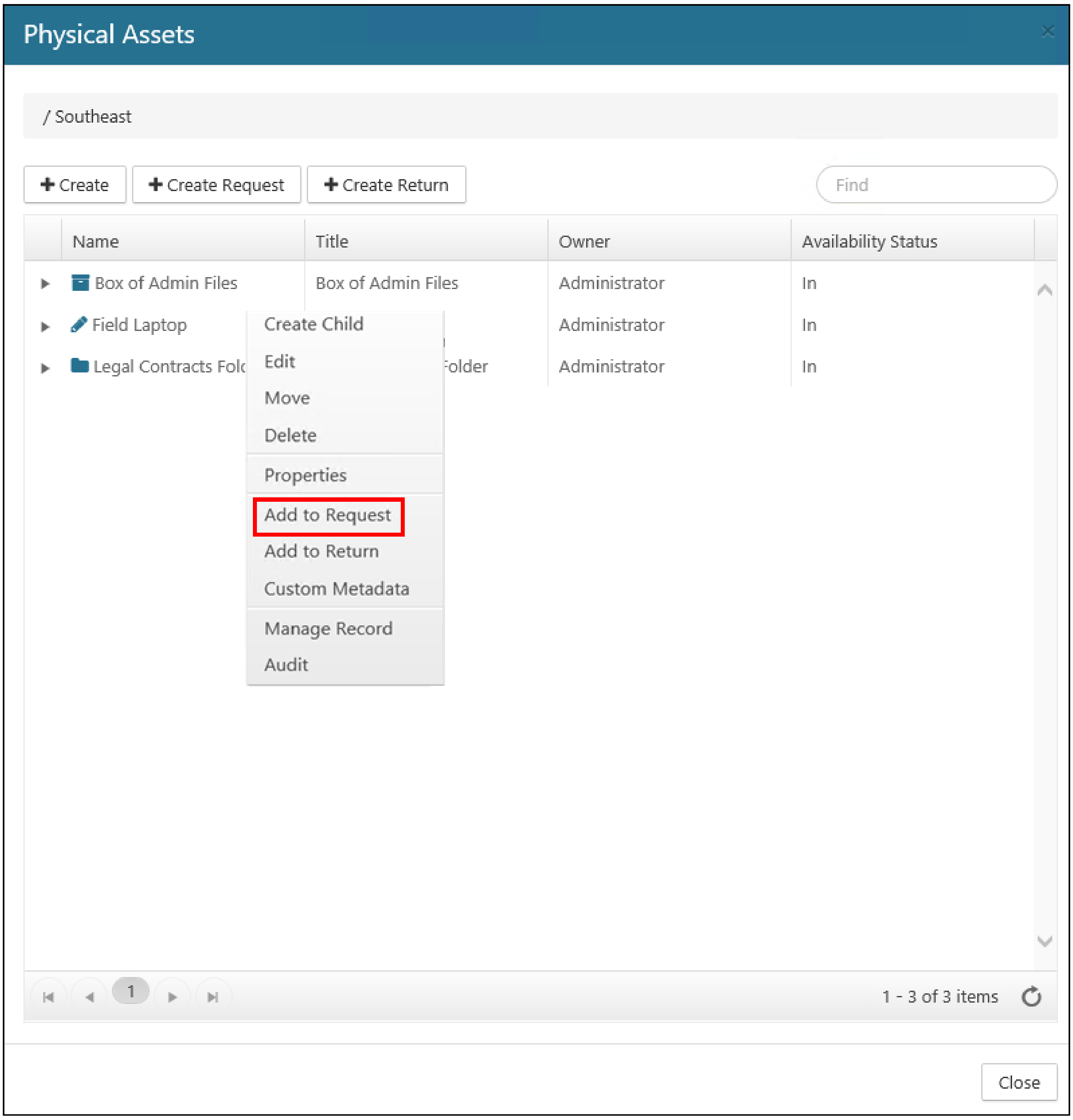
- Submitting it from an asset
- Submitting it from the My Requests page

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.)



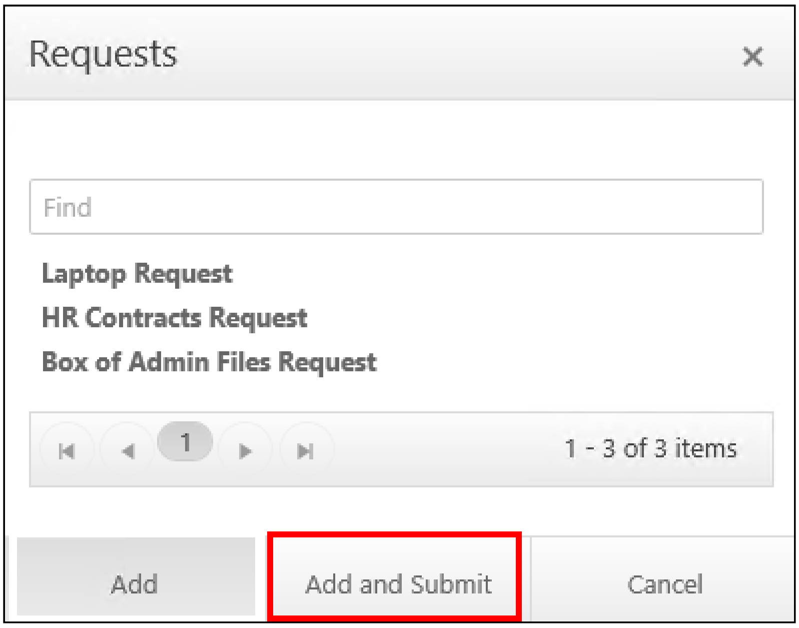
Physical Assets

/ Southeast

Name	Title	Owner	Availability Status
Box of Admin Files	Box of Admin Files	Administrator	In
Field Laptop		Administrator	In
Legal Contracts Folc	'older	Administrator	In

1 - 3 of 3 items

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



Requests

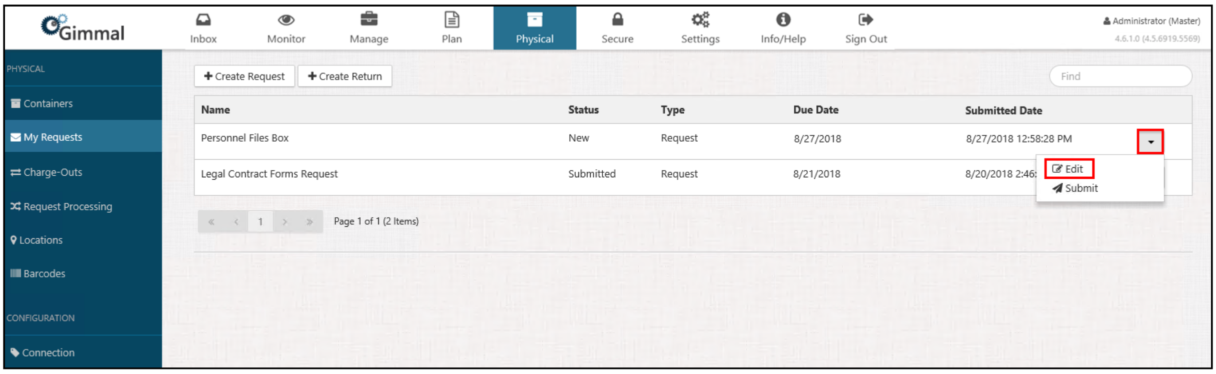
Laptop Request
HR Contracts Request
Box of Admin Files Request

1 - 3 of 3 items

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

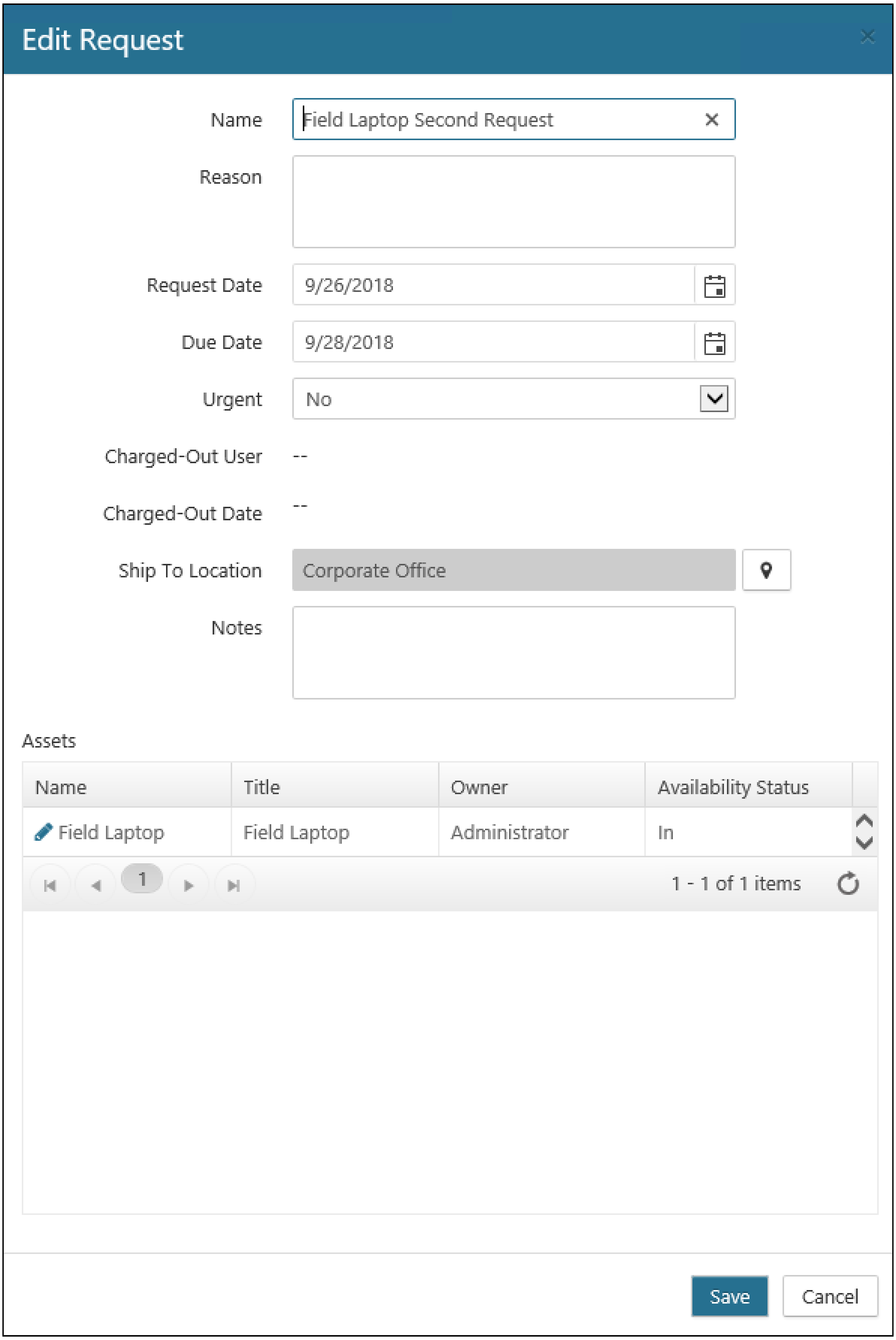
1. Select **Physical** from the Main Menu, and then select **My Requests** from the left navigation menu. The My Requests page displays
2. Locate the request you want to cancel or edit. The request must have a Status of **Submitted** if you want to cancel. Click the drop-down list on the right side,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



Name	Status	Type	Due Date	Submitted Date
Personnel Files Box	New	Request	8/27/2018	8/27/2018 12:58:28 PM
Legal Contract Forms Request	Submitted	Request	8/21/2018	8/20/2018 2:46:

Page 1 of 1 (2 Items)

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	Field Laptop Second Request
Reason	
Request Date	9/26/2018
Due Date	9/28/2018
Urgent	No
Charged-Out User	--
Charged-Out Date	--
Ship To Location	Corporate Office
Notes	

Assets

Name	Title	Owner	Availability Status
Field Laptop	Field Laptop	Administrator	In

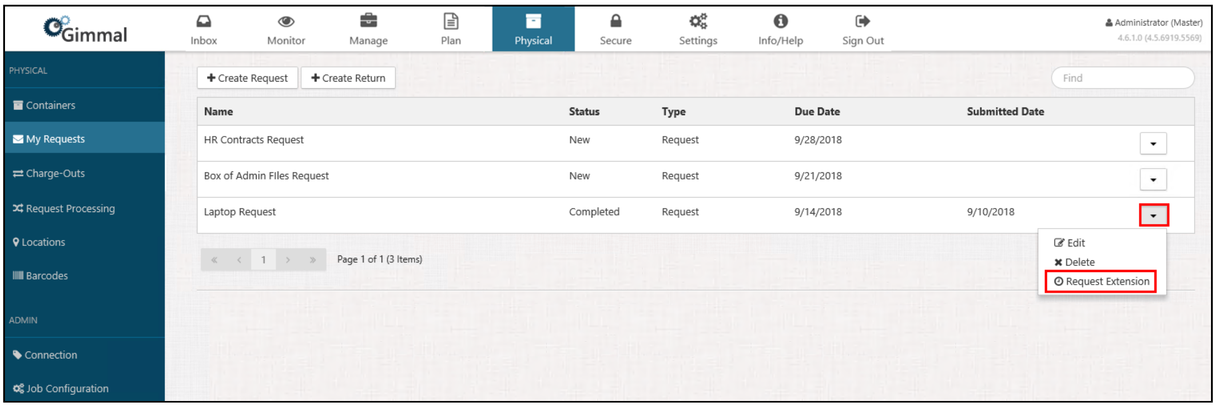
1 - 1 of 1 items

4.6.1.9 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[17]). 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**.

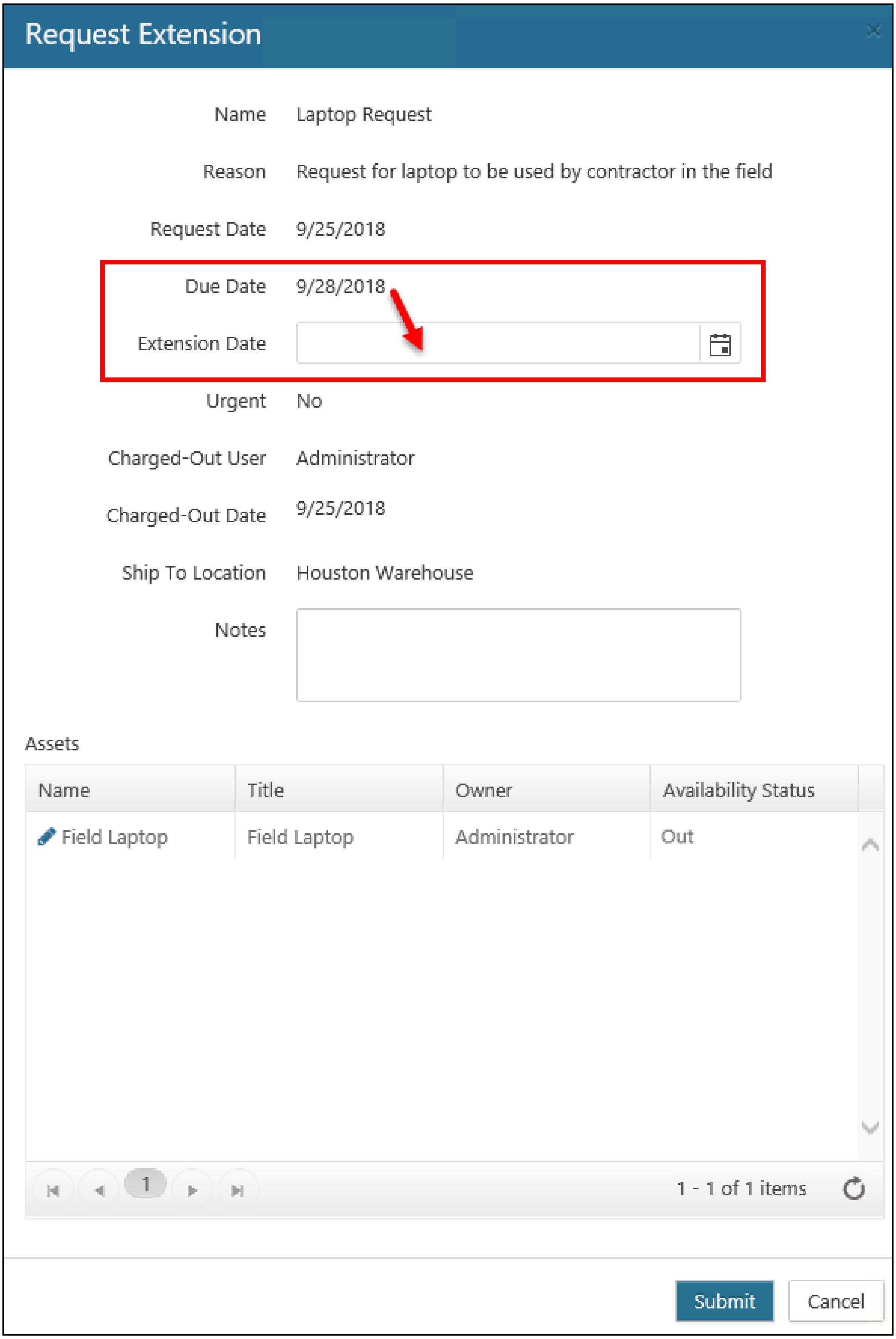


Name	Status	Type	Due Date	Submitted Date
HR Contracts Request	New	Request	9/28/2018	
Box of Admin FIles Request	New	Request	9/21/2018	
Laptop Request	Completed	Request	9/14/2018	9/10/2018

Page 1 of 1 (3 Items)

[17] 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

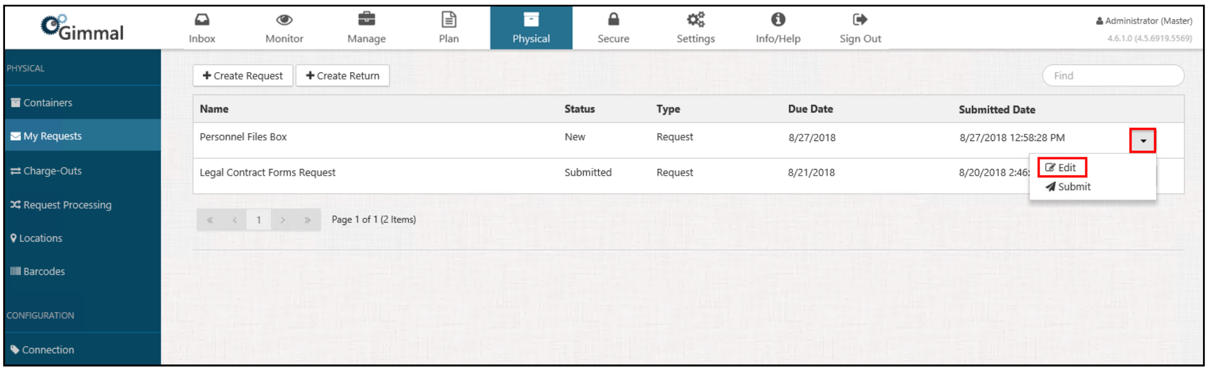
1 - 1 of 1 items

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.

4.6.1.10 Canceling and Deleting a Request

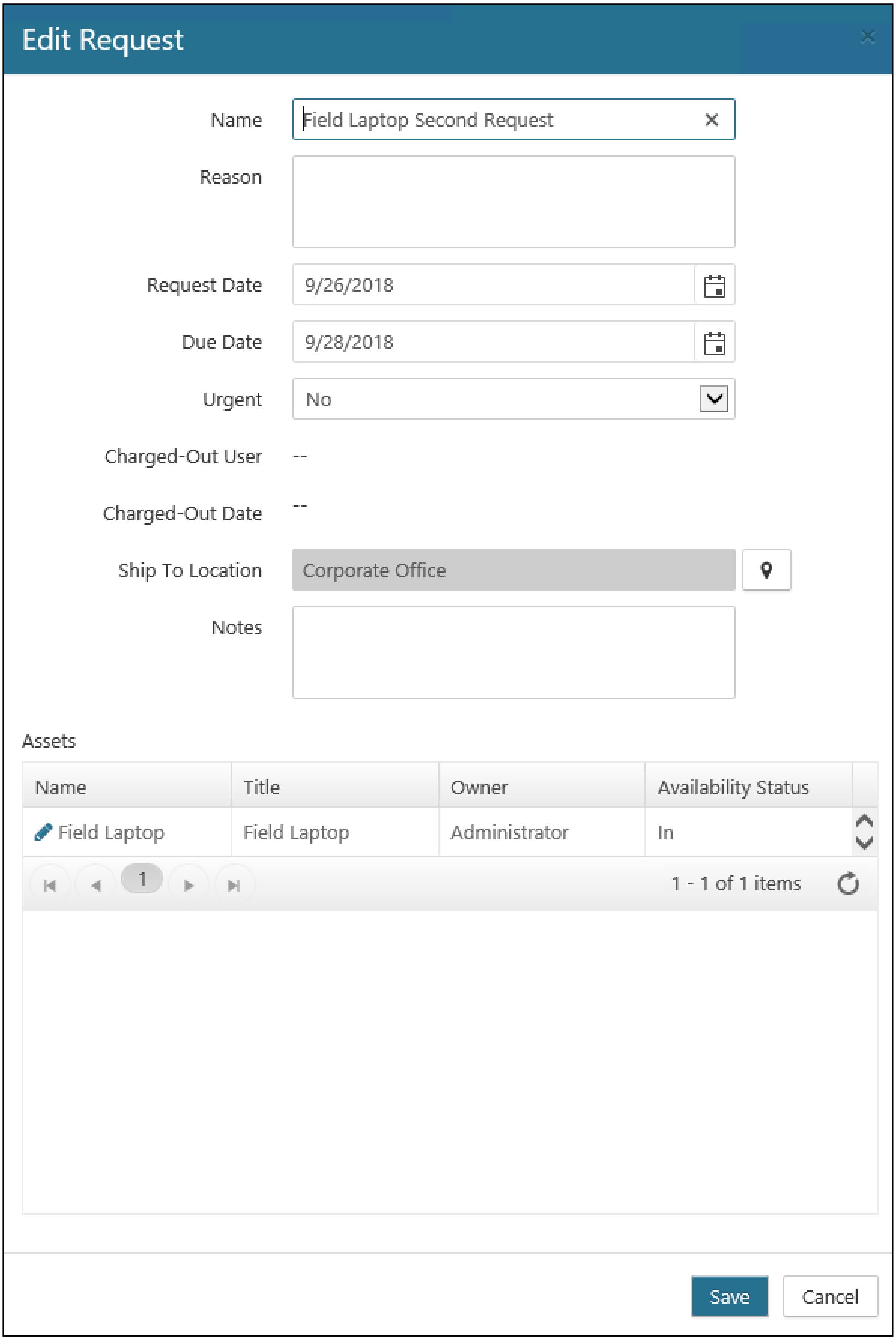
Canceling a Request

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



Name	Status	Type	Due Date	Submitted Date
Personnel Files Box	New	Request	8/27/2018	8/27/2018 12:58:28 PM
Legal Contract Forms Request	Submitted	Request	8/21/2018	8/20/2018 2:46:

The Edit Request dialog opens.



Edit Request

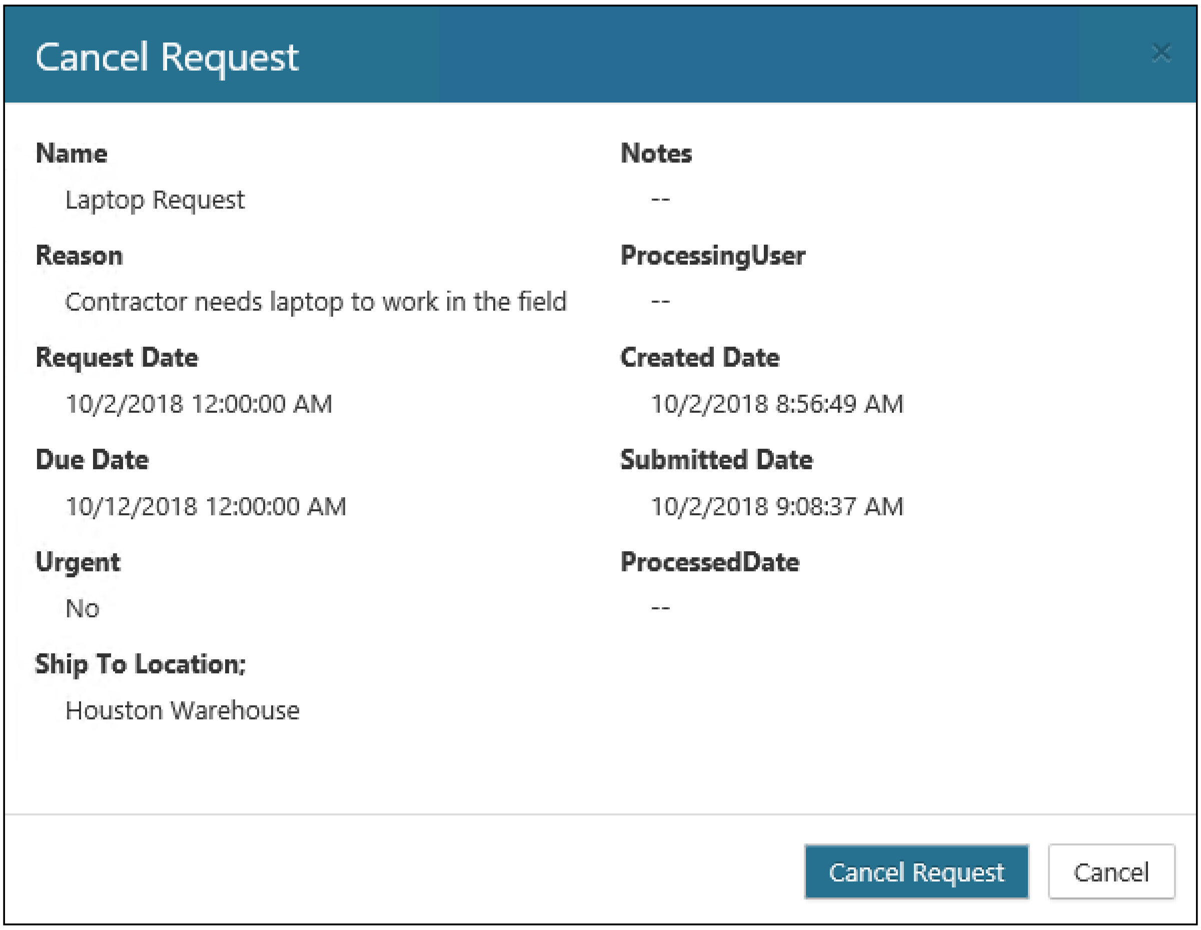
Name	Field Laptop Second Request
Reason	
Request Date	9/26/2018
Due Date	9/28/2018
Urgent	No
Charged-Out User	--
Charged-Out Date	--
Ship To Location	Corporate Office
Notes	

Assets

Name	Title	Owner	Availability Status
Field Laptop	Field Laptop	Administrator	In

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
Laptop Request

Reason
Contractor needs laptop to work in the field

Request Date
10/2/2018 12:00:00 AM

Due Date
10/12/2018 12:00:00 AM

Urgent
No

Ship To Location:
Houston Warehouse

Notes
--

ProcessingUser
--

Created Date
10/2/2018 8:56:49 AM

Submitted Date
10/2/2018 9:08:37 AM

ProcessedDate
--

Deleting a Request

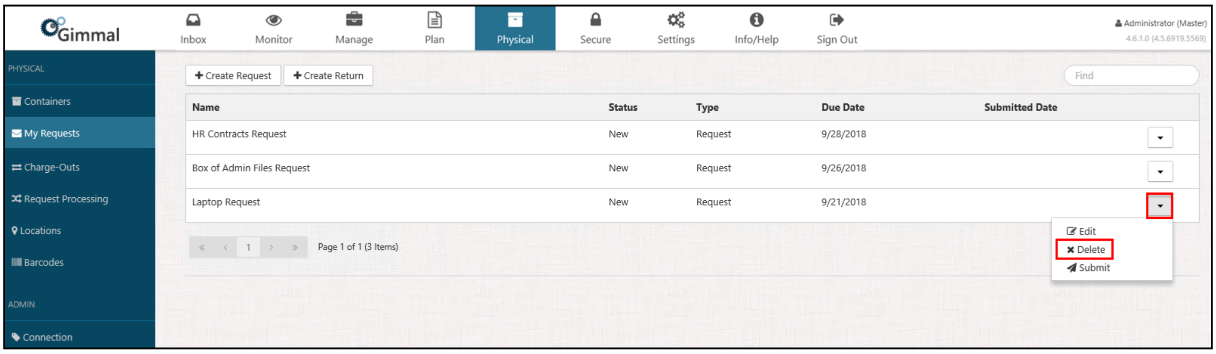
You can delete a request under the following conditions:

- 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**.



Name	Status	Type	Due Date	Submitted Date
HR Contracts Request	New	Request	9/28/2018	
Box of Admin Files Request	New	Request	9/26/2018	
Laptop Request	New	Request	9/21/2018	

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.

4.6.2 Returning an Asset

The following topics cover how to return an asset.

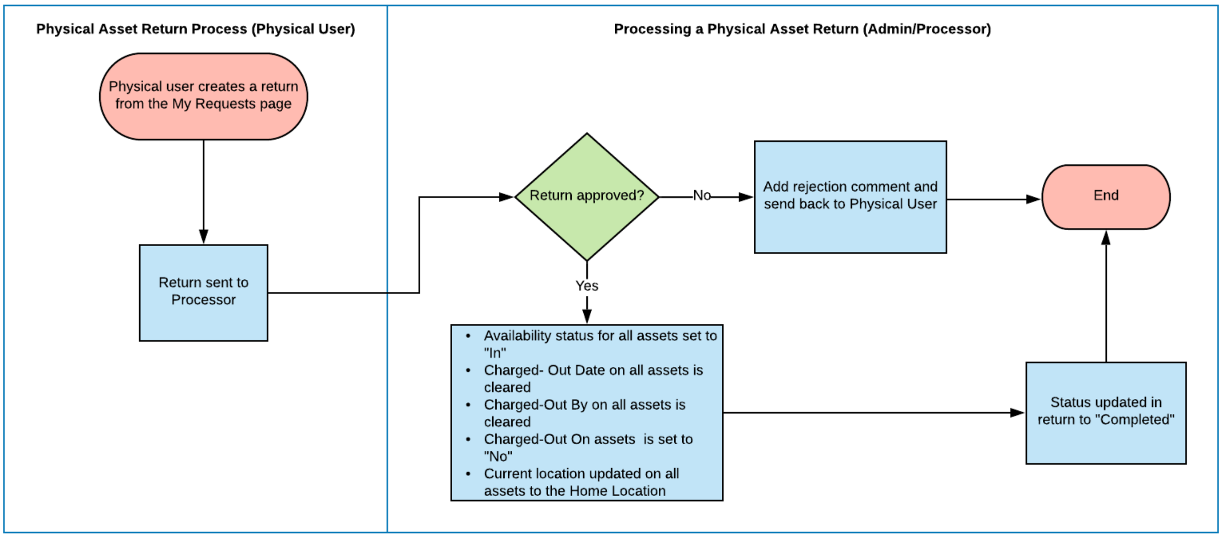
4.6.2.1 Creating a Return

4.6.2.2 Adding and Removing Assets from a Return

4.6.2.3 Submitting a Return

4.6.2.4 Canceling and Deleting a Return

The following flowchart illustrates the return process.


Physical Asset Return Process (Physical User)
Processing a Physical Asset Return (Admin/Processor)
Physical user creates a return from the My Requests page
Return sent to Processor
Return approved?
No
Yes
Add rejection comment and send back to Physical User
End
Availability status for all assets set to "In"
Charged- Out Date on all assets is cleared
Charged-Out By on all assets is cleared
Charged-Out On assets is set to "No"
Current location updated on all assets to the Home Location
Status updated in return to "Completed"

4.6.2.5 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

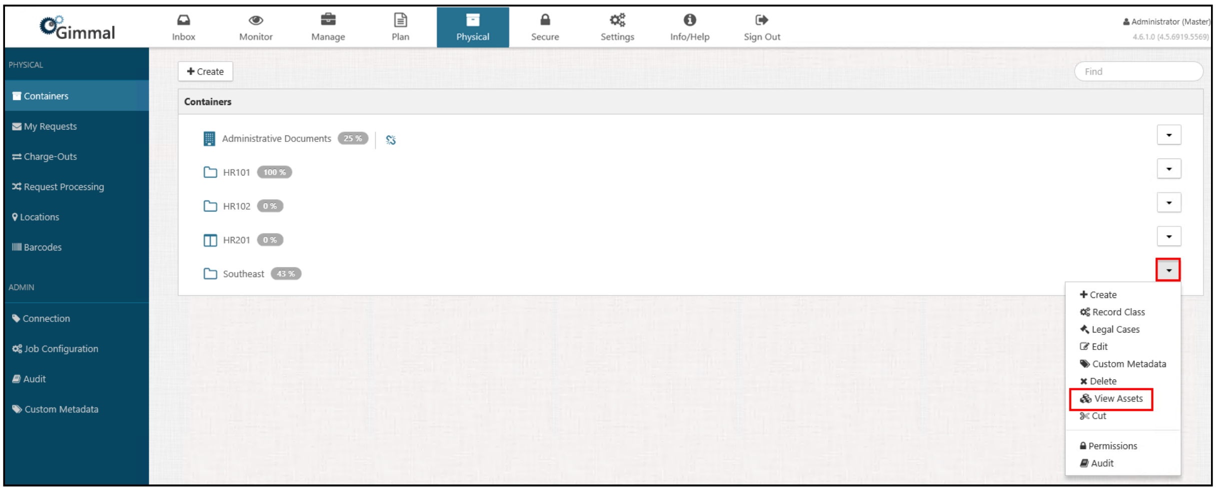
1. Select **Physical** from the Main Menu, and then **My Requests** from the left navigation menu. The My Requests page displays.
2. Click **+Create Return**. The Create Return window opens.
3. Enter the following information. An asterisk (*) indicates a required field.
   - **Name** – Enter a name/title 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[18]
   - **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[19].

Creating a Return from the View Assets Dialog

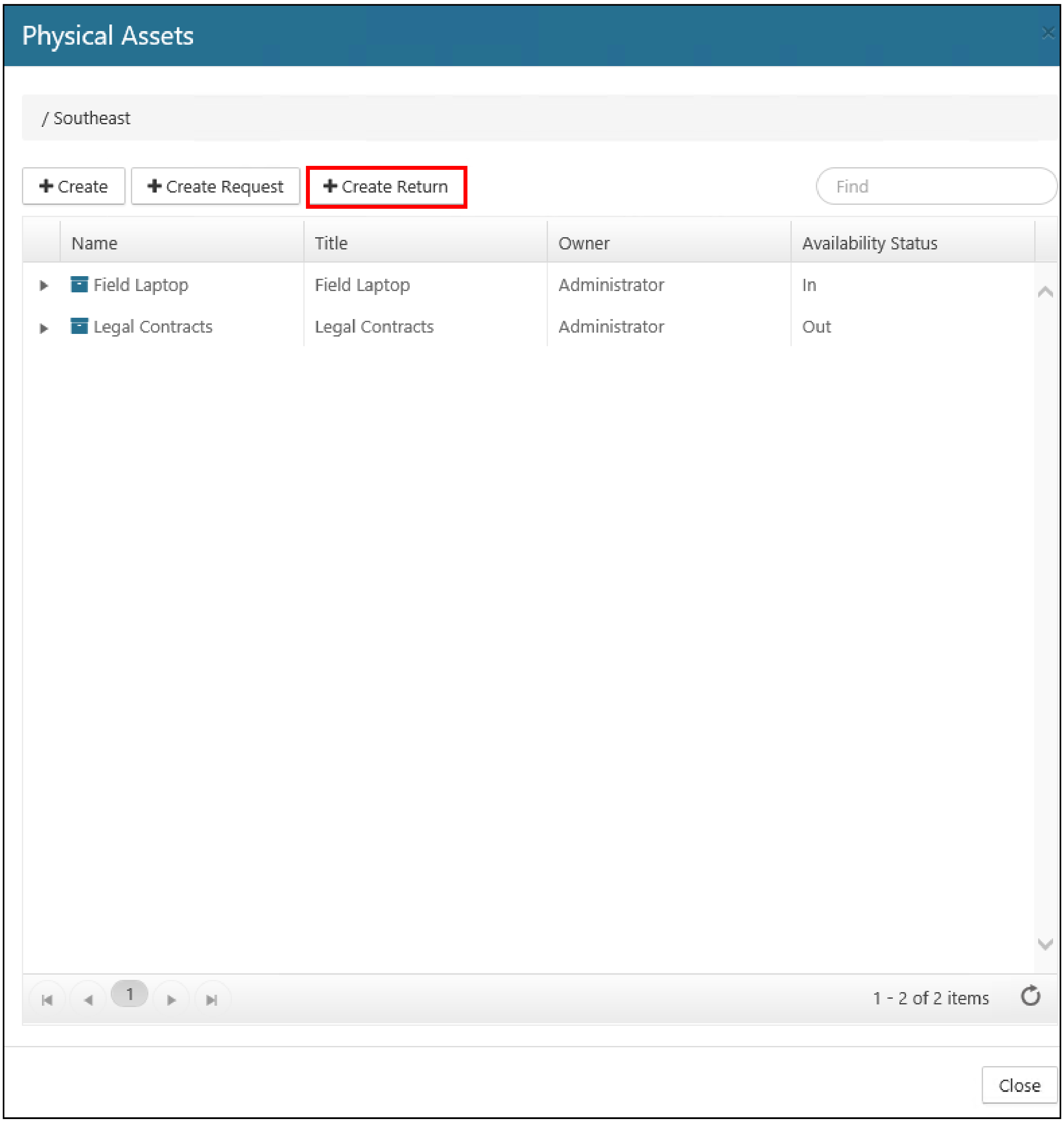
1. Select **Physical** on the Main Menu, and then **Containers** on the left navigation menu. The Containers page displays.

[18] http://docs.gimmal.com/en/5905-managing-locations.html
[19] http://docs.gimmal.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.



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

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

4.6.2.6 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 75) 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

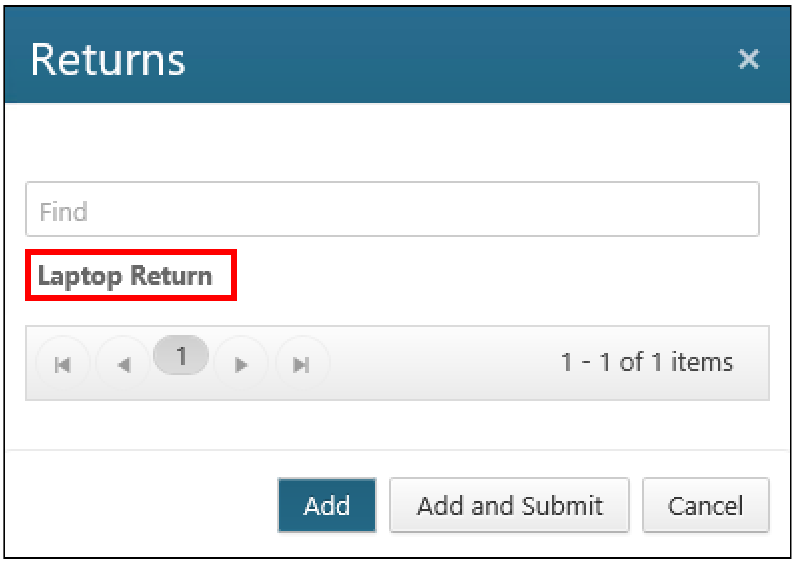
⚠

- 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.

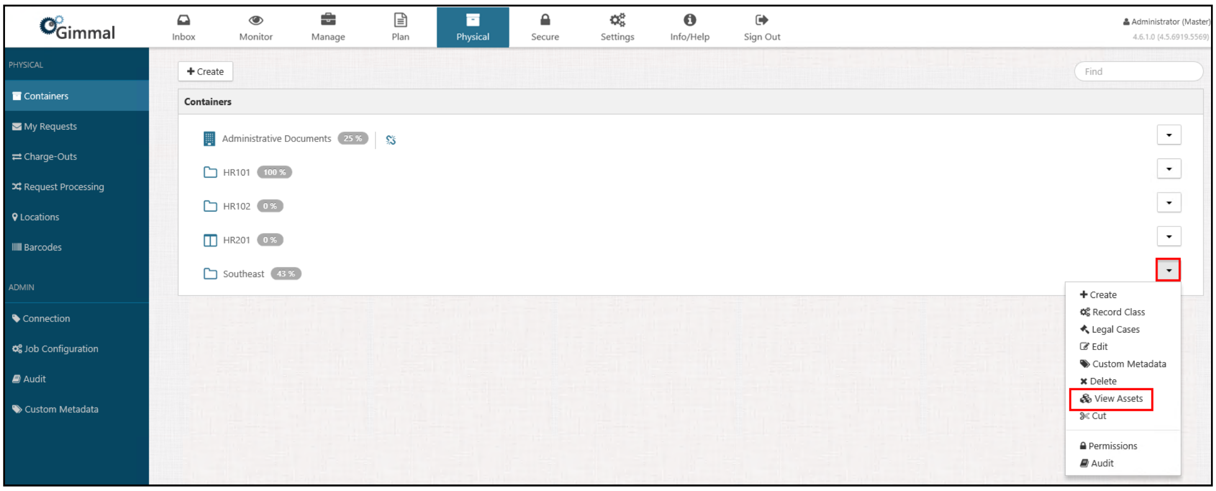
1. Select **Physical** from the Main Menu, and then **Charge-Outs** from the left navigation menu. The Charge-Outs page opens, displaying a list of your charged-out assets.
2. Locate the asset you want to return, click the drop-down arrow on the right, and select **+Add to Return**. The Returns window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



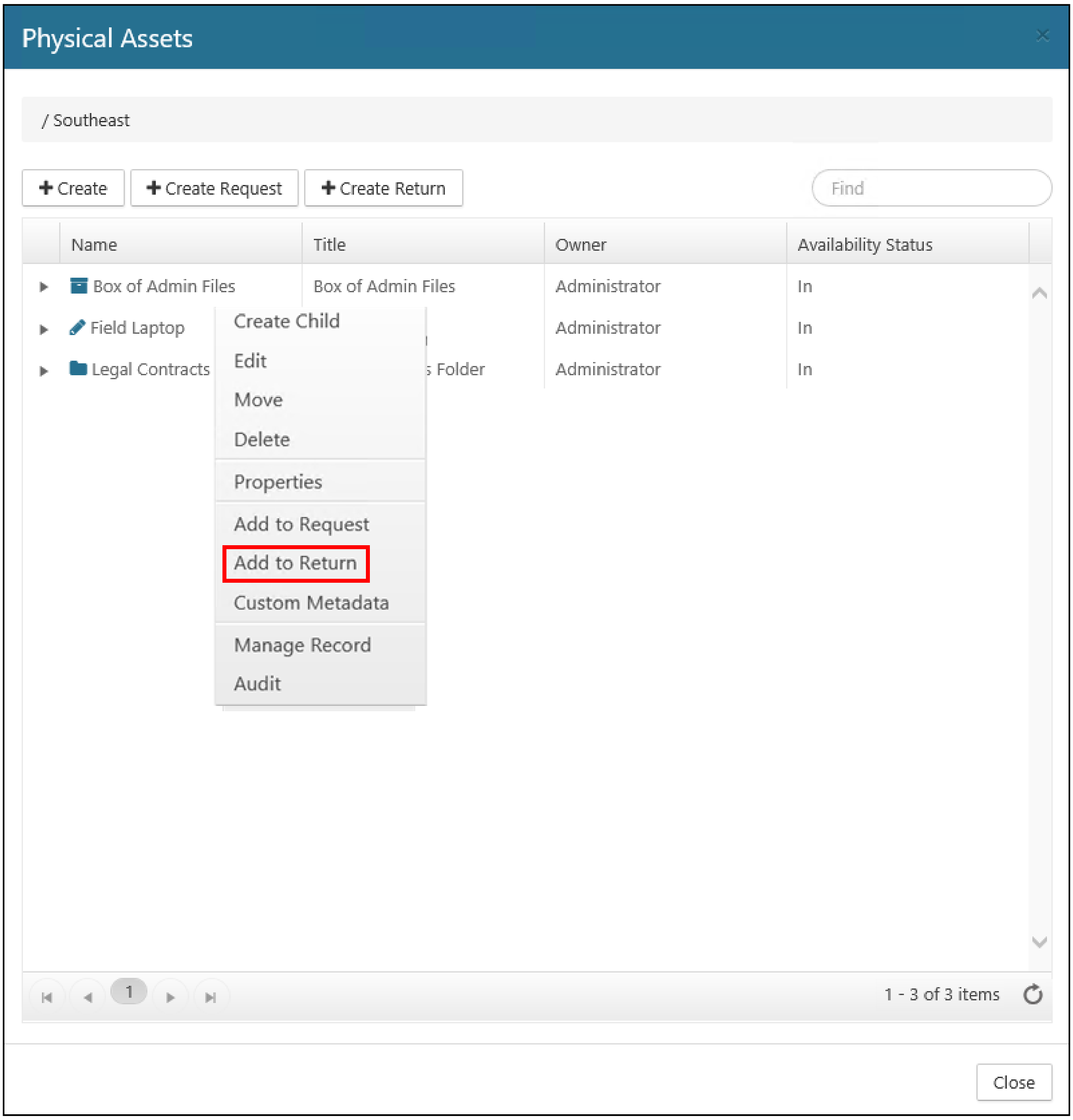
3. Perform either of the following steps:
   - Select the return you want to add the asset to, and then click **Add**. A green confirmation message displays in the upper right corner, indicating that the return was added. (You can verify the asset was added to the return by returning to the My Requests 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.)

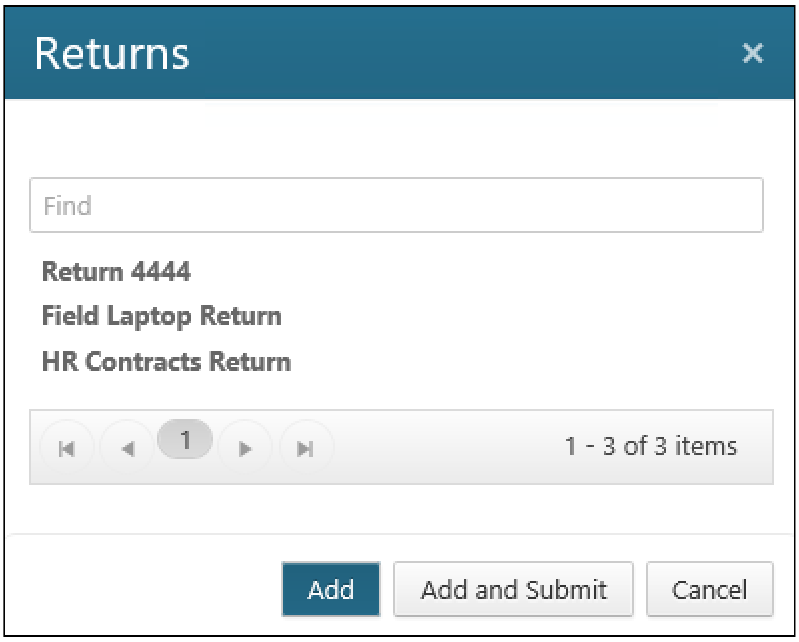


3. Click **View Assets**. The Physical Assets window displays, showing a list of all the physical assets in that container.
4. On the Physical Assets window, right-click the asset you want to add to your return and select **Add to Return**. (The drop-down options you see may vary, depending on your permissions.)



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

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

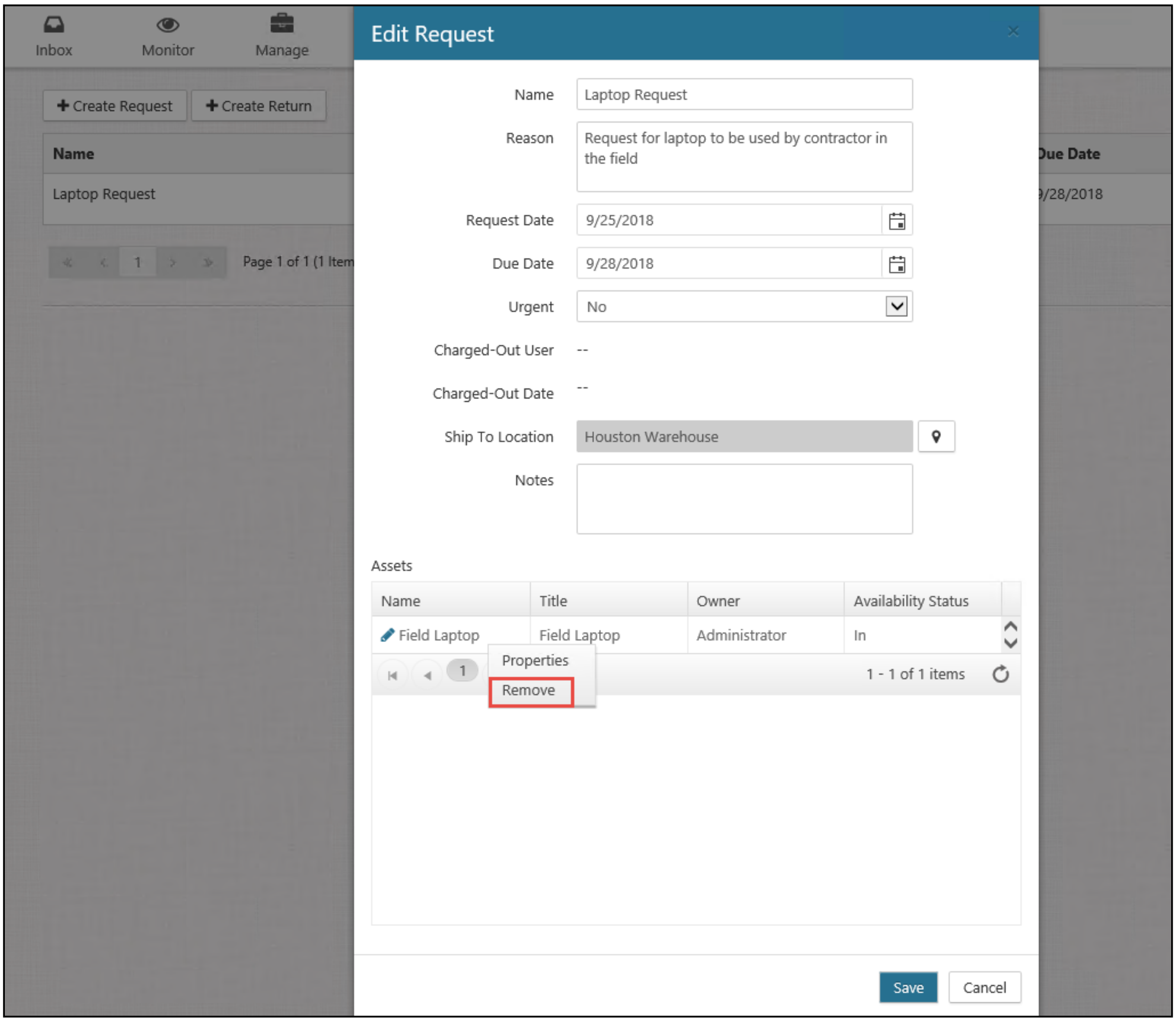


5. Perform either of the following steps:
    - Select the return you want to add the asset to, and then click **Add**. A green confirmation message displays in the upper right corner, indicating that the return was added. (You can verify the asset was added to the return by returning to the My Requests 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**.



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:

Assets

Name	Title	Owner	Availability Status
Field Laptop	Field Laptop	Administrator	In

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.

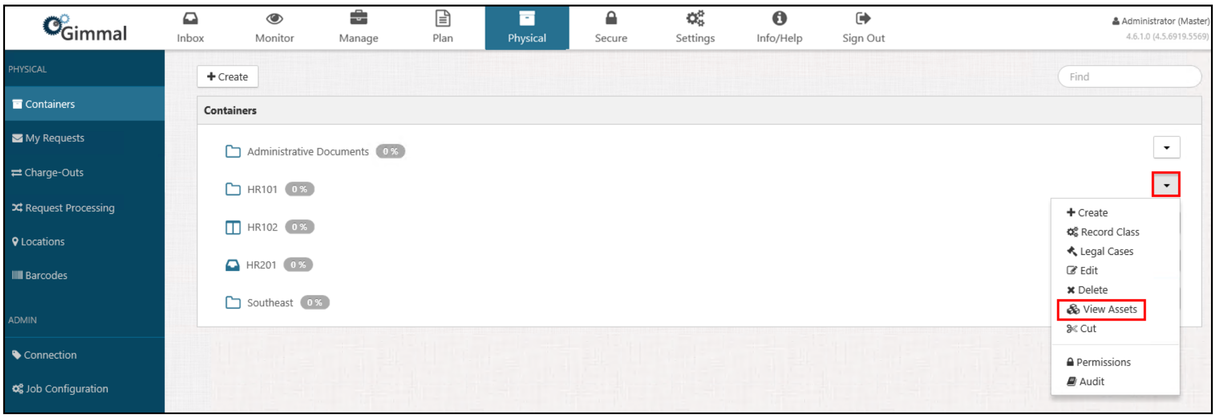
4.6.2.7 Submitting a Return

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:

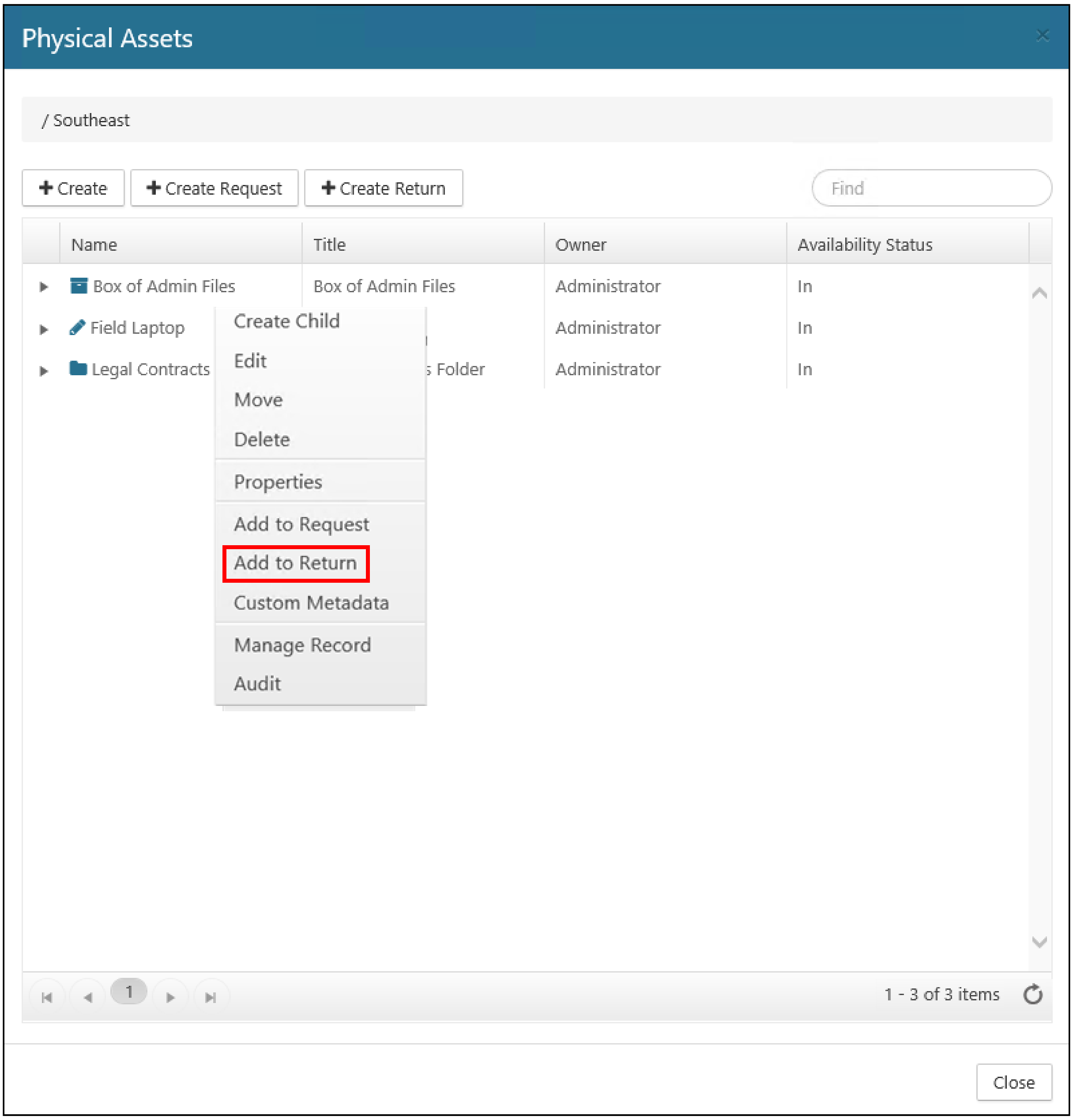
- Submitting it from the Returns window
- Submitting it from the My Requests page

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.)

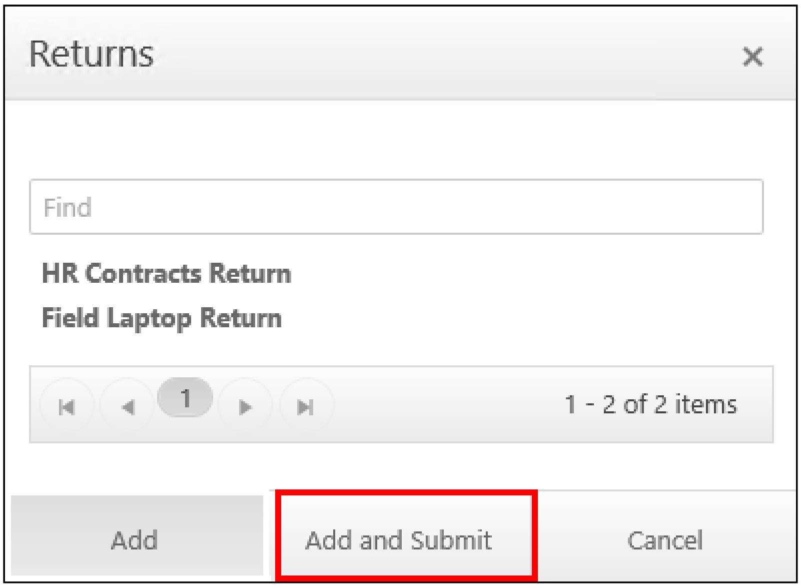


3. Click **View Assets**. The Physical Assets dialog displays, showing a list of all the physical assets in that container.
4. On the Physical Assets dialog, right-click the asset you want to add to your returm and select **Add to Request**. (The drop-down options you see may vary, depending on your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



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

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



HR Contracts Return

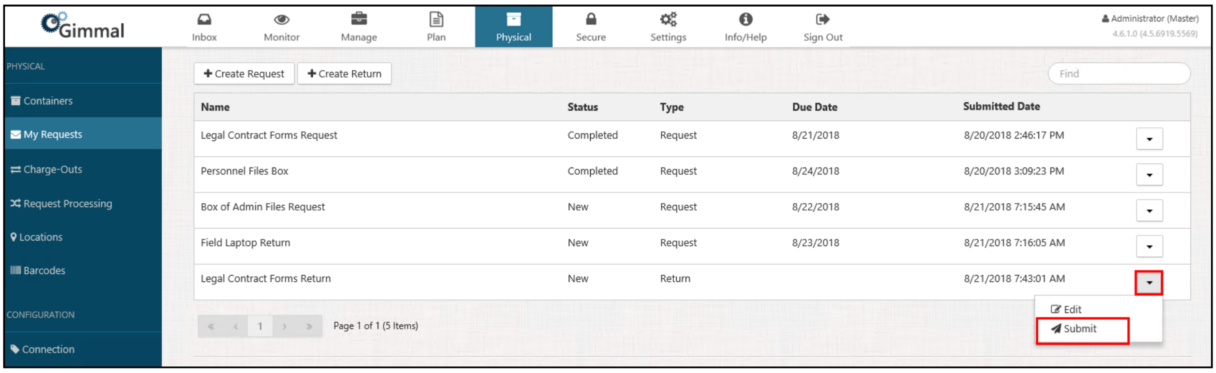
Field Laptop Return

1 - 2 of 2 items

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.)



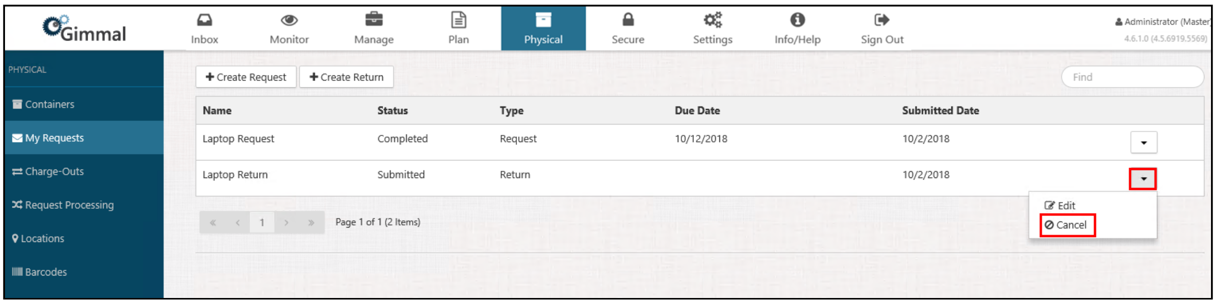
Name	Status	Type	Due Date	Submitted Date
Legal Contract Forms Request	Completed	Request	8/21/2018	8/20/2018 2:46:17 PM
Personnel Files Box	Completed	Request	8/24/2018	8/20/2018 3:09:23 PM
Box of Admin Files Request	New	Request	8/22/2018	8/21/2018 7:15:45 AM
Field Laptop Return	New	Request	8/23/2018	8/21/2018 7:16:05 AM
Legal Contract Forms Return	New	Return		8/21/2018 7:43:01 AM

Page 1 of 1 (5 Items)

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.

4.6.2.8 Canceling and Deleting a Return

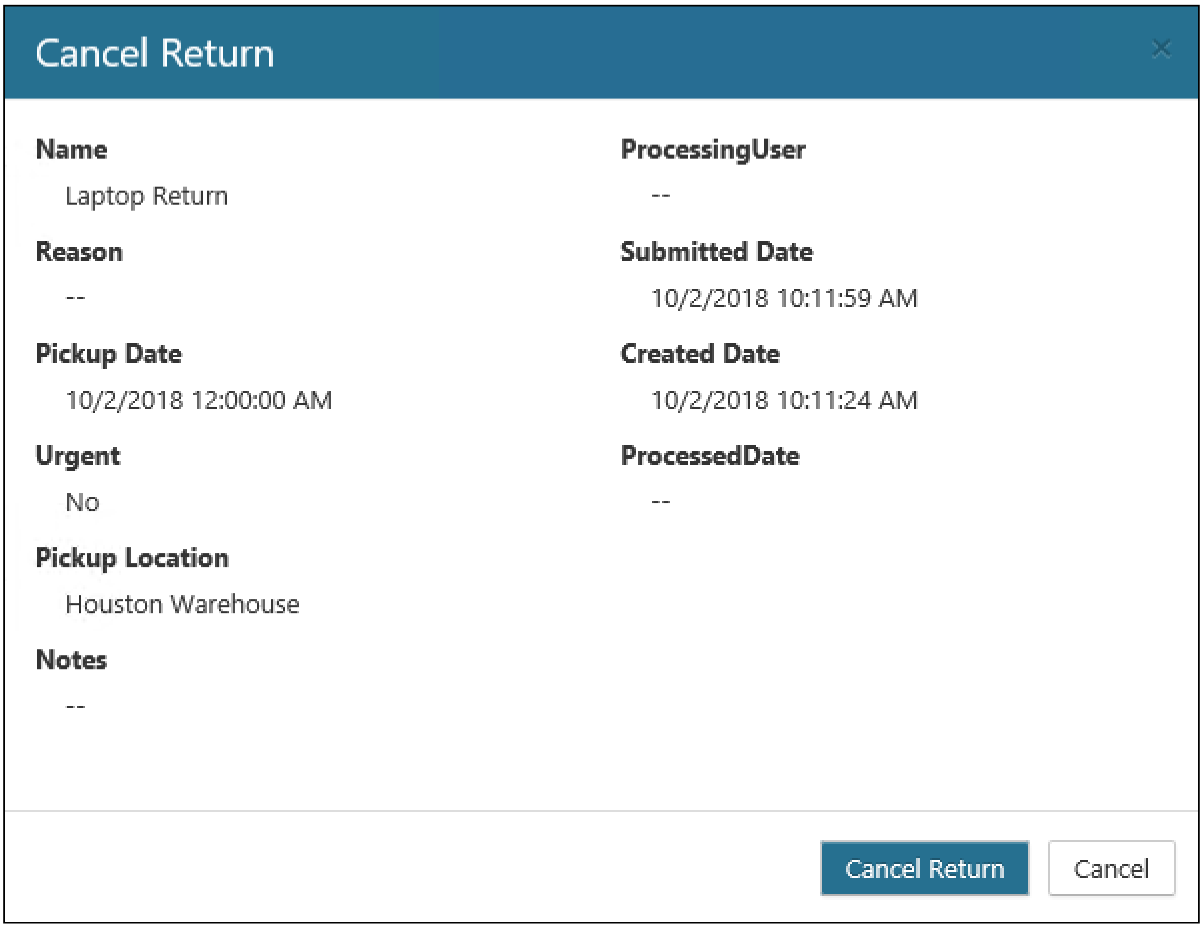
1. Select **Physical** from the Main Menu, and then select **My Requests** from the left navigation menu. The My Requests page displays
2. Locate the return you want to cancel or edit. The return must have a Status of **Submitted** if you want to cancel. Click the drop-down list on the right side, and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



Name	Status	Type	Due Date	Submitted Date
Laptop Request	Completed	Request	10/12/2018	10/2/2018
Laptop Return	Submitted	Return		10/2/2018

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**.



Name
Laptop Return

Reason
--

Pickup Date
10/2/2018 12:00:00 AM

Urgent
No

Pickup Location
Houston Warehouse

Notes
--

ProcessingUser
--

Submitted Date
10/2/2018 10:11:59 AM

Created Date
10/2/2018 10:11:24 AM

ProcessedDate
--

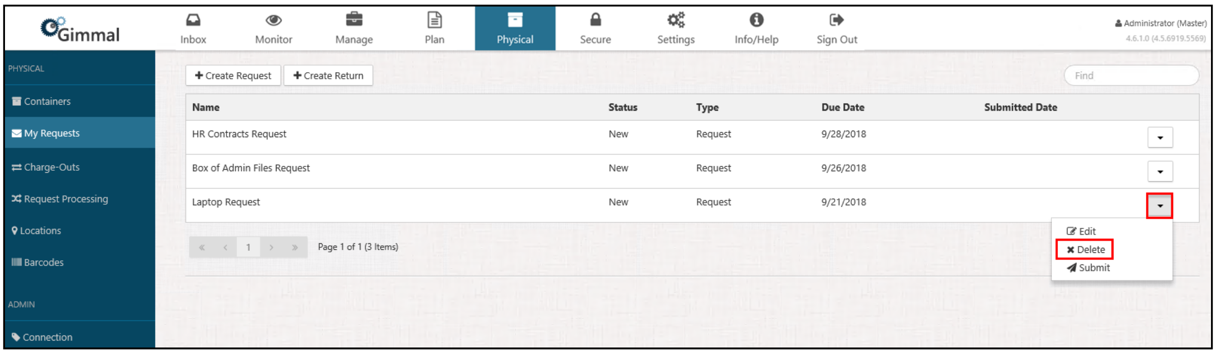
Deleting a Return

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**.



Name	Status	Type	Due Date	Submitted Date
HR Contracts Request	New	Request	9/28/2018	
Box of Admin Files Request	New	Request	9/26/2018	
Laptop Request	New	Request	9/21/2018	

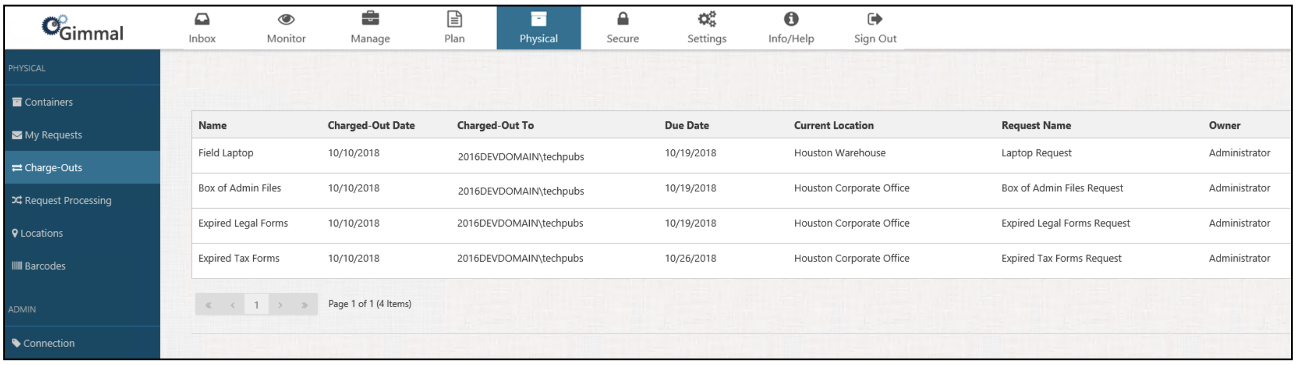
Page 1 of 1 (3 Items)

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

4.6.3 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.

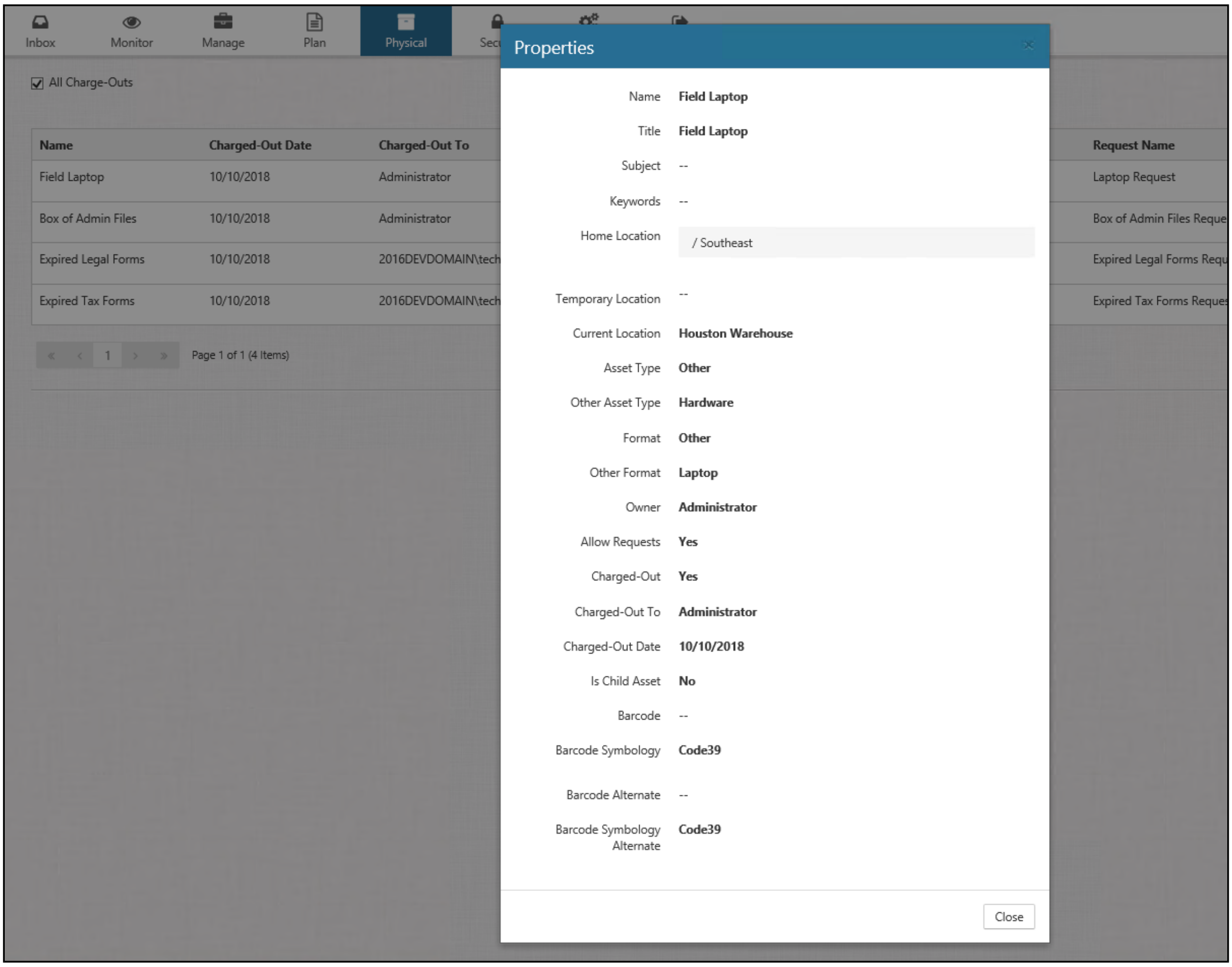


Name	Charged-Out Date	Charged-Out To	Due Date	Current Location	Request Name	Owner
Field Laptop	10/10/2018	2016DEVDOMAIN\techpubs	10/19/2018	Houston Warehouse	Laptop Request	Administrator
Box of Admin Files	10/10/2018	2016DEVDOMAIN\techpubs	10/19/2018	Houston Corporate Office	Box of Admin Files Request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

Page 1 of 1 (4 Items)

4.6.3.1 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**.



☑ All Charge-Outs

Name	Charged-Out Date	Charged-Out To	Request Name
Field Laptop	10/10/2018	Administrator	Laptop Request
Box of Admin Files	10/10/2018	Administrator	Box of Admin Files Reque
Expired Legal Forms	10/10/2018	2016DEVDOMAIN\tech	Expired Legal Forms Requ
Expired Tax Forms	10/10/2018	2016DEVDOMAIN\tech	Expired Tax Forms Reques

Page 1 of 1 (4 items)

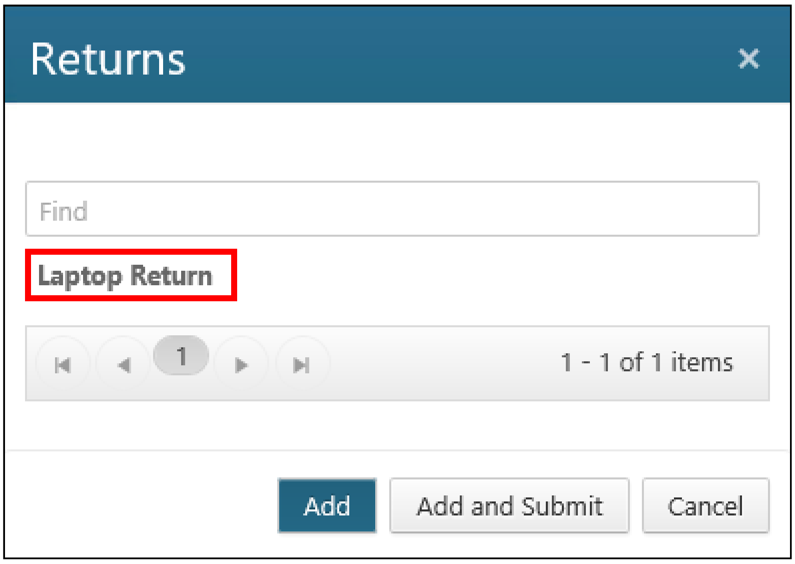
Properties

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

4.6.3.2 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.)

4.6.4 Taking Custody of an Asset

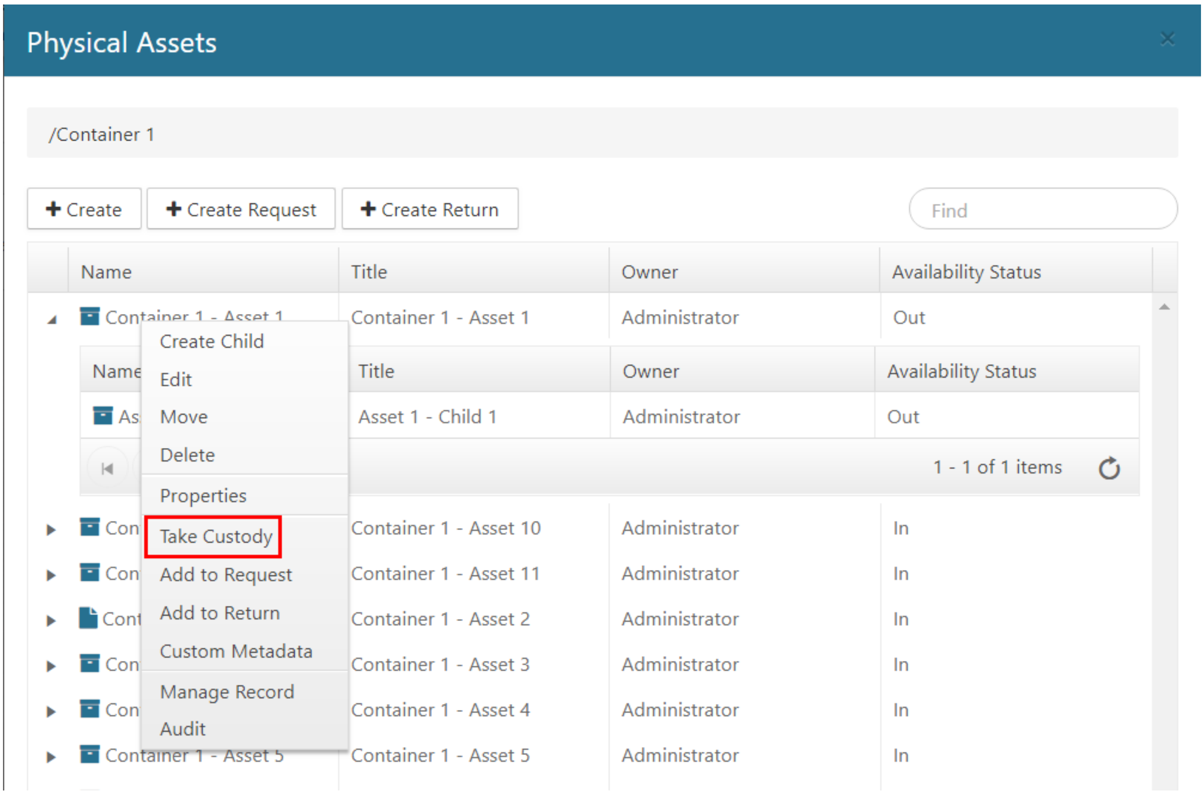
You can take custody of an asset in Physical Records Management that is charged out to someone else if you are a Physical Administrator or a Physical User with at least View permissions on the asset. Once you take custody it will be up to you to return the asset.

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

4. 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.



Name	Title	Owner	Availability Status
Container 1 - Asset 1	Container 1 - Asset 1	Administrator	Out

Name	Title	Owner	Availability Status
As	Asset 1 - Child 1	Administrator	Out

1 - 1 of 1 items

Name	Title	Owner	Availability Status
Con	Container 1 - Asset 10	Administrator	In
Con	Container 1 - Asset 11	Administrator	In
Cont	Container 1 - Asset 2	Administrator	In
Con	Container 1 - Asset 3	Administrator	In
Con	Container 1 - Asset 4	Administrator	In
Container 1 - Asset 5	Container 1 - Asset 5	Administrator	In

5 Record Manager Guide

Gimmal 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.

5.1 Building Your File Plan

5.2 Manage

5.3 Disposition

5.4 Monitor

5.5 Rule Builder

5.6 Physical Records

5.7 Creating and Managing Legal Cases and Legal Holds

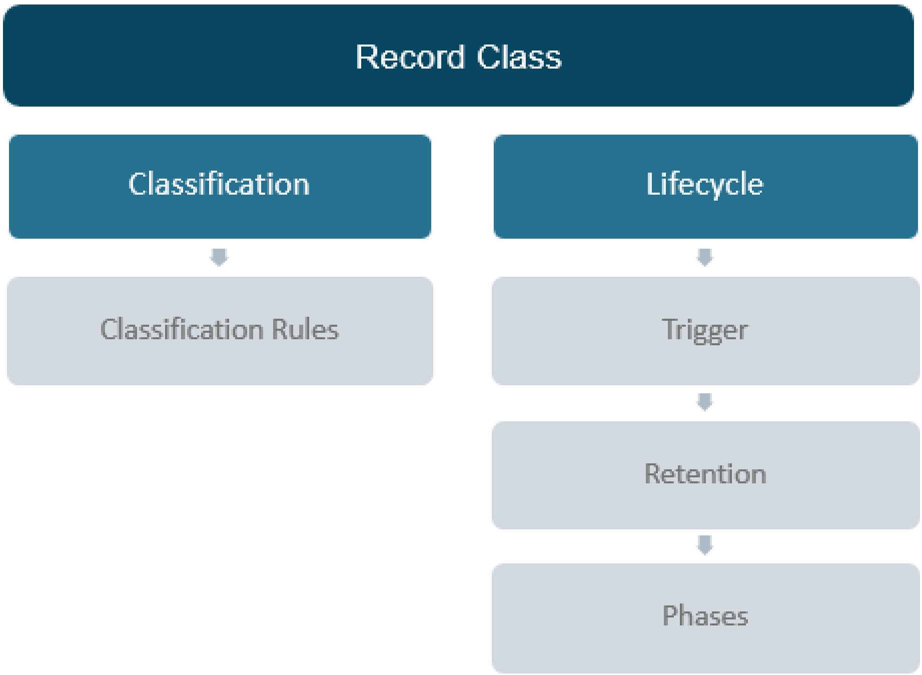
5.8 Building Your File Plan

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.



5.8.1 Triggers

5.8.2 Retentions

5.8.3 Lifecycles

5.8.4 Rule Sets

5.8.5 Editing the File Plan

5.8.6 Record Classes

5.8.7 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: • Recurring - These are typically for Case Records and are created by a recurring date. For example: ◦ 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 ◦ Employee Termination &amp; Contract Expiration
Date Property	Starts retention when a date property is met. For example: • 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: • 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.

5.8.7.1 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.

5.8.7.2 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
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**.

5.8.7.3 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).
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: • Manual • Once • Daily • Monthly • Yearly

Property	Description
Assignment Position	Defines how (Link) event occurrences are selected for a Record. This is a drop-down, and the available options are: • 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.

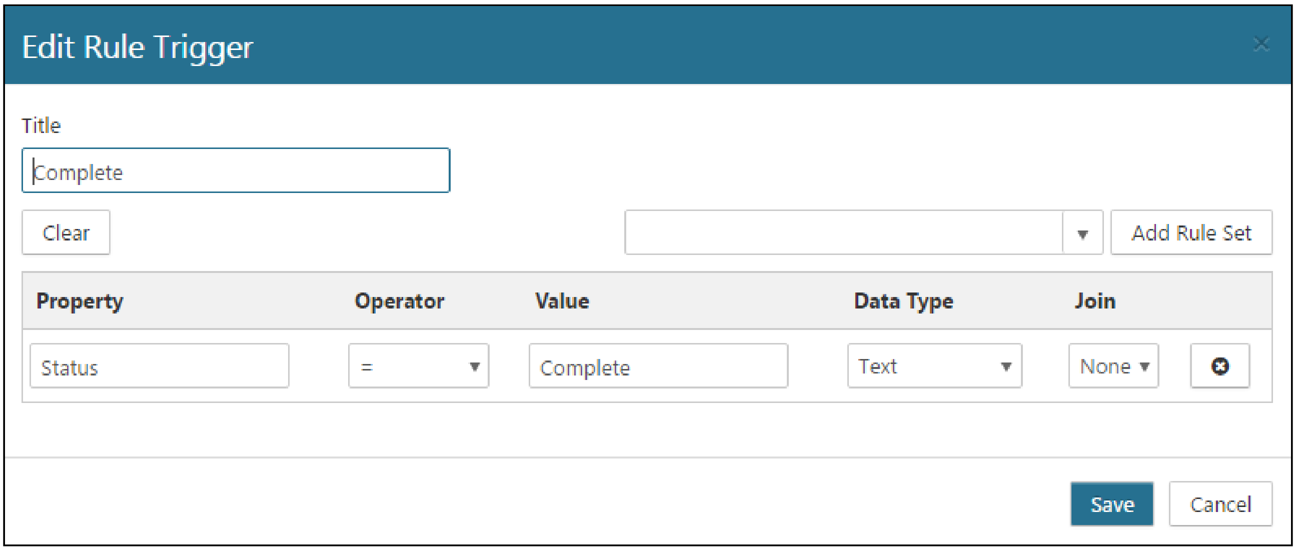
Creating an Event Trigger

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.**

5.8.7.4 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.


Edit Rule Trigger

Title: Complete

Property	Operator	Value	Data Type	Join
Status	=	Complete	Text	None

Rule Trigger Properties

The only property for a rule trigger is the Title, which must 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).
Operator	Represents the operator to use when comparing against the item. Possible values are: 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: 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 &amp; 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**

5.8.7.5 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.

5.8.8 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.

5.8.8.1 Retention Properties

Property	Description
Title	Defines the unique name of the Retention
Description	Defines the description of the Retention for informational purposes

Proper ty	Description
Author ity	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
Interva l	Defines the numeric value, which represents how long the Time Period of the Retention lasts
Time Period	Defines how the Interval is to be interpreted Supported values are: • Day(s) • Month(s) • Year(s)

5.8.8.2 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**.

5.8.9 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
Descriptio n	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.
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	Defines whether the Action is conducted automatically by the system or performed manually by the user. 1. **Automatic** – Action will be performed automatically if supported by the Connector; otherwise it will revert to Manual. 2. **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	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. This property is not required, and if it is left blank, the item will appear back in the Inbox immediately after paused. There is no limit to the number of times a record can be paused.

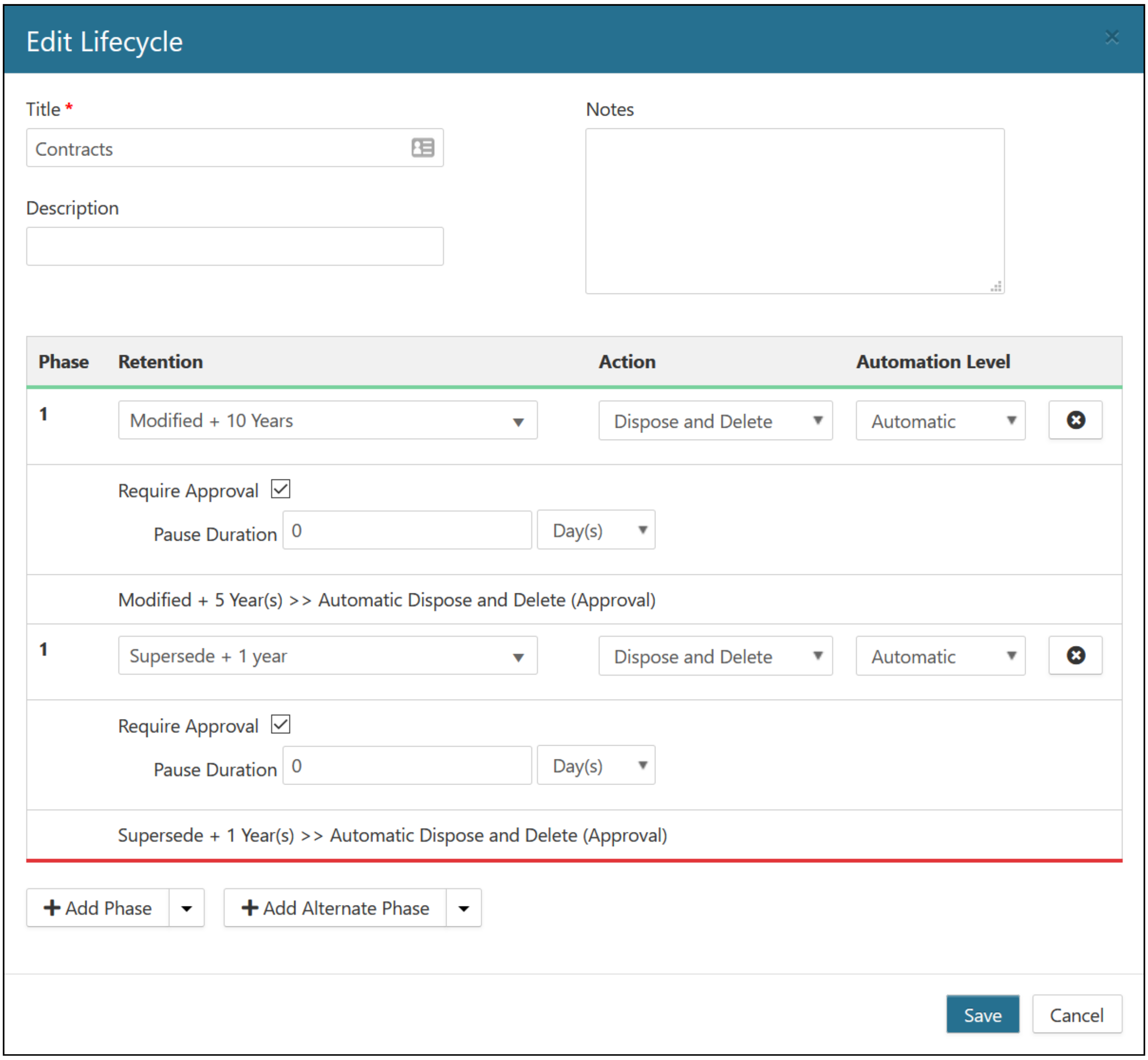
Supported Phase Actions

Action	Description
Declare Record	Flags the item as a Declared Record and locks the item in the Repository from modification and deletion. Cannot be assigned to the final phase in a lifecycle.
Dispose and Delete	Deletes the item from the Repository and removes any information about the item. Can only be assigned to the final phase in a lifecycle.

Action	Description
Dispose and Recycle	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.
Dispose and Transfer	Moves the item to a specified location within the Repository and removes any information about the item. Can only be assigned to the final phase in a lifecycle.
None	No action is performed.*Cannot be assigned to the final phase in a lifecycle
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 *: Contracts

Description:

Notes:

Phase	Retention	Action	Automation Level
1	Modified + 10 Years	Dispose and Delete	Automatic
	Require Approval ☑ Pause Duration 0 Day(s)		
	Modified + 5 Year(s) >> Automatic Dispose and Delete (Approval)		
1	Supersede + 1 year	Dispose and Delete	Automatic
	Require Approval ☑ Pause Duration 0 Day(s)		
	Supersede + 1 Year(s) >> Automatic Dispose and Delete (Approval)		

5.8.10 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.

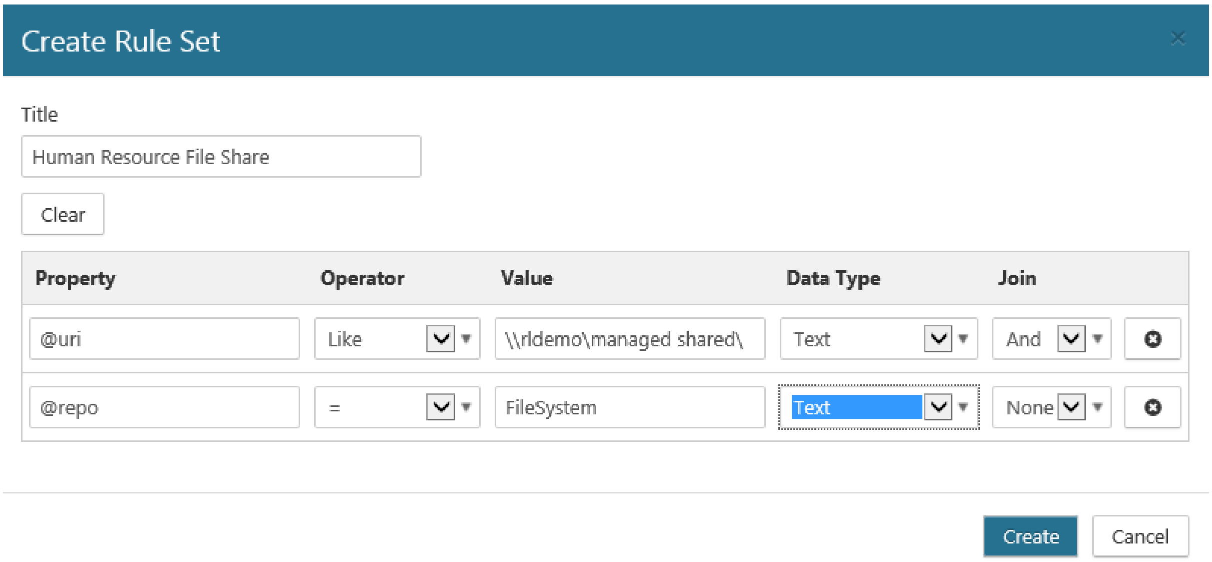
5.8.10.1 Building Rules

Building rules are similar across the software. Refer to the Rule Builder(see page 148) for more information.

5.8.10.2 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.



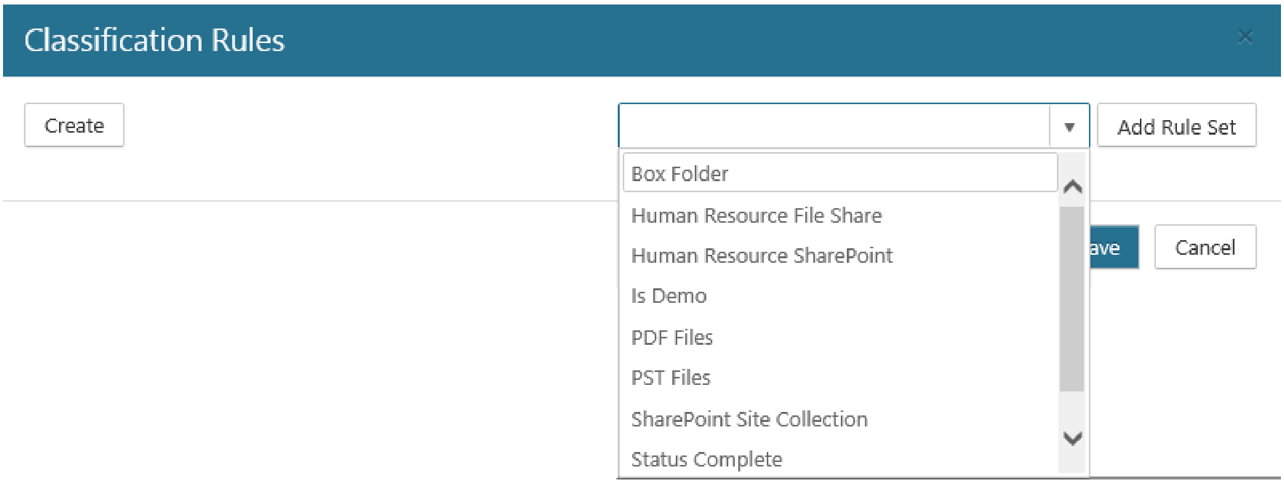
Create Rule Set

Title: Human Resource File Share

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

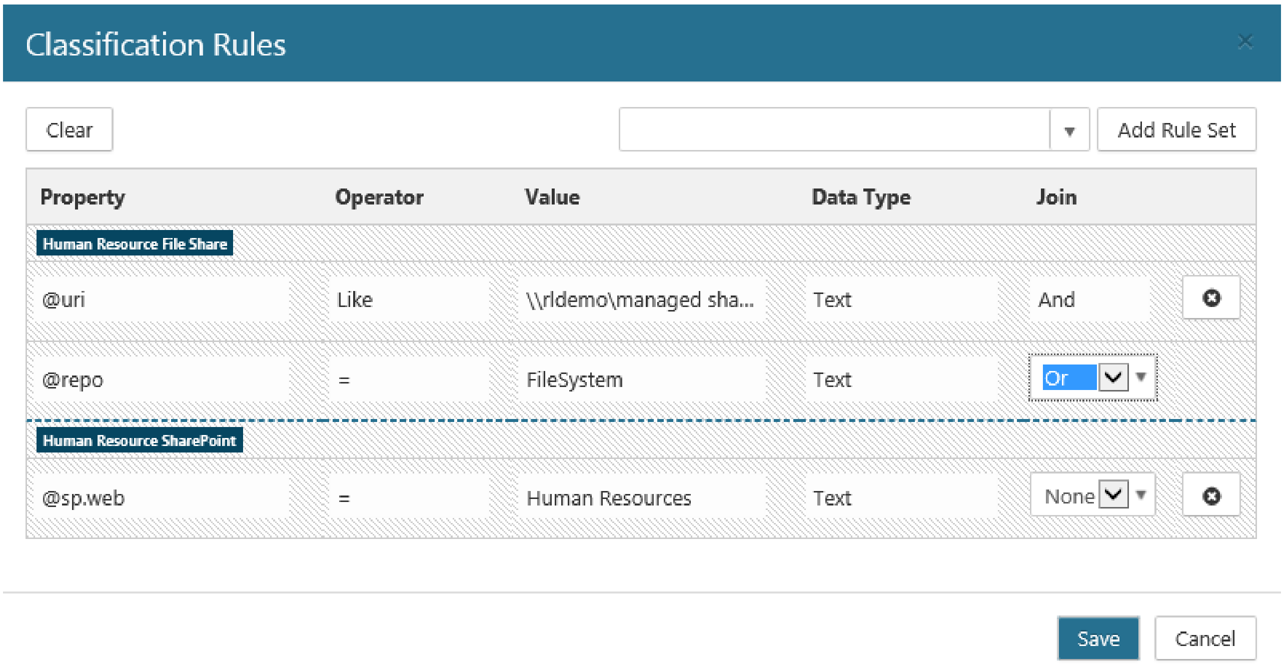
5.8.10.3 Adding Rule Sets

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

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



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

5.8.11 Editing the File Plan

Gimmal 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.

5.8.11.1 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.

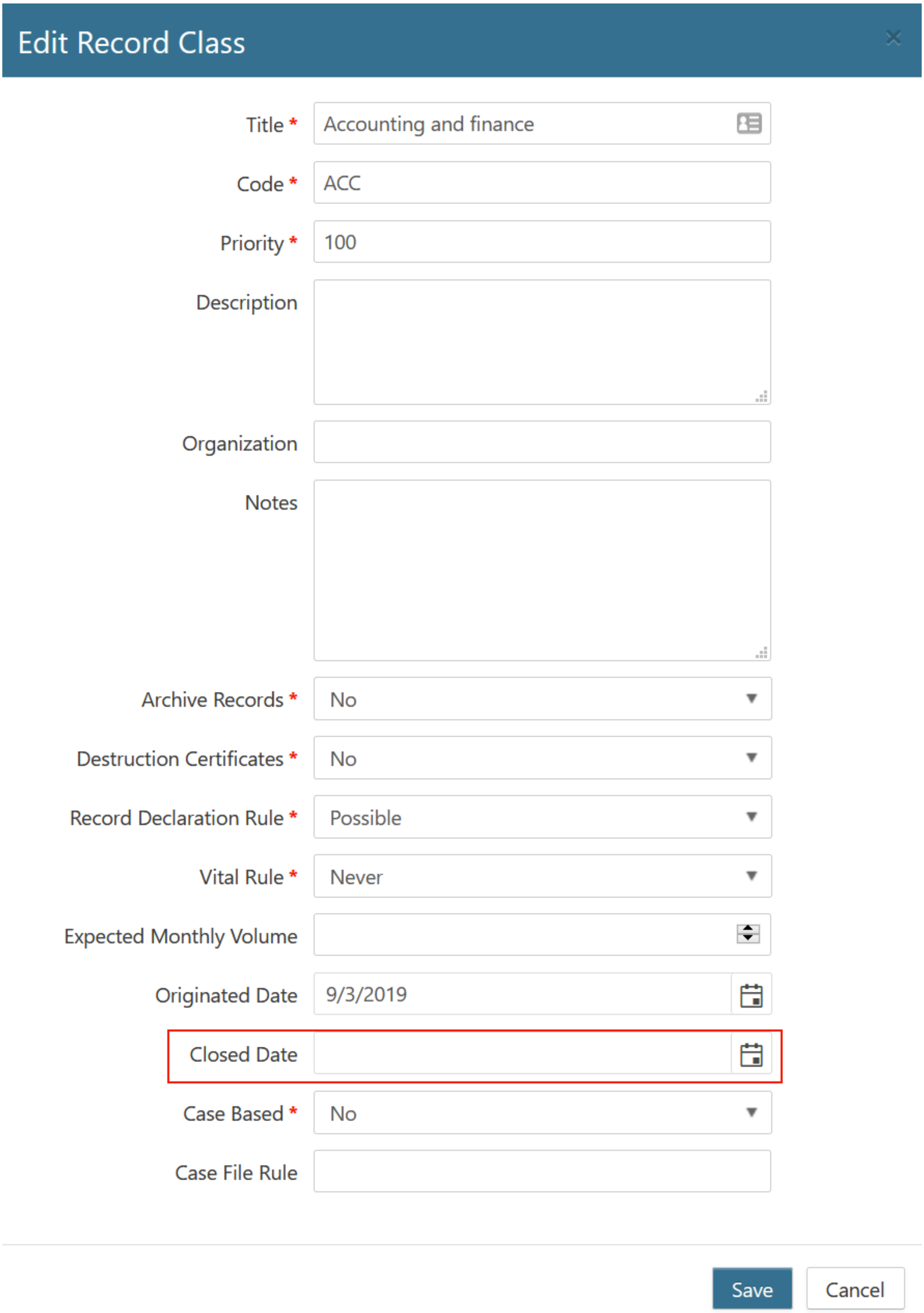
Upon saving the Lifecycle, the following behavior occurs:

- 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.

5.8.11.2 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 *	Accounting and finance
Code *	ACC
Priority *	100
Description	
Organization	
Notes	
Archive Records *	No
Destruction Certificates *	No
Record Declaration Rule *	Possible
Vital Rule *	Never
Expected Monthly Volume	
Originated Date	9/3/2019
Closed Date	
Case Based *	No
Case File Rule	

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.

5.8.12 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.)

5.8.12.1 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	Defines how Preservation Copies will be created. Possible values are: 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. **NOTE** – Enabling Preserve only works for items managed by the Microsoft 365 SharePoint Connector.
Archive Records	Defines whether the primary record data will be archived during disposition *Note: Version 4.0 and above*
Archive Record Properties	Defines whether the record properties will be archived. This is only available if Archive Records property is set to "Yes". *Note: Version 4.0 and above*
Archive Record Audits	Defines whether the audit trail will be archived. This is only available if the Archive Records property is set to "Yes". *Note: Version 4.0 and above*
Destruction Certificates	Defines whether a Destruction Certificate will be generated during disposition *Note: Version 4.0 and above*
Record Declaration Rule	Defines how items become Declared Records in the system. Possible values are: 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. It is important to understand the difference between a Record and Declared Record to understand how this property works.

Property	Description
Vital Rule	Defines how items become Vital Records in the system. Possible values are: 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[20])
Case File Rule	Specifies how Case File titles should be automatically generated (see Case-Based Record Classes[21])

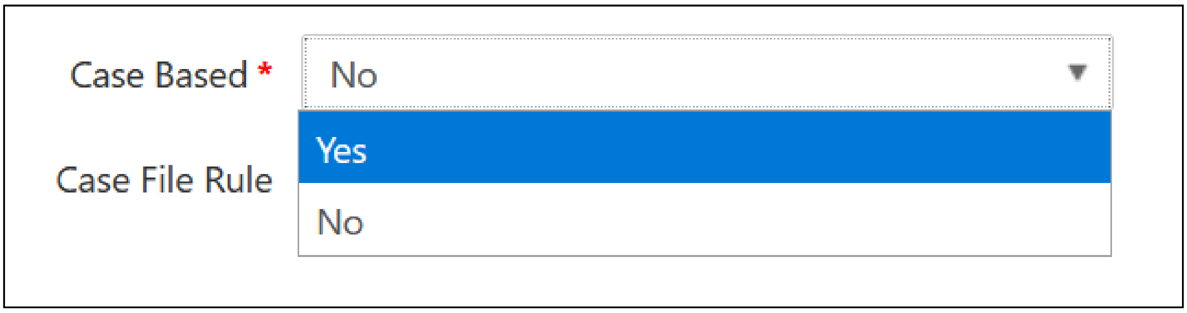
5. Click the **Create** button at the bottom of the window. The new Record Class displays on the page.

5.8.12.2 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.

[20] http://docs.gimmal.com/en/2948-case-based-record-classes.html
[21] http://docs.gimmal.com/en/2948-case-based-record-classes.html



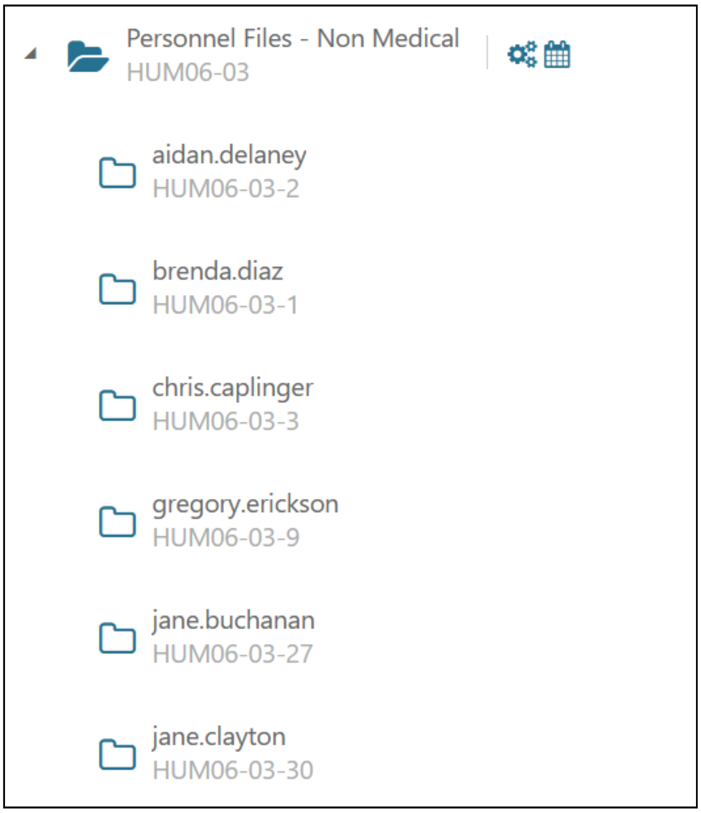
Case Based * No

Case File Rule

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.



Personnel Files - Non Medical
HUM06-03

aidan.delaney
HUM06-03-2

brenda.diaz
HUM06-03-1

chris.caplinger
HUM06-03-3

gregory.erickson
HUM06-03-9

jane.buchanan
HUM06-03-27

jane.clayton
HUM06-03-30

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".

5.8.12.3 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.

> ⓘ A higher priority is indicated by a lower numeric value (ex. 1 &gt; 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 148) describes the process of creating rules.
6. Click **Save**.

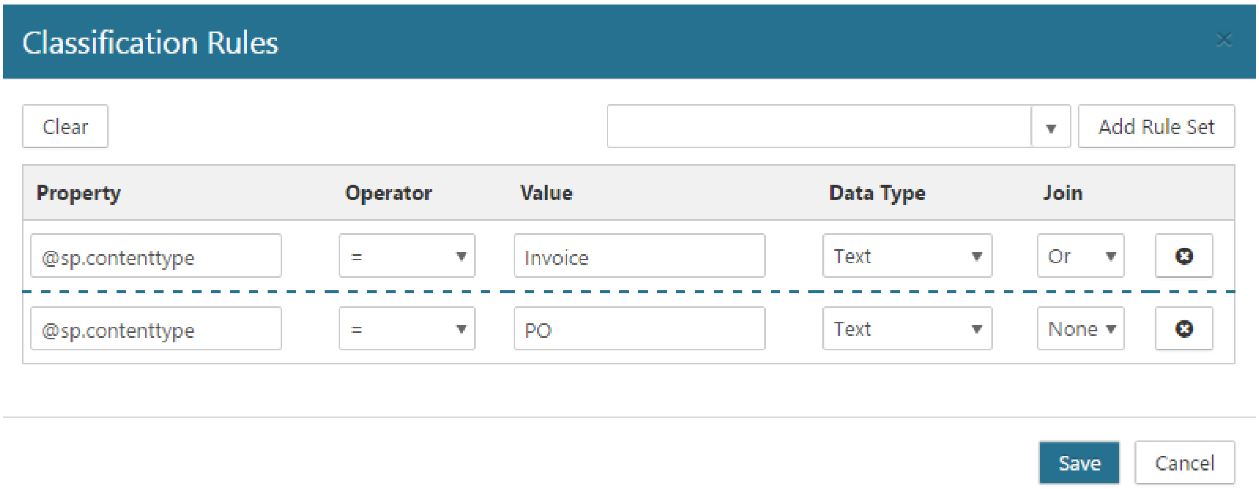
Unclassified Items and the Undefined Record Class

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.



Property	Operator	Value	Data Type	Join
@sp.contenttype	=	Invoice	Text	Or
@sp.contenttype	=	PO	Text	None

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.:

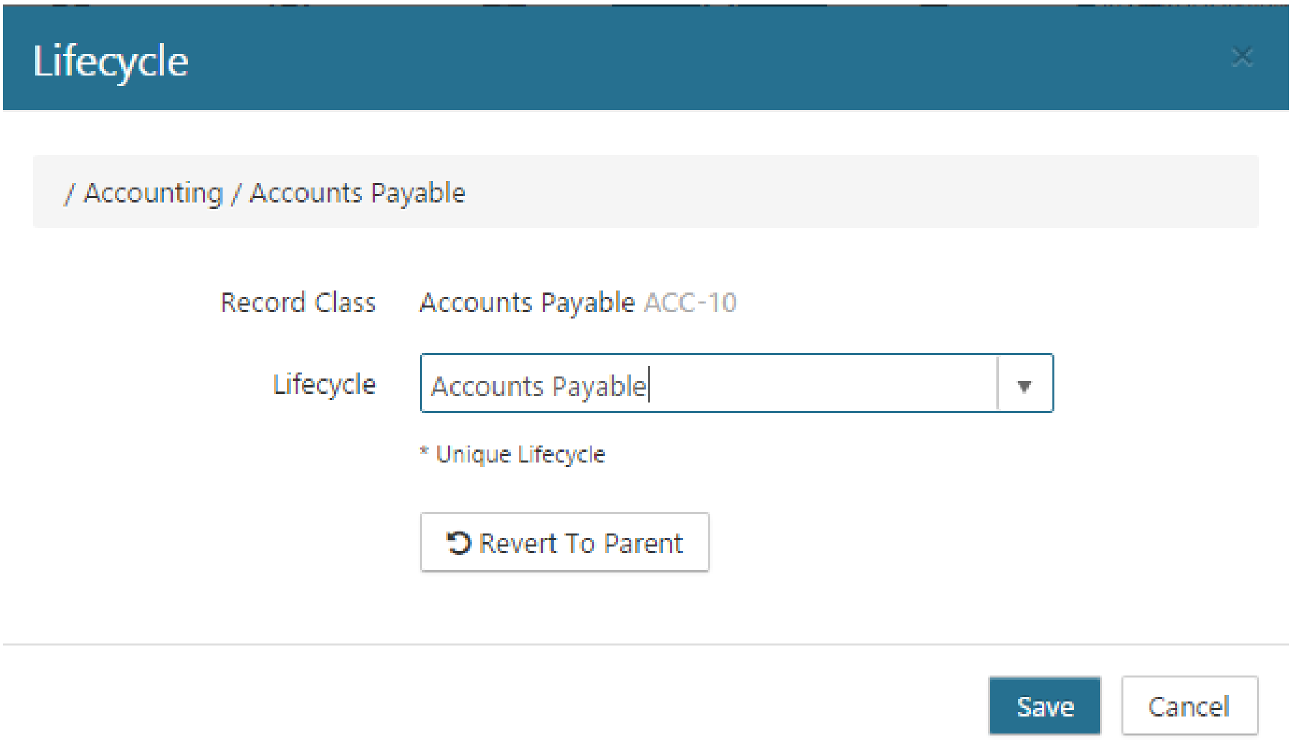
- “Content Type = Invoice” = FALSE Or “Content Type = PO” = TRUE

5.8.12.4 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**.



Lifecycle

/ Accounting / Accounts Payable

Record Class: Accounts Payable ACC-10

Lifecycle: Accounts Payable

* Unique Lifecycle

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.

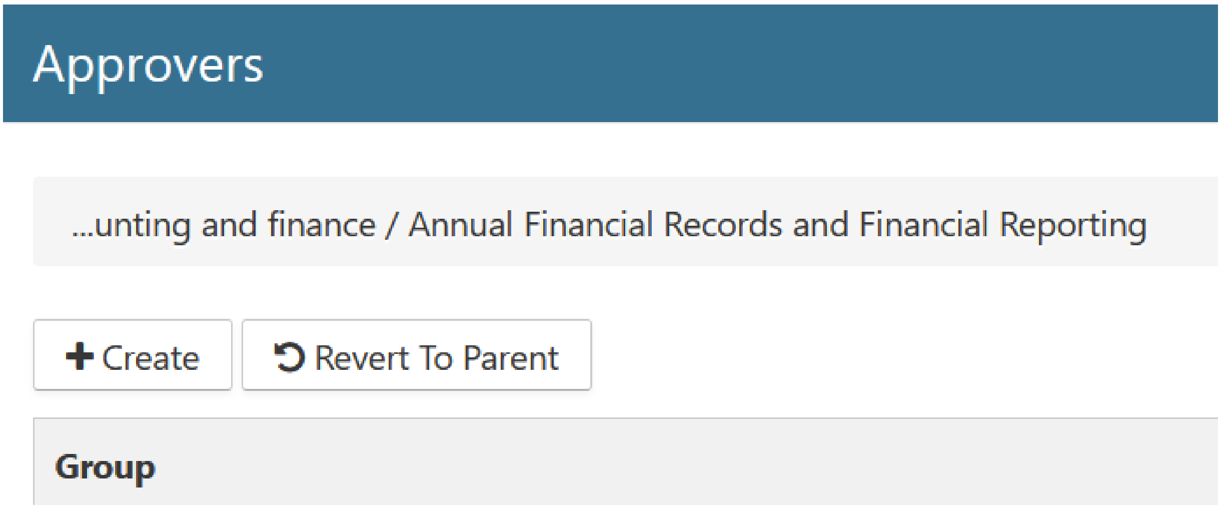
5.8.12.5 Approvers

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.

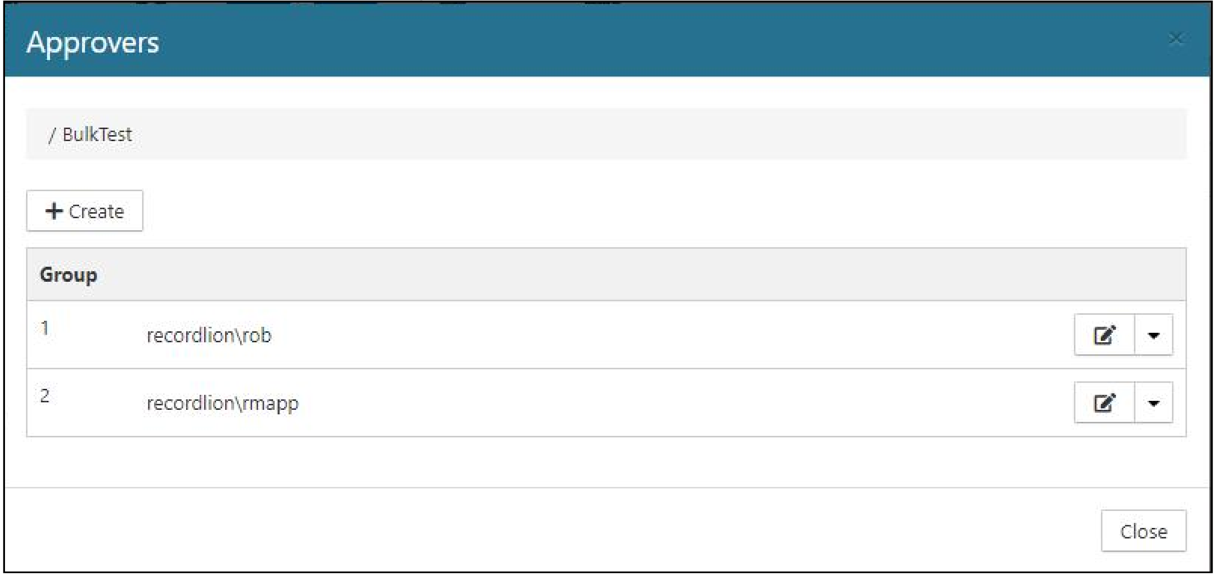

Approvers
...unting and finance / Annual Financial Records and Financial Reporting
Create
Revert To Parent
Group

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.



Approvers

/ BulkTest

+ Create

Group	
1	recordlion\rob
2	recordlion\rmapp

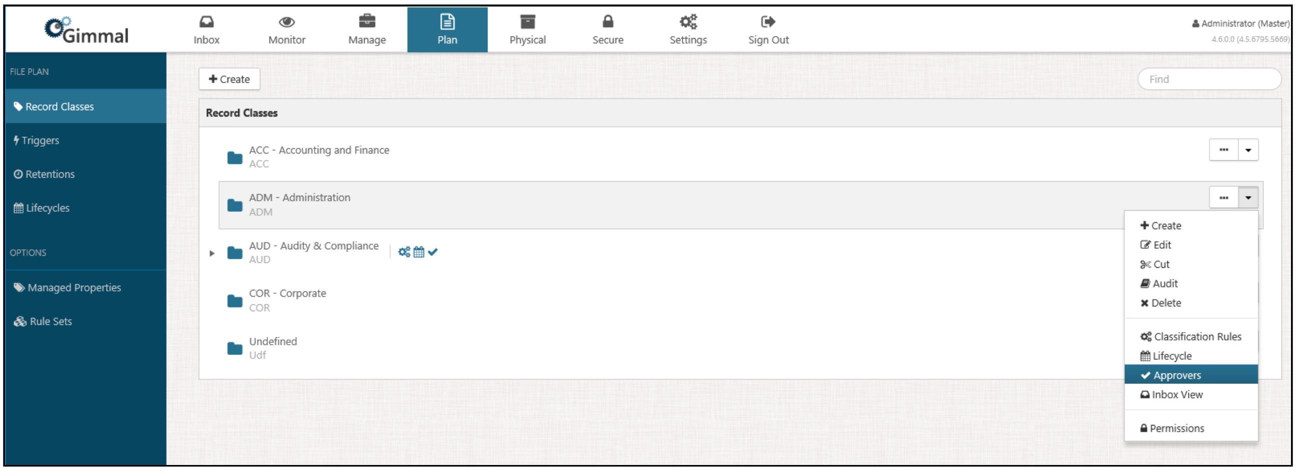
Close

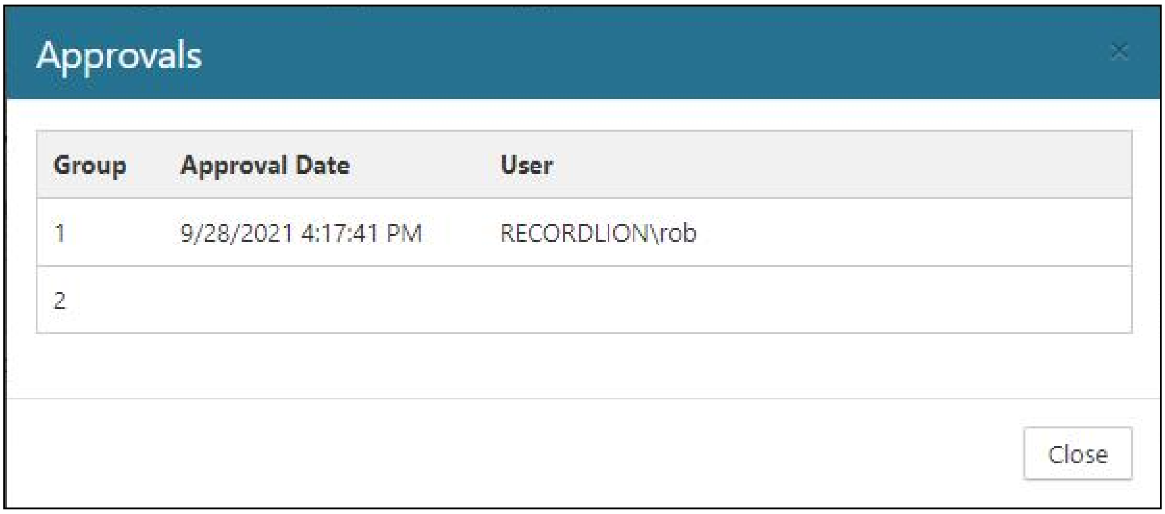
5. Click **Create**.
6. Select a User or Group, and then click **Add** (Repeat for each user in the group).
7. Click **Close**.
8. Repeat Steps 6 and 7 to define more groups.

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		

5.8.12.6 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:

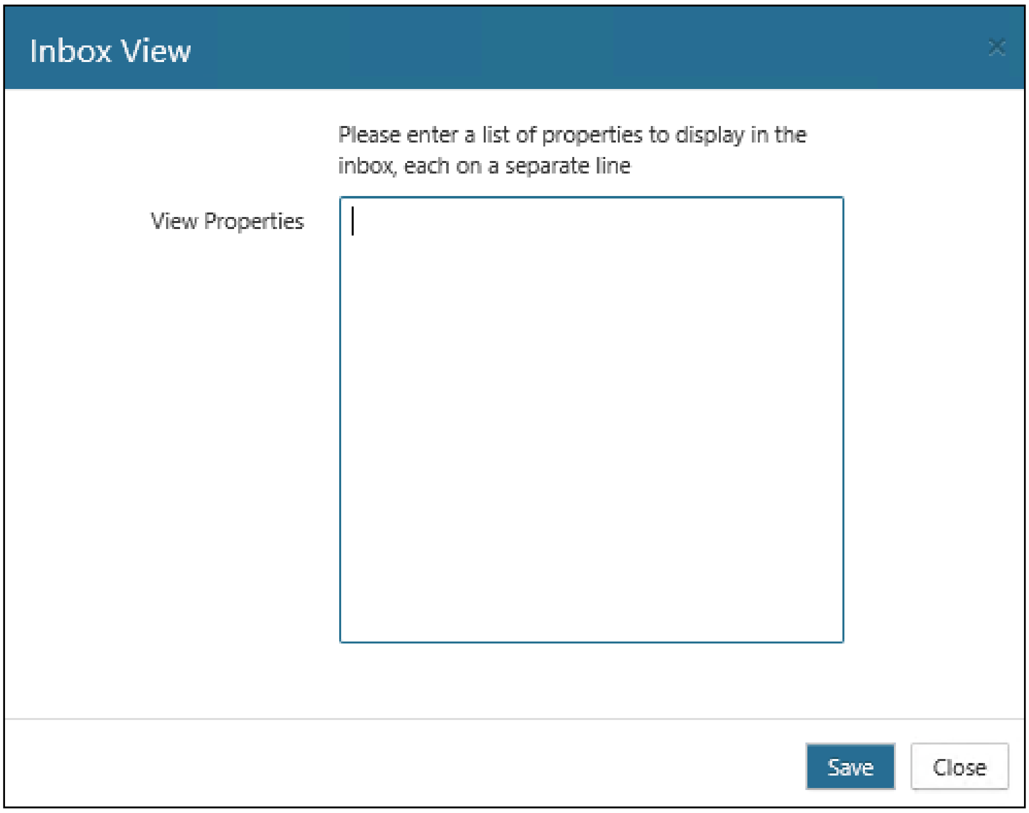
- User Preferences(see page 36)
- Global Preferences(see page 30)
- Inbox(see page 39)

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.

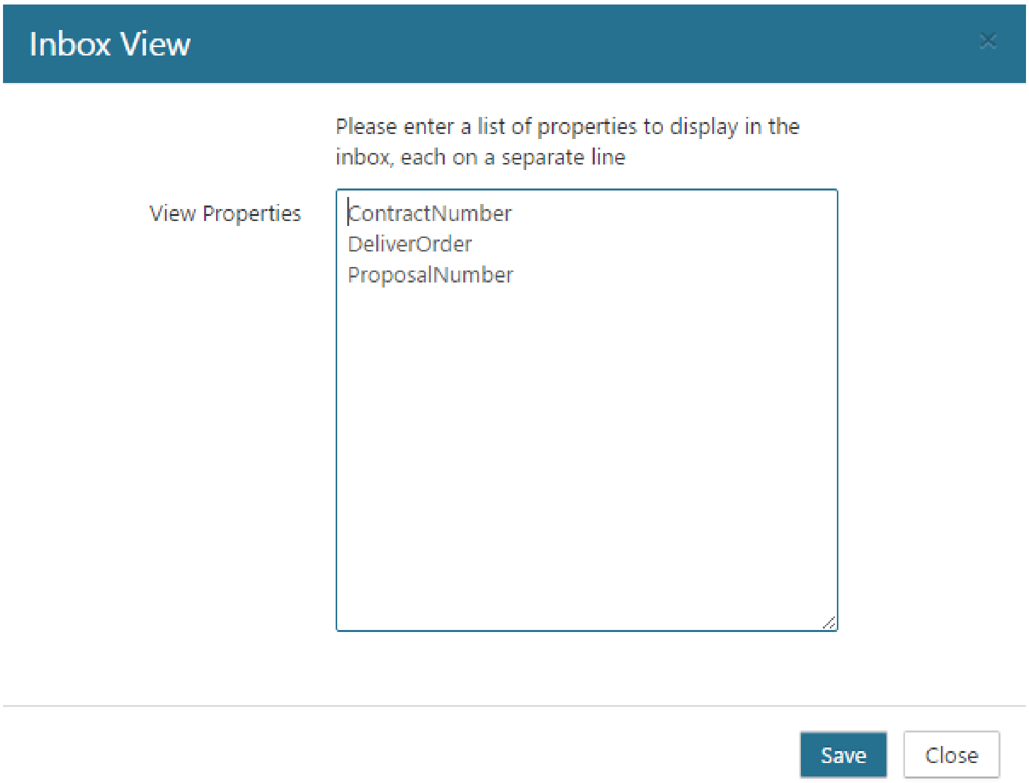


Inbox View

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

View Properties

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**



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

View Properties

```
ContractNumber
DeliverOrder
ProposalNumber
```

5.9 Manage

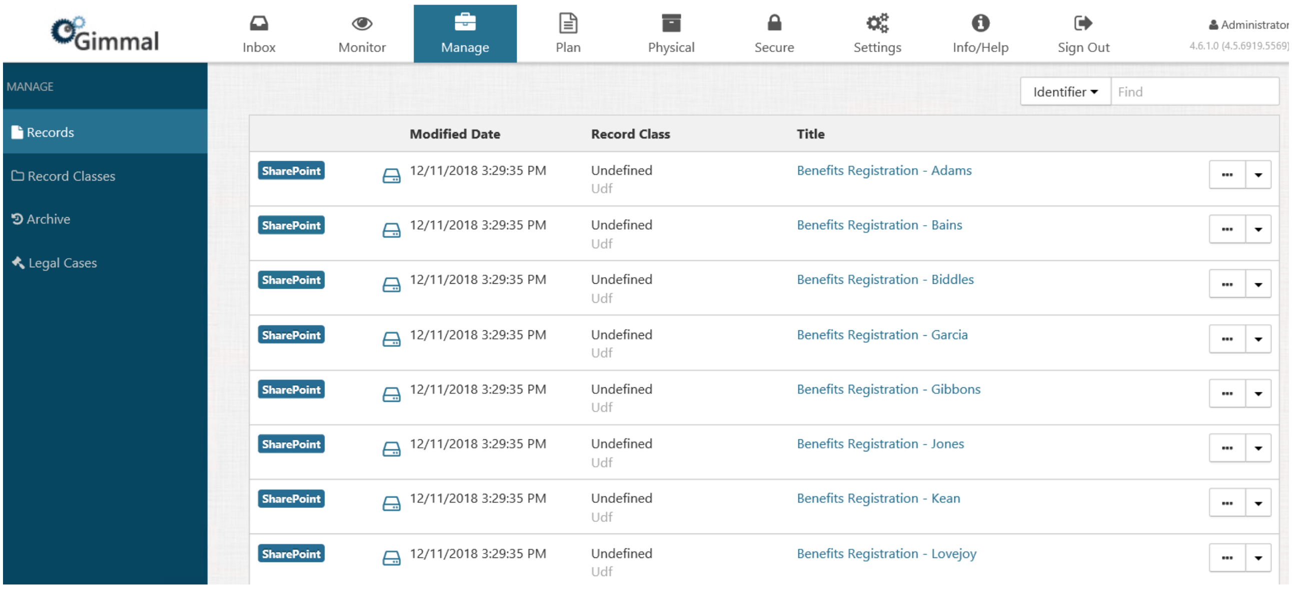
5.9.1 Manage Records 1

5.9.2 Manage Record Classes

5.9.3 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.



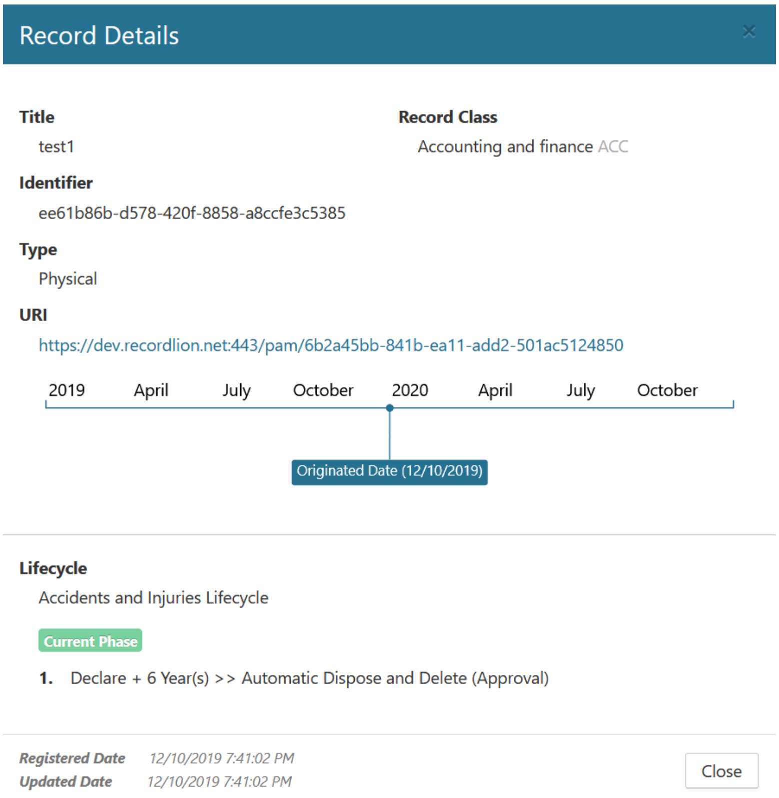
		Modified Date	Record Class	Title
SharePoint		12/11/2018 3:29:35 PM	Undefined Udf	Benefits Registration - Adams
SharePoint		12/11/2018 3:29:35 PM	Undefined Udf	Benefits Registration - Bains
SharePoint		12/11/2018 3:29:35 PM	Undefined Udf	Benefits Registration - Biddles
SharePoint		12/11/2018 3:29:35 PM	Undefined Udf	Benefits Registration - Garcia
SharePoint		12/11/2018 3:29:35 PM	Undefined Udf	Benefits Registration - Gibbons
SharePoint		12/11/2018 3:29:35 PM	Undefined Udf	Benefits Registration - Jones
SharePoint		12/11/2018 3:29:35 PM	Undefined Udf	Benefits Registration - Kean
SharePoint		12/11/2018 3:29:35 PM	Undefined Udf	Benefits Registration - Lovejoy

5.9.3.1 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
test1

Record Class
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*

5.9.3.2 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**.

5.9.3.3 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**.

5.9.3.4 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.

5.9.3.5 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.

5.9.3.6 Viewing the Record Properties

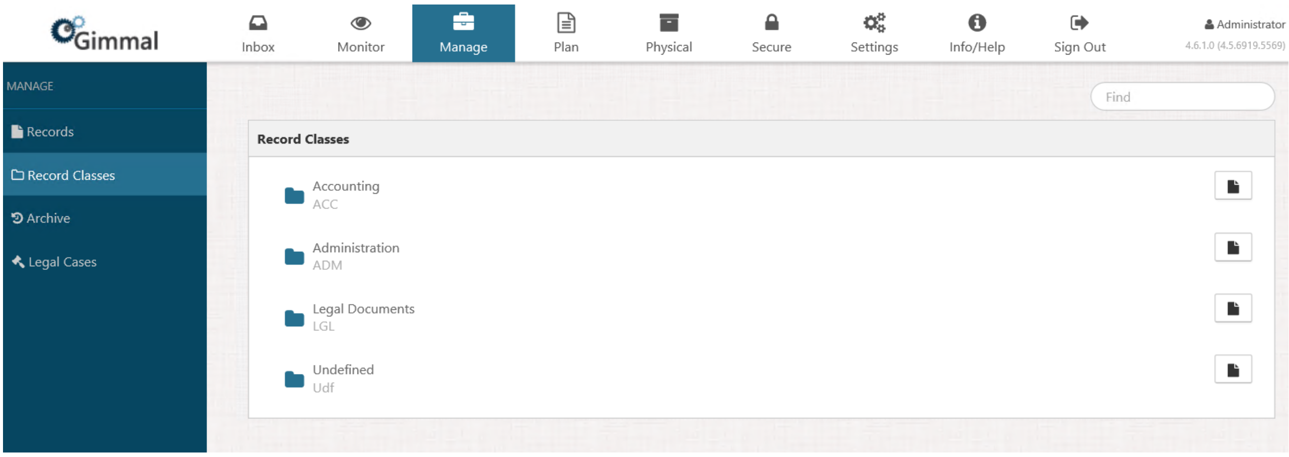
To view the Properties for an individual item, perform the following steps:

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.

5.9.4 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.



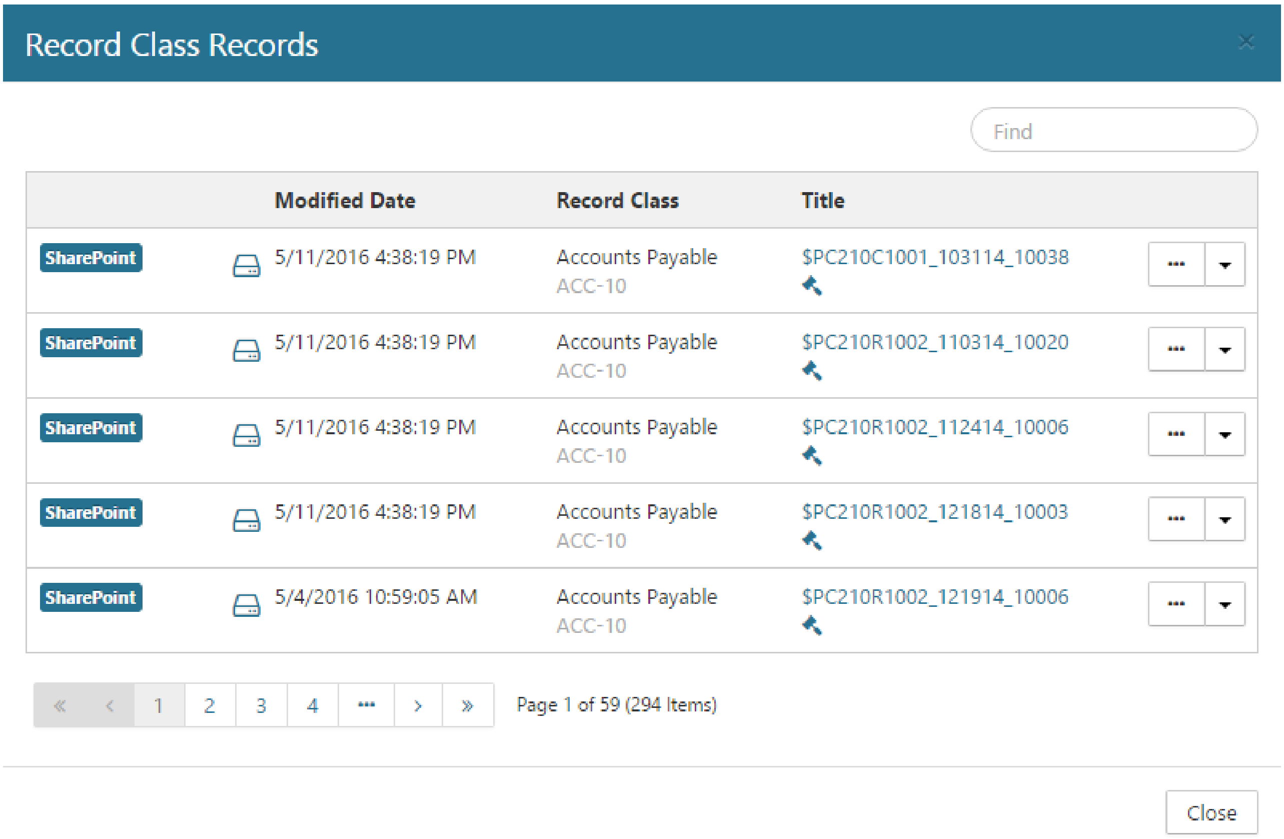
Record Classes

Accounting
ACC

Administration
ADM

Legal Documents
LGL

Undefined
Udf



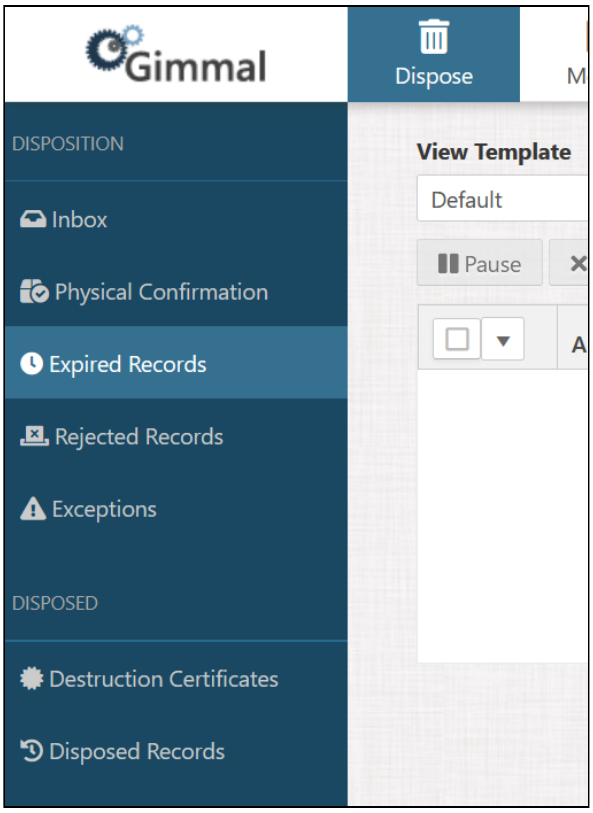
Record Class Records

		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)

5.10 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.

- Inbox 1(see page 124)
- Disposing Physical Assets(see page 130)
- Expired Records(see page 132)
- Rejected Records(see page 133)
- Legal Holds and Reclassification During Disposition(see page 135)
- Exceptions(see page 137)
- Disposed Records(see page 138)

5.10.1 Inbox 1

5.10.1.1 Overview

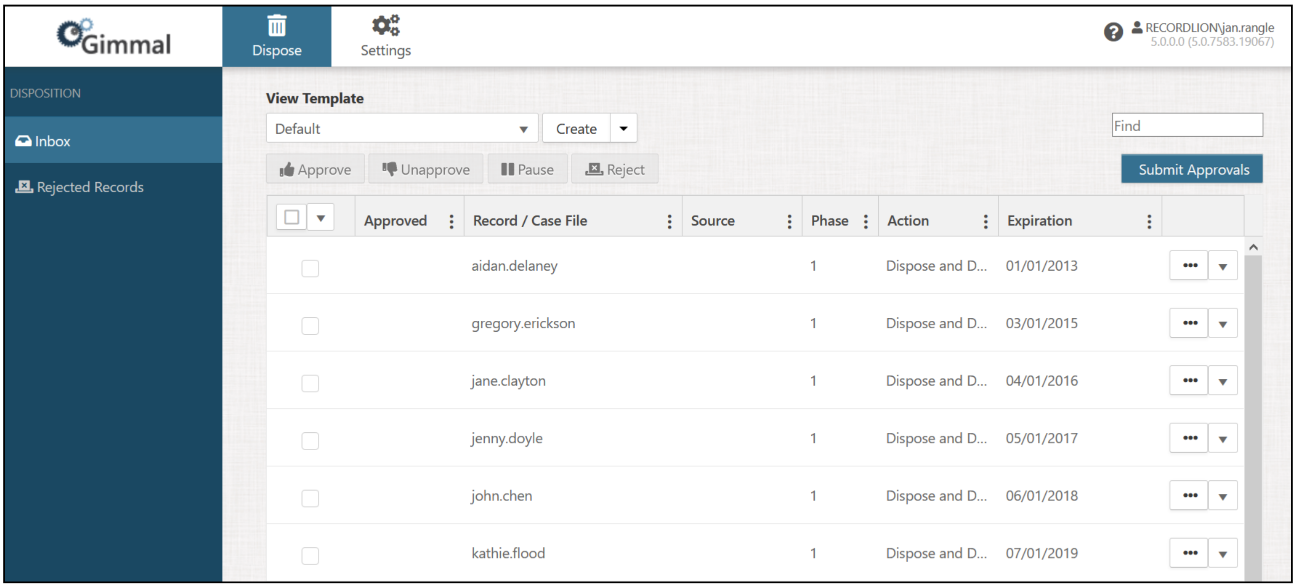
You have created Lifecycles, associated them with Record Classes, and created Event Occurrences. Now, you are ready to approve items that are waiting at the end of the retention period of a specific Lifecycle Phase, typically known as disposition. The Inbox is where you approve and submit items to either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

5.10.1.2 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 115) 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**.

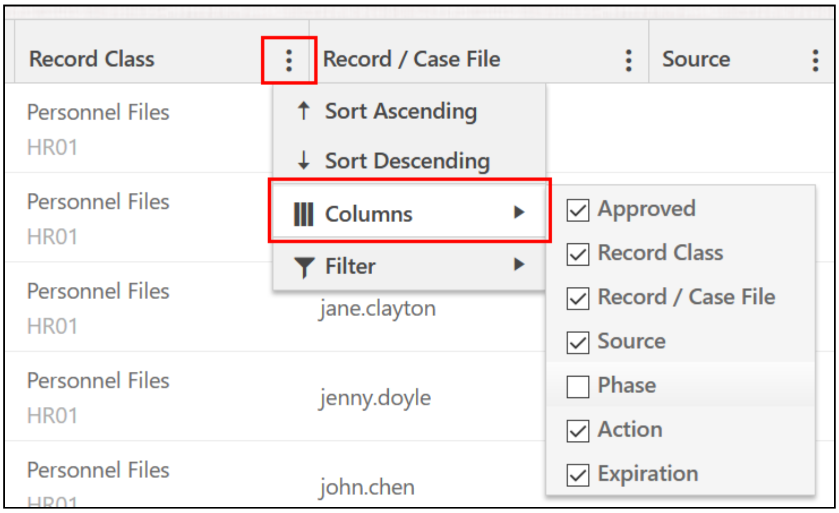


□	Approved	Record / Case File	Source	Phase	Action	Expiration
□		aidan.delaney		1	Dispose and D...	01/01/2013
□		gregory.erickson		1	Dispose and D...	03/01/2015
□		jane.clayton		1	Dispose and D...	04/01/2016
□		jenny.doyle		1	Dispose and D...	05/01/2017
□		john.chen		1	Dispose and D...	06/01/2018
□		kathie.flood		1	Dispose and D...	07/01/2019

5.10.1.3 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.



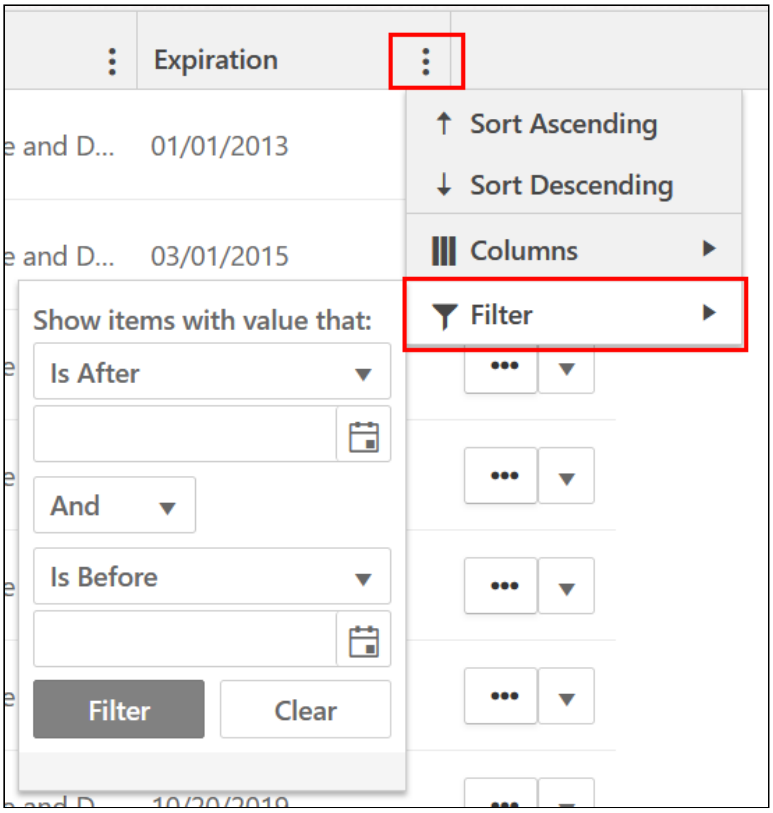
Record Class	Record / Case File	Source
Personnel Files HR01		
Personnel Files HR01		
Personnel Files HR01	jane.clayton	
Personnel Files HR01	jenny.doyle	
Personnel Files HR01	john.chen	

☑ Approved
☑ Record Class
☑ Record / Case File
☑ Source
□ Phase
☑ Action
☑ Expiration

For information on how to make a new column available, view the Adding Columns to Your Inbox Views(see page 53) topic.

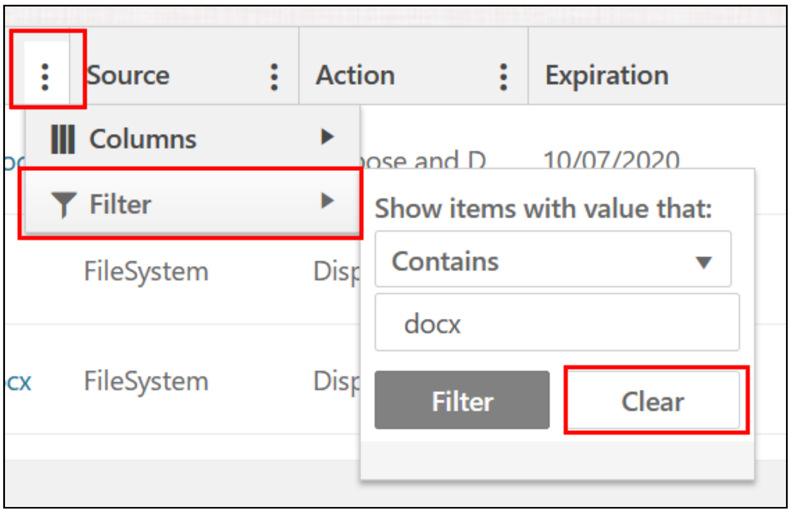
5.10.1.4 Filtering the Inbox

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.



Show items with value that:
Is After
And
Is Before

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.



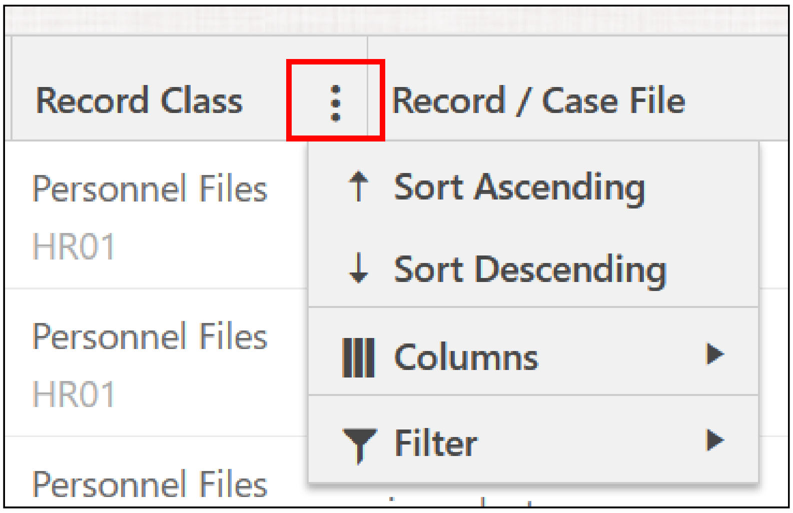
Show items with value that:
Contains
docx

5.10.1.5 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:

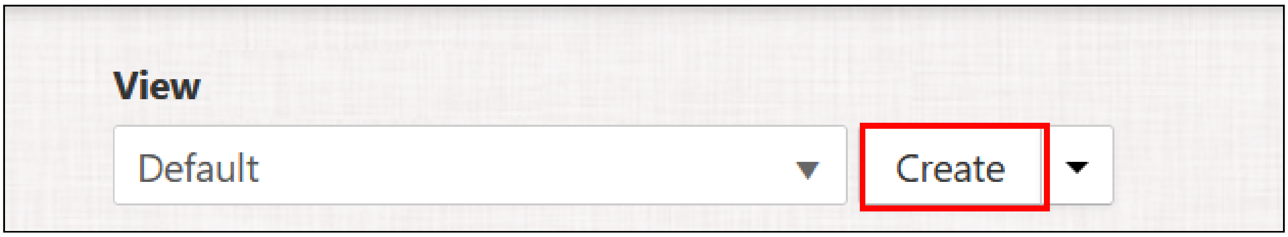
- Record Class
- Expiration Date

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



5.10.1.6 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 Inbox View(see page 117) topic. Personal views are created by clicking the Create button next to the Inbox views list.



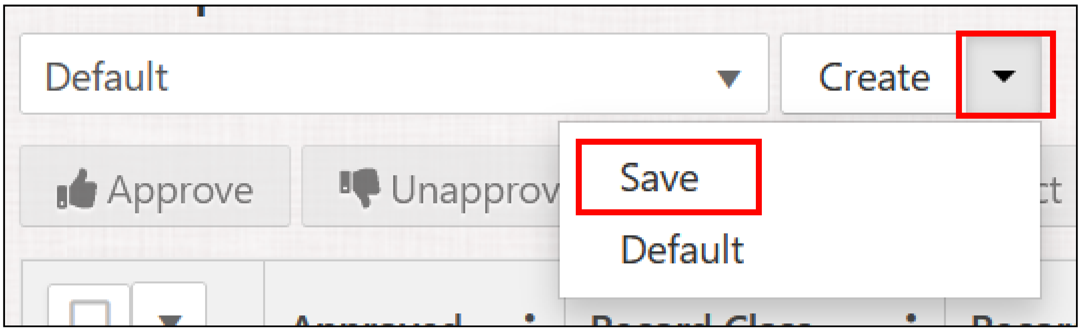
All your settings related to the current layout of the Inbox are saved including visible columns, column order, column width, filters, and any sorting.

Using a View

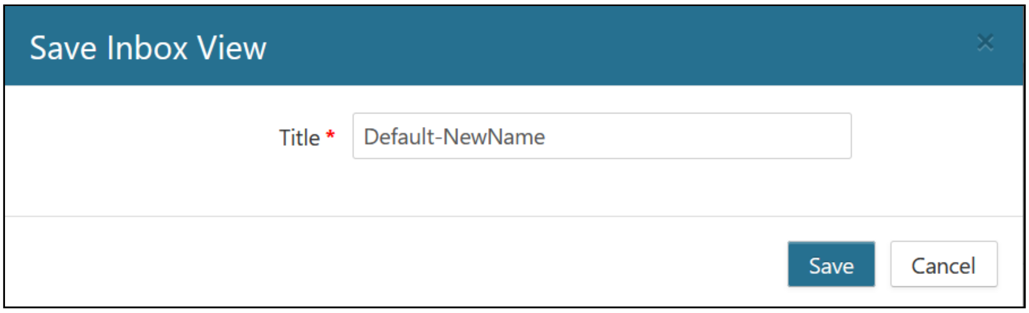
To use a saved view, simply select it from the list of views.

Saving existing View

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



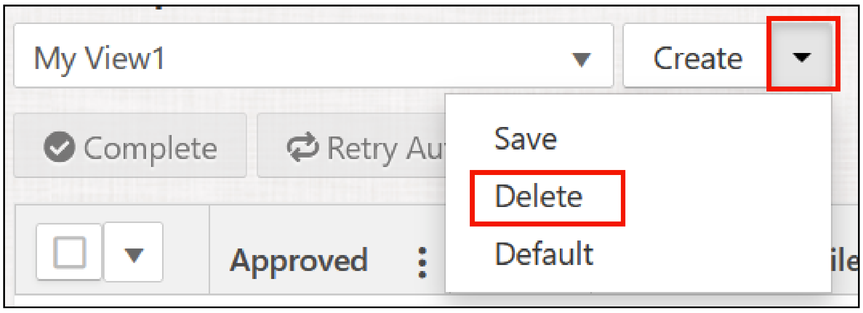
After selecting Save a window will be displayed allowing you to change the name of the view before saving it.


Save Inbox View

Title * Default-NewName

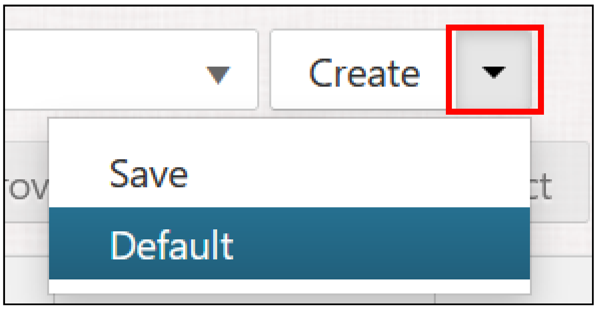
Deleting a View

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.

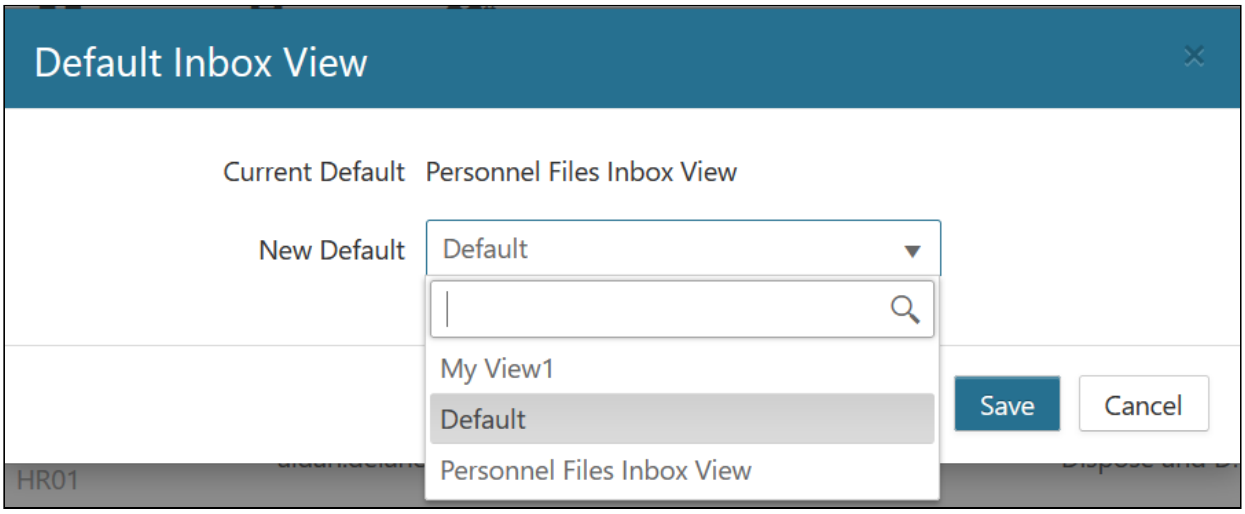


Changing the Default View

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.


Default Inbox View
Current Default Personnel Files Inbox View
New Default Default
My View1
Default
Personnel Files Inbox View
Save
Cancel

5.10.1.7 Disposition Actions

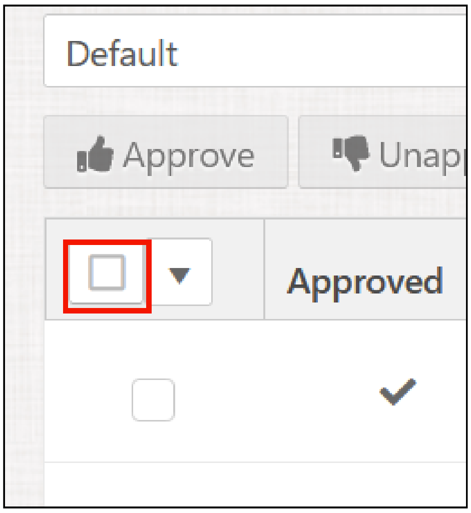
There are several actions that can be taken on records in the Inbox. These actions can be executed on one record at a time, or on any number of selected records. Each action is detailed in the following topics:

- Approving Records(see page 45)
- Unapprove(see page 47)
- Pause(see page 48)
- Reject(see page 50)
- Submitting Approvals(see page 51)
- Adding Columns to Your Inbox Views(see page 53)

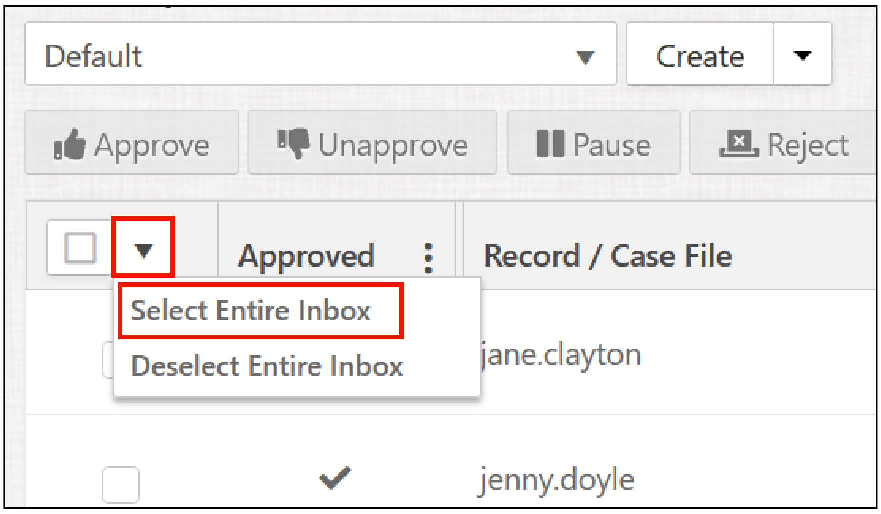
Selecting Records

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.



5.10.2 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.

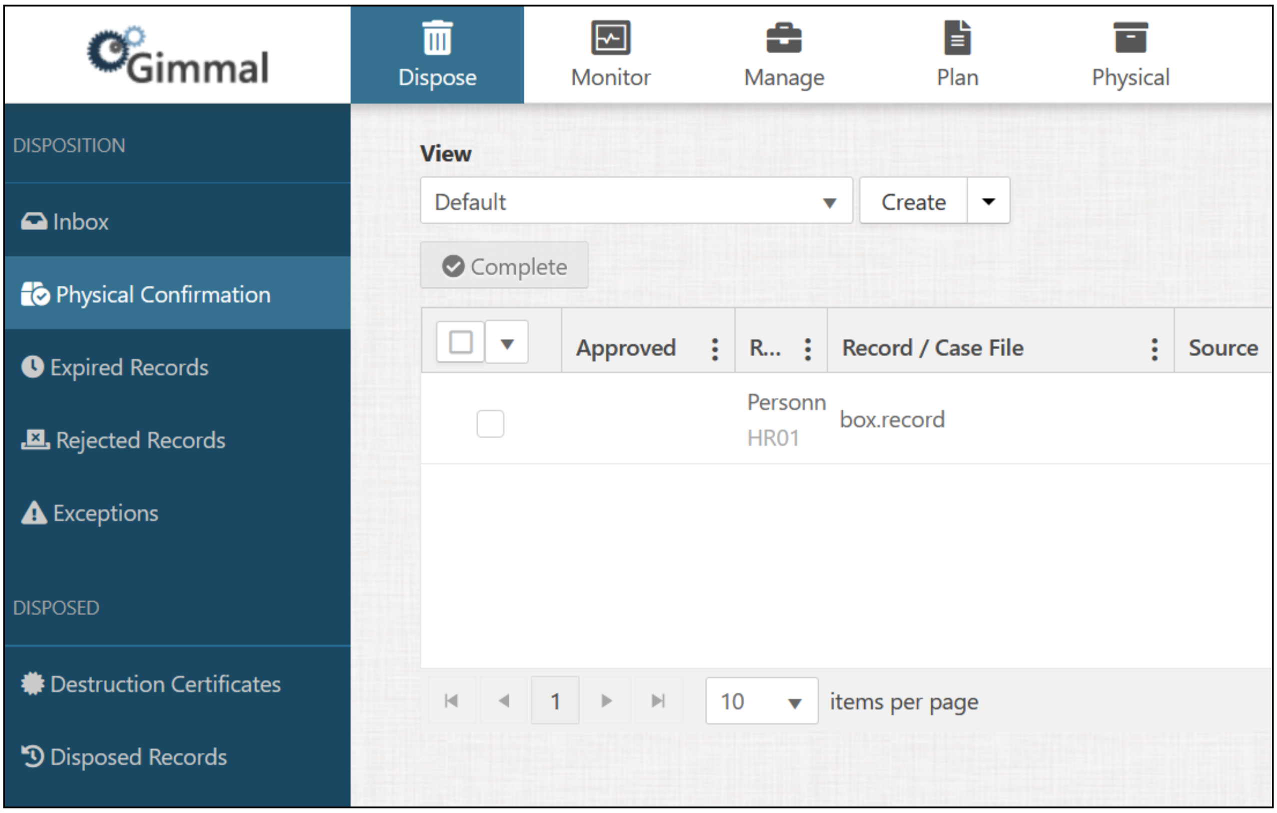
5.10.2.1 Approving Physical Records

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.

5.10.2.2 Confirming Physical Disposition

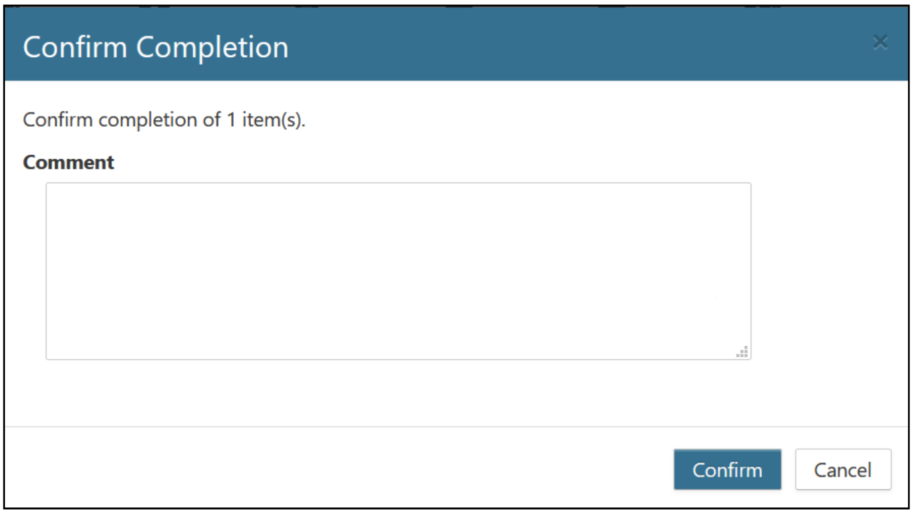
Once the asset has been submitted for disposition, it will create a task in the Physical Confirmation area to be manually completed by a records manager. Goto **Dispose → Physical Confirmation** to see the Physical Confirmation area.

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



□	Approved	R...	Record / Case File	Source
□		Personn HR01	box.record	

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.



Confirm Completion

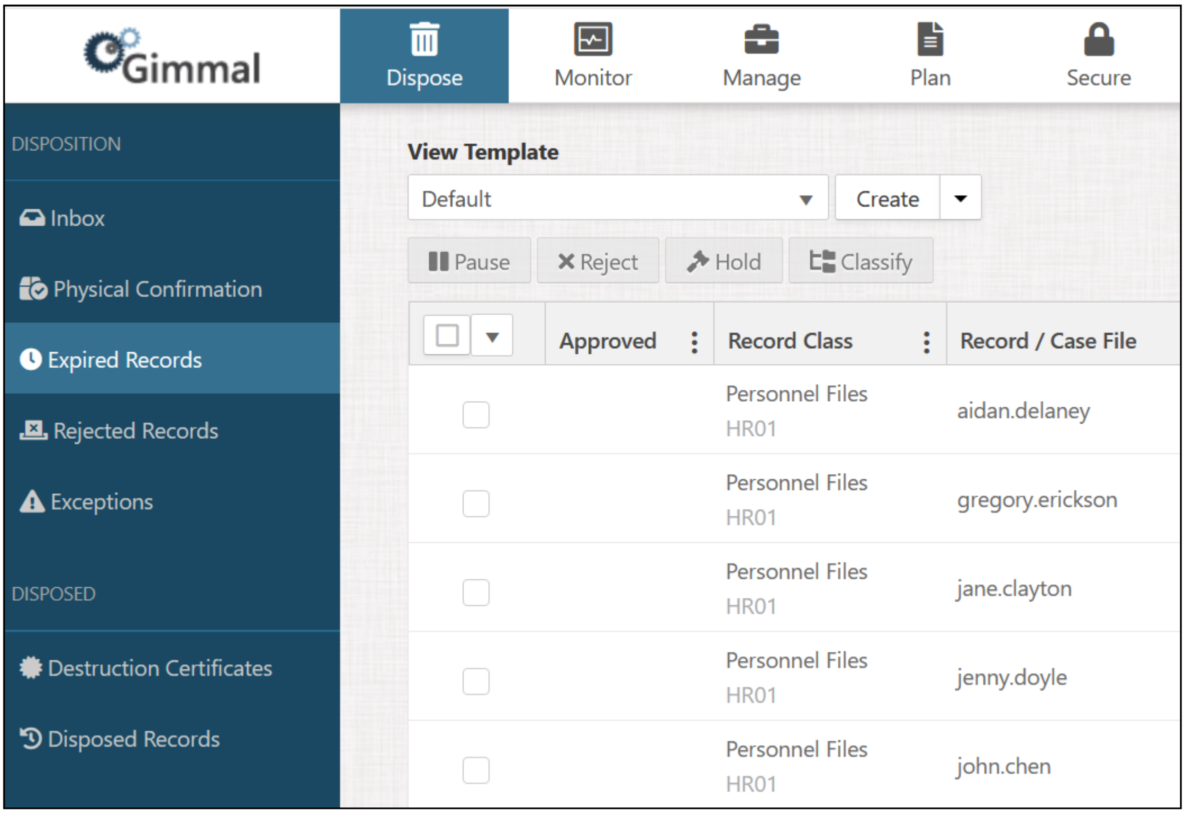
Confirm completion of 1 item(s).

Comment

5.10.3 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.



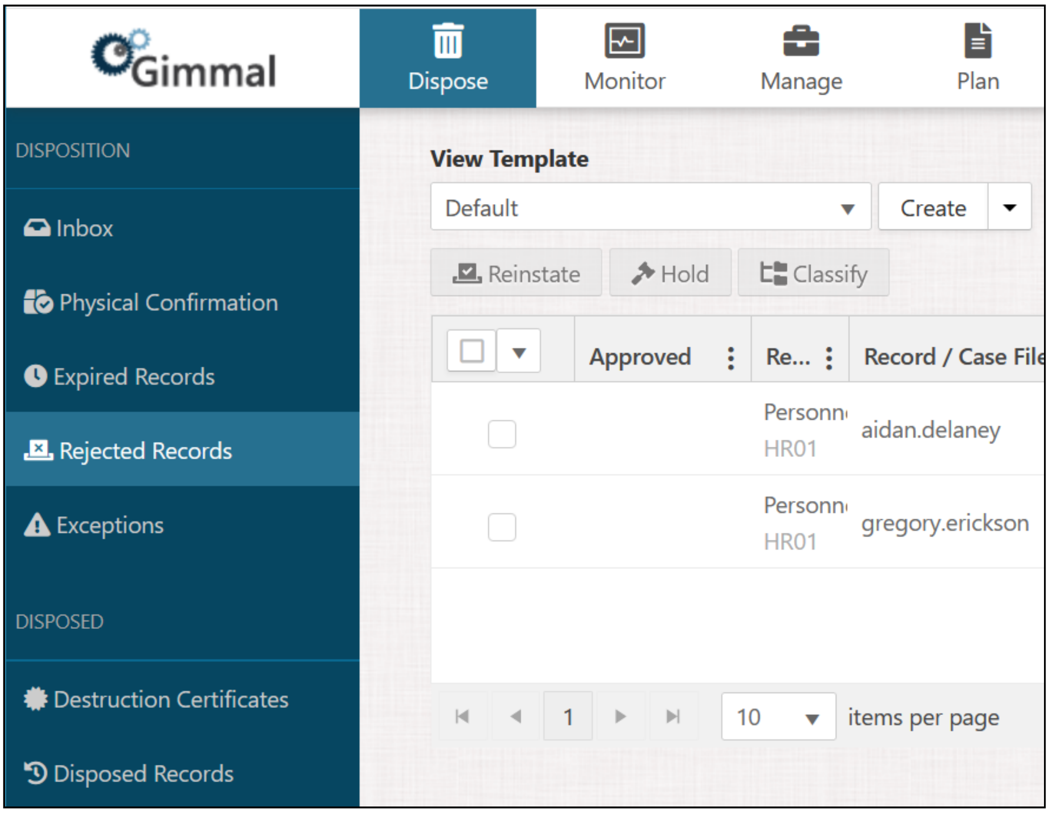
☐	Approved	Record Class	Record / Case File
☐		Personnel Files HR01	aidan.delaney
☐		Personnel Files HR01	gregory.erickson
☐		Personnel Files HR01	jane.clayton
☐		Personnel Files HR01	jenny.doyle
☐		Personnel Files HR01	john.chen

5.10.4 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.



View Template: Default

	Approved	Re...	Record / Case File
□		Personn HR01	aidan.delaney
□		Personn HR01	gregory.erickson

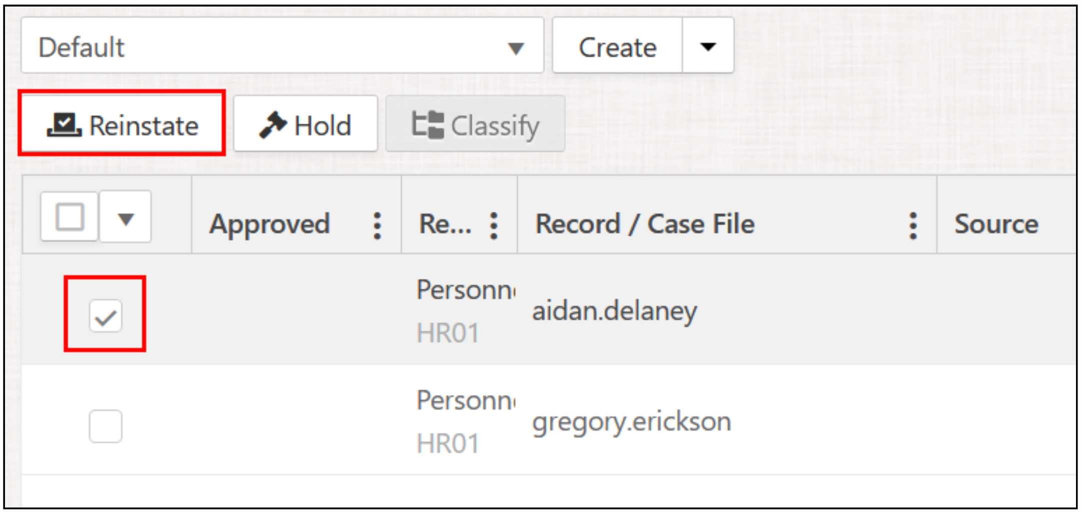
1 · 10 items per page

5.10.4.1 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.

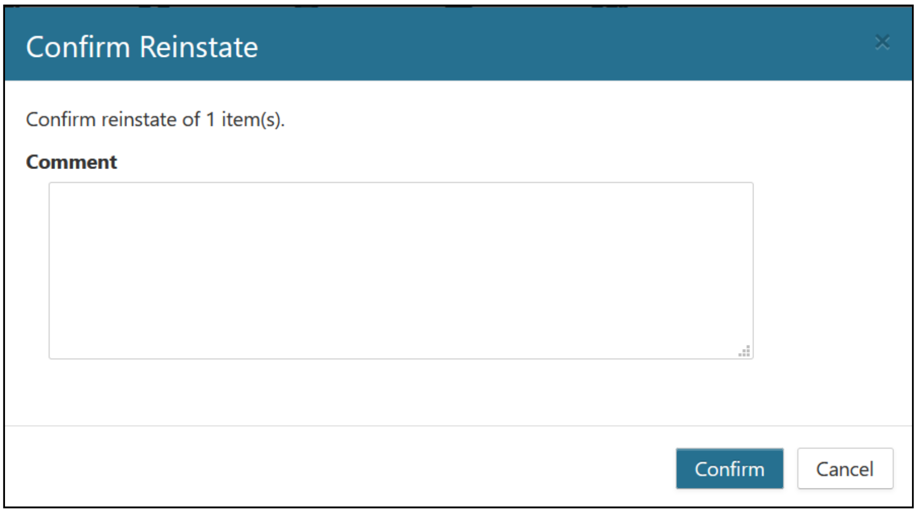
5.10.4.2 Reinstating Records

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.



□	Approved	Re...	Record / Case File	Source
☑		Personn HR01	aidan.delaney	
□		Personn HR01	gregory.erickson	

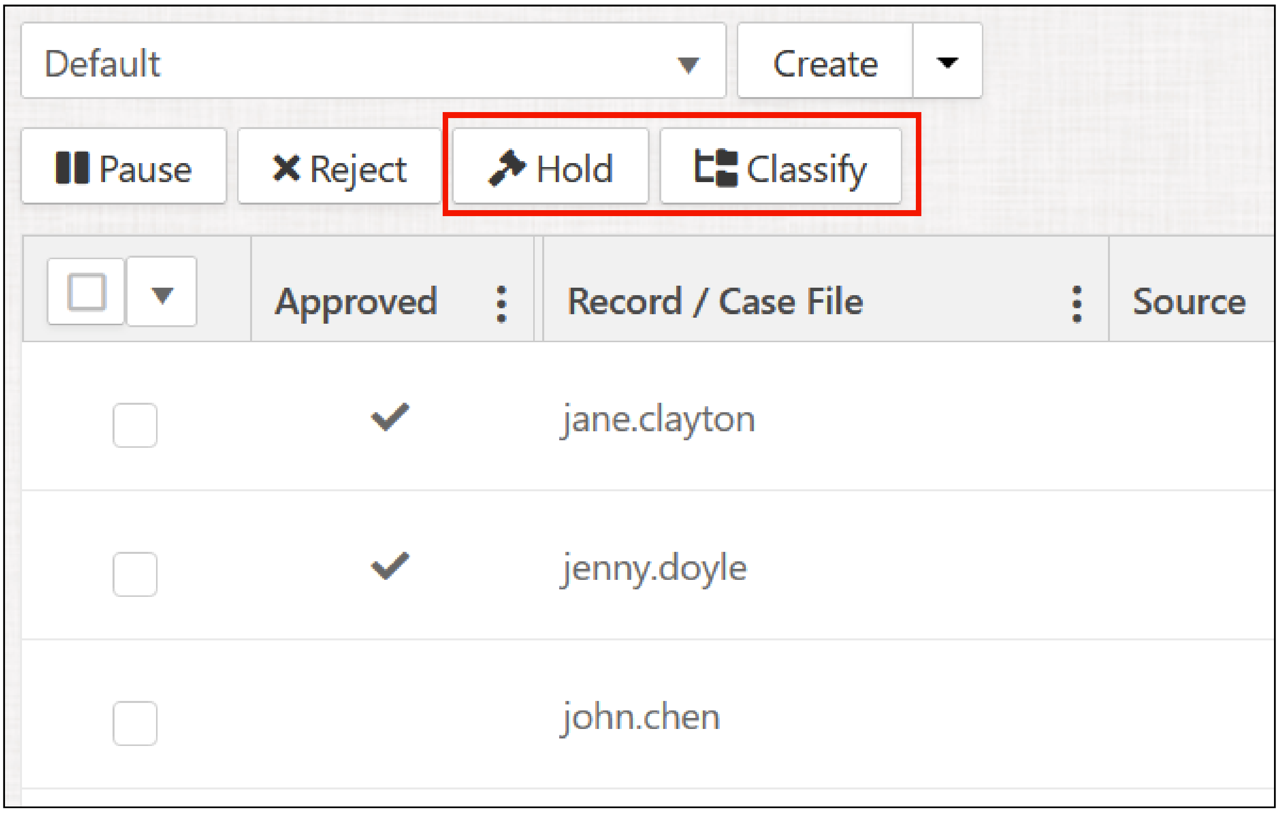
You will be prompted to confirm the reinstatement and give a reason.



Confirm reinstate of 1 item(s).

5.10.5 Legal Holds and Reclassification During Disposition

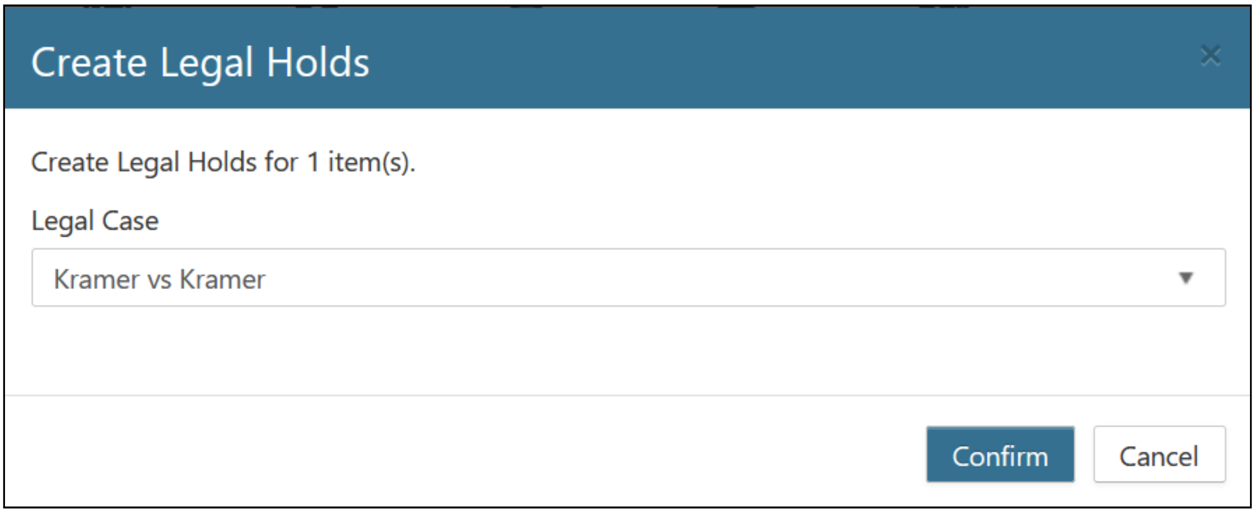
Users with the Record Manager role or higher can place items on hold or reclassify during the disposition process. These options are available in the Inbox, Expired Records, and Rejected Records.



□	Approved	Record / Case File	Source
□	✓	jane.clayton	
□	✓	jenny.doyle	
□		john.chen	

5.10.5.1 Legal Hold

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


Create Legal Holds

Create Legal Holds for 1 item(s).

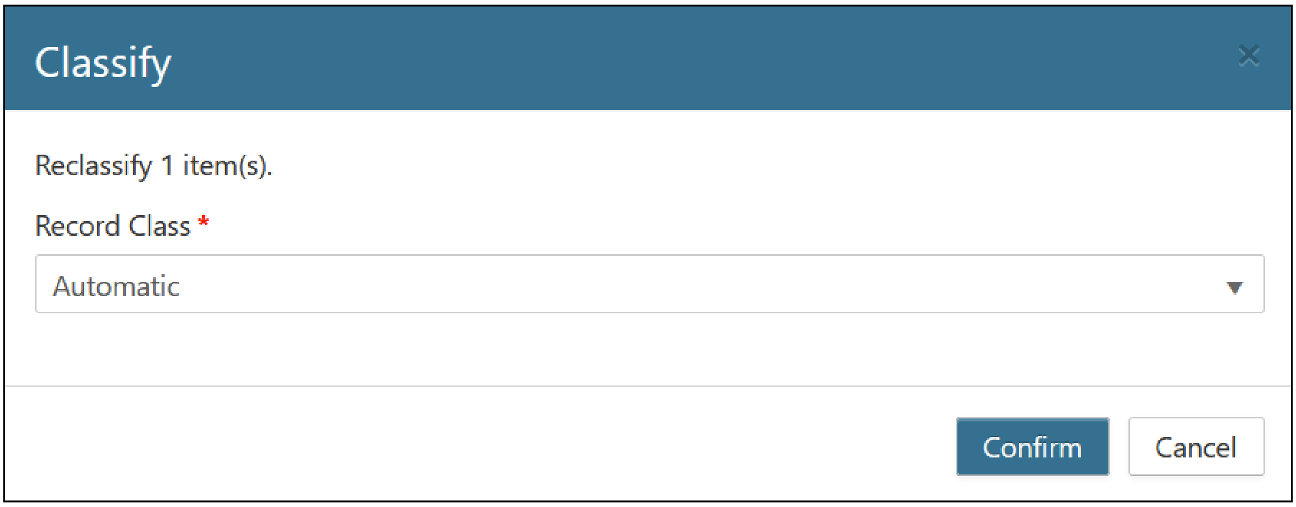
Legal Case: Kramer vs Kramer

Select a legal case and click the Confirm button.

5.10.5.2 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.



Classify

Reclassify 1 item(s).

Record Class *

Automatic

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.

5.10.6 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.

5.10.6.1 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

5.10.6.2 Complete

Complete will remove the exception and take no further action.

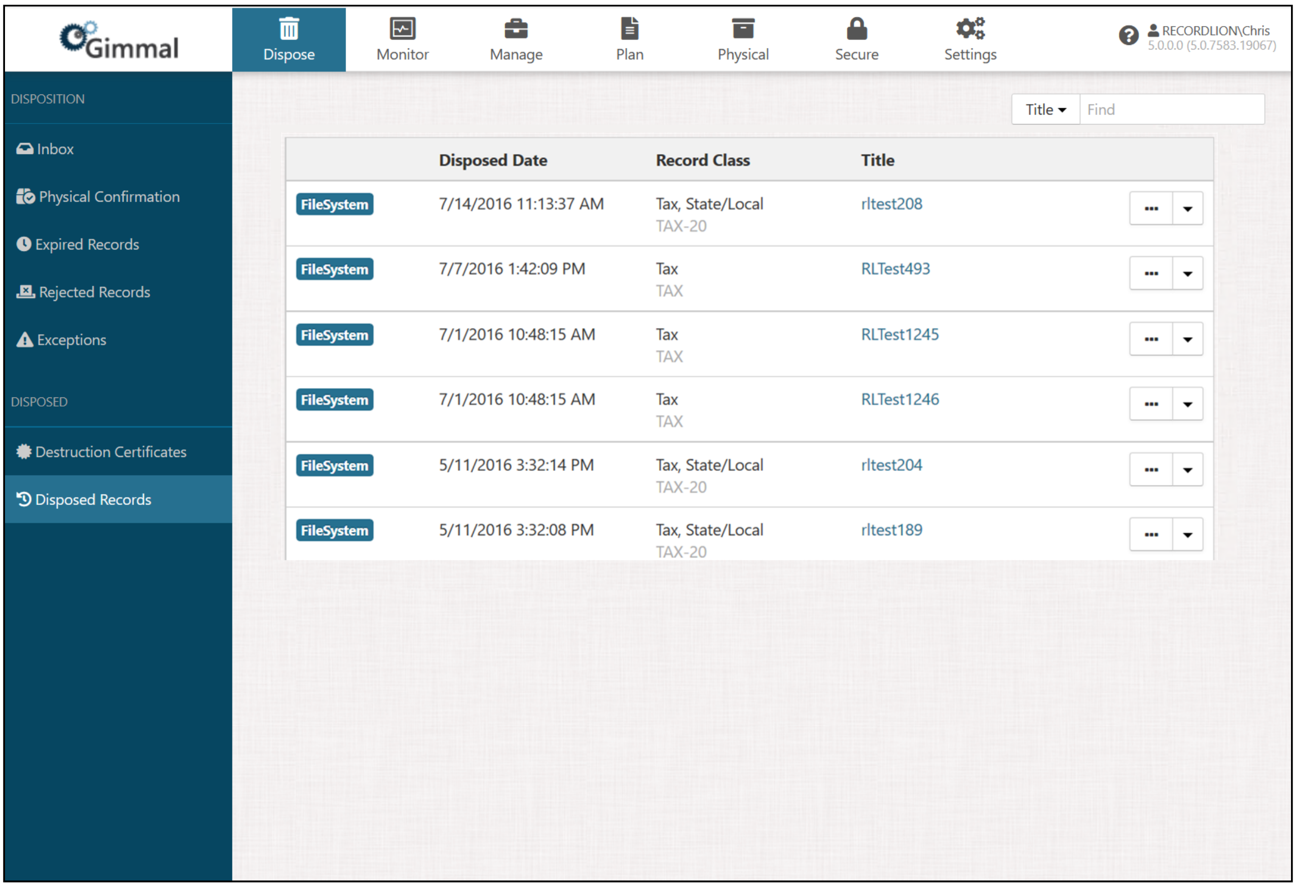
5.10.7 Disposed Records

ⓘ 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.

5.11 Monitor

5.11.1 Dashboard

5.11.2 Reports

5.11.3 Destruction Certificates

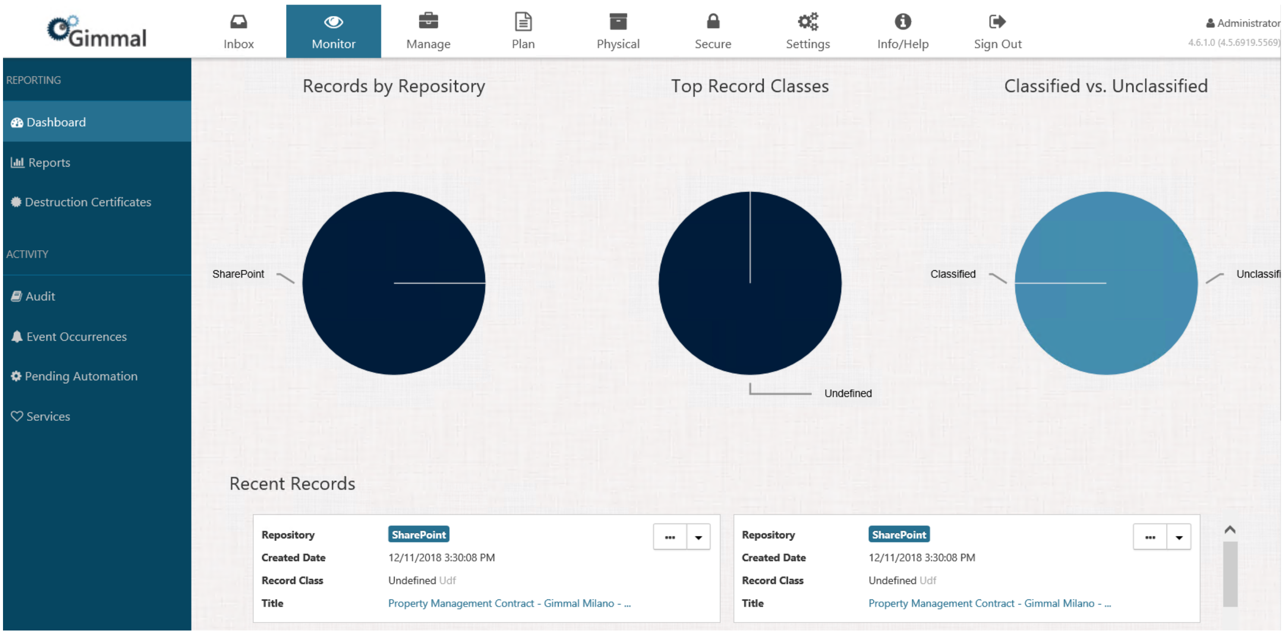
5.11.4 Audit

5.11.5 Event Occurrences

5.11.6 Pending Automation

5.11.7 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.



Repository SharePoint
Created Date 12/11/2018 3:30:08 PM
Record Class Undefined Udf
Title Property Management Contract - Gimmal Milano - ...

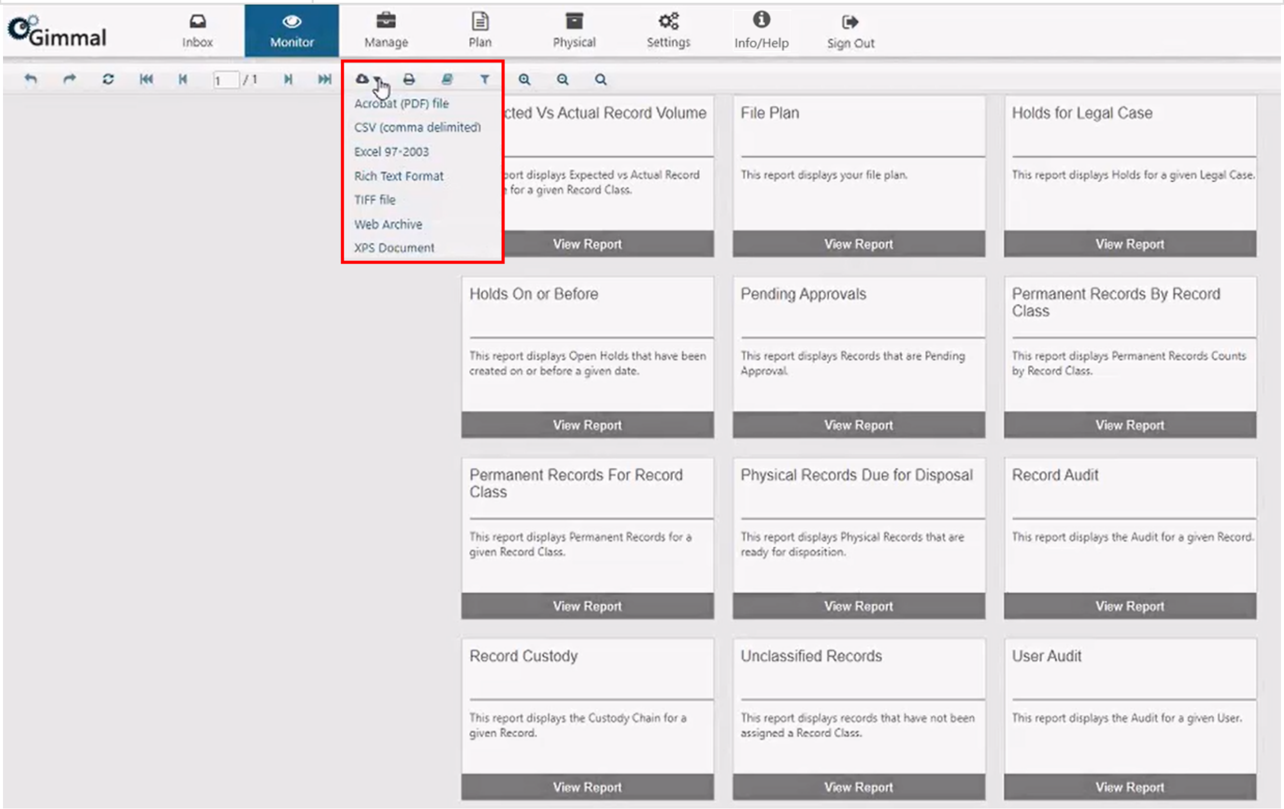
Repository SharePoint
Created Date 12/11/2018 3:30:08 PM
Record Class Undefined Udf
Title Property Management Contract - Gimmal Milano - ...

5.11.8 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



cted Vs Actual Record Volume

ort displays Expected vs Actual Record for a given Record Class.

File Plan

This report displays your file plan.

Holds for Legal Case

This report displays Holds for a given Legal Case.

Holds On or Before

This report displays Open Holds that have been created on or before a given date.

Pending Approvals

This report displays Records that are Pending Approval.

Permanent Records By Record Class

This report displays Permanent Records Counts by Record Class.

Permanent Records For Record Class

This report displays Permanent Records for a given Record Class.

Physical Records Due for Disposal

This report displays Physical Records that are ready for disposition.

Record Audit

This report displays the Audit for a given Record.

Record Custody

This report displays the Custody Chain for a given Record.

Unclassified Records

This report displays records that have not been assigned a Record Class.

User Audit

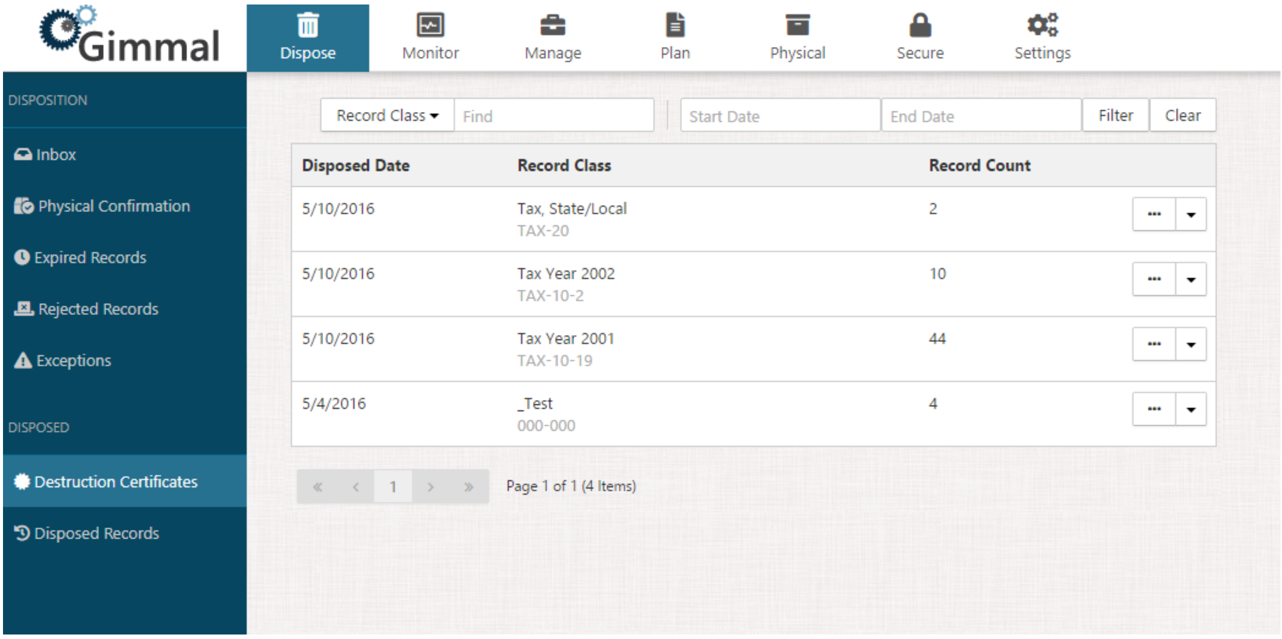
This report displays the Audit for a given User.

5.11.9 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:

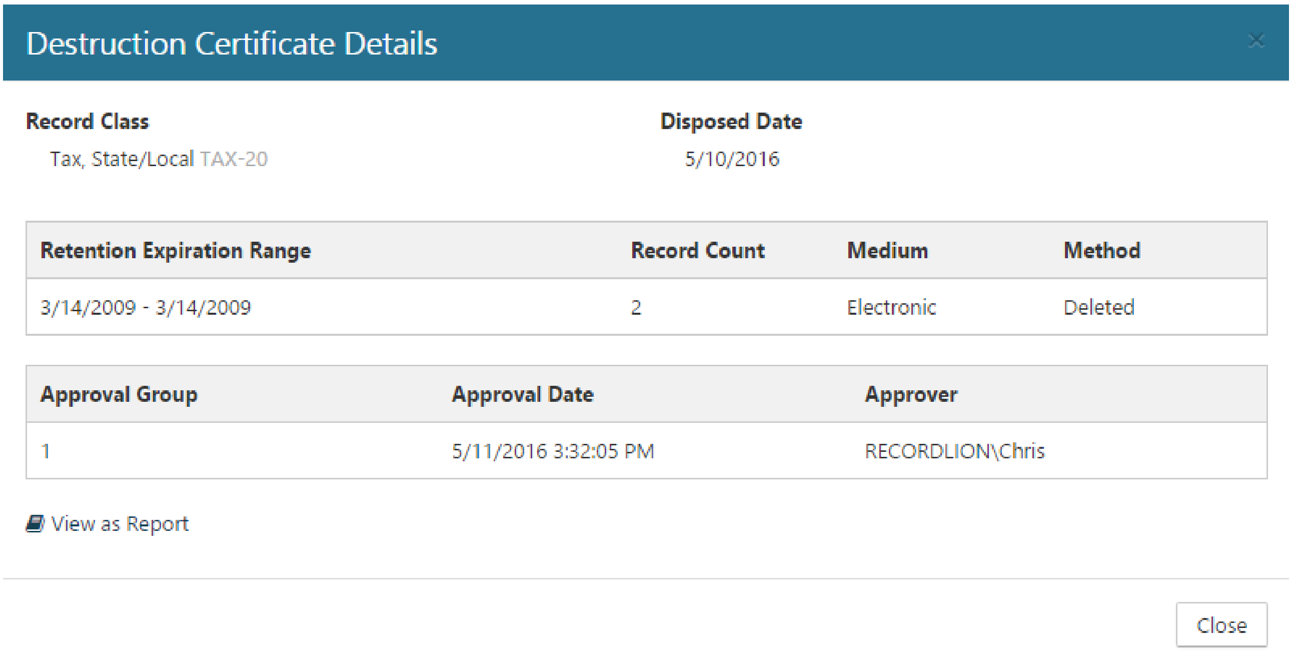
- You must enable the Destruction Certificate property on the Create/Edit Record Class dialog. For more information, see Record Class Properties.
- The disposition action of the lifecycle must require approval.



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

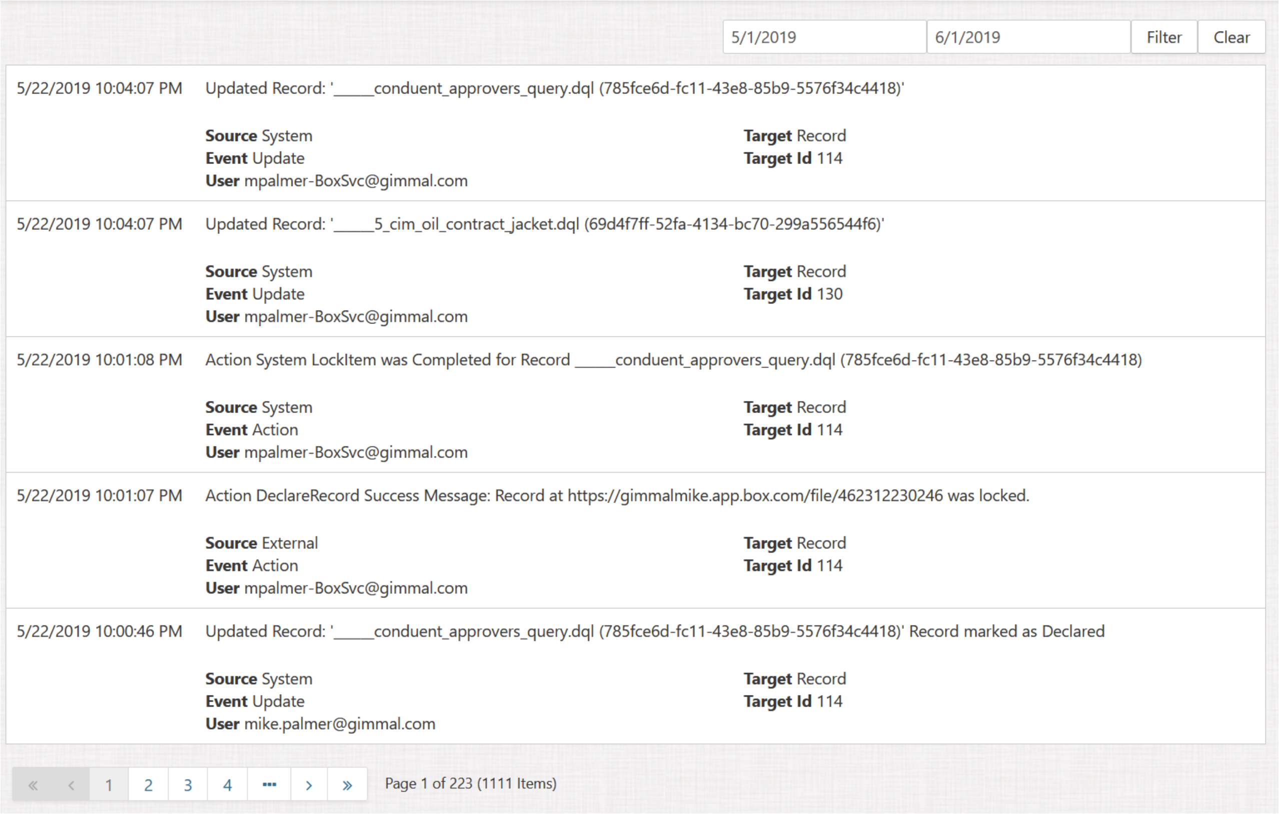
Disposed Date
5/10/2016

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

5.11.10 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.



5/22/2019 10:04:07 PM Updated Record: '_____conduent_approvers_query.dql (785fce6d-fc11-43e8-85b9-5576f34c4418)'

Source System
Event Update
User mpalmer-BoxSvc@gimmal.com
Target Record
Target Id 114

5/22/2019 10:04:07 PM Updated Record: '_____5_cim_oil_contract_jacket.dql (69d4f7ff-52fa-4134-bc70-299a556544f6)'

Source System
Event Update
User mpalmer-BoxSvc@gimmal.com
Target Record
Target Id 130

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
Event Action
User mpalmer-BoxSvc@gimmal.com
Target Record
Target Id 114

5/22/2019 10:01:07 PM Action DeclareRecord Success Message: Record at https://gimmalmike.app.box.com/file/462312230246 was locked.

Source External
Event Action
User mpalmer-BoxSvc@gimmal.com
Target Record
Target Id 114

5/22/2019 10:00:46 PM Updated Record: '_____conduent_approvers_query.dql (785fce6d-fc11-43e8-85b9-5576f34c4418)' Record marked as Declared

Source System
Event Update
User mike.palmer@gimmal.com
Target Record
Target Id 114

Page 1 of 223 (1111 Items)

5.11.11 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)

5.11.11.1 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.

5.11.11.2 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?	Defines if this Event Occurrence should target specific items. Options include: • **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".

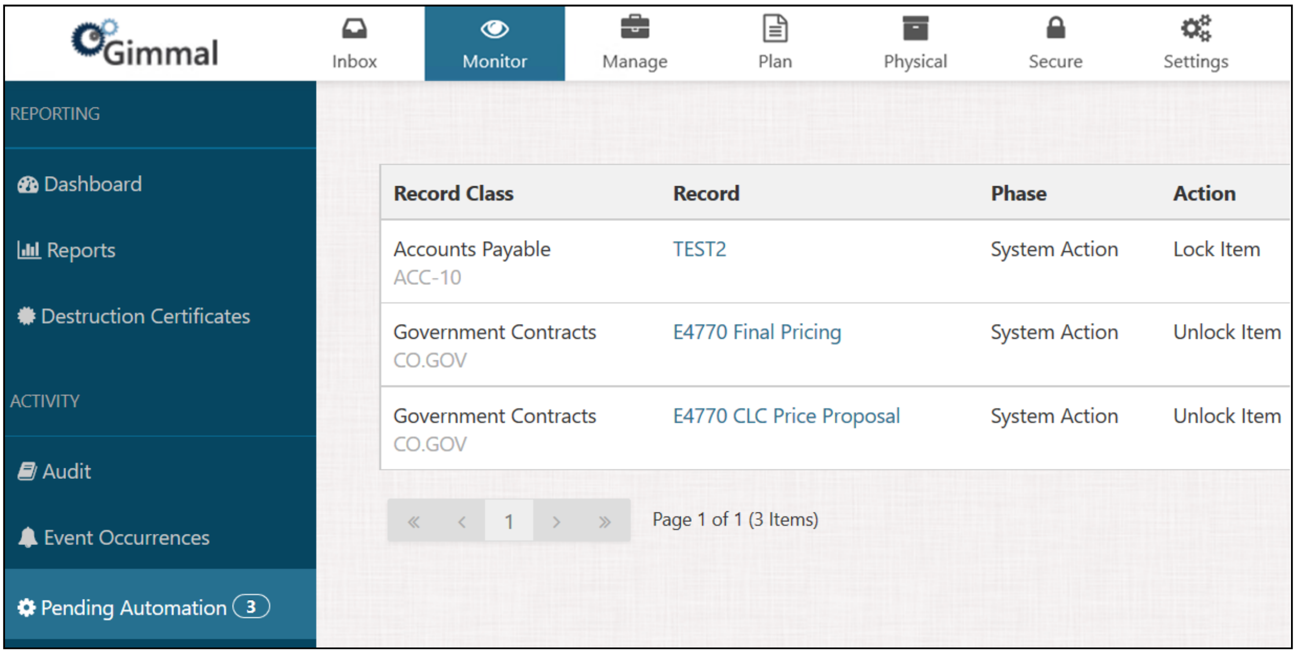
Property	Description
Target Property	Defines the Target Property that should be targeted; only displays if you select "Records with Property Value".
Target Value	Defines the Target Value that should be targeted based on the Target Property selected; only displays if you select "Records with Property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

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])

5.11.12 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.



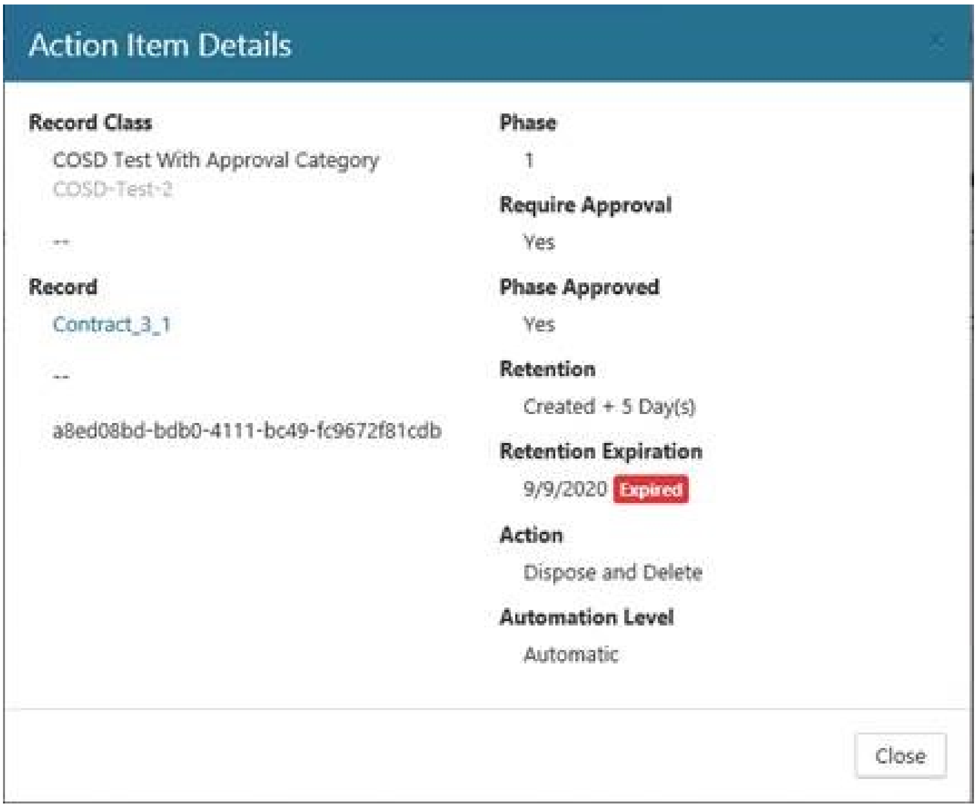
Record Class	Record	Phase	Action
Accounts Payable ACC-10	TEST2	System Action	Lock Item
Government Contracts CO.GOV	E4770 Final Pricing	System Action	Unlock Item
Government Contracts CO.GOV	E4770 CLC Price Proposal	System Action	Unlock Item

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

--

Record

Contract_3_1

--

a8ed08bd-bdb0-4111-bc49-fc9672f81cdb

Phase

1

Require Approval

Yes

Phase Approved

Yes

Retention

Created + 5 Day(s)

Retention Expiration

9/9/2020 Expired

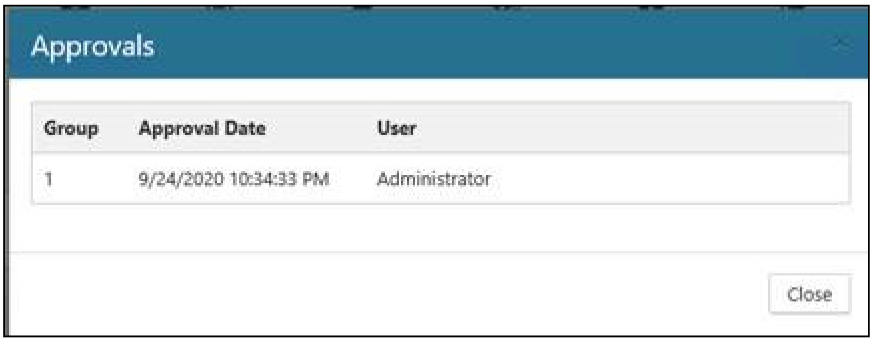
Action

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

5.12 Rule Builder

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

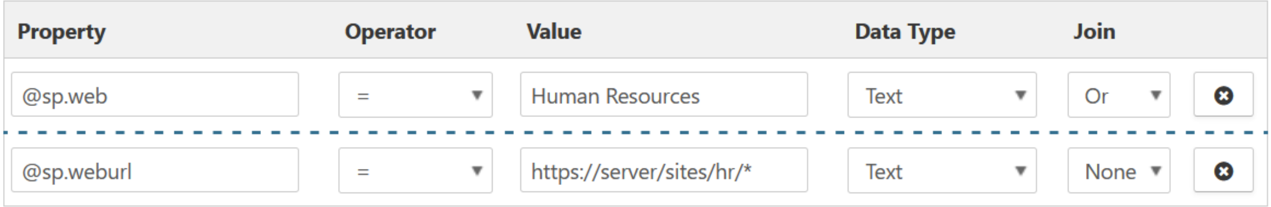
5.12.1 Rule Components

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. All possible tokens are available on the Rule Tokens(see page 150) page.
Operator	Represents the operator to use when comparing against the item. Possible values are: • < (less than) • <= (less than or equal to) • = (equal to) • > (greater than) • >= (greater than or equal to) • Like(see page 155) • Not = (not equal to) • Starts With • Matches(see page 155)
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: • Date • Date and Time • Text • Number
Join	Represents how individual rules are combined within the list. • AND - All rules using subsequent AND joins are nested together • OR - Does not nest, instead if separate sets of AND rules, for example (Exp1 AND Exp2) OR (Exp3) OR (Exp4 AND Exp5)

5.12.2 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 151) and SharePoint Tokens (see page 154)for a complete list.

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



Property	Operator	Value	Data Type	Join	
@sp.web	= ▼	Human Resources	Text ▼	Or ▼	✖
@sp.weburl	= ▼	https://server/sites/hr/*	Text ▼	None ▼	✖

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 SharePoint Property Value Formatting(see page 154) page for specific usage.

5.12.3 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*

5.12.4 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.

5.12.4.1 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
@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

5.12.4.2 Altitude Tokens

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

5.12.4.3 Documentum Tokens

Token	Description
@dctm.docbase	The DocBase where the document resides

Token	Description
@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

5.12.4.4 Exchange Tokens

Token	Description
@ex.from	Sender
@ex.owner	Owner of the mailbox the item is in
@ex.to[22]	Recipients
@ex.cc[23]	CC'd recipients

5.12.4.5 File Share Tokens

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

[22] http://ex.to
[23] http://ex.cc

5.12.4.6 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.assethomelocation	The "Home Location" value attached to the asset
@prm.assetcurrentlocation	The "Current Location" value attached to the asset
@prm.owner	The owner listed for the asset
@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	The following asset metadata can be used: • Any Custom field (if configured) • Title • Subject • Asset Type • Format For specificity, use @repo = physical to only affect physical assets

5.12.4.7 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 "/ accounting"
@sp.folderurl	The server relative URL of the item's parent folder, for example, "/accounting/ap"
@sp.contenttype	The name of the item's content type
@sp.title	The Title property from SharePoint
SharePoint Column Display Name	Any SharePoint Column Display Name can be used in Classification Rules

5.12.5 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.

5.12.5.1 SharePoint and SharePoint Online

Property Type	Property Value Formatting	Notes
Single line of text	Text Value	
Multiple lines of text	Text Value	

Property Type	Property Value Formatting	Notes
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	
Managed Metadata	Term1|Term2|Term3	

5.12.6 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.

5.12.6.1 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

5.12.6.2 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

5.13 Physical Records

5.13.1 Locations

5.13.2 Containers

5.13.3 Assets

5.13.4 Barcode Schemes

5.13.5 Request and Returns

5.13.6 Custom Metadata and Templates

5.13.7 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.

5.13.7.1 Creating a New Location

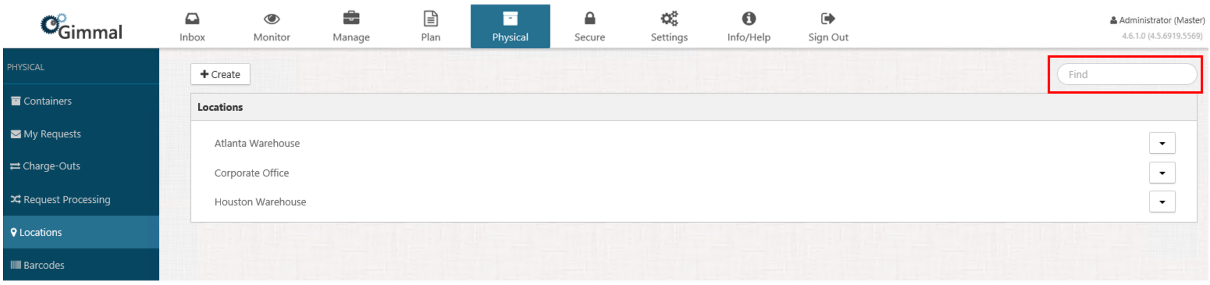
To create a new location, perform the following steps:

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.

5.13.7.2 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.



Locations

Atlanta Warehouse

Corporate Office

Houston Warehouse

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.

5.13.7.3 Editing and Deleting a Location

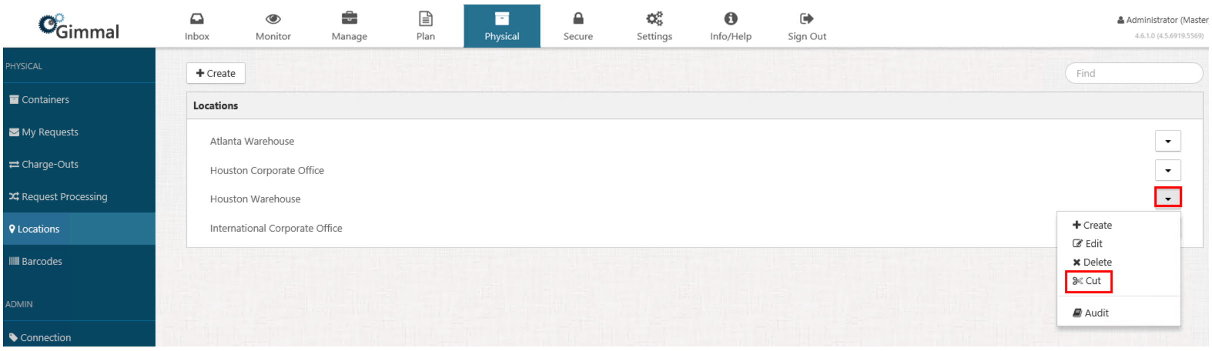
Take the same steps as creating a location, but select Edit or Delete instead.

5.13.7.4 Moving a Location

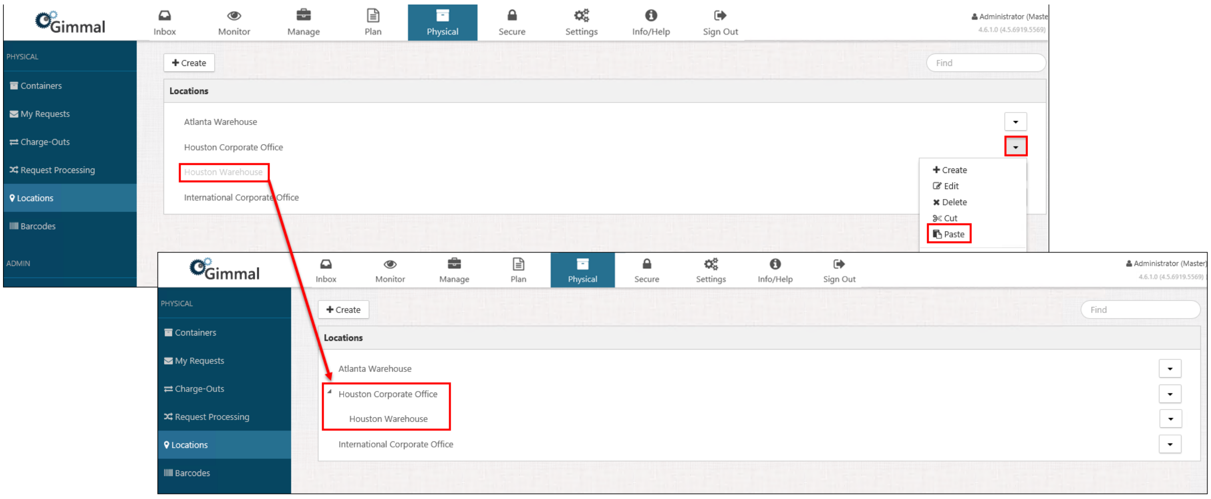
The only purpose for moving a location is to move it to a different parent or to/from the root. It may appear that you can reoder the Location, but the page will refersh and place them back in alphabetical order.

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.



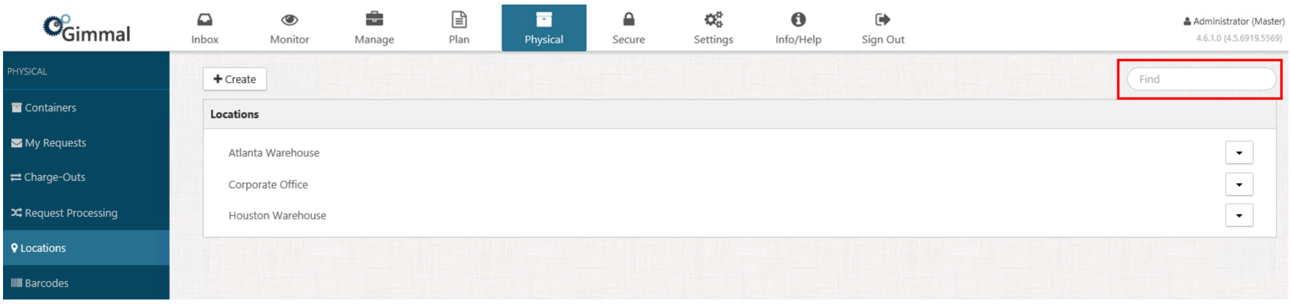
Drag and Drop

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.)

5.13.7.5 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.



Locations

Atlanta Warehouse

Corporate Office

Houston Warehouse

5.13.8 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.

5.13.8.1 Managing Container Permissions

5.13.8.2 Container Properties

5.13.8.3 Creating a Container

5.13.8.4 Searching for a Container

5.13.8.5 Making changes to containers

5.13.8.6 Record Classes and Containers

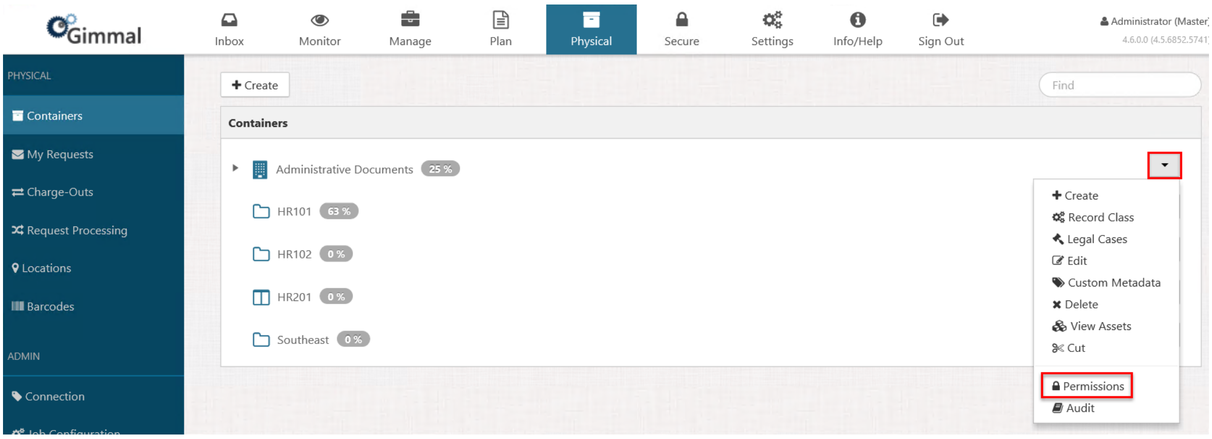
5.13.8.7 Legal Cases and Holds on Containers

5.13.8.8 Managing Container Permissions

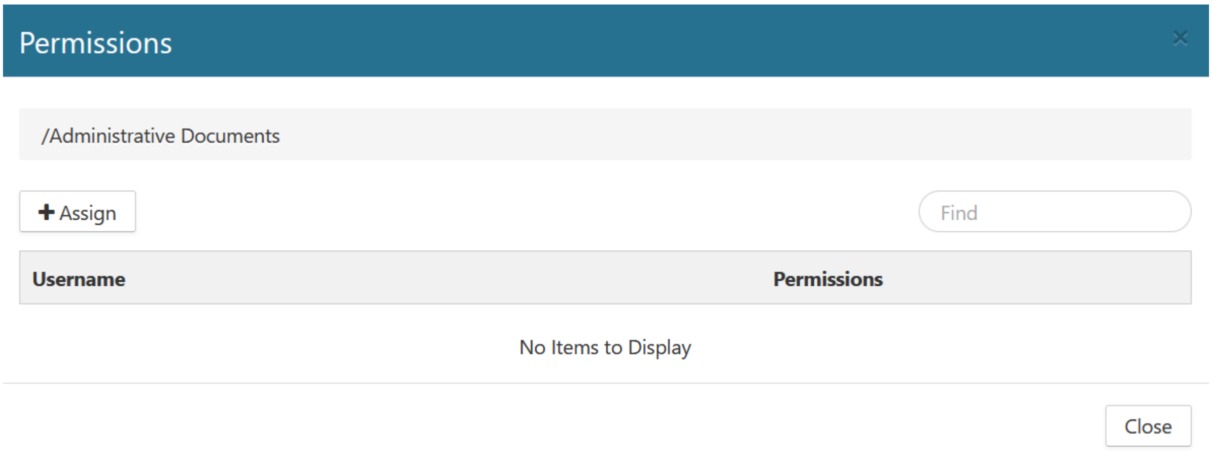
Containers have their own set of permissions, which are required in order for the Physical User to perform certain tasks involving parent containers and child containers. This topic describes how to set, edit, and remove permissions. It also describes permission inheritance, with respect to parent and child containers. An overview of container permissions can be found in the Physical Records Permission Overview(see page 226) 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**.



Permissions

/Administrative Documents

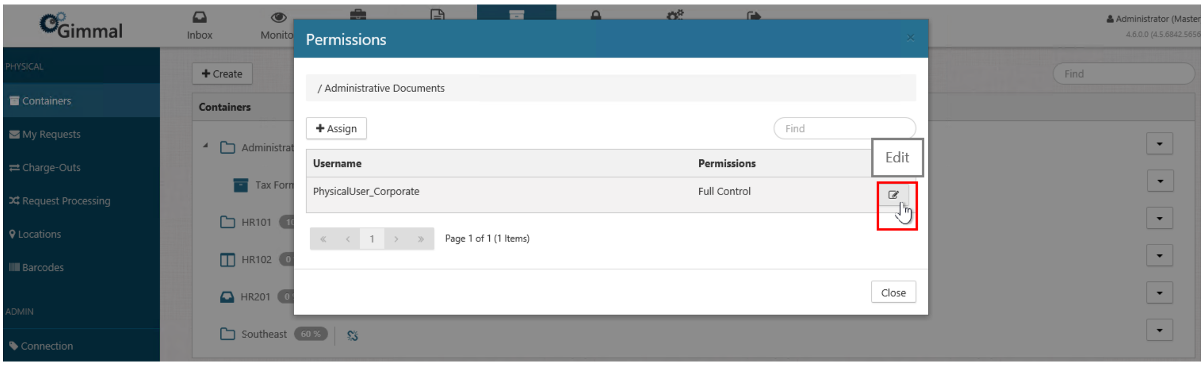
Username	Permissions

No Items to Display

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.



Permissions

/ Administrative Documents

Username	Permissions
PhysicalUser_Corporate	Full Control

Page 1 of 1 (1 Items)

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.

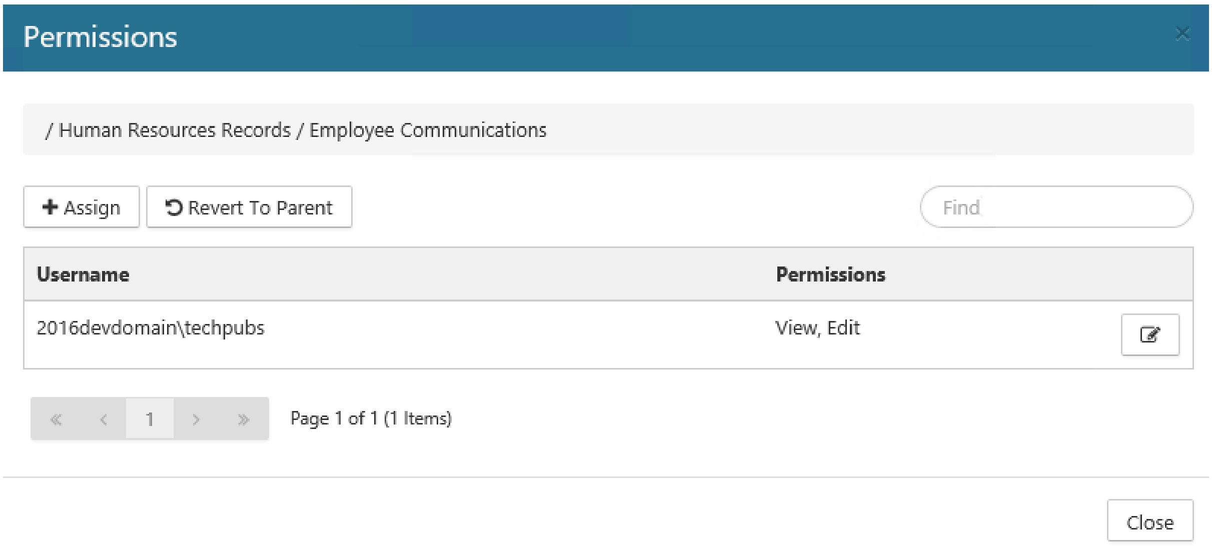
Removing Permissions for a Container

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[24].
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.



Permissions

/ Human Resources Records / Employee Communications

Username	Permissions
2016devdomain\techpubs	View, Edit

Page 1 of 1 (1 Items)

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.

5.13.8.9 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.

[24] http://docs.gimmal.com/en/6109-creating---searching-for-new-container.html

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.
Node Type	Location	Yes	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.) 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. 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. 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.
Location Type	Yes	Folder	The location type that only displays if you select **Location** as your node type. Options are: - Aisle - Bin - Box - Cabinet - Drawer - Folder - Shelf - Warehouse

Property	Required	Default	Description
Capacity	No		The maximum number of physical assets in a container. Does not include assets in any child containers. 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: □ If capacity is not entered, a numerical count of the parent container's assets will display. For example: □ If capacity reaches 100% for a container, you can still add additional child containers, but you cannot add additional physical assets.
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.

5.13.8.10 Creating a Container

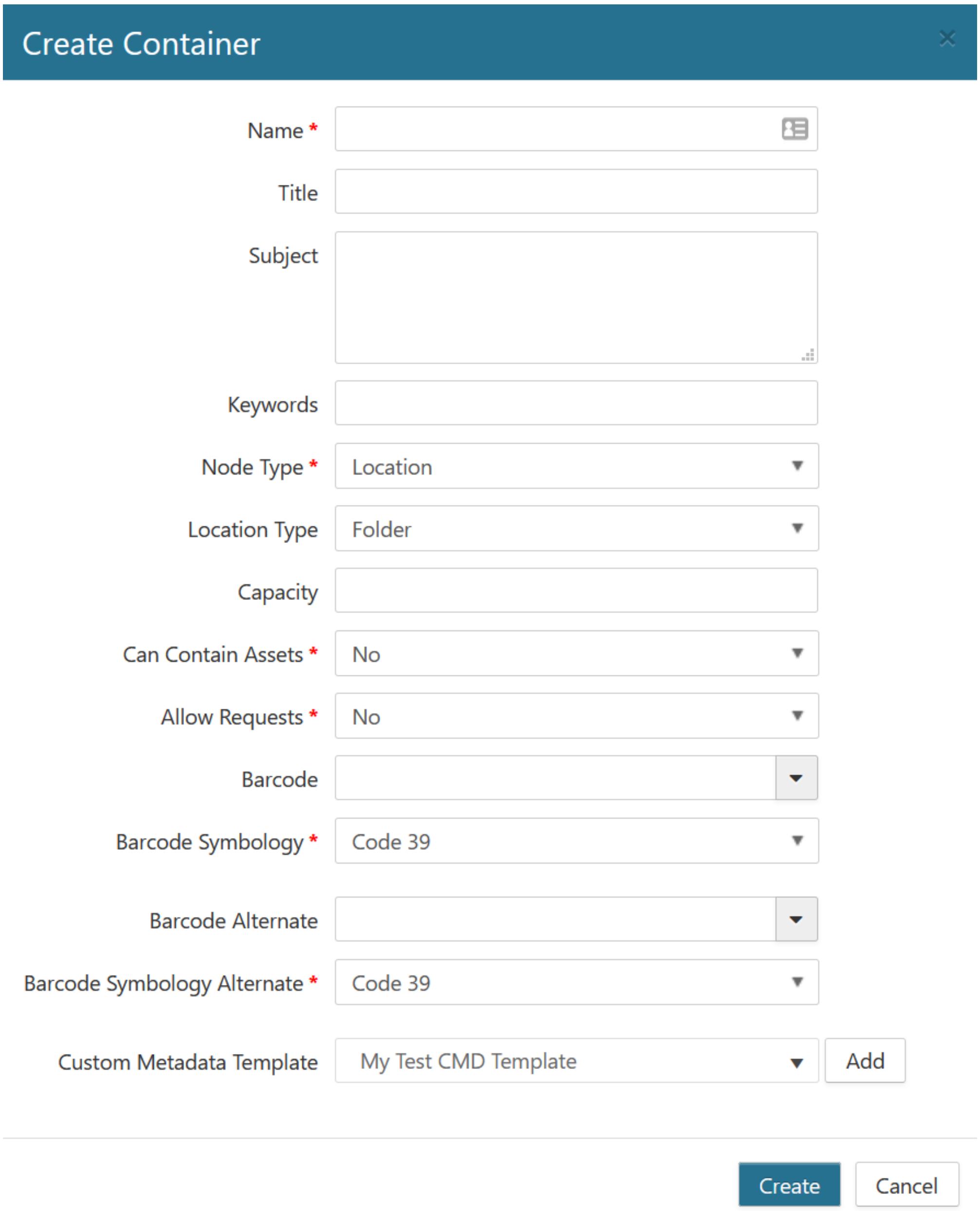
A container is a logical or location-based structure used for organizing and managing physical assets. For example, a location-based container could be a shelf, and the boxes that are stored on the shelf (which represent the physical assets). For logical-based, the container can be anything, a charge-code, 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.



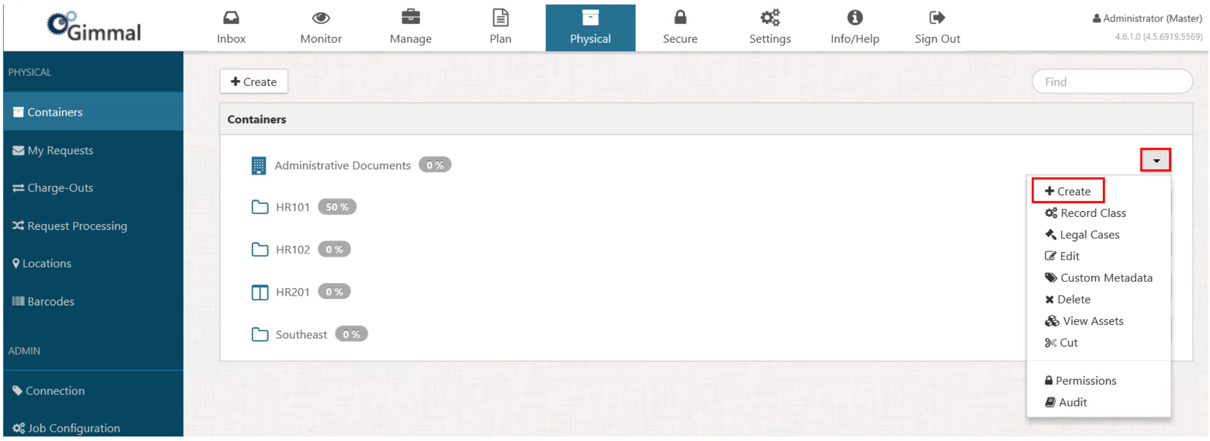
Create Container

Name *	
Title	
Subject	
Keywords	
Node Type *	Location
Location Type	Folder
Capacity	
Can Contain Assets *	No
Allow Requests *	No
Barcode	
Barcode Symbology *	Code 39
Barcode Alternate	
Barcode Symbology Alternate *	Code 39
Custom Metadata Template	My Test CMD Template

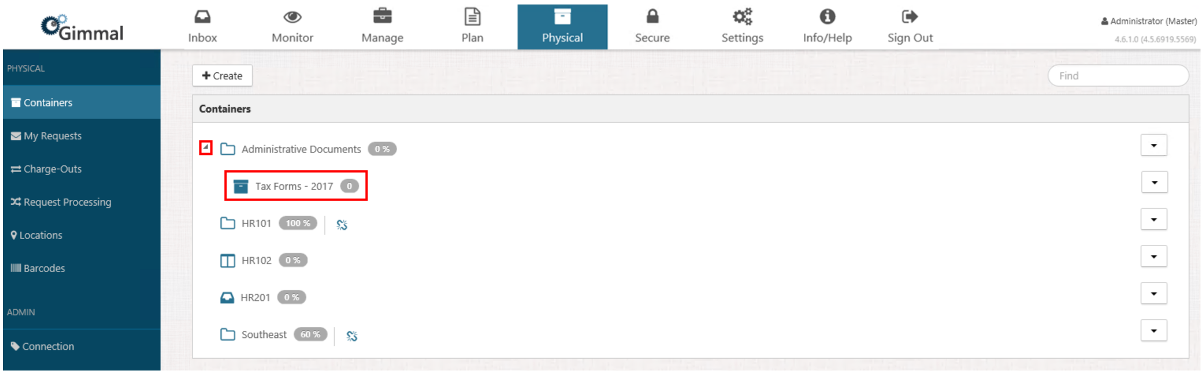
4. Enter the required and optional fields as described in Container Properties(see page 162).
5. Click **Create**. The new container displays on the Containers page.

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 162).
5. Click **Create**, and then expand the parent container. The new child container displays under the parent container.

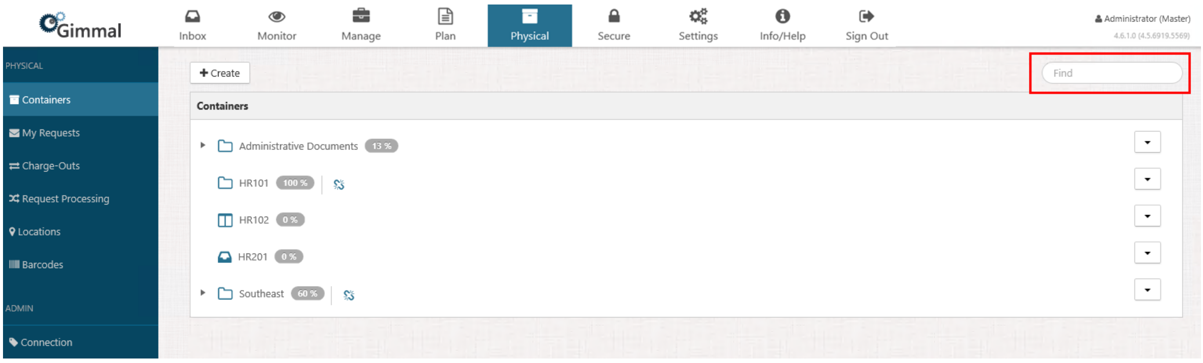


5.13.8.11 Searching for a Container

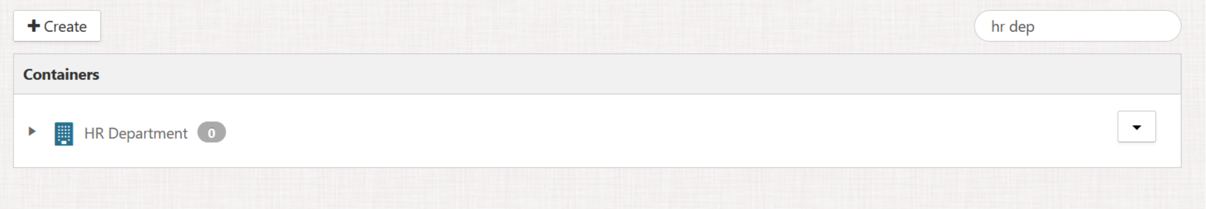
Your containers list can have potentially thousands of entries. As a result, Physical Records Management enables you to search the containers list by **name** or **title** to easily find a specific container.

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).

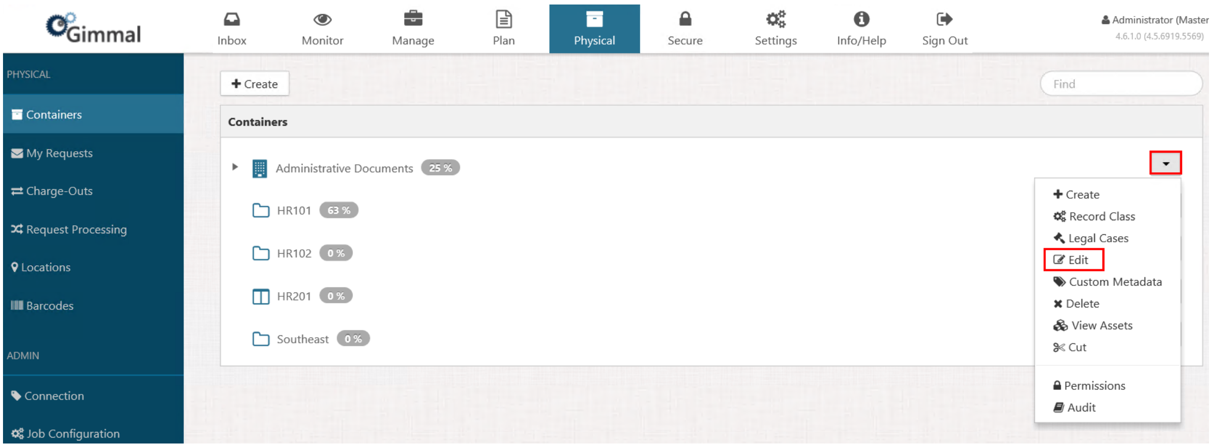


5.13.8.12 Making changes to containers

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.)



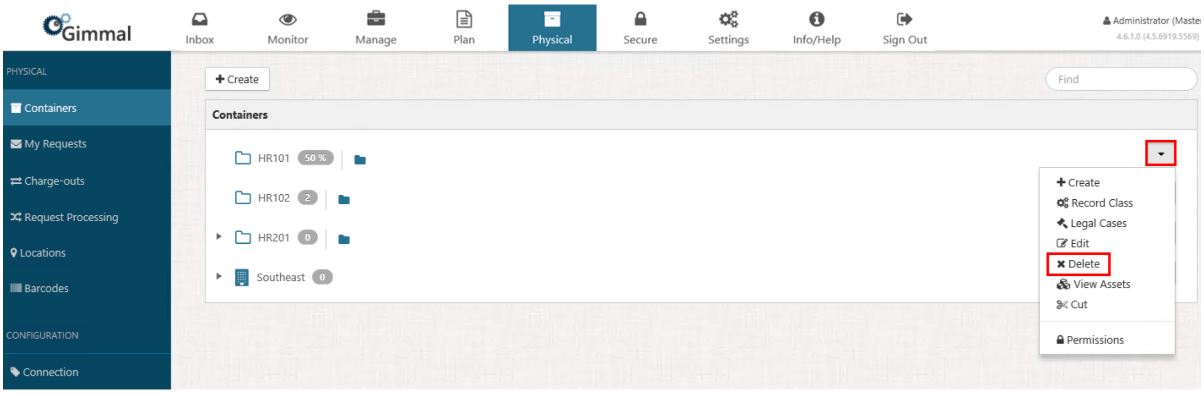
3. Click **Edit**. The Edit Container dialog opens.
4. Make your desired changes to the properties and then click **Save**. The container updates on the Containers page.

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

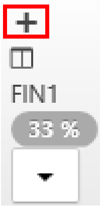
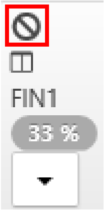
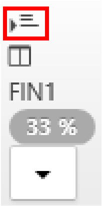
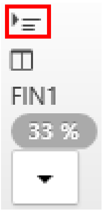
Perform the following steps to move a container by cutting and pasting it.

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.

	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.)

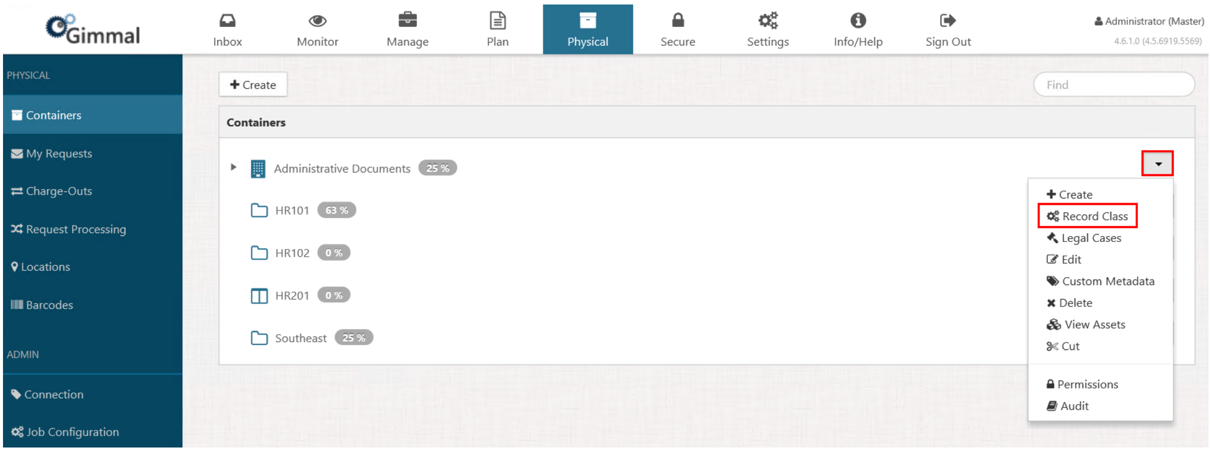
5.13.8.13 Record Classes and Containers

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[25] 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.)



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.

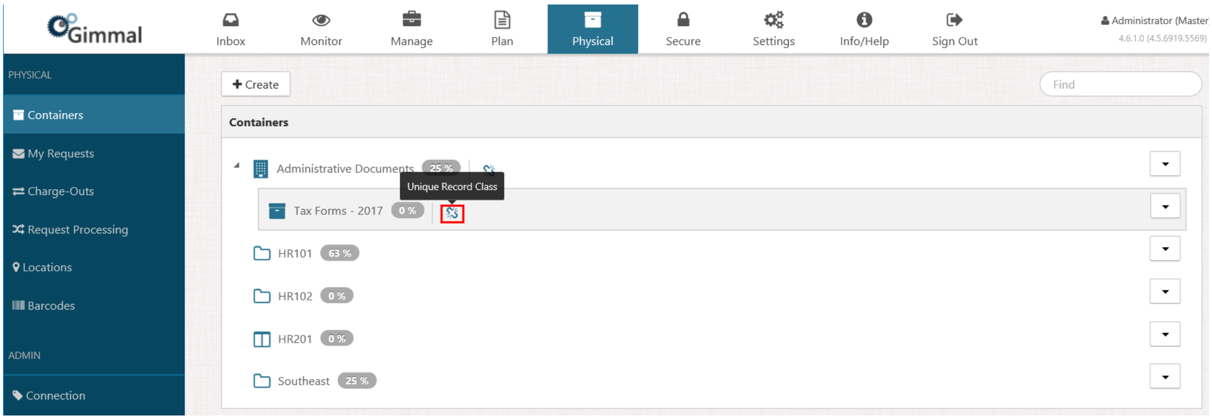
> ⓘ When you create a child container, the child container inherits the same record class from the parent container. This is indicated by the "Inheriting Record Class" icon to the right of the child container name.

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.

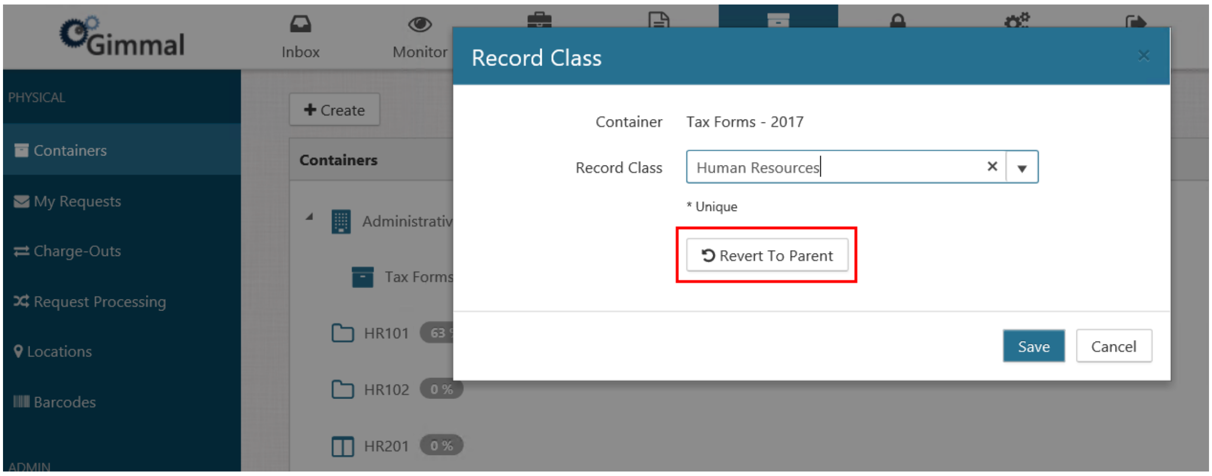
[25] http://docs.gimmal.com/en/1641-record-classes.html

1. Create a container, and then create a child container. (For more information, see Creating Containers(see page 164)
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.

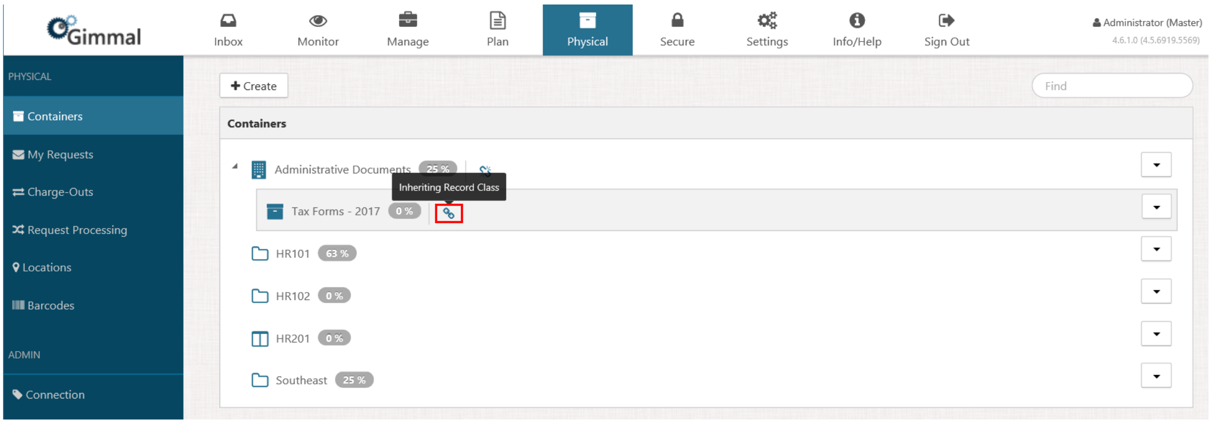


Container Tax Forms - 2017

Record Class Human Resources

* Unique

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.



5.13.8.14 Legal Cases and Holds on Containers

Legals holds created in Gimmal 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.

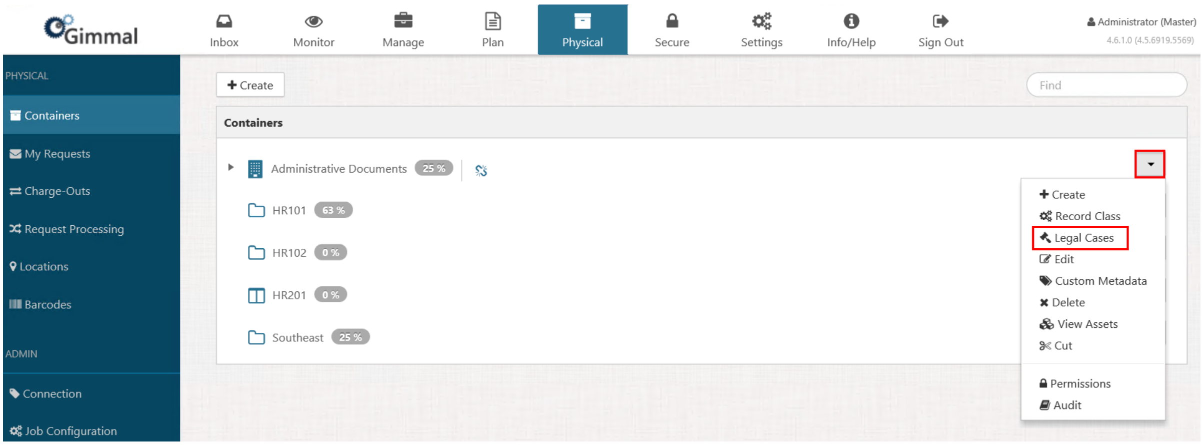
Legal holds do not "cascade" down to other child containers. You have to repeat this process for each container in the hierarchy.

- 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[26].
- To add a legal hold to a physical asset, see Adding a Legal Hold to a Physical Asset[27].

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.)

[26] http://docs.gimmal.com/en/6127-adding-a-legal-hold-to-a-physical-asset.html
[27] http://docs.gimmal.com/en/6127-adding-a-legal-hold-to-a-physical-asset.html



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.

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.

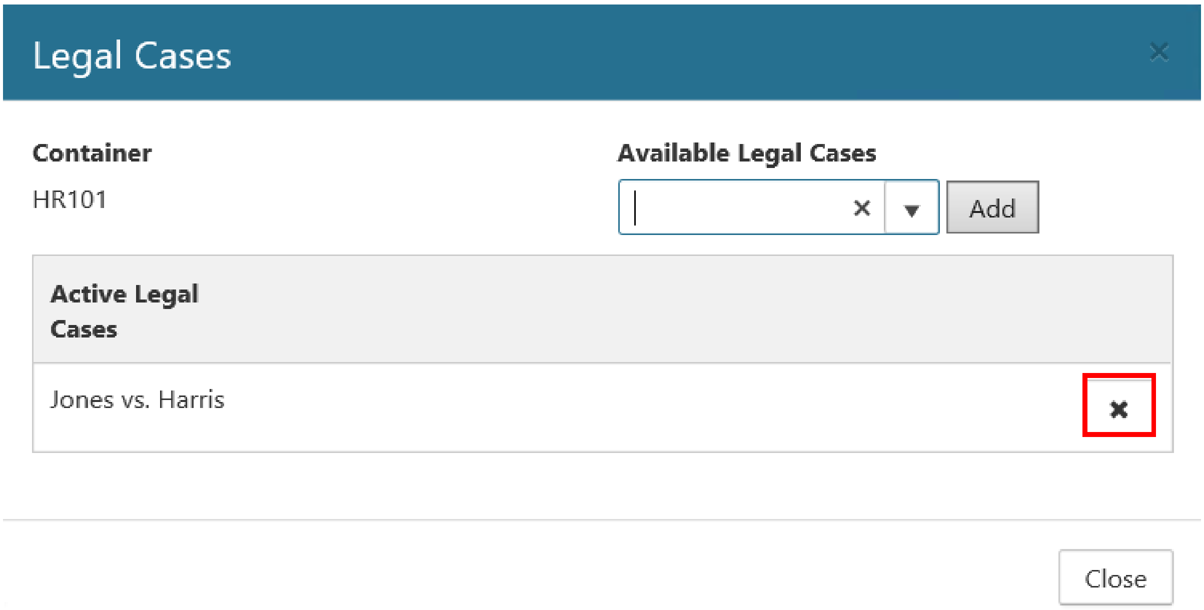
Removing a Legal Case that was Added to a Container

- 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.

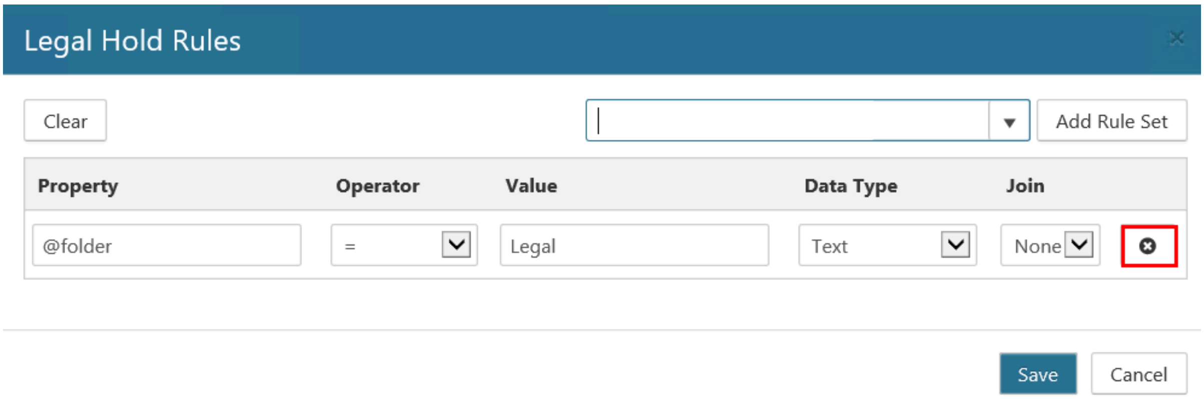


3. Click the **X** next to the legal case(s) you want to remove. The legal case is removed from the list.
4. Click **Close**.

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.



Property	Operator	Value	Data Type	Join
@folder	=	Legal	Text	None

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.

5.13.9 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).

5.13.9.1 Asset Properties

5.13.9.2 Associating Assets to a Record Class

5.13.9.3 Creating Physical Assets

5.13.9.4 Modifying Existing Assets

5.13.9.5 Copying Assets

5.13.9.6 Searching for Assets

5.13.9.7 Viewing Asset Properties and Record Details

5.13.9.8 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.

Property	Required	Default	Description
Home Location	Yes	**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. **Logical-based Container:** Unknown	The Home Location field is container (node)-specific. **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. **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.
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[28] for more information on creating locations and applying them to a physical asset.
Asset Type	Yes	Box	Defines the type of physical asset you're creating. Possibilities are: • Box • Document • Folder • Other
Other Asset Type	No		If the Asset Type "Other", this property becomes available.

[28] http://docs.gimmal.com/en/5905-managing-locations.html

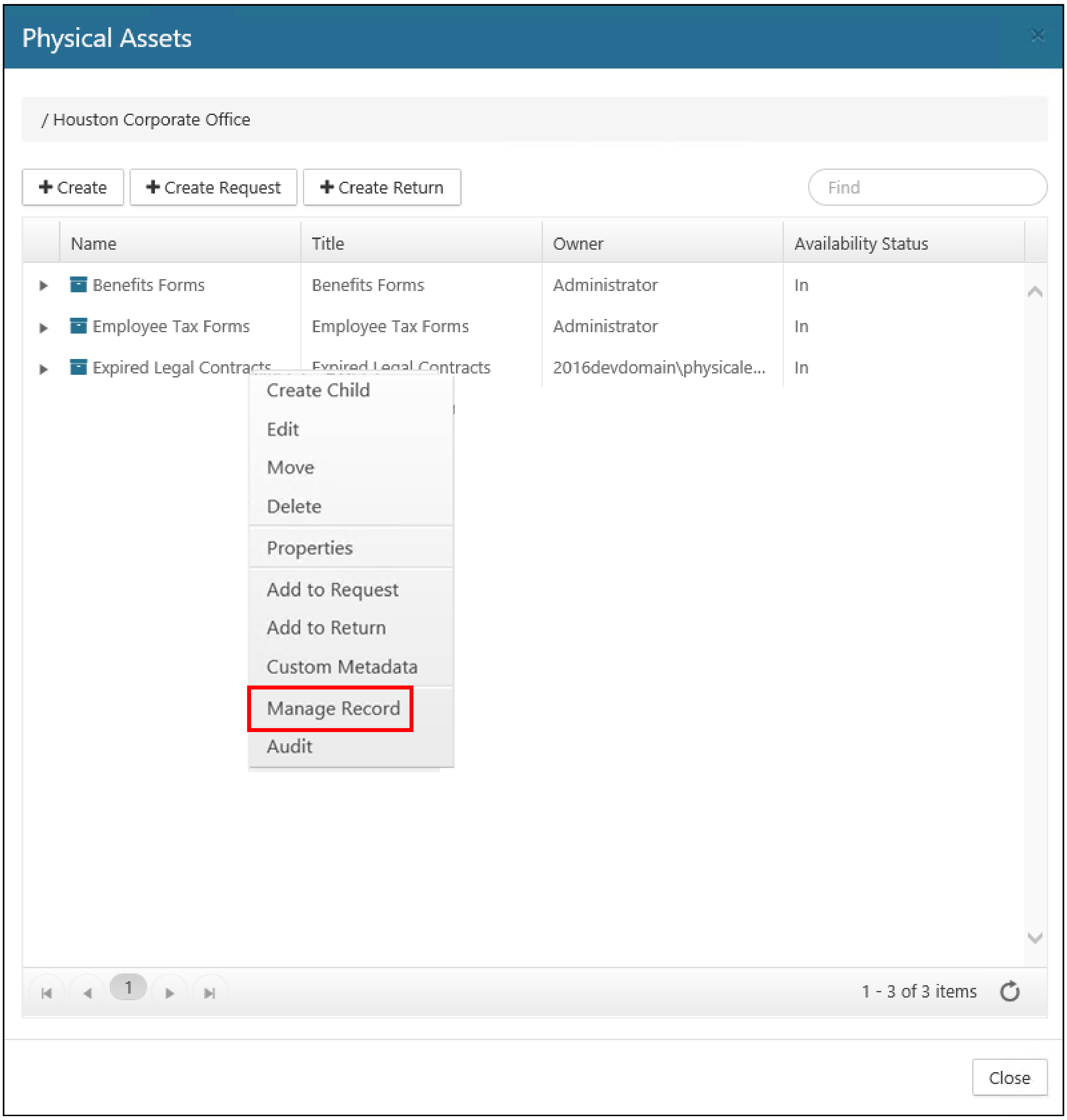
Property	Required	Default	Description
Format	No	Yes	Defines the format of the physical asset. Possibilities are: • None • CD • DVD • Film • Microfiche • Microfilm • Mixed • Negative • Optical • Paper • Slide • Tape • Video • X-Ray • Other
Other Format	No		If the Format "Other", this property becomes 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.
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.

Property	Required	Default	Description
Barcode Symbology Alternate			The type of barcode symbology to use for the Barcode Alternate.

5.13.9.9 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 **Container**s 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.

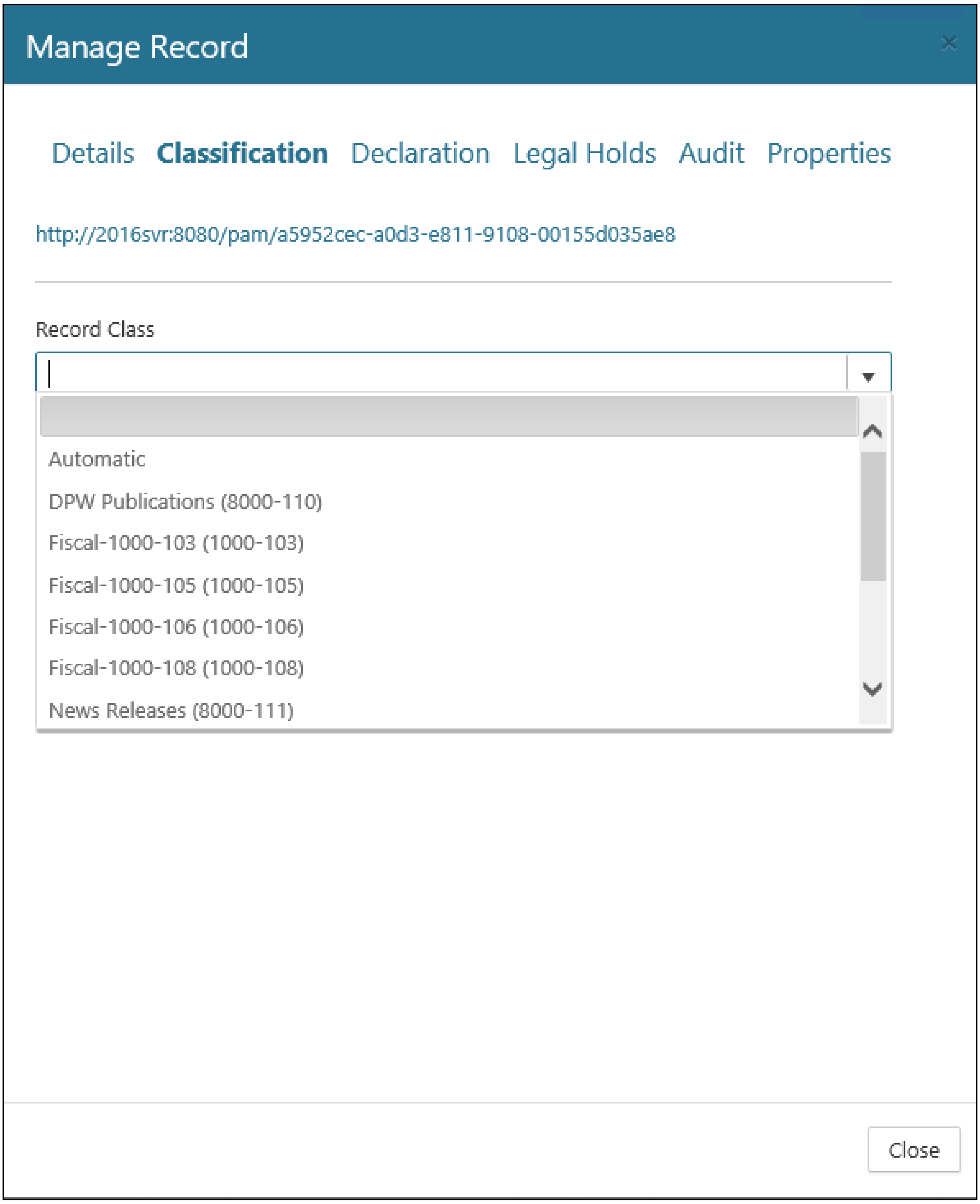


Physical Assets

/ Houston Corporate Office

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

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**.



http://2016svr:8080/pam/a5952cec-a0d3-e811-9108-00155d035ae8

Record Class

Automatic
DPW Publications (8000-110)
Fiscal-1000-103 (1000-103)
Fiscal-1000-105 (1000-105)
Fiscal-1000-106 (1000-106)
Fiscal-1000-108 (1000-108)
News Releases (8000-111)

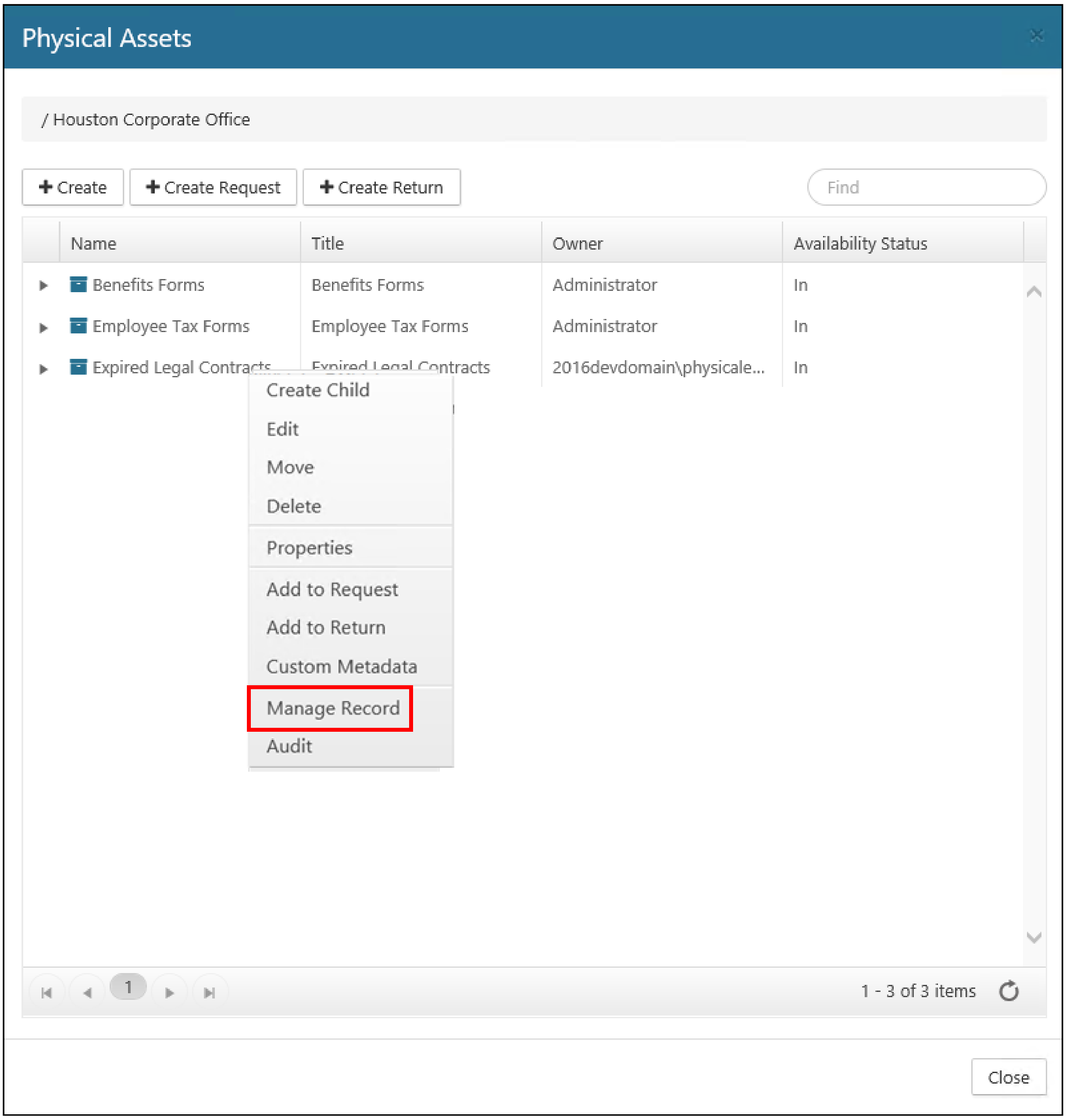
6. Click **Close** to close the dialog.

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 214) 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.

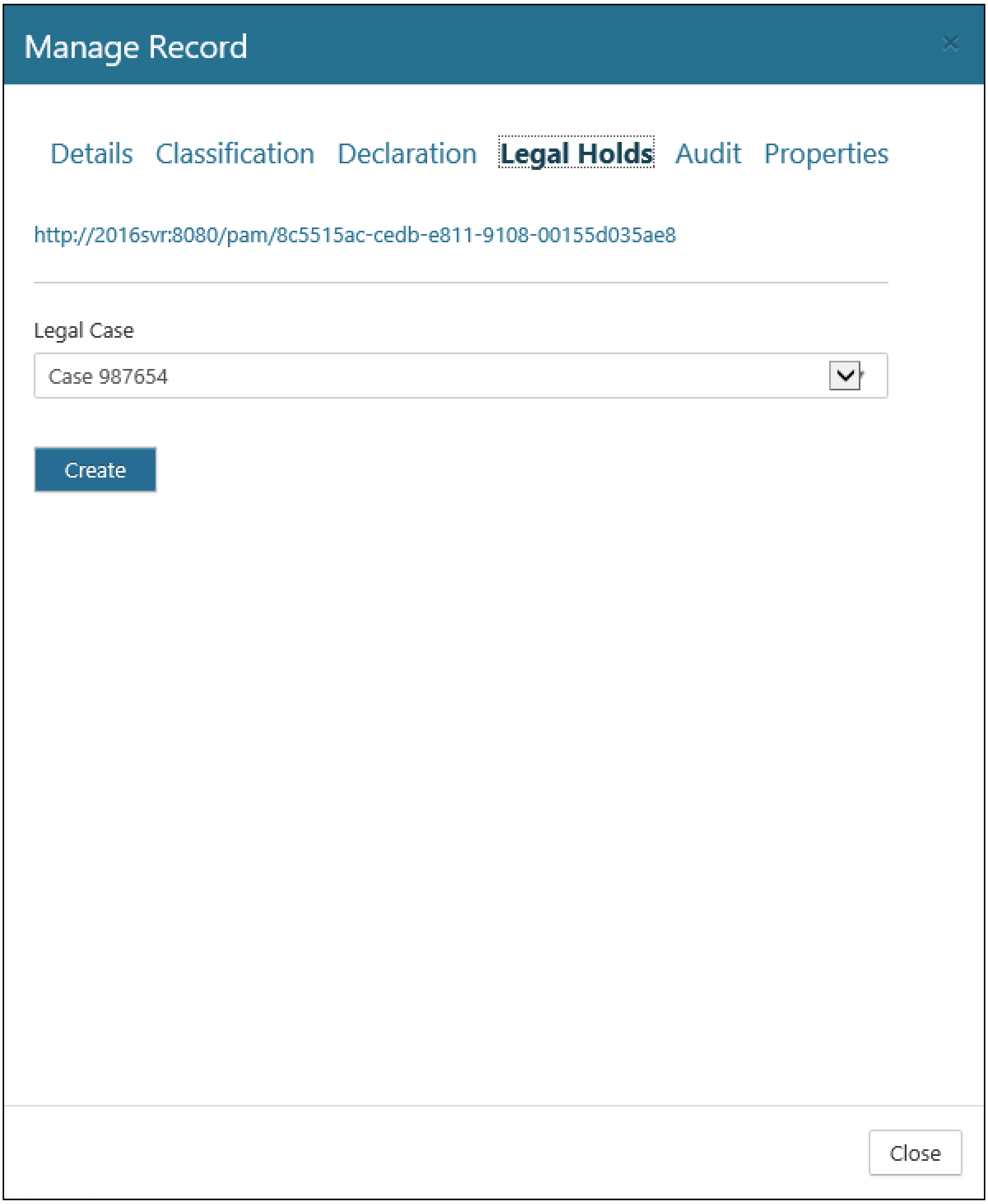


/ Houston Corporate Office

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

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**.



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

Legal Case: Case 987654

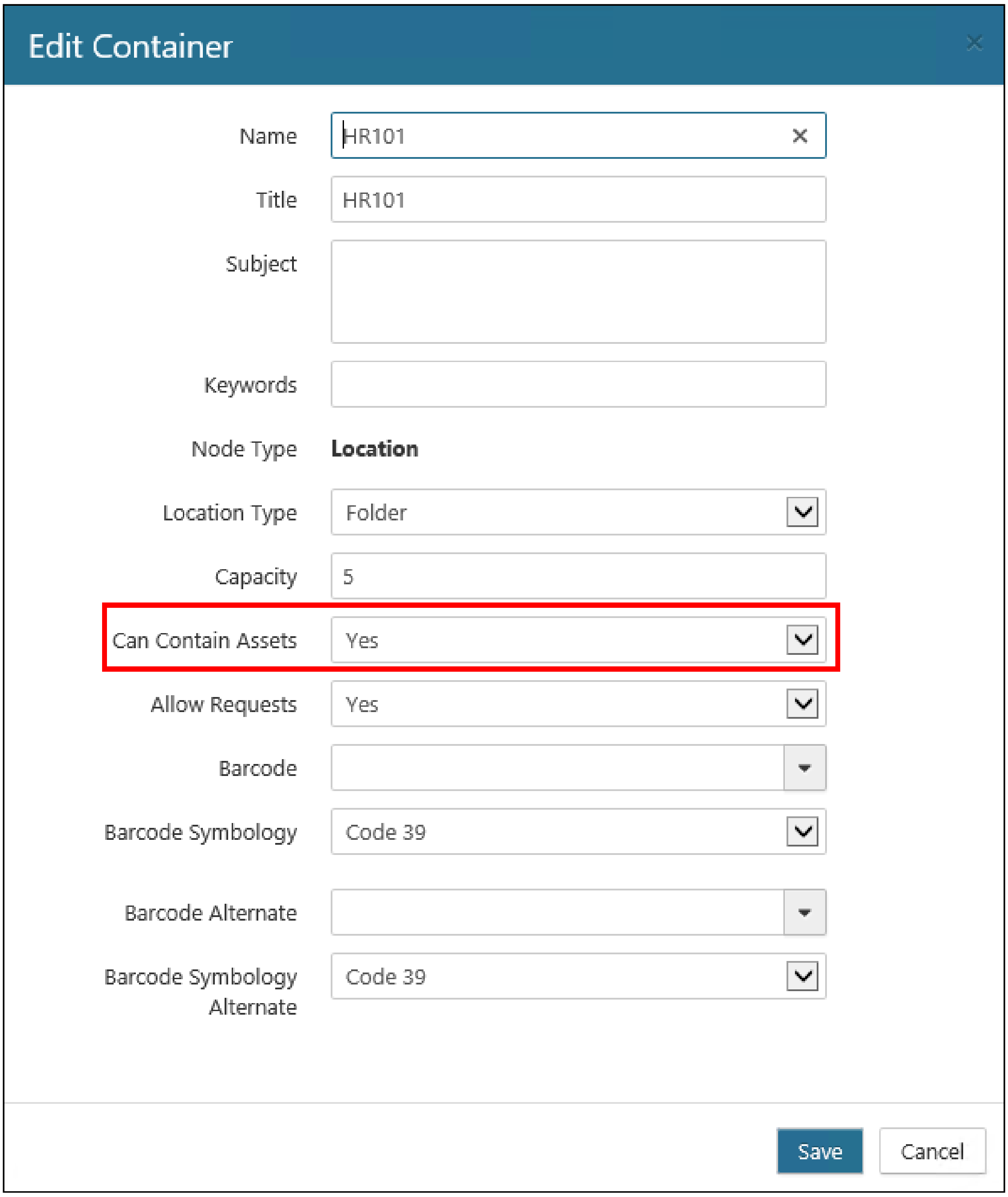
5.13.9.10 Creating Physical Assets

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.

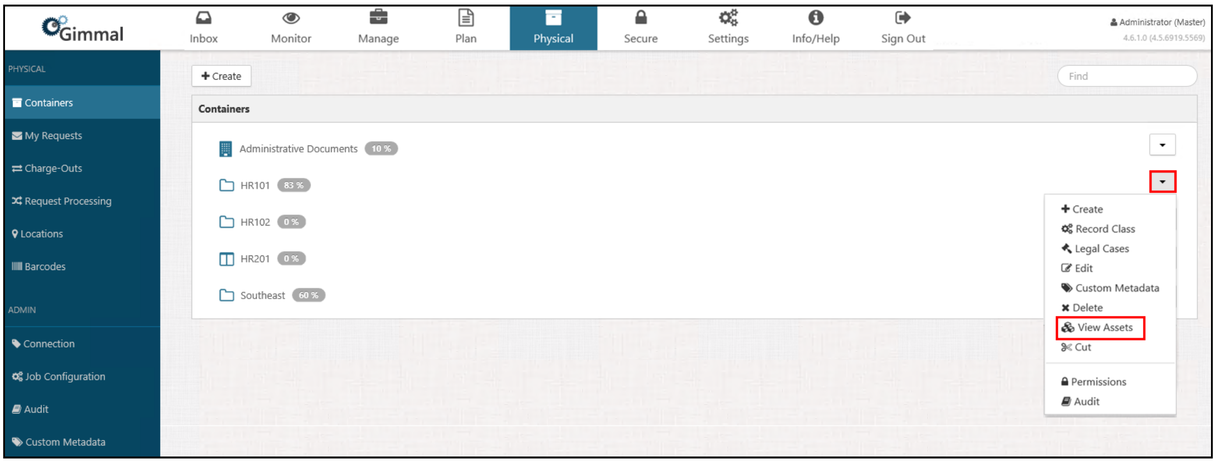


Edit Container

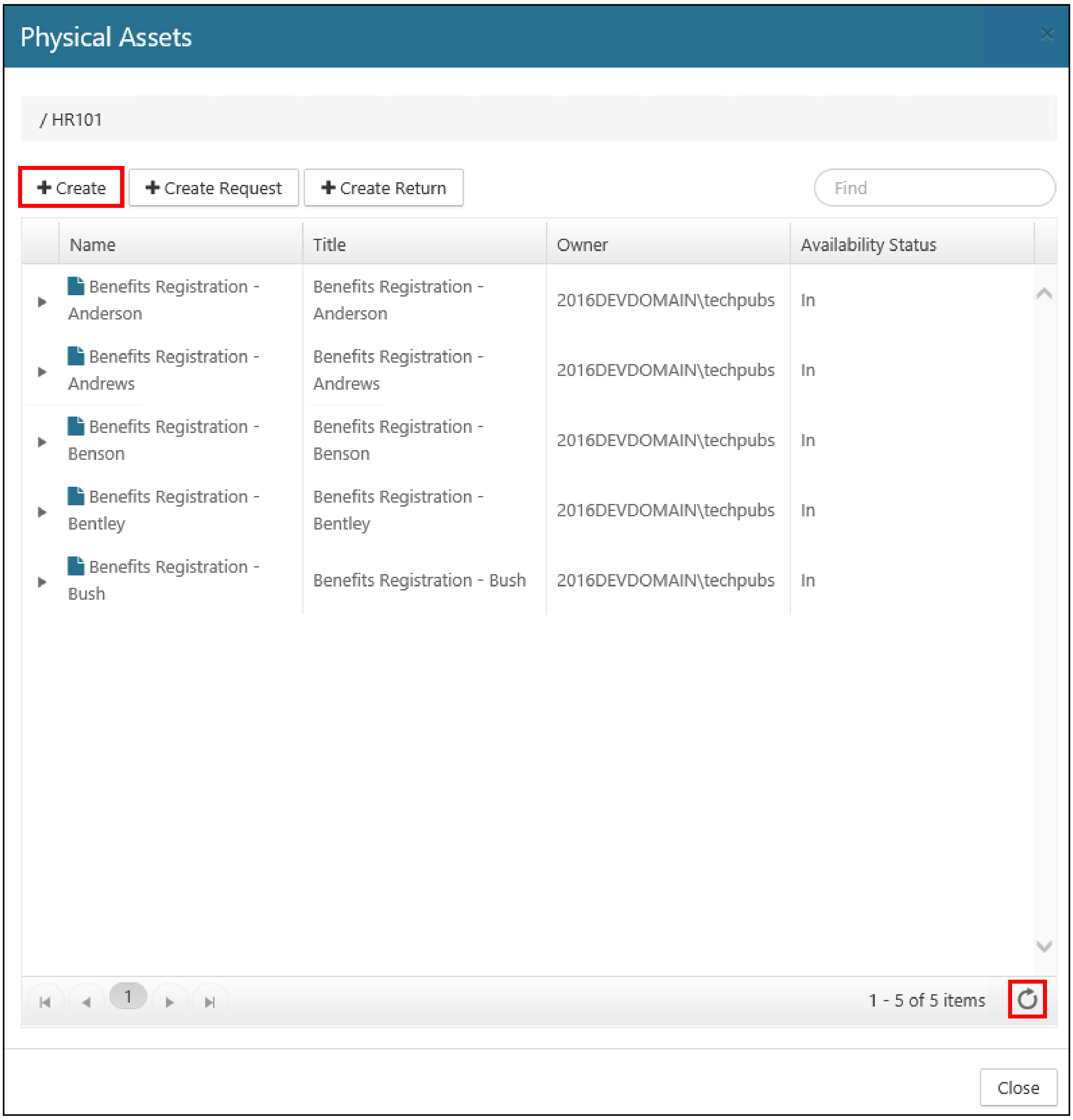
Name	HR101
Title	HR101
Subject	
Keywords	
Node Type	**Location**
Location Type	Folder
Capacity	5
Can Contain Assets	Yes
Allow Requests	Yes
Barcode	
Barcode Symbology	Code 39
Barcode Alternate	
Barcode Symbology Alternate	Code 39

- 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.



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

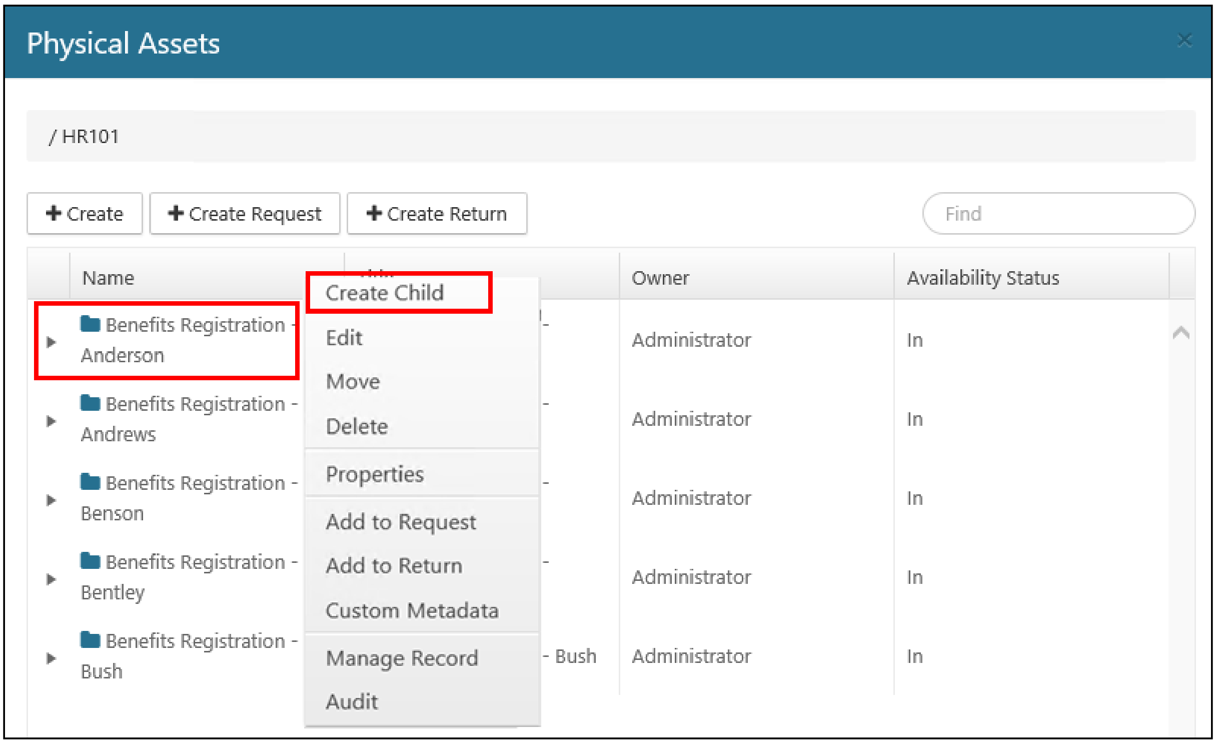
⚠ If the asset you are expecting is not displayed, click the refresh icon on the lower right of the window.

4. Click **+Create**. The Create Asset dialog opens.
5. Enter the asset properties(see page 176).
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.

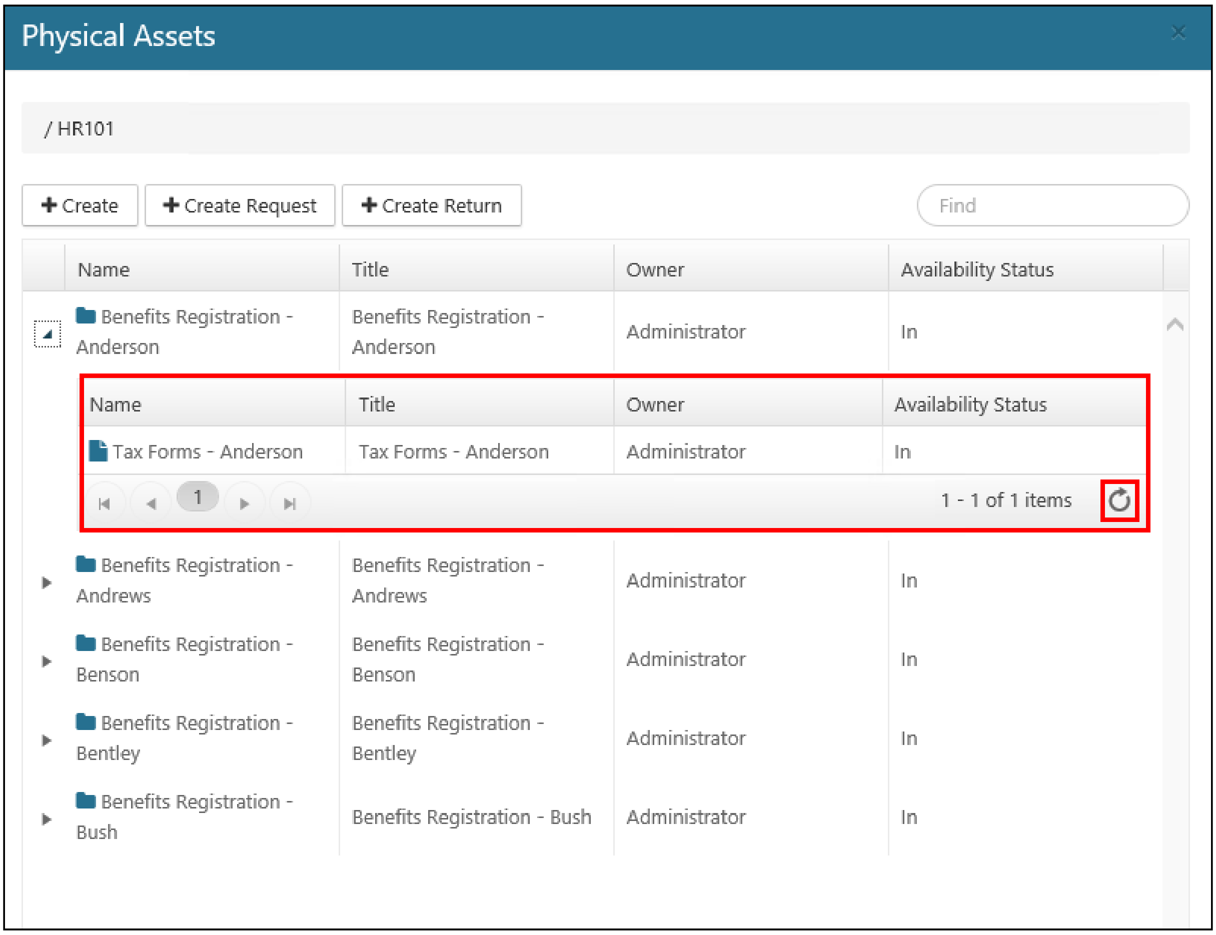


Name		Owner	Availability Status
Benefits Registration - Anderson	-	Administrator	In
Benefits Registration - Andrews	-	Administrator	In
Benefits Registration - Benson	-	Administrator	In
Benefits Registration - Bentley	-	Administrator	In
Benefits Registration - Bush	- Bush	Administrator	In

4. Enter the asset properties[29]. (The **Name (unique)**, **Home Location**, **Asset Type**, **Format**, and **Owner** fields are required.)

[29] http://docs.gimmal.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.



Name	Title	Owner	Availability Status
Benefits Registration - Anderson	Benefits Registration - 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

Name	Title	Owner	Availability Status
Tax Forms - Anderson	Tax Forms - Anderson	Administrator	In

5.13.9.11 Modifying Existing Assets

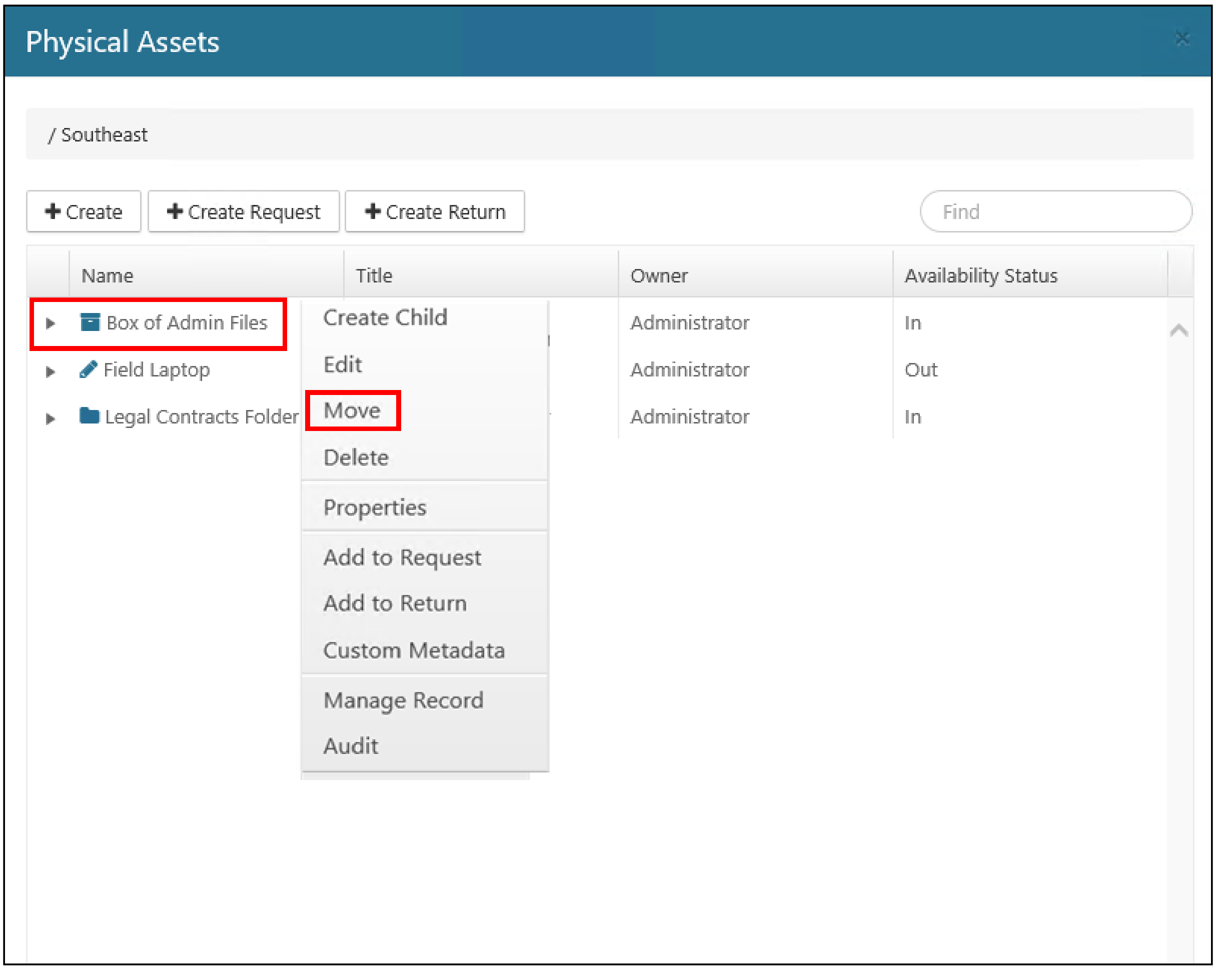
Moving an Asset

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.

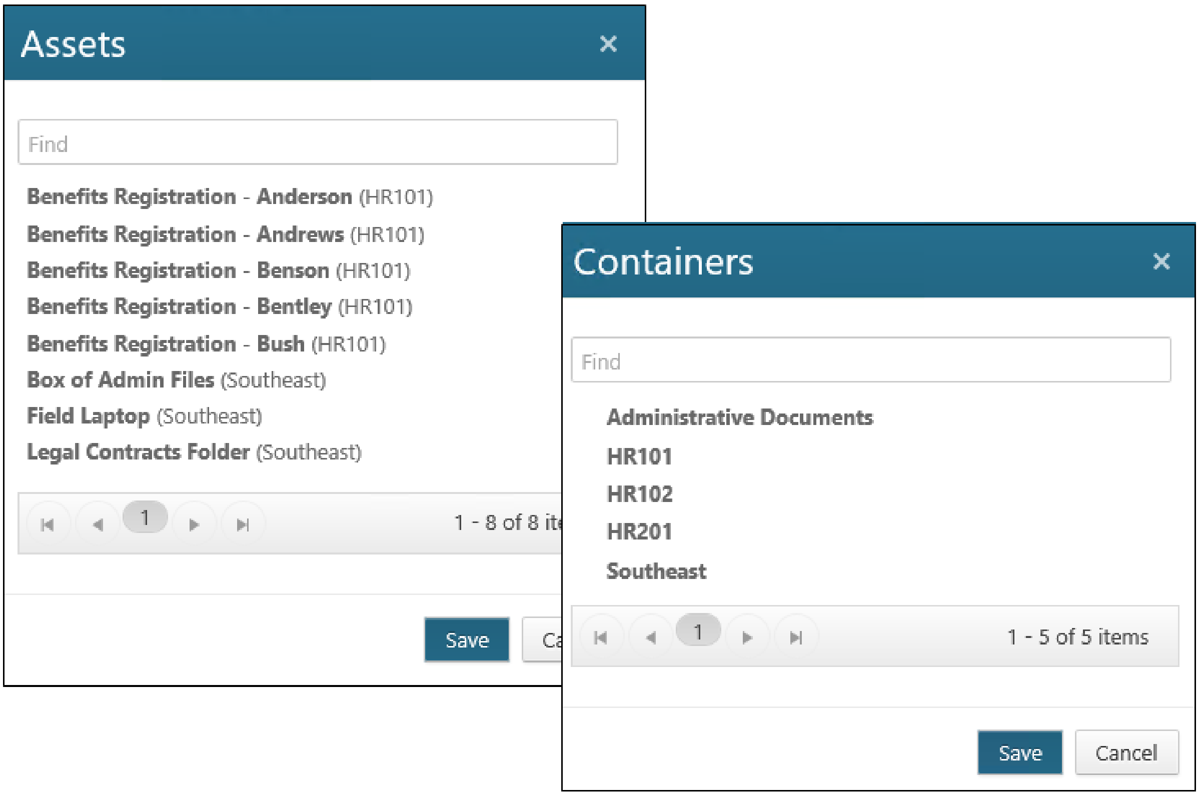
To move a physical asset, perform the following steps:

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**.



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

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.



Assets

Find

Benefits Registration - Anderson (HR101)
Benefits Registration - Andrews (HR101)
Benefits Registration - Benson (HR101)
Benefits Registration - Bentley (HR101)
Benefits Registration - Bush (HR101)
Box of Admin Files (Southeast)
Field Laptop (Southeast)
Legal Contracts Folder (Southeast)

Containers

Find

Administrative Documents
HR101
HR102
HR201
Southeast

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.

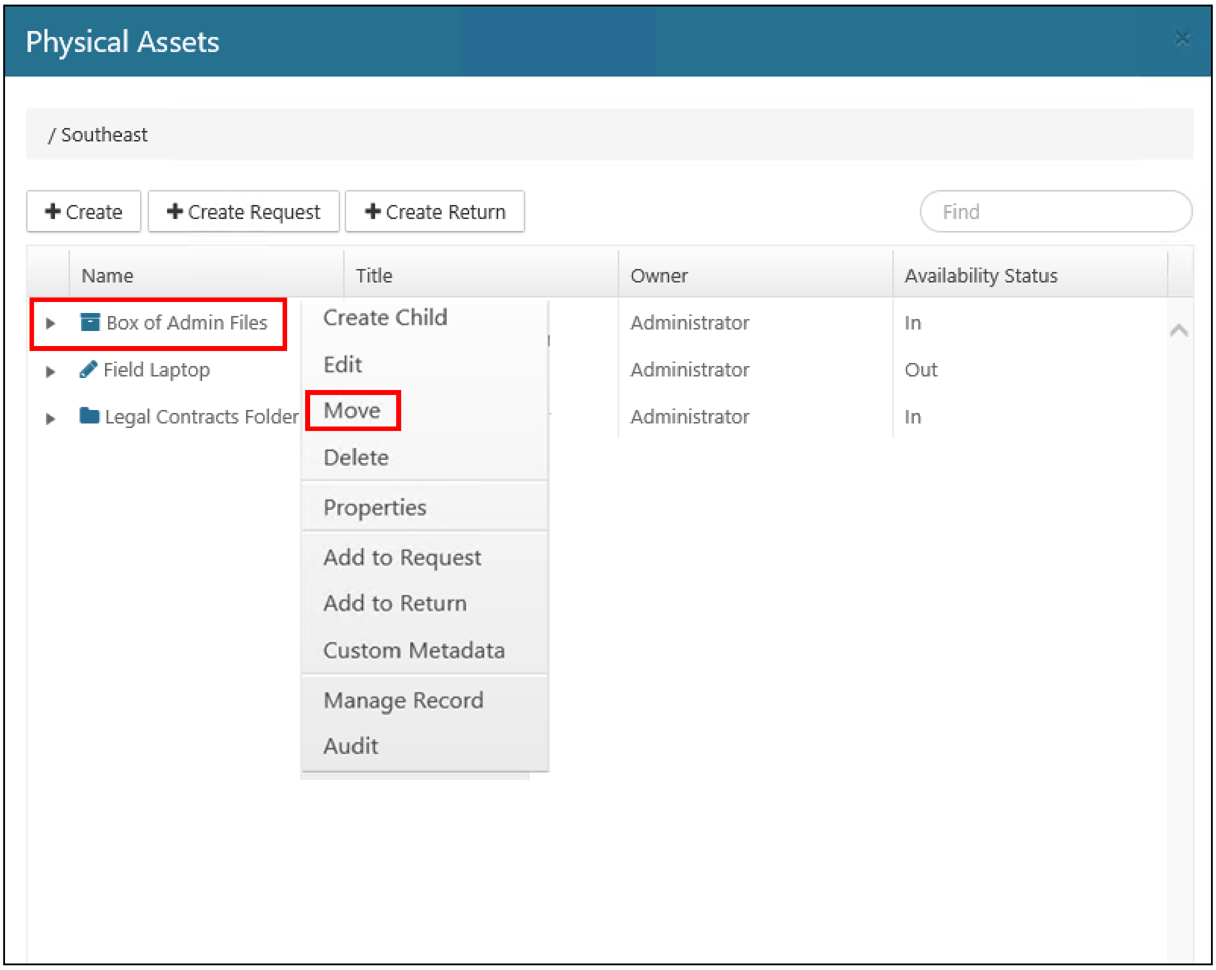
Editing & Deleting an Asset

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.



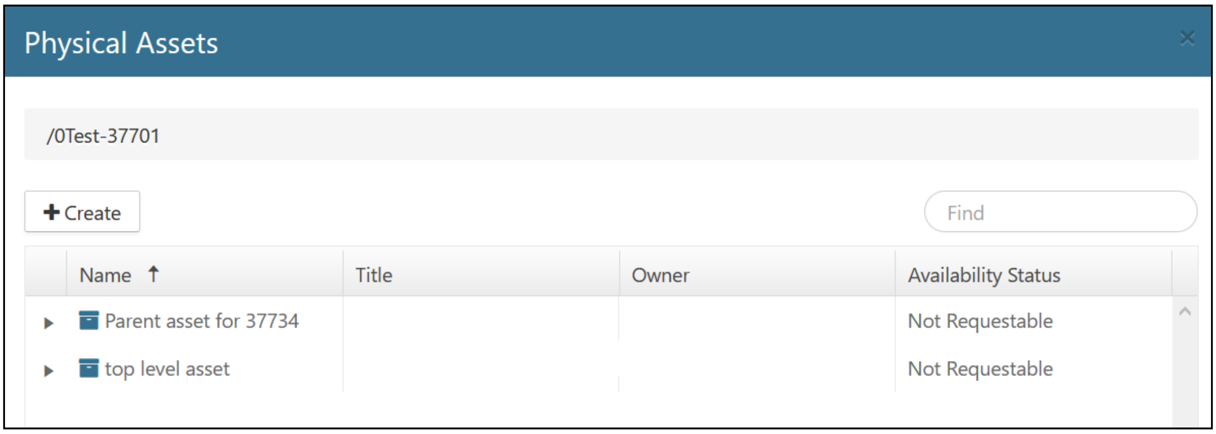
Name	Title	Owner	Availability Status
Box of Admin Files		Administrator	In
Field Laptop		Administrator	Out
Legal Contracts Folder		Administrator	In

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 176) 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.

5.13.9.12 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.



Physical Assets

/0Test-37701

Name	Title	Owner	Availability Status
Parent asset for 37734			Not Requestable
top level asset			Not Requestable

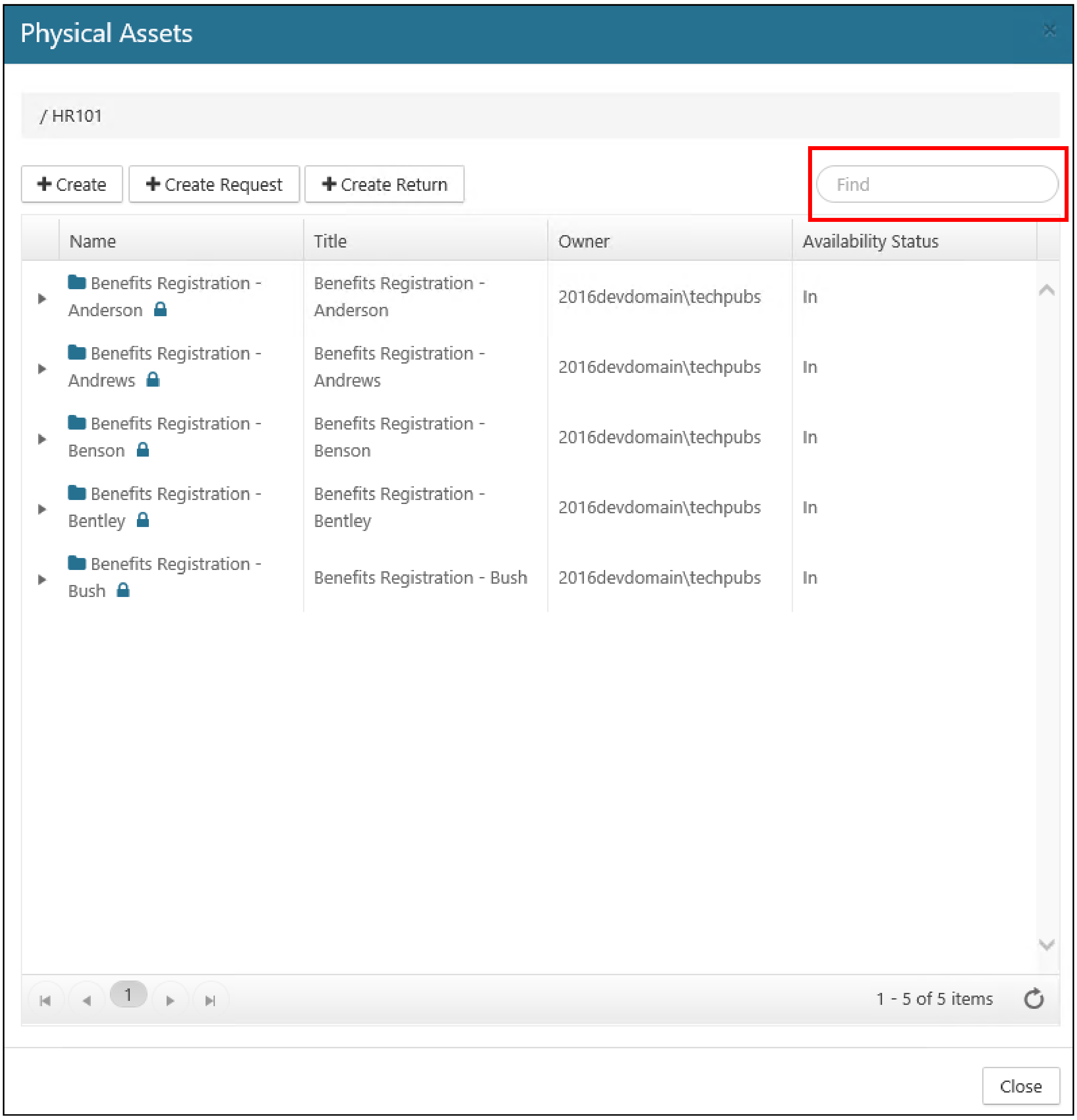
4. Right-click on the physical asset you want to copy, and select Copy.
5. The Copy Asset window opens, which lists the name of the asset you want to copy, and lets you select whether to copy it to a parent container or a parent asset.
6. From the Copy to drop-down list, select Container or Asset.
7. 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.

5.13.9.13 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.



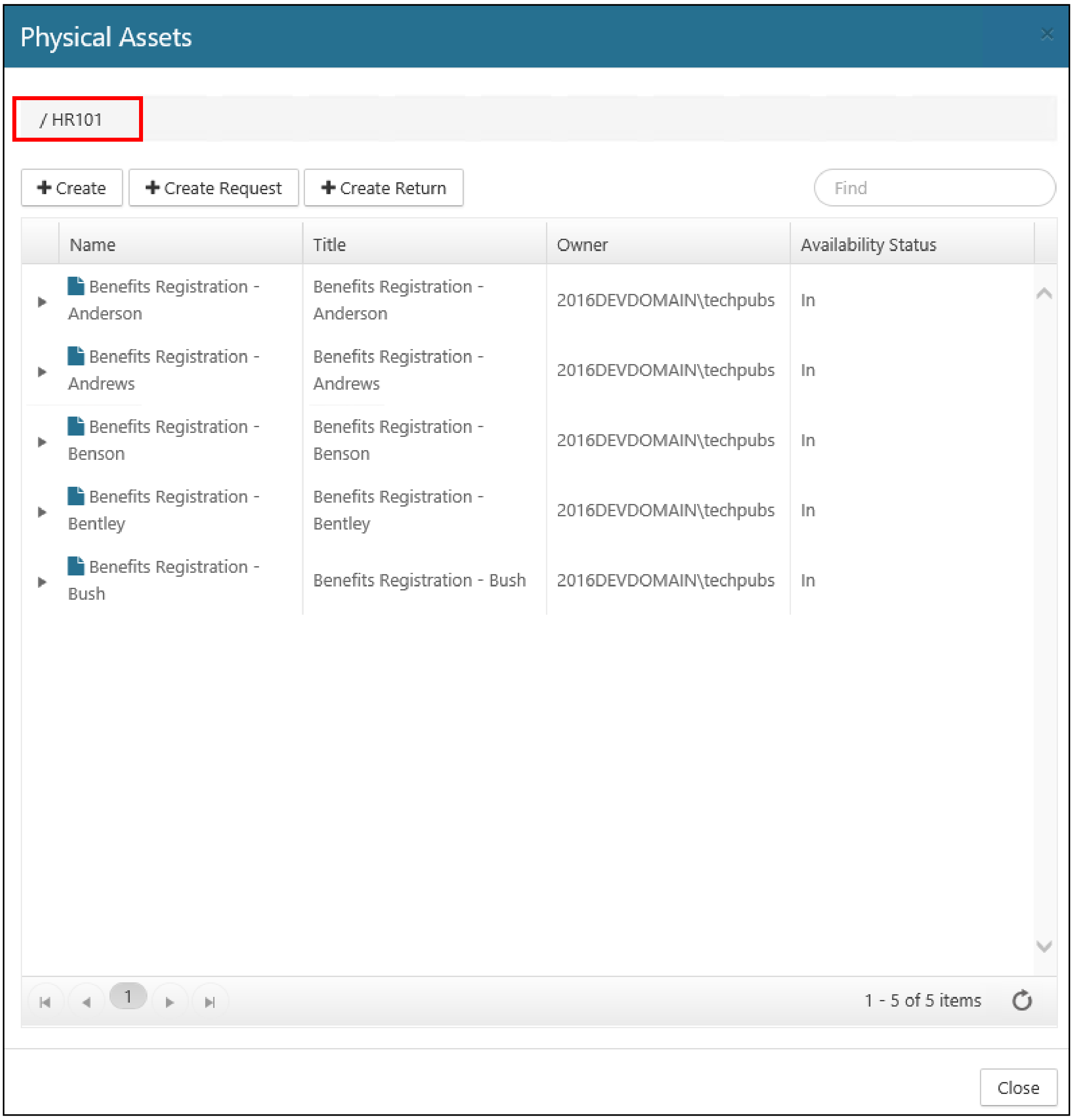
Name	Title	Owner	Availability Status
Benefits Registration - Anderson	Benefits Registration - Anderson	2016devdomain\techpubs	In
Benefits Registration - Andrews	Benefits Registration - Andrews	2016devdomain\techpubs	In
Benefits Registration - Benson	Benefits Registration - Benson	2016devdomain\techpubs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

5.13.9.14 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.

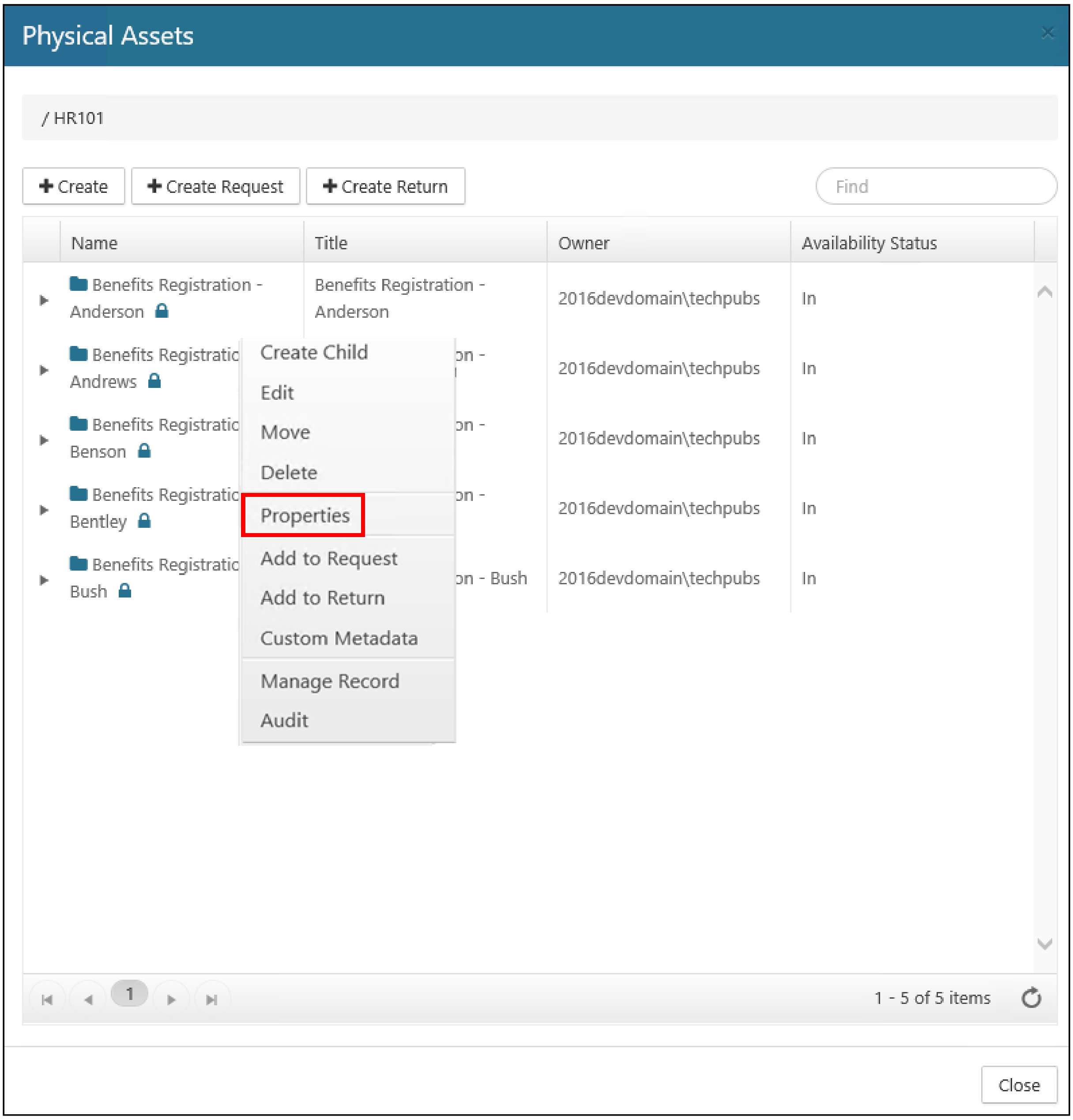


Name	Title	Owner	Availability Status
Benefits Registration - Anderson	Benefits Registration - Anderson	2016DEVDOMAIN\techpubs	In
Benefits Registration - Andrews	Benefits Registration - Andrews	2016DEVDOMAIN\techpubs	In
Benefits Registration - Benson	Benefits Registration - Benson	2016DEVDOMAIN\techpubs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



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

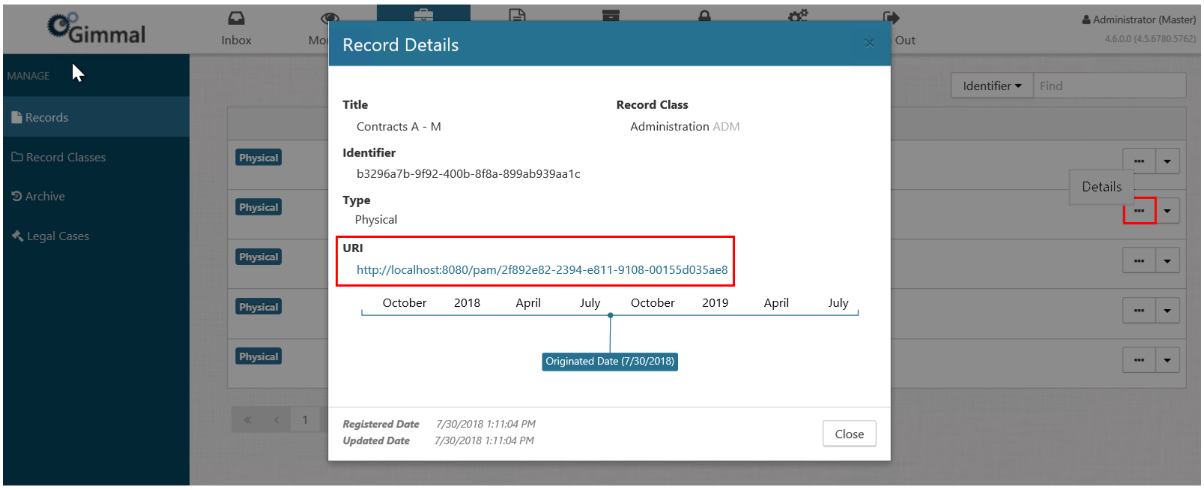
Viewing Asset Record Details

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.



Record Details

Title
Contracts A - M

Record Class
Administration ADM

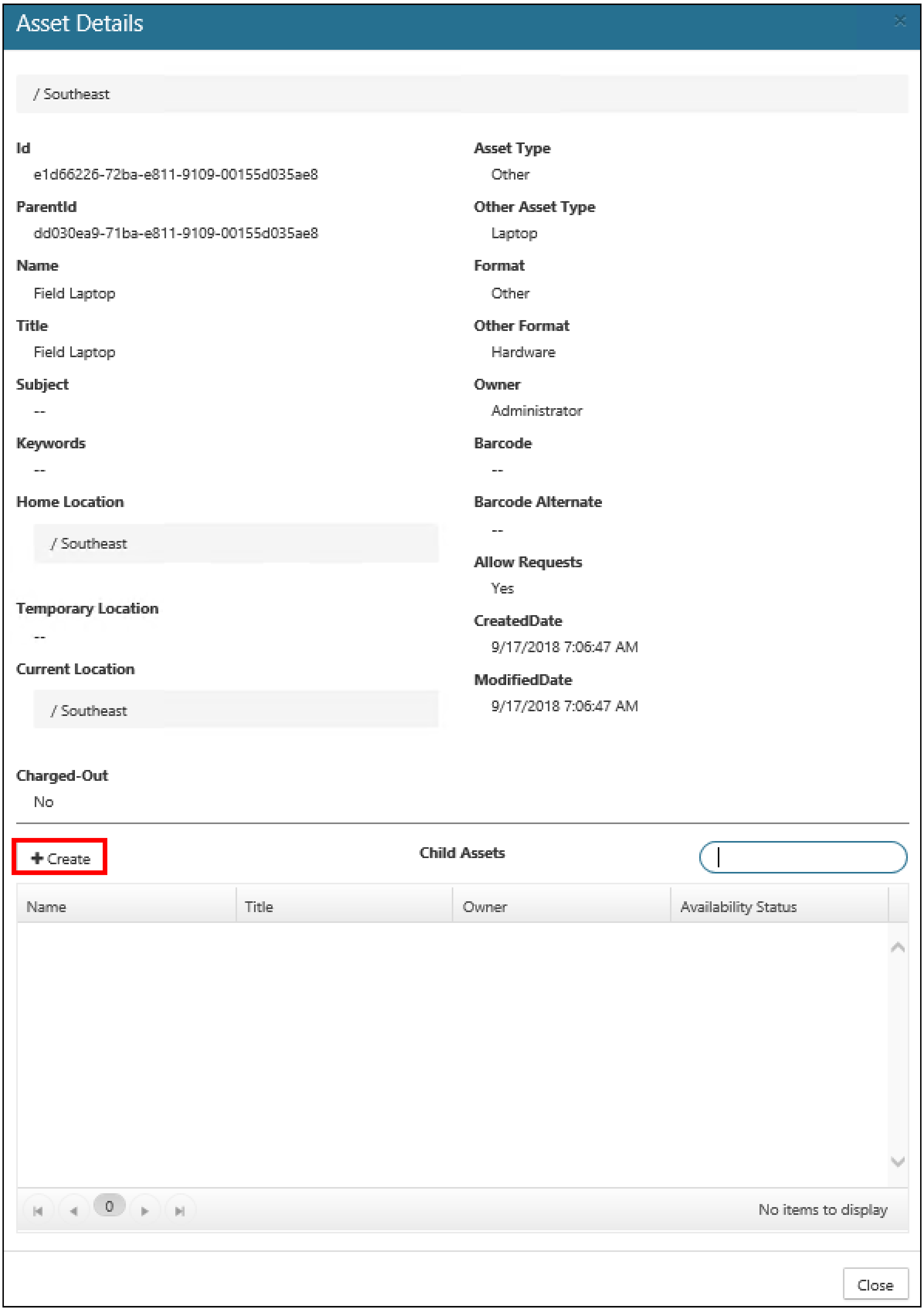
Identifier
b3296a7b-9f92-400b-8f8a-899ab939aa1c

Type
Physical

URI
http://localhost:8080/pam/2f892e82-2394-e811-9108-00155d035ae8

Registered Date 7/30/2018 1:11:04 PM
Updated Date 7/30/2018 1:11:04 PM

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



Asset Details

/ Southeast

Id
e1d66226-72ba-e811-9109-00155d035ae8

ParentId
dd030ea9-71ba-e811-9109-00155d035ae8

Name
Field Laptop

Title
Field Laptop

Subject
--

Keywords
--

Home Location
/ Southeast

Temporary Location
--

Current Location
/ Southeast

Charged-Out
No

Asset Type
Other

Other Asset Type
Laptop

Format
Other

Other Format
Hardware

Owner
Administrator

Barcode
--

Barcode Alternate
--

Allow Requests
Yes

CreatedDate
9/17/2018 7:06:47 AM

ModifiedDate
9/17/2018 7:06:47 AM

Child Assets

Name	Title	Owner	Availability Status

5. If you choose to add additional child assets, click the **+Create** button, and perform the steps described in Creating a Child Asset(see page 184). (Physical Users must have container permissions set to **Edit** or higher on this container to create additional child assets.)

5.13.10 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.

5.13.10.1 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

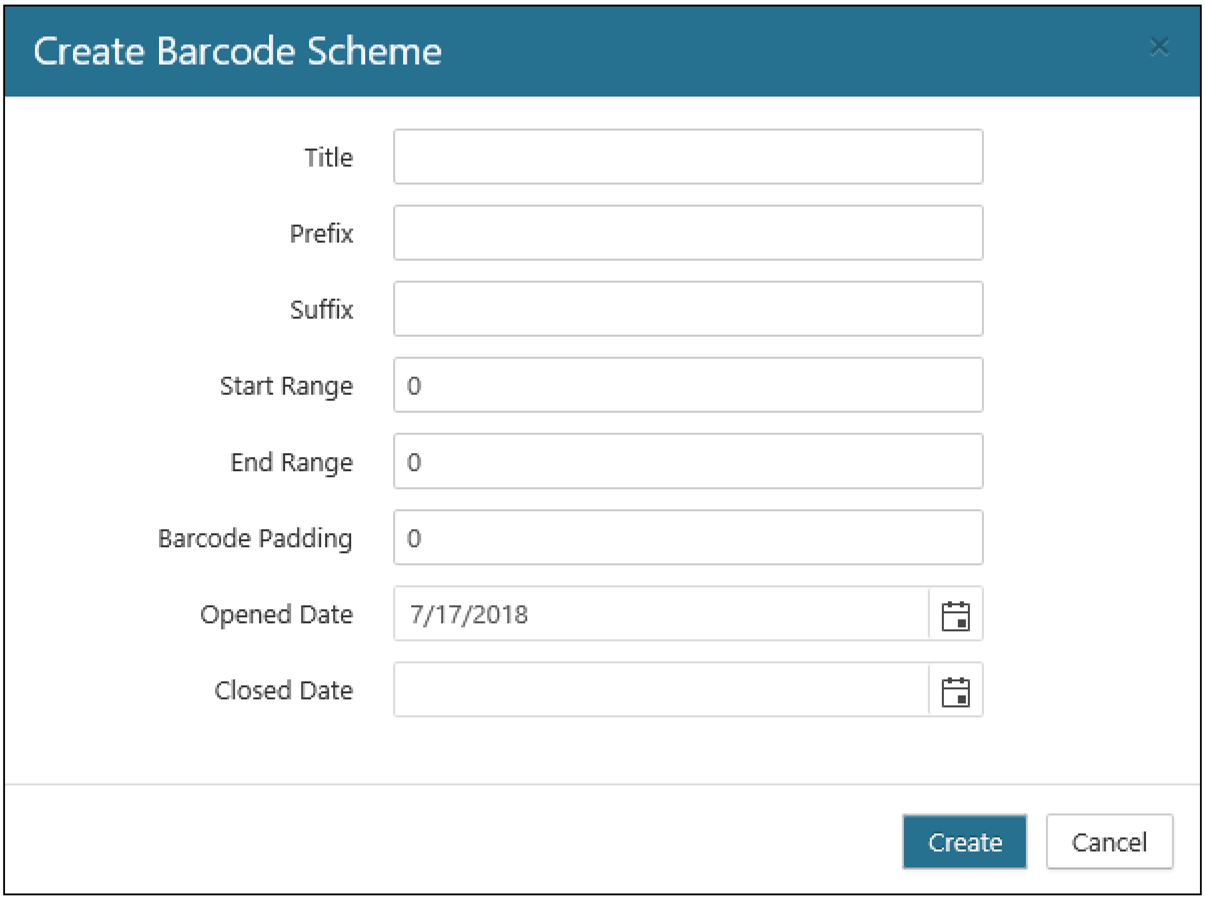
5.13.10.2 Barcode Uniqueness

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.

5.13.10.3 Creating a New Barcode Scheme

1. 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: 0

End Range: 0

Barcode Padding: 0

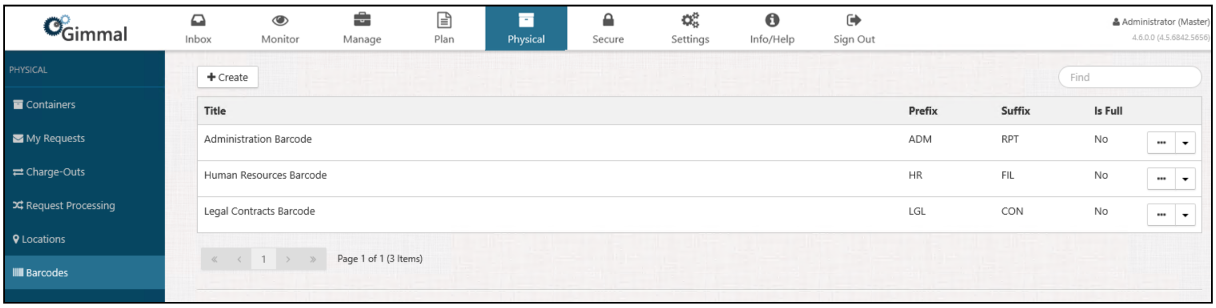
Opened Date: 7/17/2018

Closed Date

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)

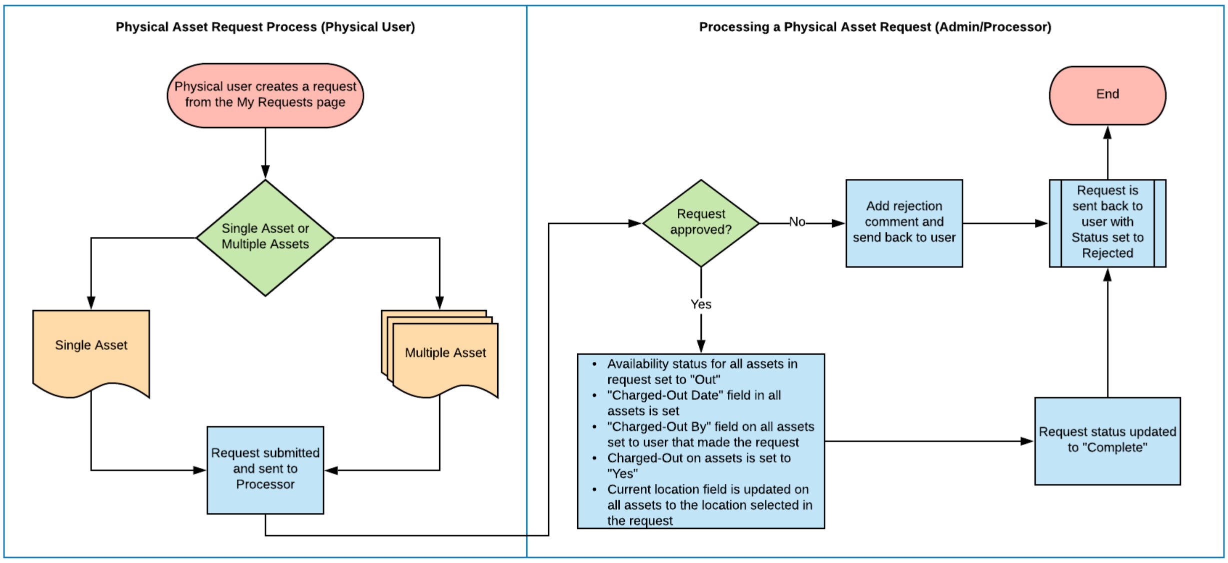
5.13.10.4 Editing or Deleting Barcode Scheme

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.

5.13.11 Request and Returns

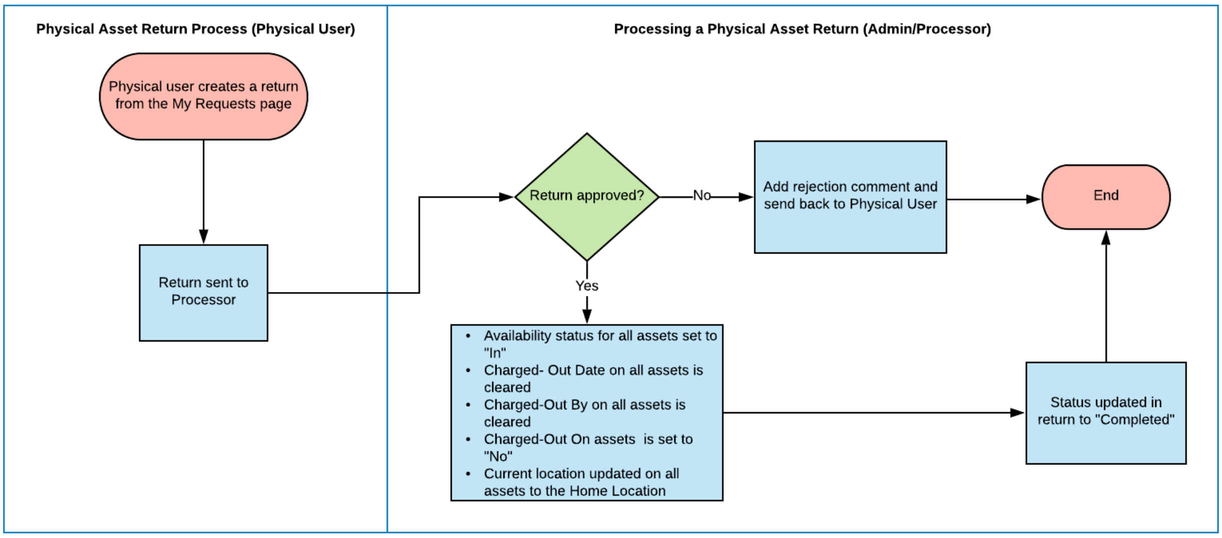
The Physical Administrator is responsible for processing the requests and returns that have been submitted by the Physical User. The following flowchart illustrates the physical asset request/charge-out process, and the flowchart below illustrates the physical asset return/charge-in process. See the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

5.13.11.1 Processing Request



Physical Asset Request Process (Physical User)
Processing a Physical Asset Request (Admin/Processor)
Physical user creates a request from the My Requests page
Single Asset or Multiple Assets
Single Asset
Multiple Asset
Request submitted and sent to Processor
Request approved?
No
Yes
Add rejection comment and send back to user
Request is sent back to user with Status set to Rejected
End
• Availability status for all assets in request set to "Out"
• "Charged-Out Date" field in all assets is set
• "Charged-Out By" field on all assets set to user that made the request
• Charged-Out on assets is set to "Yes"
• Current location field is updated on all assets to the location selected in the request
Request status updated to "Complete"

5.13.11.2 Processing Return


Physical Asset Return Process (Physical User)
Processing a Physical Asset Return (Admin/Processor)
Physical user creates a return from the My Requests page
Return sent to Processor
Return approved?
No
Add rejection comment and send back to Physical User
End
Yes
• Availability status for all assets set to "In"
• Charged- Out Date on all assets is cleared
• Charged-Out By on all assets is cleared
• Charged-Out On assets is set to "No"
• Current location updated on all assets to the Home Location
Status updated in return to "Completed"

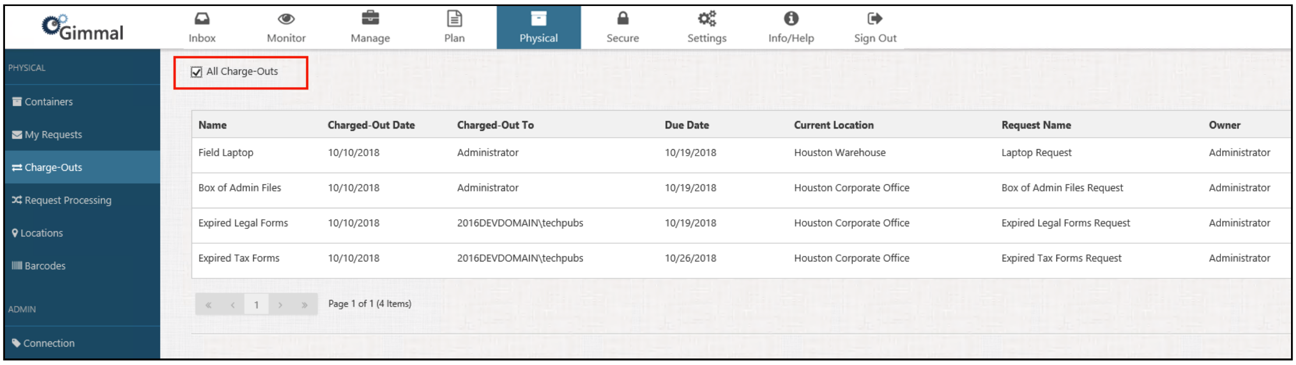
5.13.11.3 Managing All Charge-Outs

Managing charge-outs is generally covered in the Managing Charge-Outs(see page 87) 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.



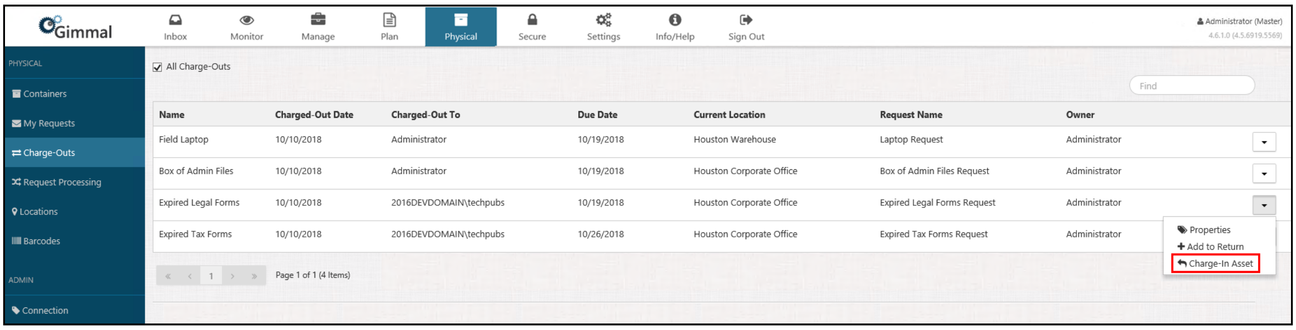
☑ All Charge-Outs

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

« ‹ 1 › » Page 1 of 1 (4 Items)

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.



☑ All Charge-Outs

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

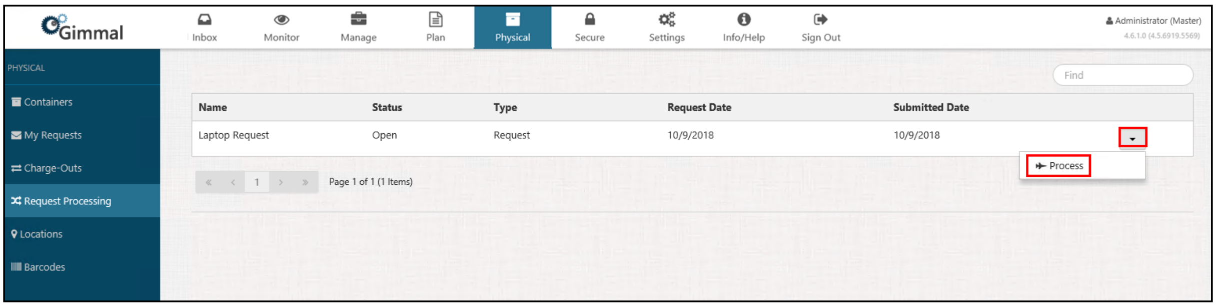
Page 1 of 1 (4 Items)

5.13.11.4 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

Page 1 of 1 (1 Items)

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.

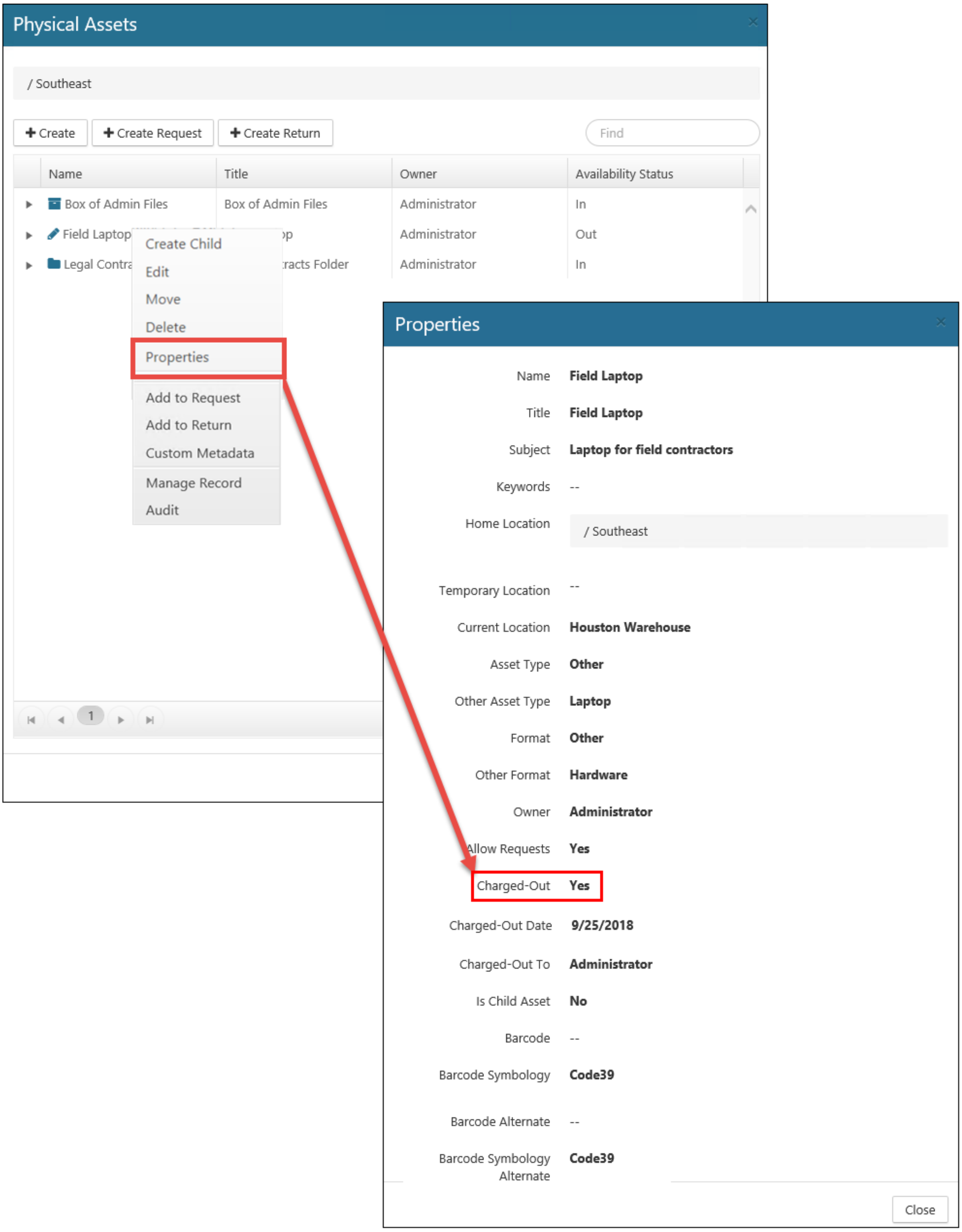
3. Determine if you will approve or reject the request by performing either of the following steps:
   - To approve the return, click **Approve**. The process starts to run and the request disappears from the Return Processing page. As soon as the Return Processor job is complete, the return reappears 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".



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

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

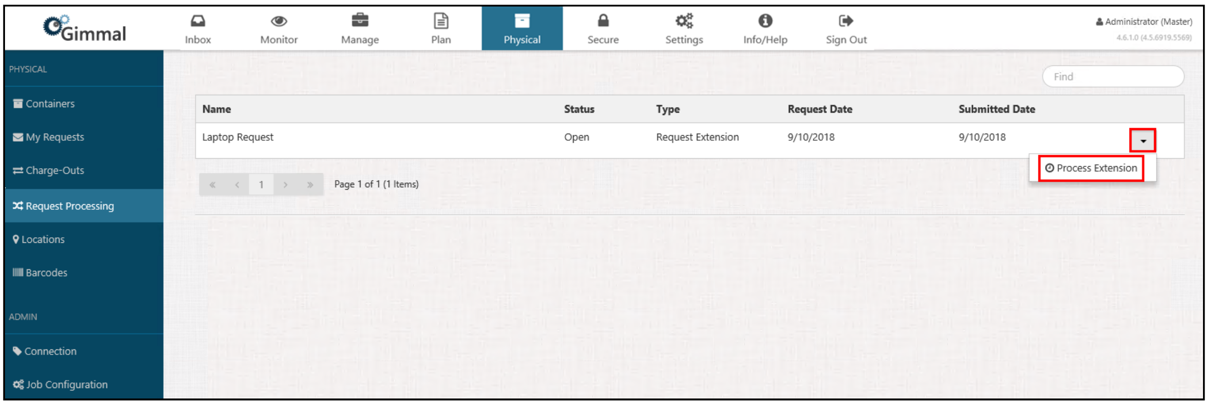
5.13.11.5 Processing a Request Extension

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.

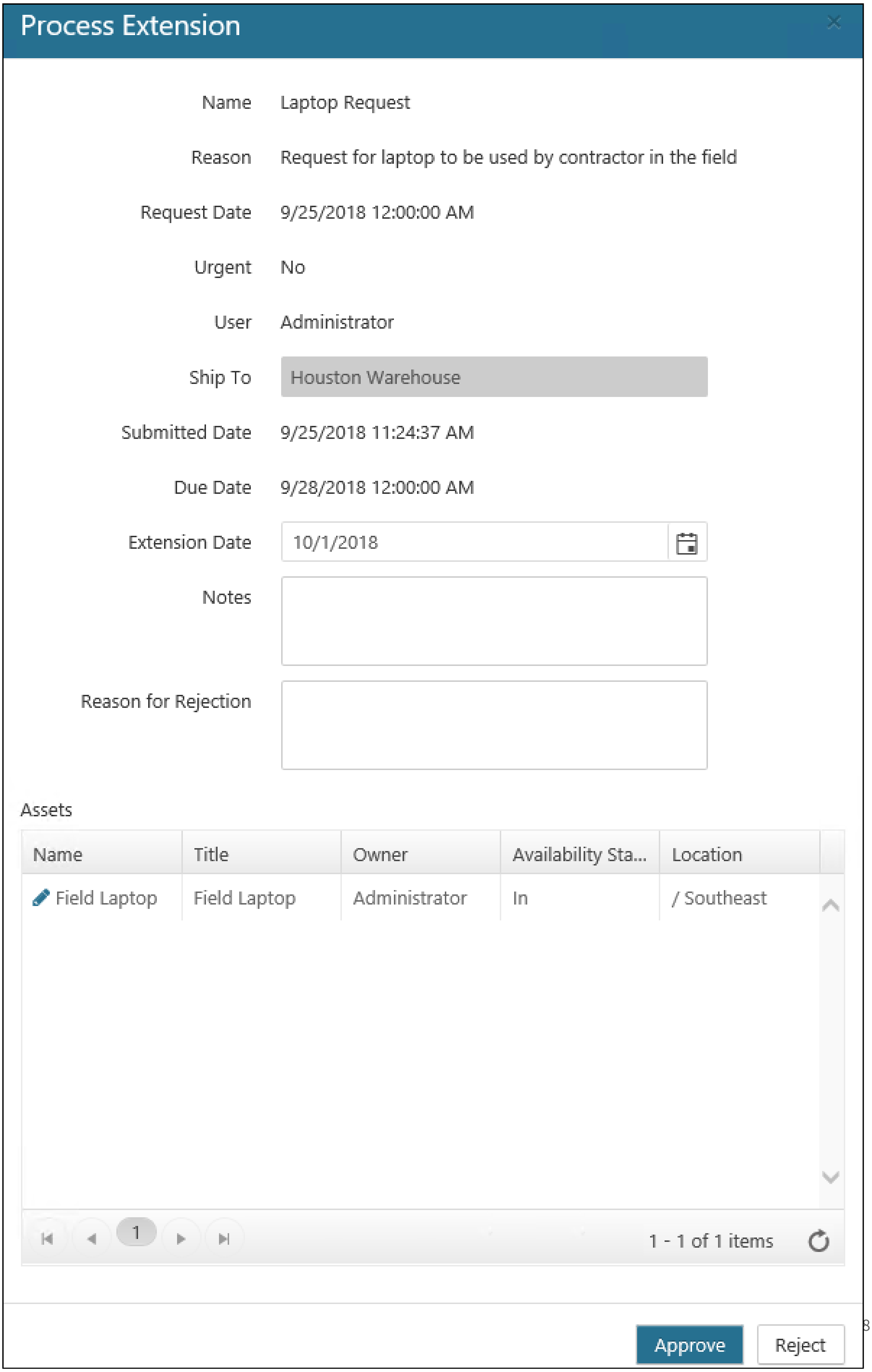
To process the request extension, perform the following steps:

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.



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

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	10/1/2018
Notes	
Reason for Rejection	

Assets

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

1 - 1 of 1 items

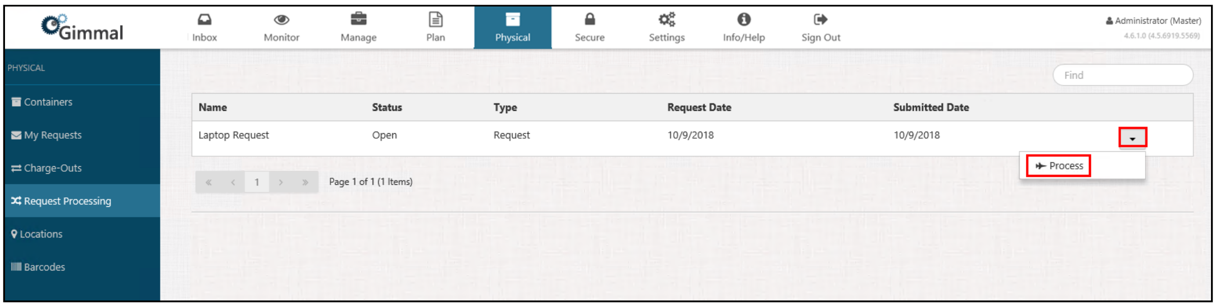
The Process Extension dialog opens, showing the properties associated with the request, as well as the physical asset that was initially requested (under the Assets section). Note that you can right-click on the asset to view its properties.

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.

5.13.11.6 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**.



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

Page 1 of 1 (1 Items)

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

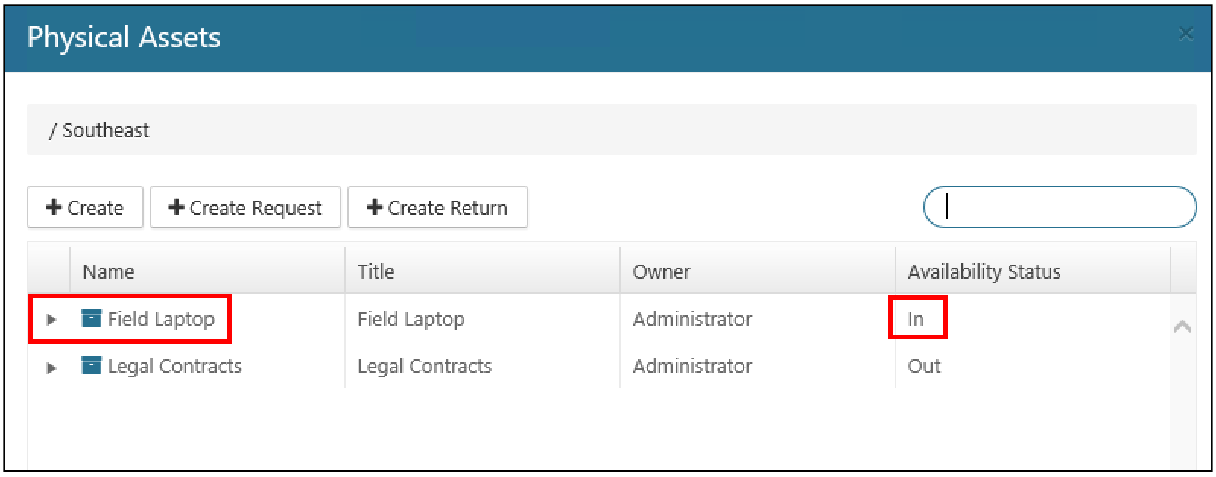
- The **Request Date** is the date the user wants the asset delivered to them.
- The **Due Date** is the date the asset needs to be returned by.
- The **Submitted Date** is the date the user submitted the request.

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:

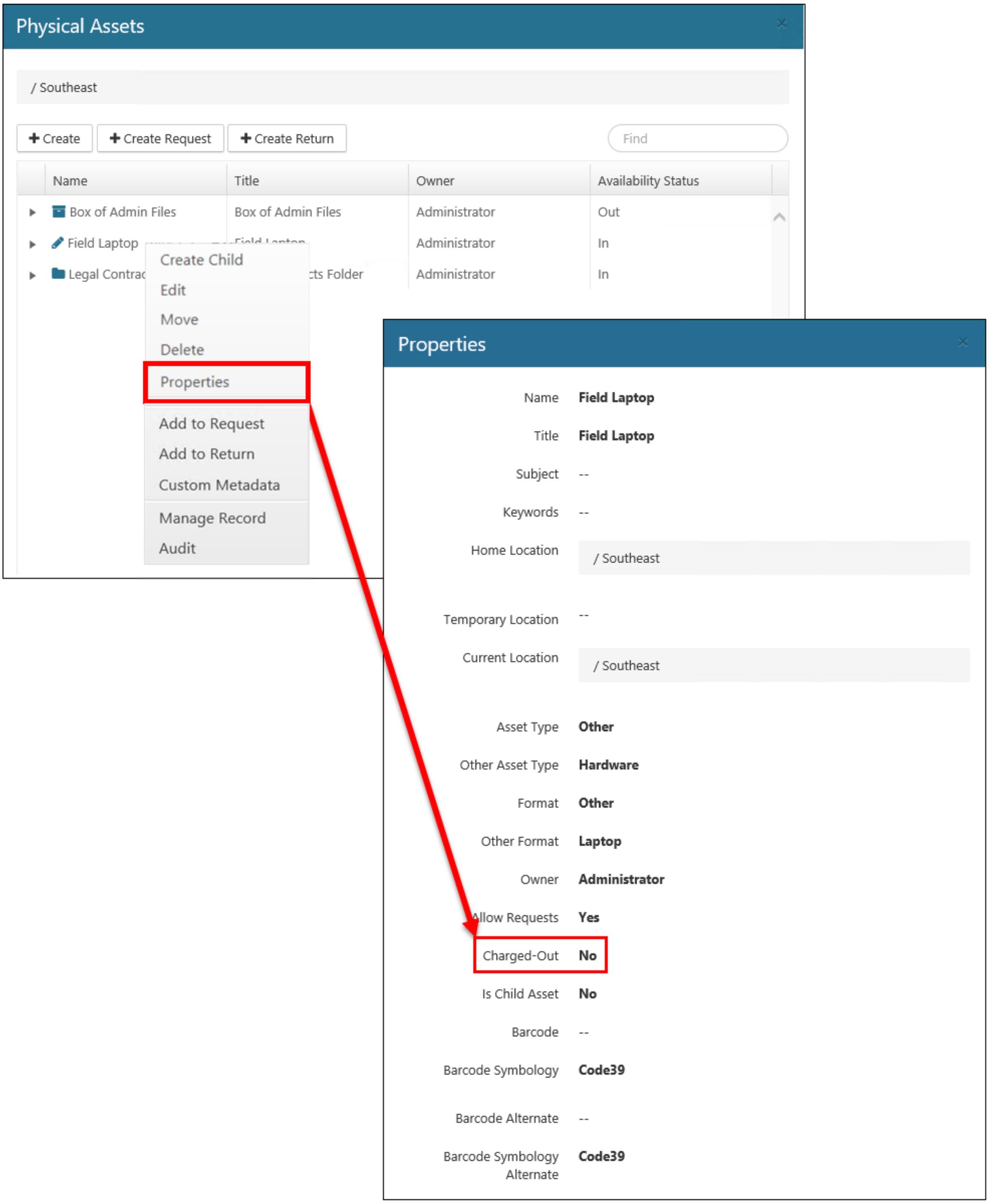
1. Navigate to the Physical Assets dialog from the container that is holding the asset that was requested.



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.)

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



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

Properties

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**

5.13.12 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.

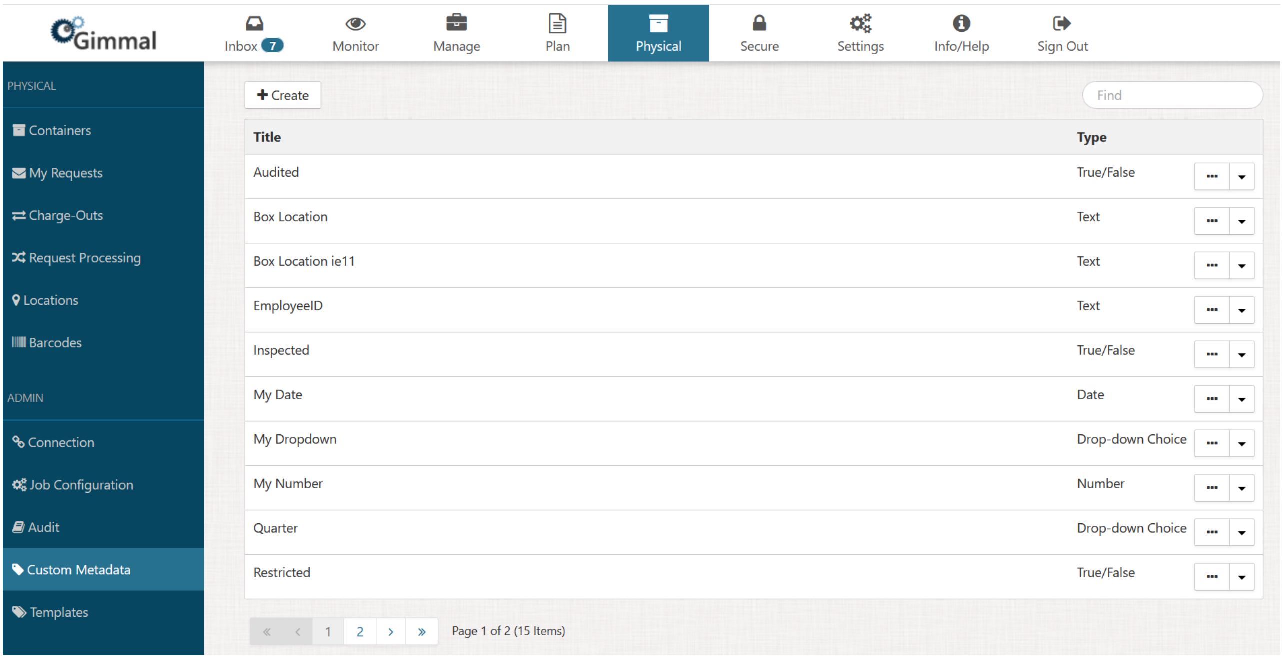
When associated with assets, the custom metadata will become part of the records and available for use in rules throughout the core Records Management product.

5.13.12.1 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

« ‹ 1 2 › » Page 1 of 2 (15 Items)

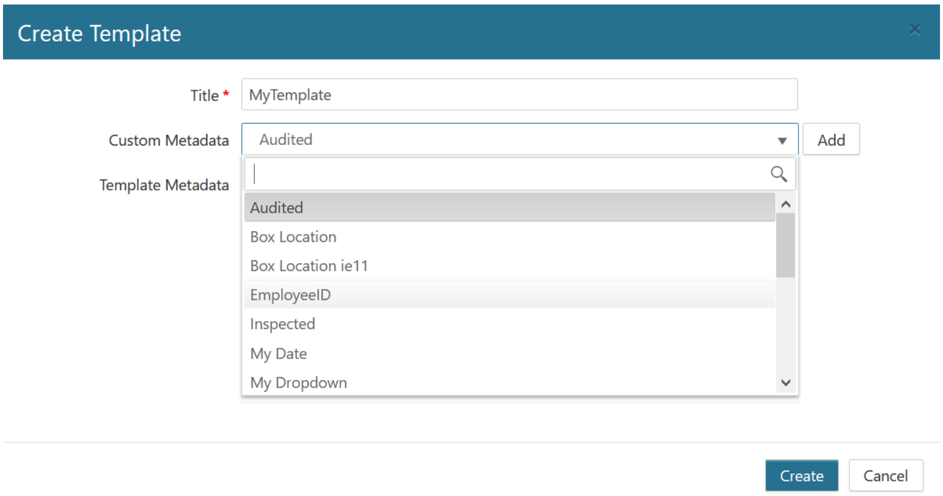
From here you can create new metadata by selecting +Create, or edit an existing property using the dropdown menu on the right side of any existing property.

5.13.12.2 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



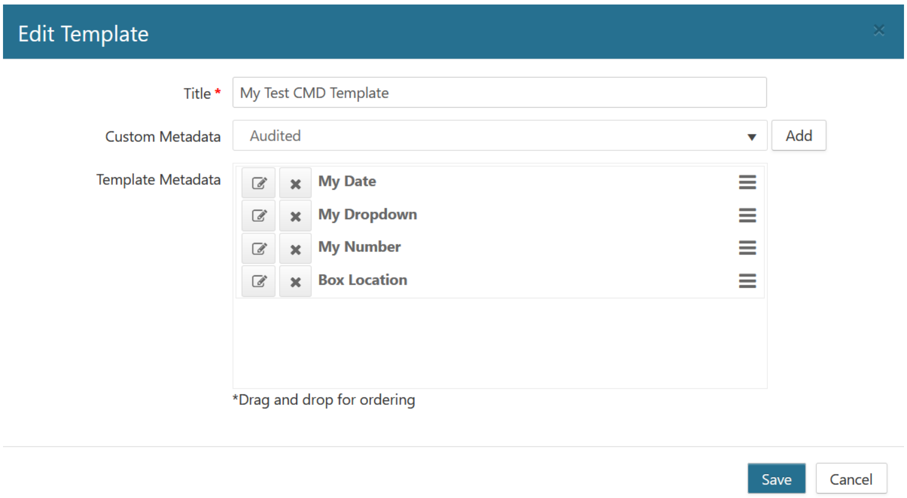
Create Template

Title * MyTemplate

Custom Metadata: Audited

Template Metadata

3. Remove or rearrange the properties as necessary



Edit Template

Title * My Test CMD Template

Custom Metadata: Audited

Template Metadata:
- My Date
- My Dropdown
- My Number
- Box Location

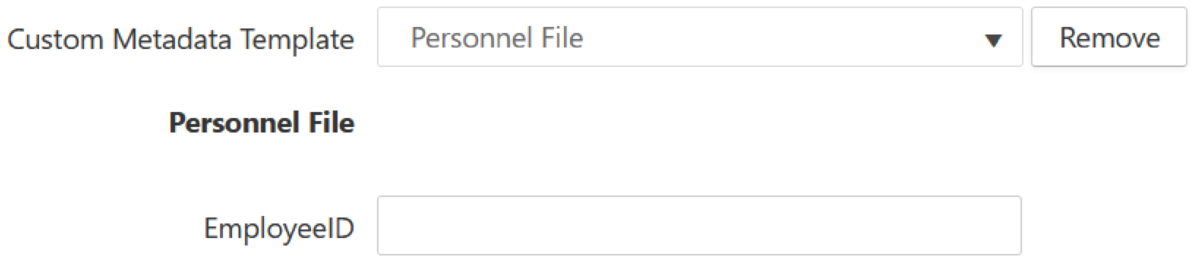
*Drag and drop for ordering

4. Click the **Create** button

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

5.13.12.3 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

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.

5.14 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.

5.14.1 Legal Case Properties

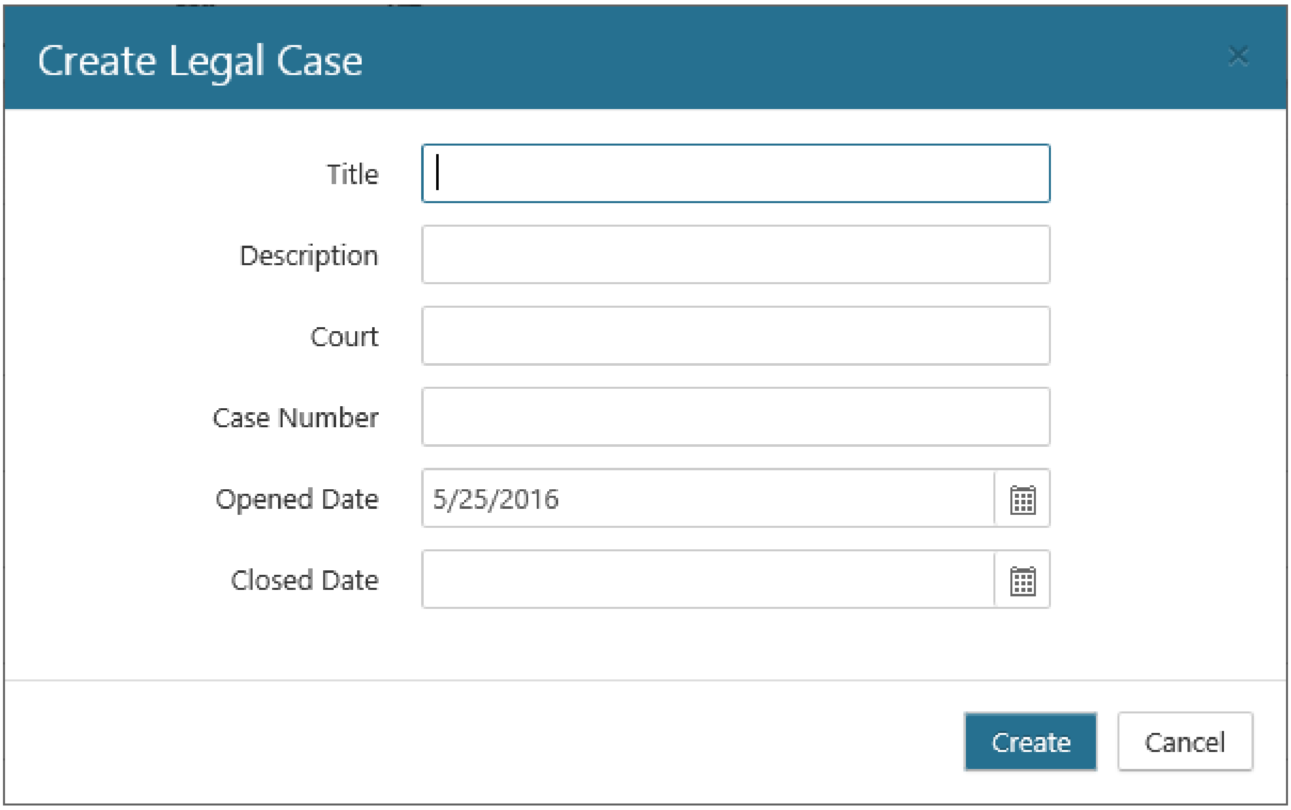
Property	Description
Title	Defines the unique name of the Legal Case
Description	Defines the description of the Legal Case for informational purposes
Court	Defines the Court who is seeing this Legal Case
Case Number	Defines the Case Number for the Legal Case
Opened Date	Defines the date the Legal Case 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.

5.14.2 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

5.14.3 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.

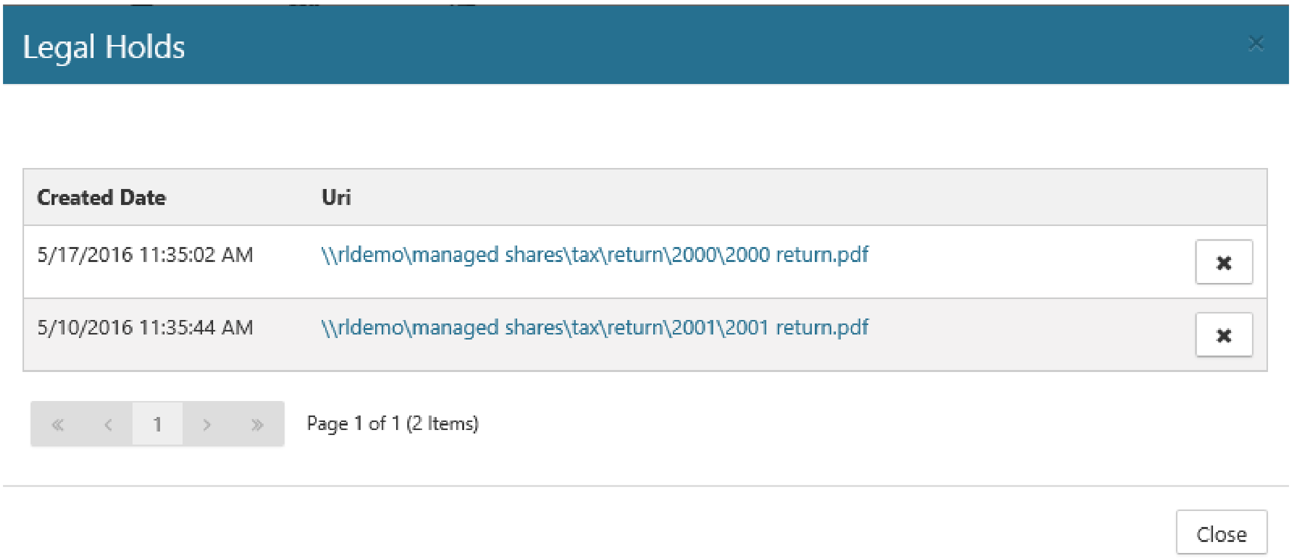
To create a Legal Hold Rule, perform the following steps as a user or Physical Administrator who is assigned a Record Manager account:

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 148) 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**

5.14.4 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	✖

Page 1 of 1 (2 Items)

6 Global Record Manager Guide

Gimmal 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.

The topics in this Guide are for Global Record Managers. Other record manager tasks, including creating the File Plan are available in the Record Manager Guide.

6.1 Record Class Permissions

6.2 Record Class Permissions

6.2.1 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**.

6.2.2 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

6.2.2.1 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**

6.2.2.2 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**.

6.2.3 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.

7 Administrator Guide

The Administrator Guide covers topics that are only available to administrators, such as deployment, global configurations, and security.

7.1 Plan Your Deployment

7.2 Managing Security

7.3 Connector Deployment

7.4 Physical Records Management Deployment

7.5 Monitoring Services

7.6 Migration Utility

7.7 Filtering Records by Rules and Metadata

7.8 Plan Your Deployment

These are the deployment options for the Gimmal Records Management products.

	Server	**Cloud**	**UK Cloud**	**CAN Cloud**
Gimmal Records Management Core	Yes	Yes	Yes	Yes
Altitude Connector	Yes	No	No	No
Box Connector	Yes	Yes	No	No
Documentum Connector	Yes	No	No	No
FileNet Connector	Yes	No	No	No

	Server	Cloud	UK Cloud	CAN Cloud
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

7.9 Managing Security

Security in Gimmal 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 than 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:

7.9.9 Account Types

There are three types of account types available in they system; **Master Account**, **User Account**, and **Service Account**.

7.9.9.1 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 28) the first time you logged in.

7.9.9.2 User Account

The User Account is the typical account that is created in the system. User accounts are given Security Roles(see page 222) 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.

7.9.9.3 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 Gimmal Cloud for Records Management. If the Giimmal Cloud is being used, the username format is: {service account name}@{tenant domain} (e.g. spocservice@gimmal.com[30], or fscservice@companyname.com[31]), otherwise, the format is just: {service account name}. For more information, see Directing the Connector to Records Management.

7.9.10 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.

7.9.10.1 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.

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.

7.9.10.2 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.

[30] mailto:spocservice@gimmal.com

[31] mailto:fscservice@companyname.com

7.9.10.3 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.

7.9.10.4 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 115)topic.

7.9.10.5 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

7.9.10.6 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.

7.9.11 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**			
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***	

Permission	**System Admin**	**Global Record Manager**	**Record Manager**	**User**
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**	
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****

Permission	System Admin	Global Record Manager	Record Manager	User
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

7.9.12 Permission Overview

Permissions allow users certain type of access to records and containers. The specifics permissions are detailed in this section.

7.9.12.1 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 217) for more information.

7.9.12.2 Physical Records

Accounts with the Physical User role wll 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.

Permission	Comment
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.

7.9.13 Creating a Service Account

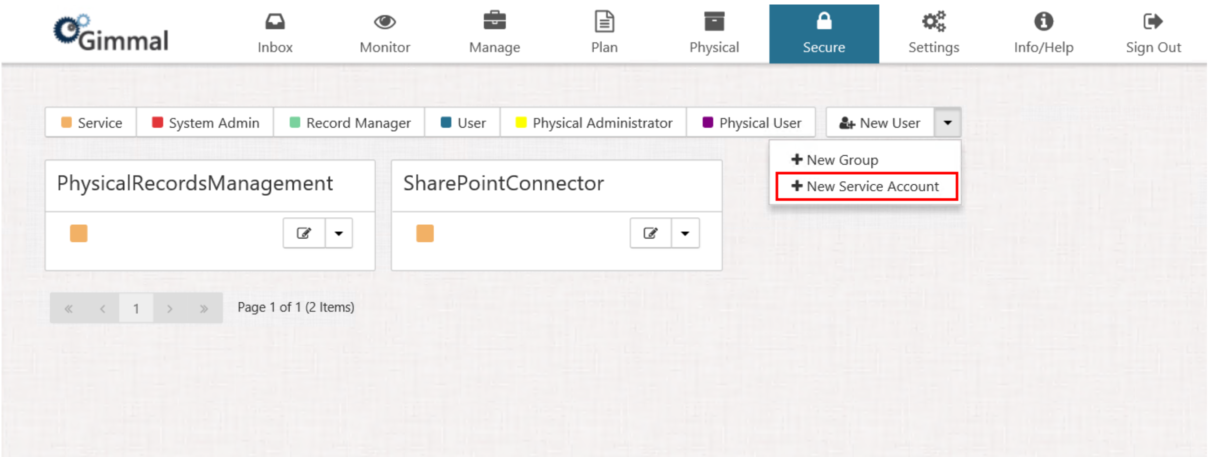
Service Accounts are created and managed locally within Records Management. They differ from the other account types because these accounts are created locally and not associated with the registered Identity Provider, such as Windows Accounts if using the out-of-the-box Identity Provider. The purpose 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:

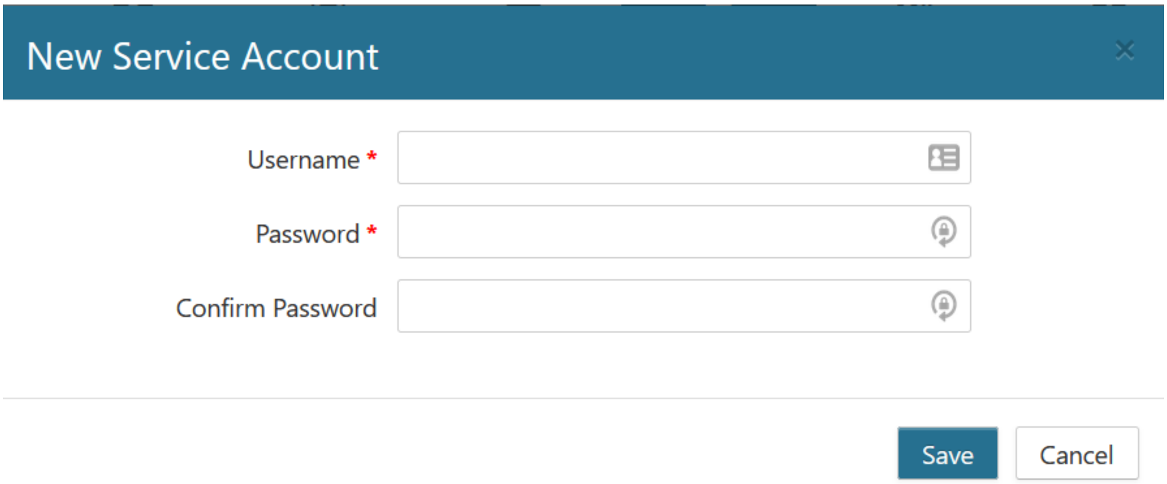
1. Login to Records Management as a user with a **Master** account or a **System Admin** account.
2. Select **Secure** on the Main Menu.

   The Security page displays.



3. Select the New User drop-down, and then select **+New Service Account**.

   The New Service Account window opens.



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 Gimmal Cloud deployment for Records Management. If the cloud tenant is being used, the username format is: {service account name}@{tenant domain} (e.g. spocservice@gimmal.com[32], or fscservice@companyname.com[33]), 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

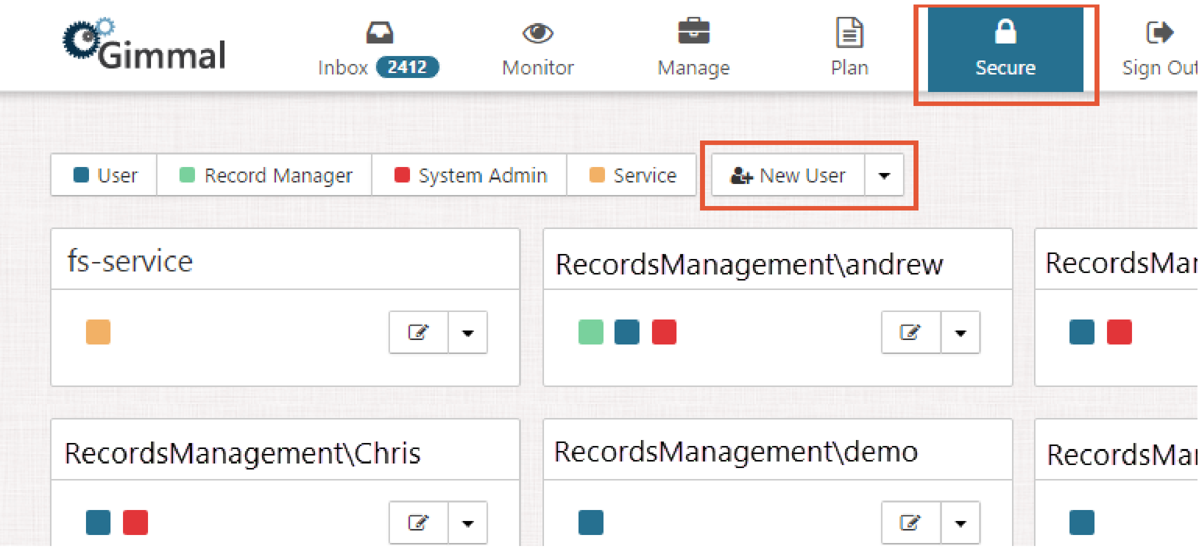
7.9.14 Granting and Revoking User Access

7.9.14.1 Granting Access

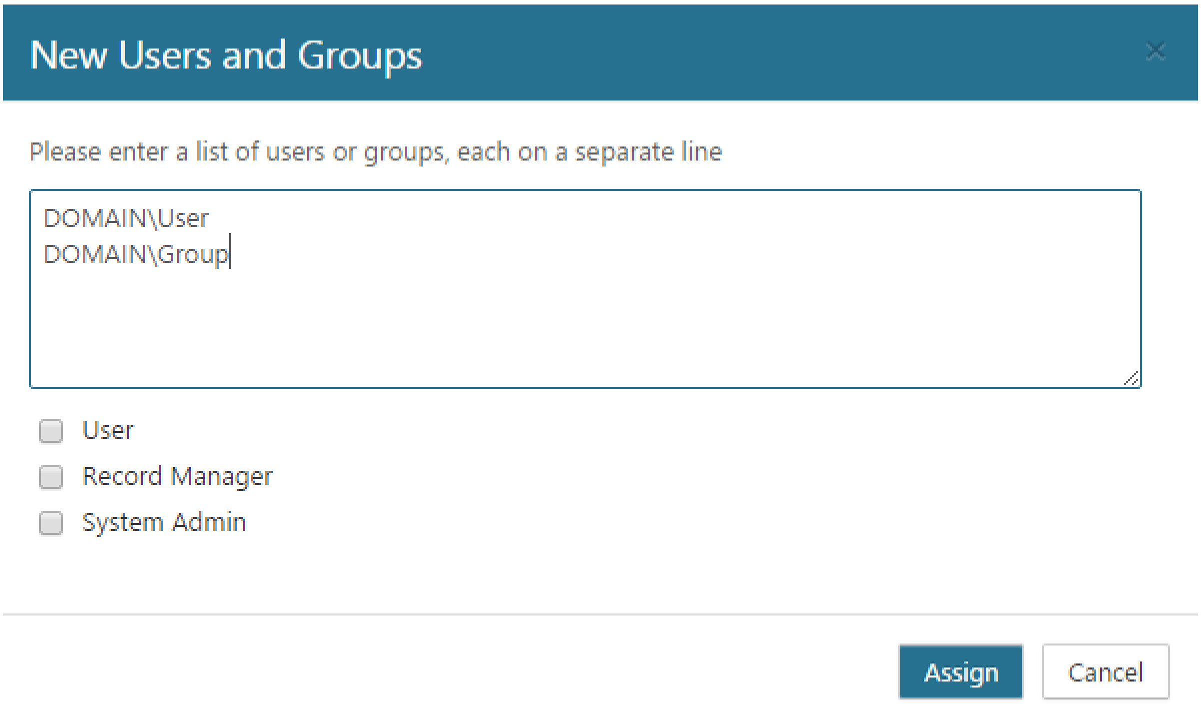
To grant users access to the system, perform the following actions:

1. Select **Secure** from Main Menu
2. Select **New User**

[32] mailto:spocservice@gimmal.com
[33] mailto:fscservice@companyname.com



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, Gimmal Cloud customers must also email support@gimmal.com[34] and provide Gimmal their users' email address(es). Gimmal must add these email addresses to the Records Management permitted users list. This will enable Gimmal to authenticate users for the Gimmal Cloud environment.

Use Windows Domain Users and/or Groups in the following format:

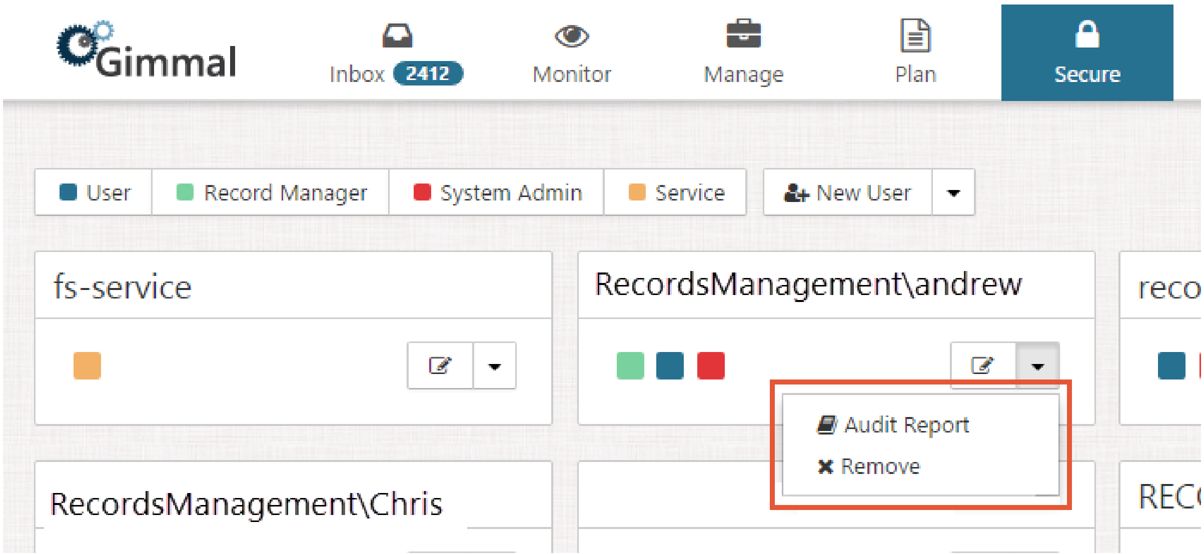
- DOMAIN\User
- DOMAIN\Group

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.

7.9.14.2 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.
3. Select **Remove** from the menu and confirm.



[34] mailto:support@gimmal.com

7.9.15 Creating Local Groups

7.9.15.1 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

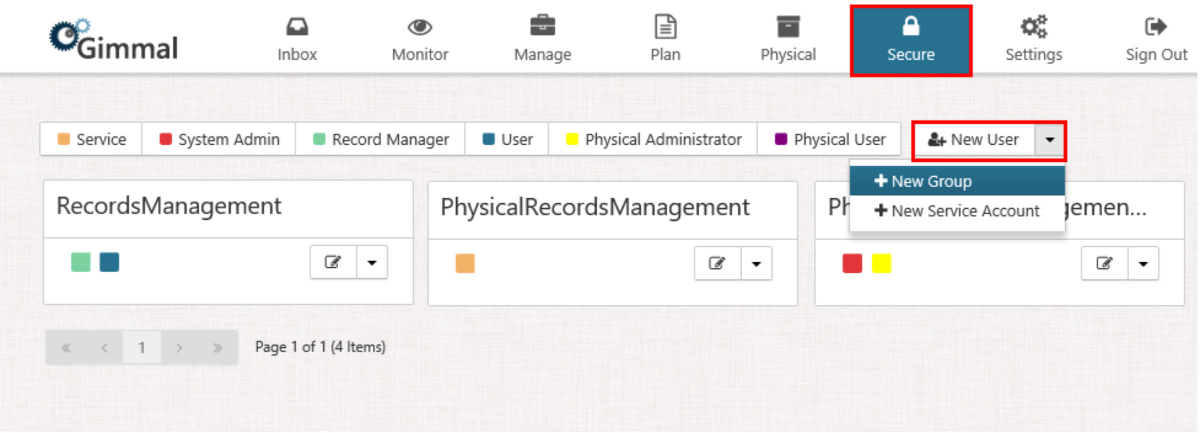
7.9.15.2 Local Groups

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**.

7.9.16 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 423) of the PowerShell section.

7.10 Connector Deployment

7.10.1 Box Connector

7.10.2 Documentum Connector

7.10.3 FileNet Connector

7.10.4 Microsoft 365 SharePoint Connector

7.10.5 SharePoint Online Connector

7.10.6 SharePoint Server Connector

7.10.7 Universal File Share Connector

7.10.8 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 Gimmal Cloud for Records Management, the Box Connector is typically also hosted by the Gimmal 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

7.10.8.1 Box Connector Planning and Requirements

7.10.8.2 Box Connector On-Premise Installation

7.10.8.3 Configuring Box

7.10.8.4 Box Connector Configuration

7.10.8.5 Box Connector Jobs

7.10.8.6 Removing the On-Premise Box Connector

7.10.8.7 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 "Gimmal 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

Box Connector Server		
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, Gimmal 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[35] To verify that your operating system supports TLS 1.2, read the Support for TLS 1.2 section of Microsoft's documentation[36].

7.10.8.8 Box Connector On-Premise Installation

⚠ On-Premise installation of the Box Connector is not required if your connector is being hosted by Gimmal.

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 Gimmal 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 Gimmal 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

[35] https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls#systemdefaulttlsversions
[36] https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls#support-for-tls-12

- Box User app Client Secret
- Box Url
- Box Enterprise ID

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 Gimmal Box Service is created in Windows to perform the actions necessary to enable Gimmal 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.

7.10.8.9 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 > Account & Billing** page.

Custom Subdomain

You must configure your box account to use a custom subdomain. This enables the Gimmal Box Connector to uniquely identify requests to/from your Box account back to your Gimmal Box Connector subscription.

- 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 a Box App in order for the connector to communicate with your Box account. You may either create a Box User App or Box Server-to-Server App.

Box User App

This is a Standard OAuth 2.0 app in Box. For more details, please see the Box documentation for an OAuth Application Setup[37]. This app allows you to manage the connector through a web browser.

1. Create a new, or choose an existing, Box app that uses the **Standard OAuth 2.0** authentication method.
2. Configure the app:
    a. **Redirect URI -** Enter one of the following options:
        i. SaaS-TEST
            - Existing Customers (pre-Feb. 27th, 2021) use https://test-conn-box.recordlion.net
            - New Customers (post-Feb. 27th, 2021) use https://box-records.gimmal.build
        ii. SaaS-PRODUCTION
            - Existing Customers (pre-Feb. 27th, 2021) use https://app-conn-box.recordlion.net
            - New Customers (post-Feb. 27th, 2021) use https://box-records.gimmal.cloud
        iii. For an on-premise install use your local Gimmal Box web application.
    b. **Application Scopes** - Select all of the following:
        i. Read all files and folders stored in Box
        ii. Read and write all files and folders stored in Box
        iii. If your organization is using Box Governance, also select Manage Retention Policies
    c. **CORS Domains** - Enter one of the following options. It should match the redirect URI you selected above for TEST or PRODUCTION:
        i. SaaS-TEST
            - Existing Customers (pre-Feb. 27th, 2021) use https://test-conn-box.recordlion.net
            - New Customers (post-Feb. 27th, 2021) use https://box-records.gimmal.build
        ii. SaaS-PRODUCTION
            - Existing Customers (pre-Feb. 27th, 2021) use https://app-conn-box.recordlion.net
            - New Customers (post-Feb. 27th, 2021) use https://box-records.gimmal.cloud
        iii. For an on-premise install use your local Gimmal Box web application.
    d. Click **Save Changes**

Box Server-to-Server App

This is an OAuth 2.0 with JWT app in Box. For more details, please see the Box documentation for a JWT Application Setup[38]. This app enables the connector to communicate with your Box account as a background service without any user interaction.

1. Create a new, or choose an existing, Box app that uses the **OAuth 2.0 with JWT** authentication method.
2. Configure the app:
    a. **Application Access** is Enterprise
    b. **Application Scopes** - Select all of the following:
        i. Read all files and folders stored in Box
        ii. Read and 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

[37] https://developer.box.com/en/guides/applications/custom-apps/oauth2-setup/
[38] https://developer.box.com/en/guides/applications/custom-apps/jwt-setup/

    c. **Advanced Features**:
        i. **Perform Actions as Users** is enabled
        ii. **Generate User Access Tokens** is enabled
3. **Generate a Public/Private Keypair** by following the instructions in the Box documentation[39].
4. **CORS Domains** is one of the following options. It should match the redirect URI you configured in the Standard OAuth 2.0 app previously.
    a. SaaS-TEST
        - Existing Customers (pre-Feb. 27th, 2021) use https://test-conn-box.recordlion.net
        - New Customers (post-Feb. 27th, 2021) use https://box-records.gimmal.build
    b. SaaS-PRODUCTION
        - Existing Customers (pre-Feb. 27th, 2021) use https://app-conn-box.recordlion.net
        - New Customers (post-Feb. 27th, 2021) use https://box-records.gimmal.cloud
    c. For an on-premise install use your local Gimmal Box web application.
5. Click **Save Changes**
6. Follow the steps in the Box documentation for Granting Access for the Application in Your Enterprise[40].

7.10.8.10 Box Connector Configuration

The Gimmal 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 Gimmal 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 Gimmal 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[41]. If you are hosting your own instance of Records

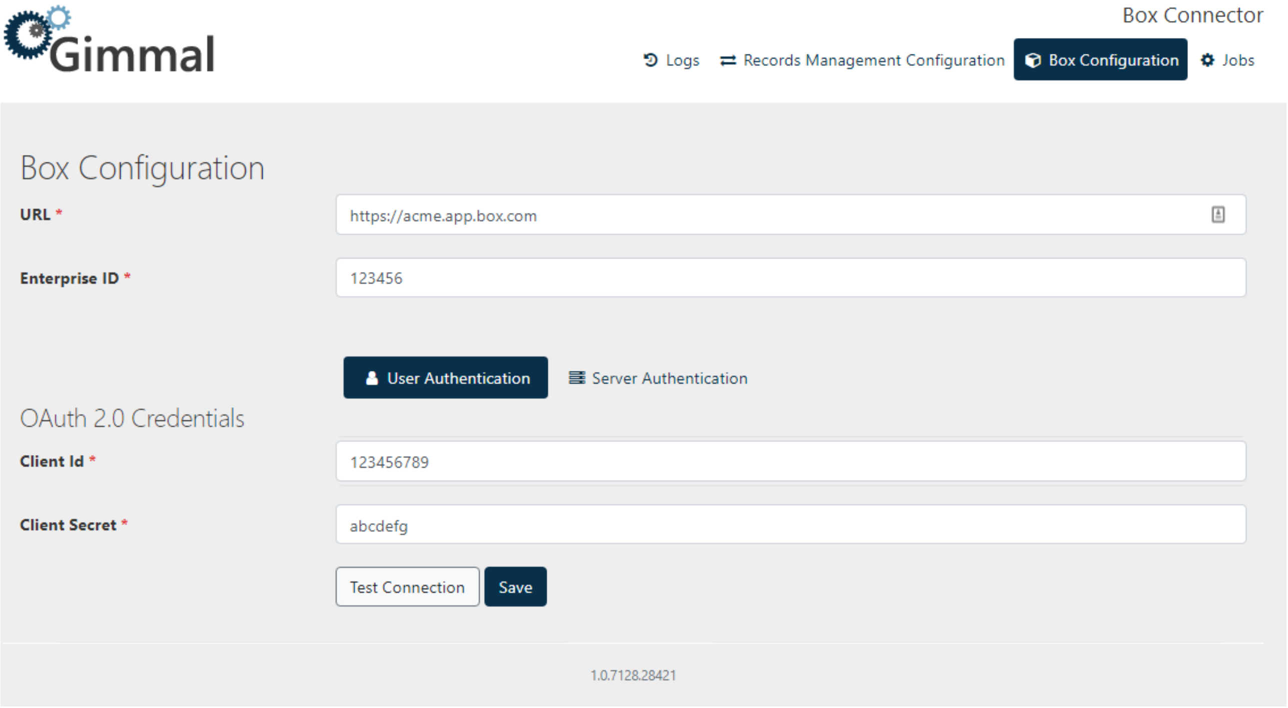
[39] https://developer.box.com/docs/setting-up-a-jwt-app#section-step-2-generate-a-public-private-keypair
[40] https://developer.box.com/docs/setting-up-a-jwt-app#section-step-3-grant-access-for-the-application-in-your-enterprise
[41] mailto:box-svc@domain.com

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 236).



Box Configuration

URL * https://acme.app.box.com

Enterprise ID * 123456

OAuth 2.0 Credentials

Client Id * 123456789

Client Secret * abcdefg

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[42].
- **Enterprise ID:** This field is your Box enterprise ID.

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

[42] https://acme.app.box.com/

This section is pre-populated by Gimmal 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 Gimmal 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.

7.10.8.11 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 servcie 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:

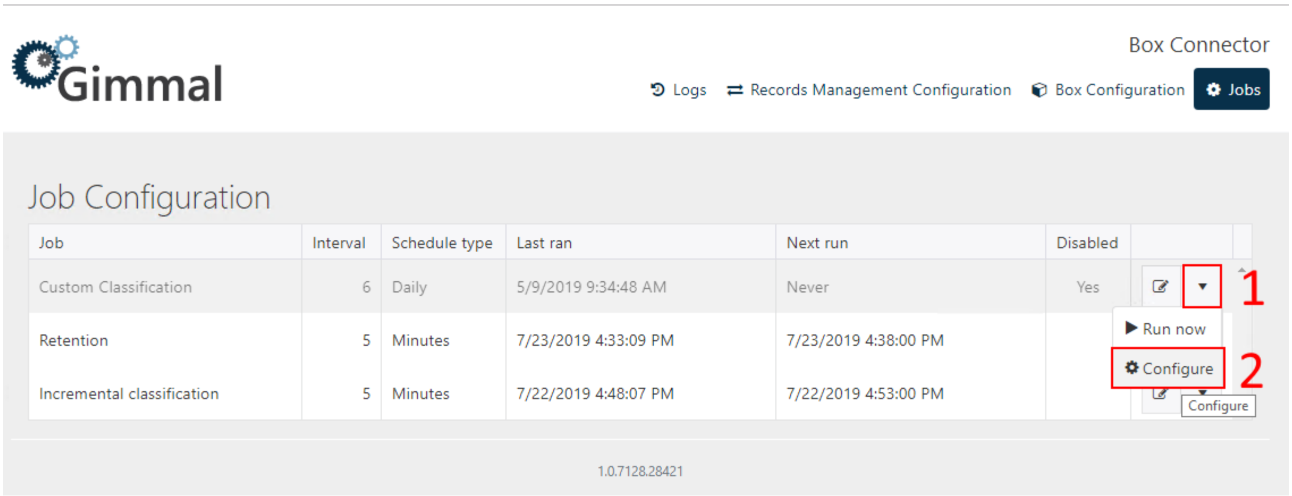
- Lock item (declare record, permanent, and legal holds)
- Unlock item (undeclare record and legal holds)
- Dispose and delete

⚠ 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 “Gimmal 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

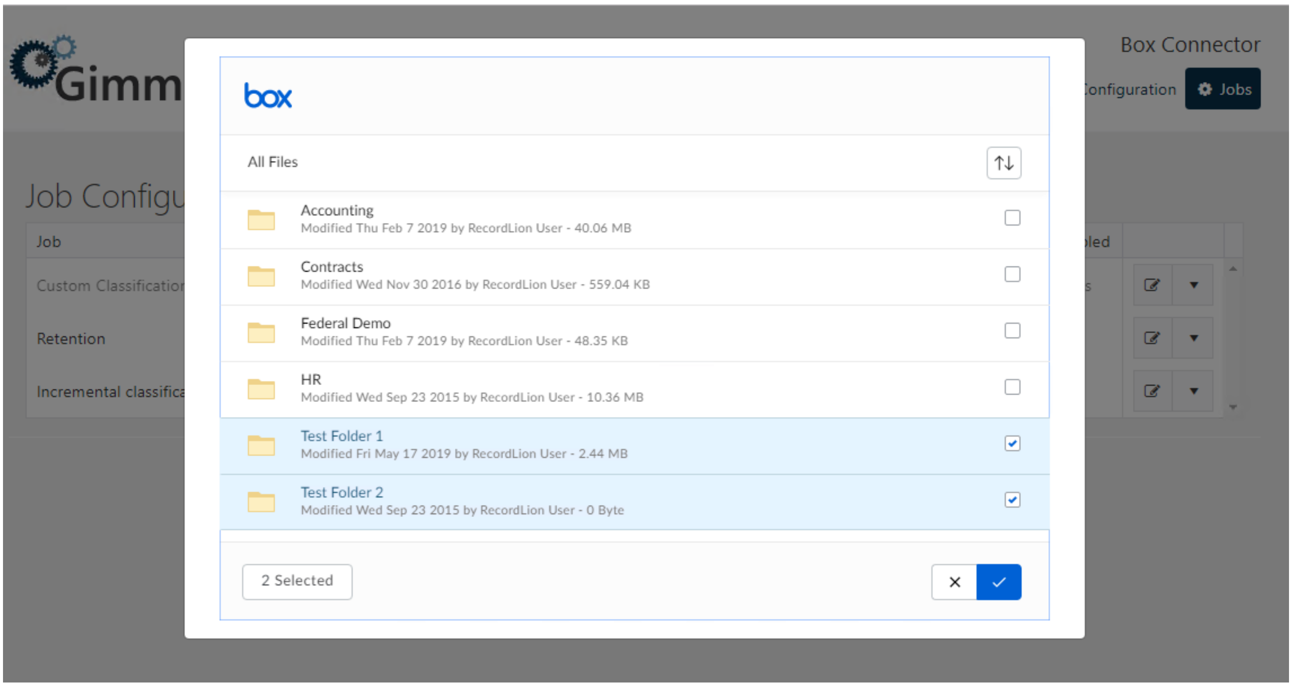
Typically, this job would only be used once when the Connector is initially deployed in your Box account. It is primarily used recursively to classify all the existing documents within the selected root folders of your Box account. To configure the Custom Classification Job, first select Configure from the drop-down.



Job Configuration

Job	Interval	Schedule type	Last ran	Next run	Disabled
Custom Classification	6	Daily	5/9/2019 9:34:48 AM	Never	Yes
Retention	5	Minutes	7/23/2019 4:33:09 PM	7/23/2019 4:38:00 PM	
Incremental classification	5	Minutes	7/22/2019 4:48:07 PM	7/22/2019 4:53:00 PM	

Once open, select the root folders in Box to crawl.



Accounting Modified Thu Feb 7 2019 by RecordLion User - 40.06 MB	☐
Contracts Modified Wed Nov 30 2016 by RecordLion User - 559.04 KB	☐
Federal Demo Modified Thu Feb 7 2019 by RecordLion User - 48.35 KB	☐
HR Modified Wed Sep 23 2015 by RecordLion User - 10.36 MB	☐
Test Folder 1 Modified Fri May 17 2019 by RecordLion User - 2.44 MB	☑
Test Folder 2 Modified Wed Sep 23 2015 by RecordLion User - 0 Byte	☑

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.

7.10.8.12 Removing the On-Premise Box Connector

To uninstall the Box Connector, perform the following steps:

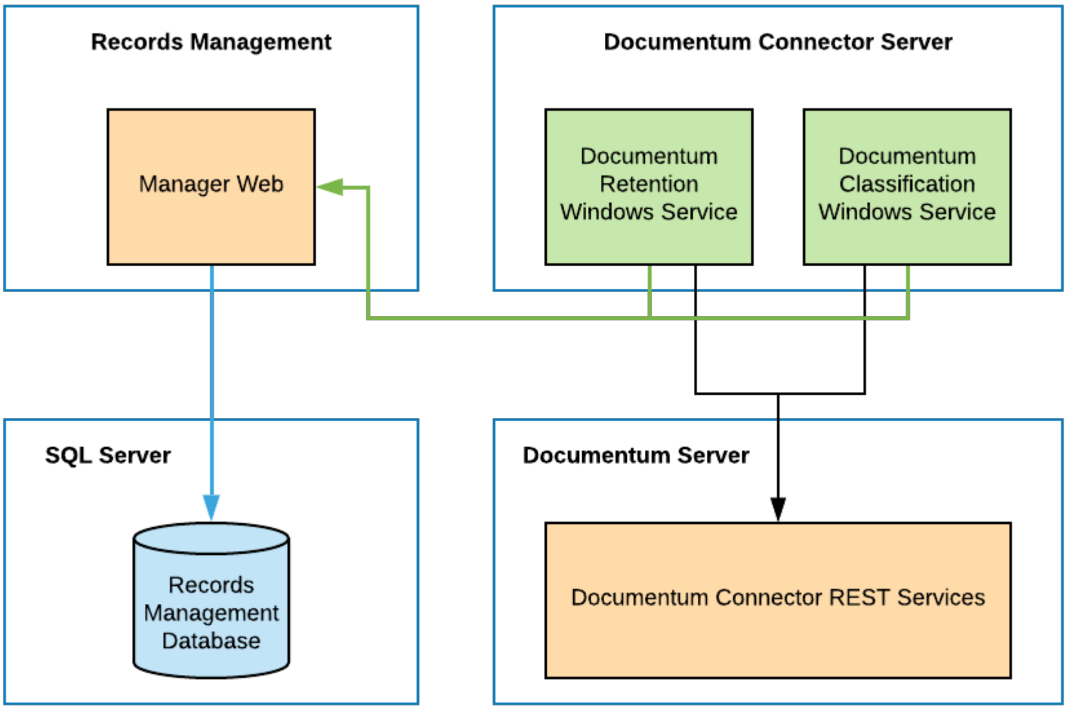
1. On the server that hosts the Box Connector, navigate to the Windows Control Panel and select **Uninstall a Program** from the Programs section.
2. On the “Uninstall or change a program screen”, locate the **Gimmal Box Connector** and double-click it. A dialog displays, asking you to confirm the uninstallation.
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 **Gimmal Box Connector Web**.
6. Verify that the **Gimmal Box Service** is no longer displayed in the Windows Services list.

7.10.9 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.

7.10.9.1 Documentum Connector Architecture


Records Management
Manager Web
Documentum Connector Server
Documentum Retention Windows Service
Documentum Classification Windows Service
SQL Server
Records Management Database
Documentum Server
Documentum Connector REST Services

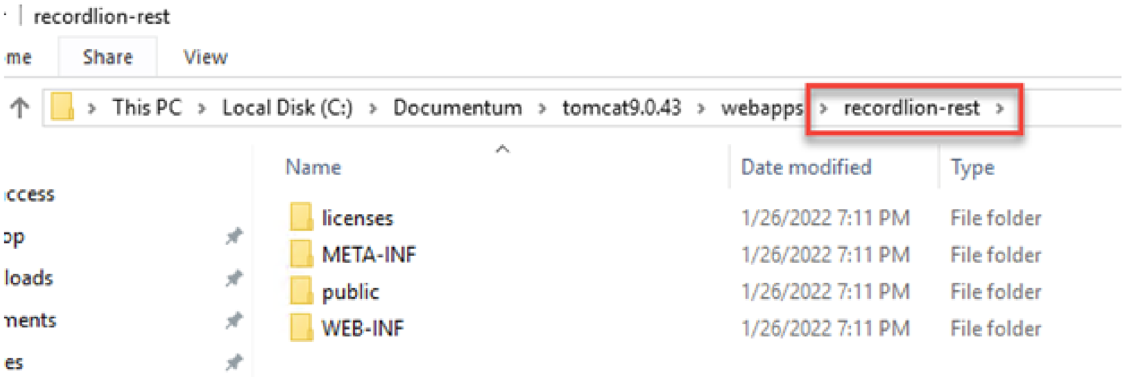
7.10.9.2 Documentum Connector Upgrade from 5.0 to 5.1

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:

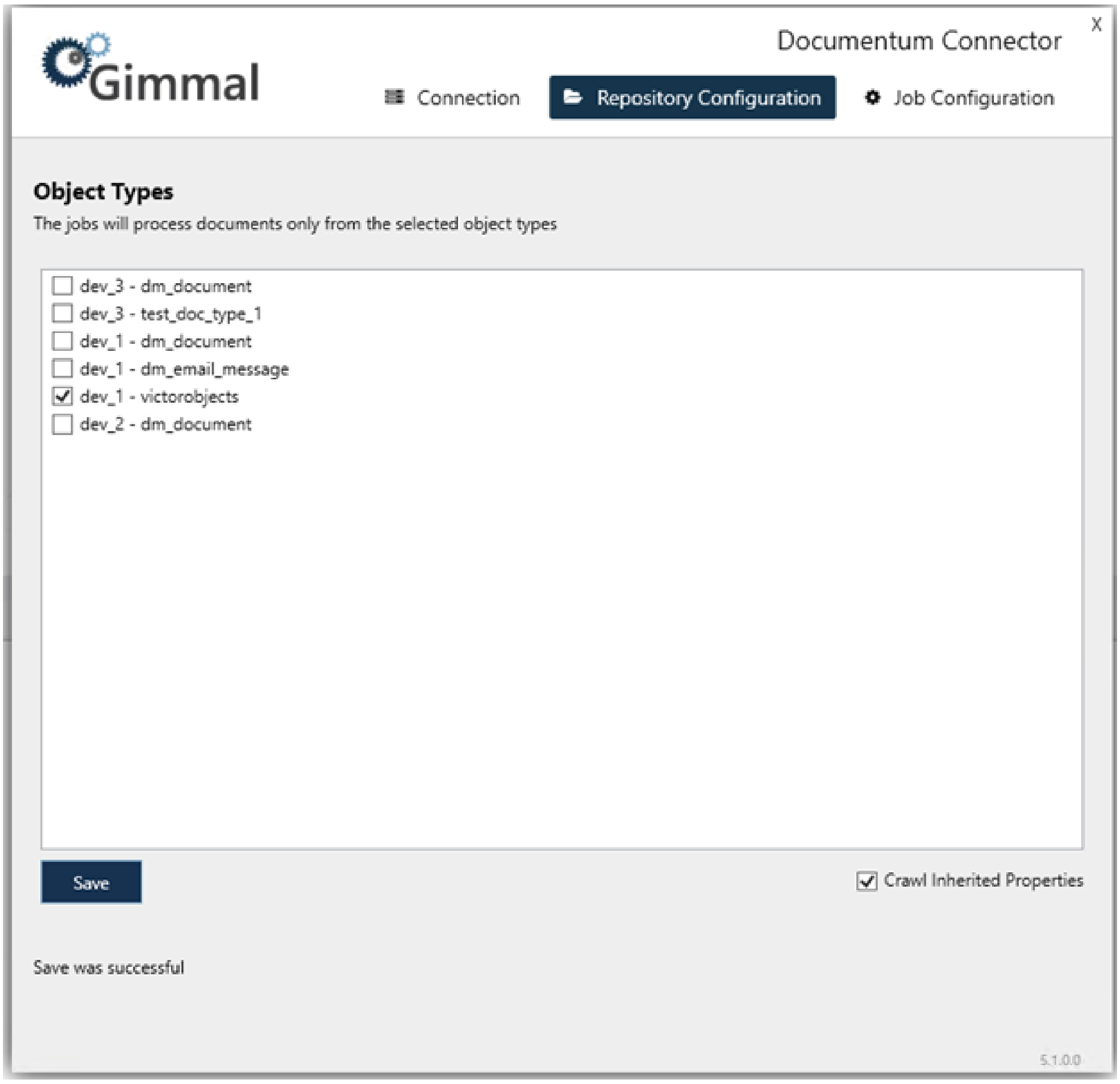
1. Make a copy of the **dfc.properties** file to use during the upgrade.
   a. Remote Desktop into the Documentum web server with Administrative privileges.
   b. Locate the **recordlion-rest folder** (see below)


recordlion-rest
me
Share
View
This PC > Local Disk (C:) > Documentum > tomcat9.0.43 > webapps > recordlion-rest >
ccess
op
loads
nents
es

Name	Date modified	Type
licenses	1/26/2022 7:11 PM	File folder
META-INF	1/26/2022 7:11 PM	File folder
public	1/26/2022 7:11 PM	File folder
WEB-INF	1/26/2022 7:11 PM	File folder

   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 Gimmal 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.



Object Types

The jobs will process documents only from the selected object types

- □ dev_3 - dm_document
- □ dev_3 - test_doc_type_1
- □ dev_1 - dm_document
- □ dev_1 - dm_email_message
- ☑ dev_1 - victorobjects
- □ dev_2 - dm_document

☑ Crawl Inherited Properties

Save was successful

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:
   - Gimmal Documentum Classification Service

- Gimmal Documentum Retention Service

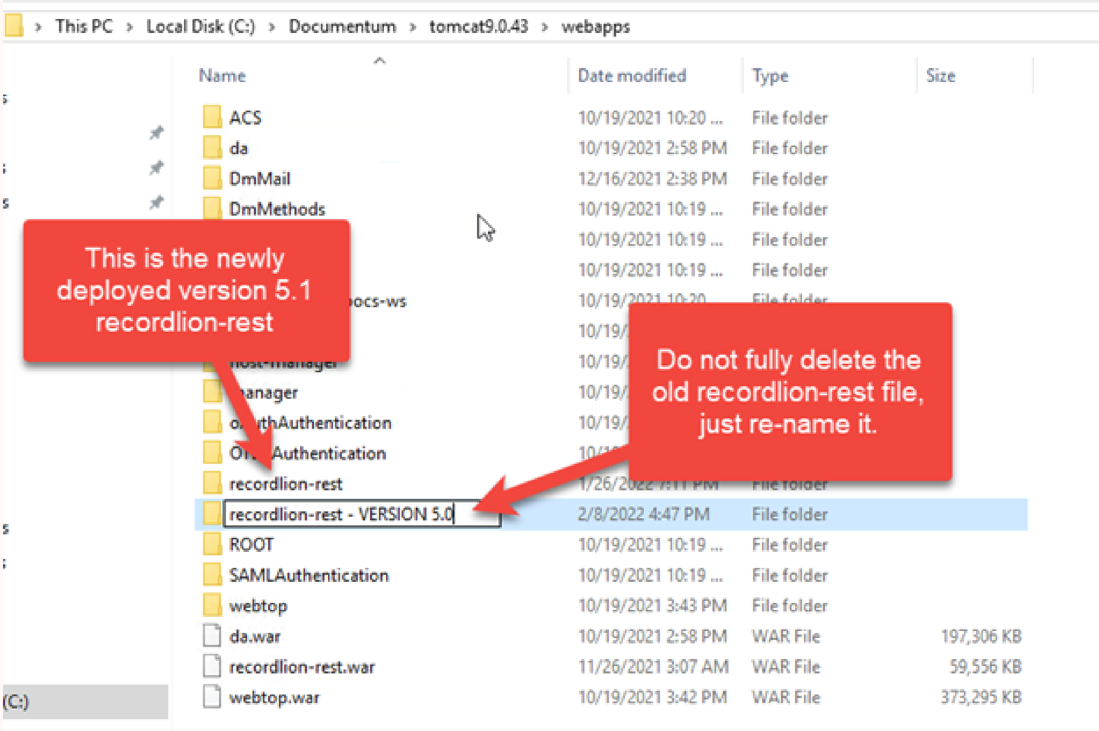
3. Download the Documentum Connector ISOs from the Gimmal Software Downloads[43] site. If you do not have access to the software download site, please contact Gimmal Support[44]
4. Using the provided ISO, install version 5.1 of the Documentum Connector by using these steps[45].

> ⚠ 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.

5. Deploy the **recordlion-rest** war file by following these steps[46].

> ⓘ 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**).



This PC › Local Disk (C:) › Documentum › tomcat9.0.43 › webapps
(C:)
This is the newly deployed version 5.1 recordlion-rest
Do not fully delete the old recordlion-rest file, just re-name it.

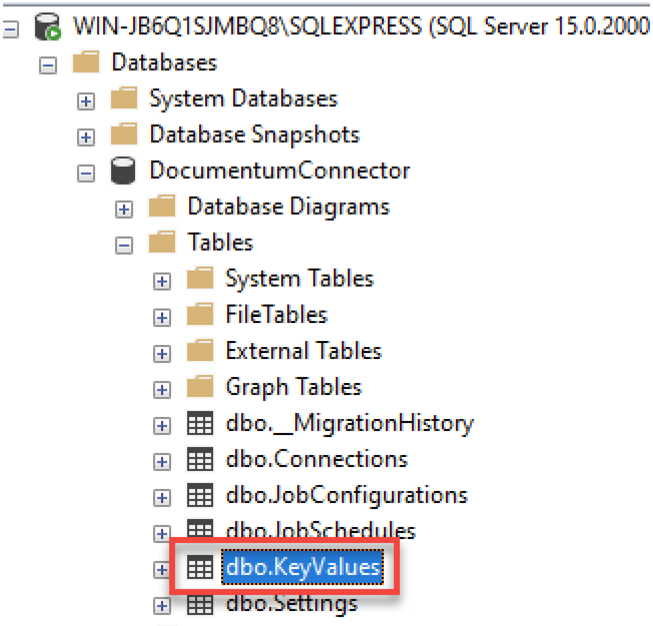
Name	Date modified	Type	Size
ACS	10/19/2021 10:20 ...	File folder	
da	10/19/2021 2:58 PM	File folder	
DmMail	12/16/2021 2:38 PM	File folder	
DmMethods	10/19/2021 10:19 ...	File folder	
[illegible]	10/19/2021 10:19 ...	File folder	
[illegible]	10/19/2021 10:19 ...	File folder	
ocs-ws	10/19/2021 10:20	File folder	
[illegible]	10/19/	[illegible]	
host-manager	10/19/	[illegible]	
anager	10/19/	[illegible]	
o thAuthentication	10/19/	[illegible]	
OI Authentication	10/1	[illegible]	
recordlion-rest	1/26/2022 7:11 PM	File folder	
recordlion-rest - VERSION 5.0	2/8/2022 4:47 PM	File folder	
ROOT	10/19/2021 10:19 ...	File folder	
SAMLAuthentication	10/19/2021 10:19 ...	File folder	
webtop	10/19/2021 3:43 PM	File folder	
da.war	10/19/2021 2:58 PM	WAR File	197,306 KB
recordlion-rest.war	11/26/2021 3:07 AM	WAR File	59,556 KB
webtop.war	10/19/2021 3:42 PM	WAR File	373,295 KB

6. Update the **dfc.properties** file for the **recordlion-rest** by following these steps[47].

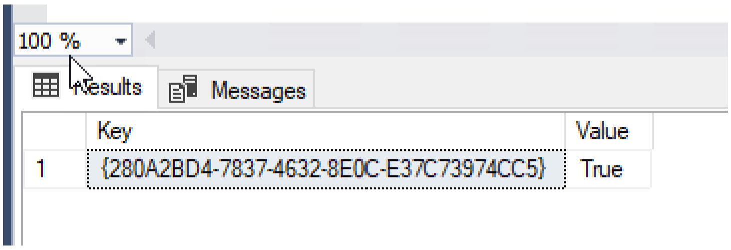
[43] https://gimmal1.sharepoint.com/sites/EXT-Software/SitePages/Home.aspx
[44] https://support.gimmal.com
[45] https://docs.gimmal.com/rm/5.1/Server/documentum-connector-installation
[46] https://docs.gimmal.com/rm/5.1/Server/documentum-services-installation
[47] https://docs.gimmal.com/rm/5.1/Server/applying-documentum-foundation-class-properties

> ⚠ 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**



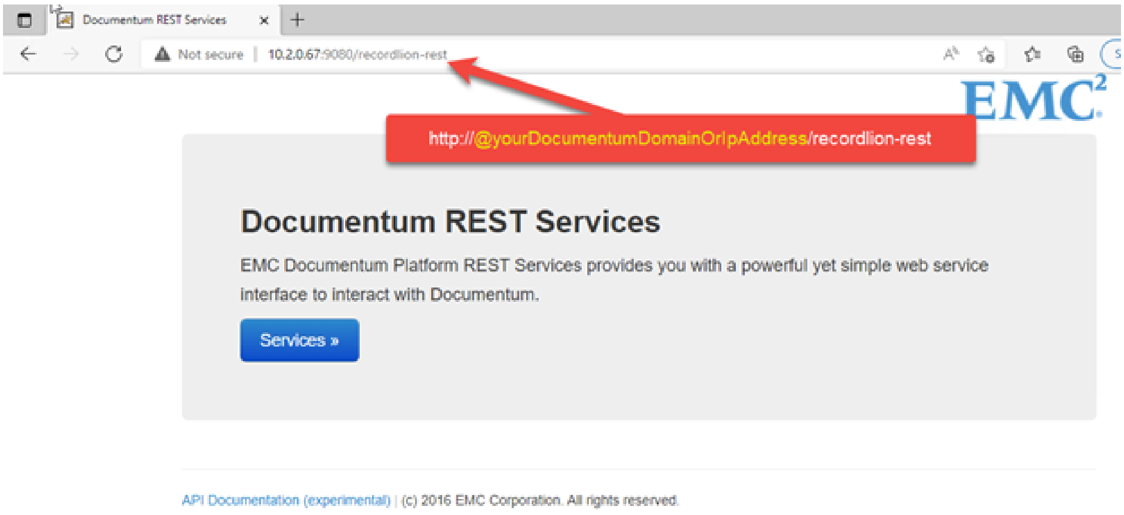
   b. Confirm that there is an initial entry in the **KeyValues** table that has a value of **True**



	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*[48]-, and confirm that the web page below renders

[48] http://yourdocumentumdomainoripaddress/recordlion-rest



http://@yourDocumentumDomainOrIpAddress/recordlion-rest

Documentum REST Services

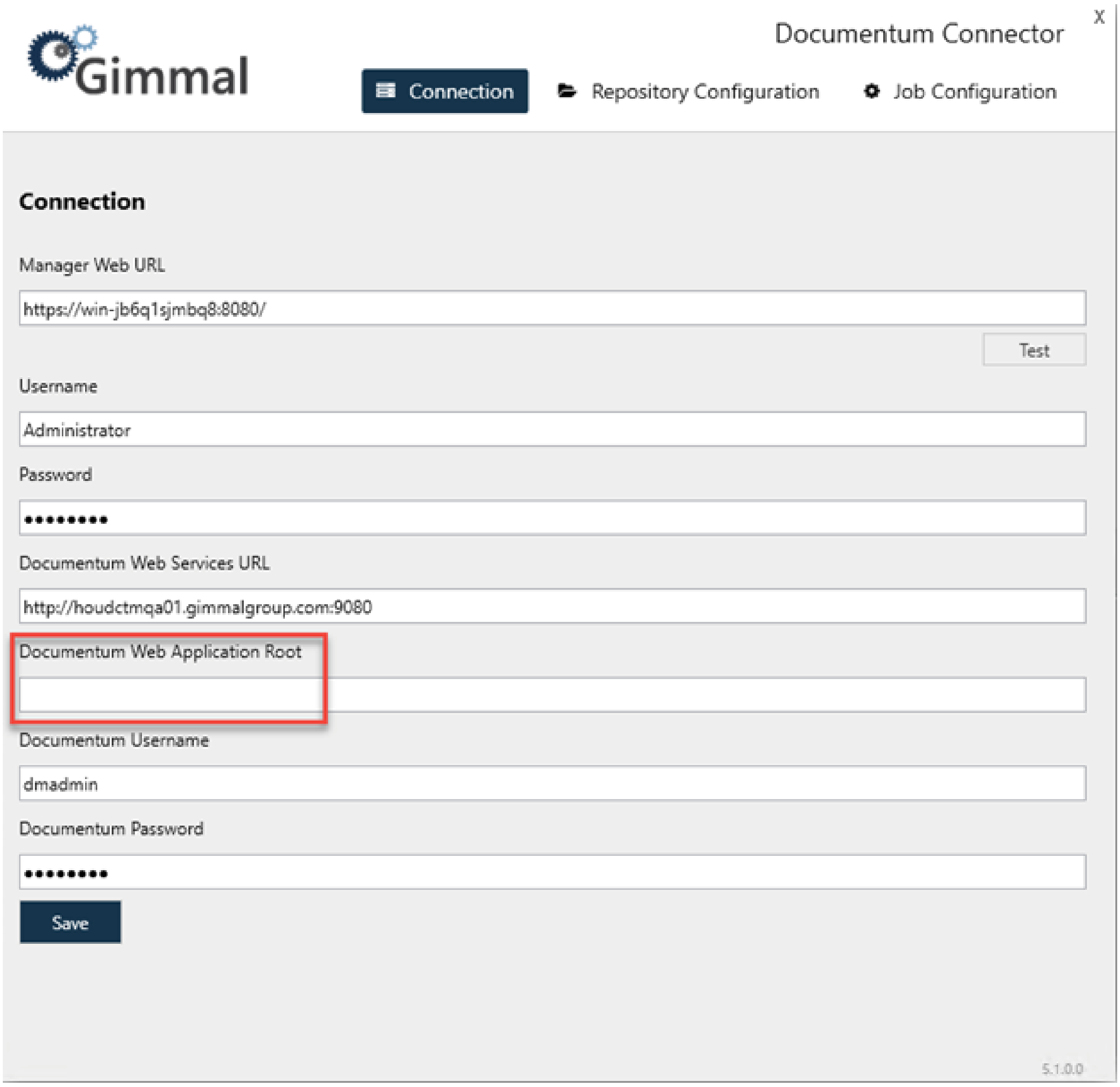
EMC Documentum Platform REST Services provides you with a powerful yet simple web service interface to interact with Documentum.

API Documentation (experimental) | (c) 2016 EMC Corporation. All rights reserved.

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.



Connection

Manager Web URL: https://win-jb6q1sjmbq8:8080/

Username: Administrator

Password: ••••••••

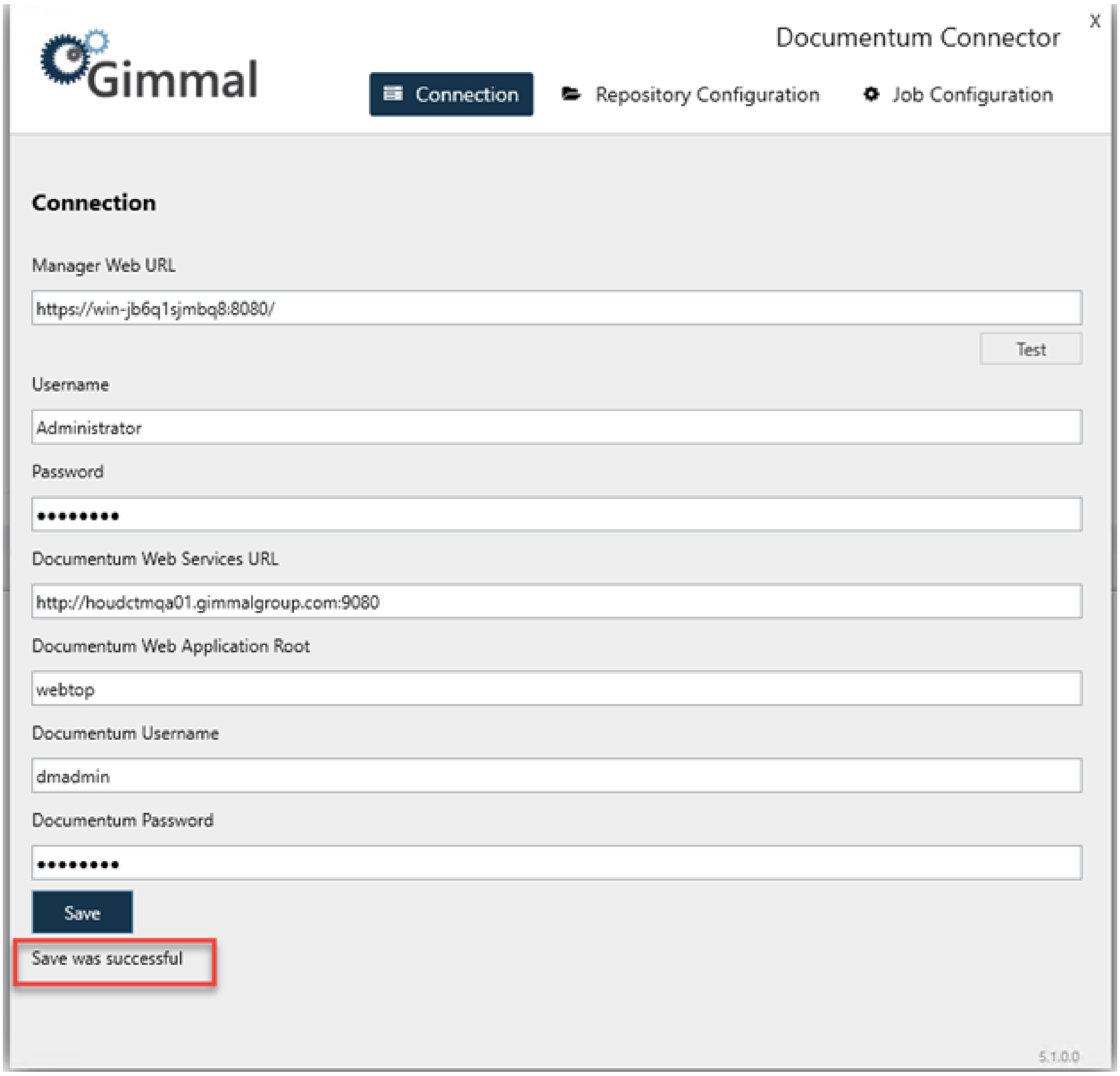
Documentum Web Services URL: http://houdctmqa01.gimmalgroup.com:9080

Documentum Web Application Root:

Documentum Username: dmadmin

Documentum Password: ••••••••

4. Enter the 'Documentum Web Application Root' value, then click 'Save'. You will receive a confirmation if this is successful.



Connection

Manager Web URL: https://win-jb6q1sjmbq8:8080/

Username: Administrator

Password: ••••••••

Documentum Web Services URL: http://houdctmqa01.gimmalgroup.com:9080

Documentum Web Application Root: webtop

Documentum Username: dmadmin

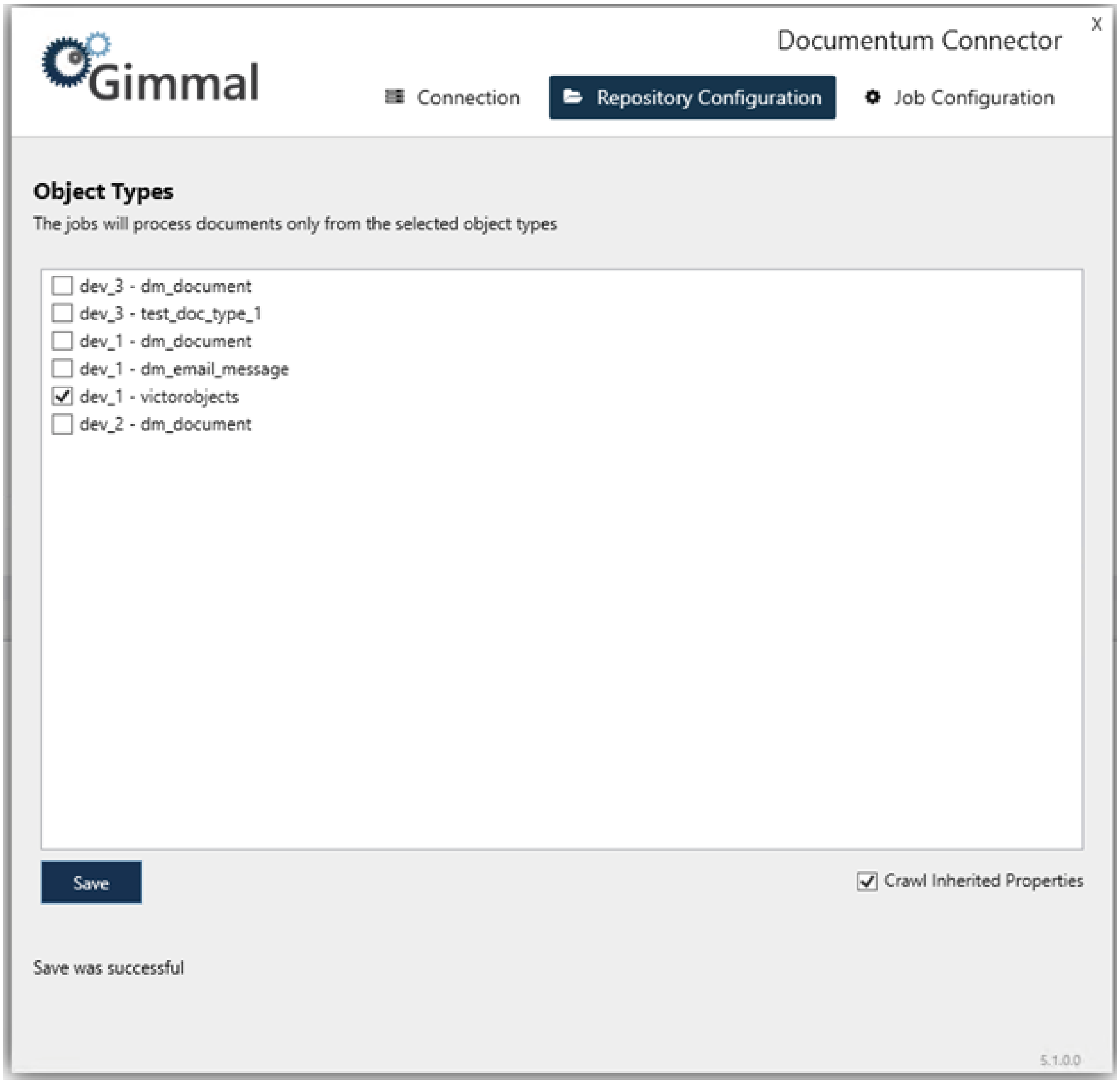
Documentum Password: ••••••••

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.

5. Restart the machine to clear any potential credential caches before proceeding to the next steps.
6. 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.



Object Types

The jobs will process documents only from the selected object types

- □ dev_3 - dm_document
- □ dev_3 - test_doc_type_1
- □ dev_1 - dm_document
- □ dev_1 - dm_email_message
- ☑ dev_1 - victorobjects
- □ dev_2 - dm_document

Save

☑ Crawl Inherited Properties

Save was successful

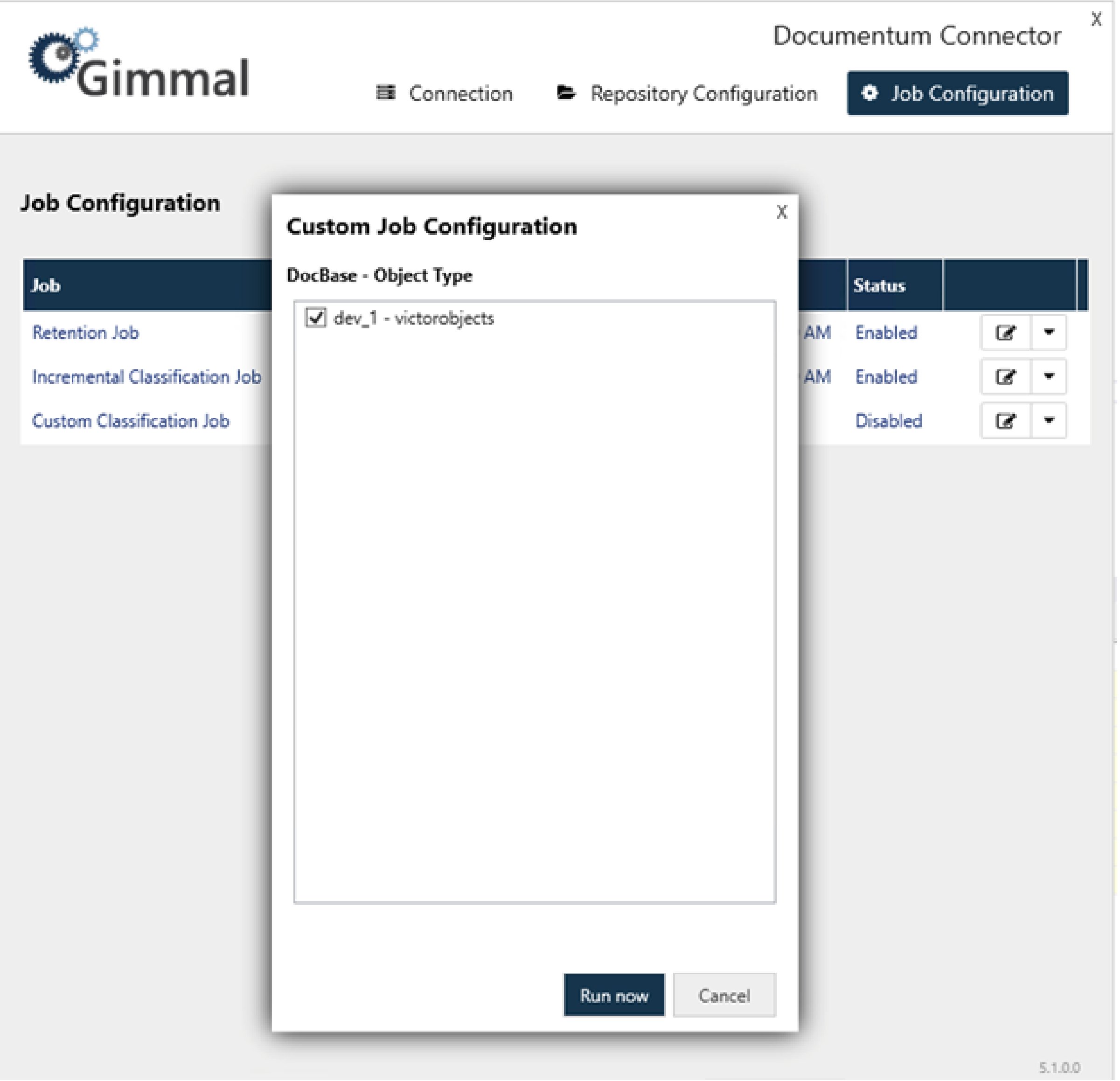
5.1.0.0

7. Start Documentum Connector Services:
   - Gimmal Documentum Classification Service
   - Gimmal 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.



Job Configuration

Job		Status	
Retention Job	AM	Enabled	
Incremental Classification Job	AM	Enabled	
Custom Classification Job		Disabled	

Custom Job Configuration

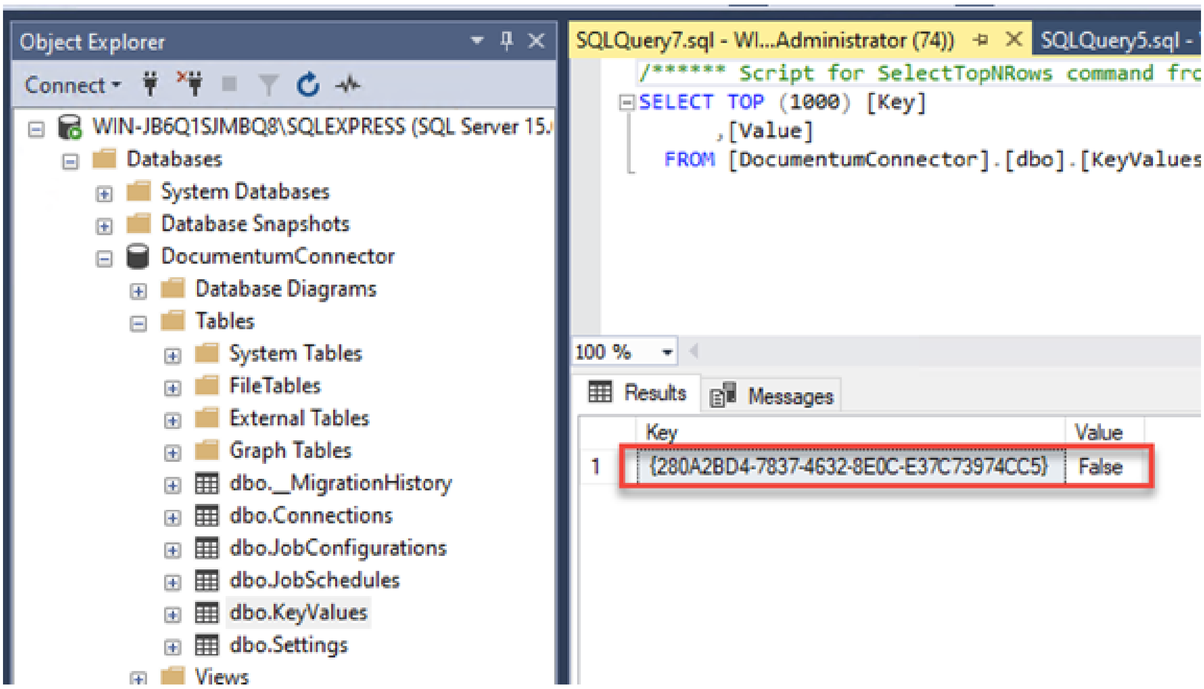
DocBase - Object Type

☑ dev_1 - victorobjects

Run now   Cancel

10. 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.



```
/****** Script for SelectTopNRows command fro
SELECT TOP (1000) [Key]
      ,[Value]
  FROM [DocumentumConnector].[dbo].[KeyValues
```

	Key	Value
1	{280A2BD4-7837-4632-8E0C-E37C73974CC5}	False

11. Upgrade to version 5.1 is complete. If you wish, you can go ahead and re-enable retention and incremental classification and proceed normally.

7.10.9.3 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 Gimmal 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, Gimmal 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, Gimmal 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[49] To verify that your operating system supports TLS 1.2, read the Support for TLS 1.2 section of Microsoft's documentation[50].

Database Server

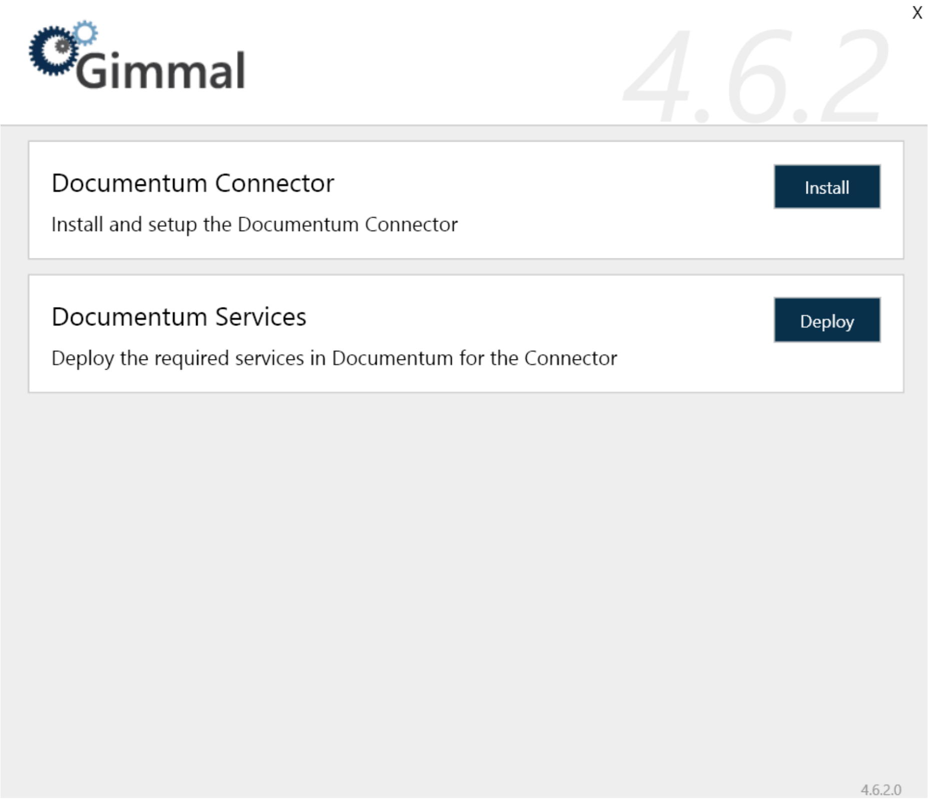
- SQL Server 2016 or greater
- 100 MB for Documentum Database

7.10.9.4 Documentum Connector Installation

Ensure that you run the installer as the Local Administrator.

Upon launching the Documentum Connector installer, the following screen displays:

[49] https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls#systemdefaulttlsversions
[50] https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls#support-for-tls-12



Documentum Connector

Install and setup the Documentum Connector

Documentum Services

Deploy the required services in Documentum for the Connector

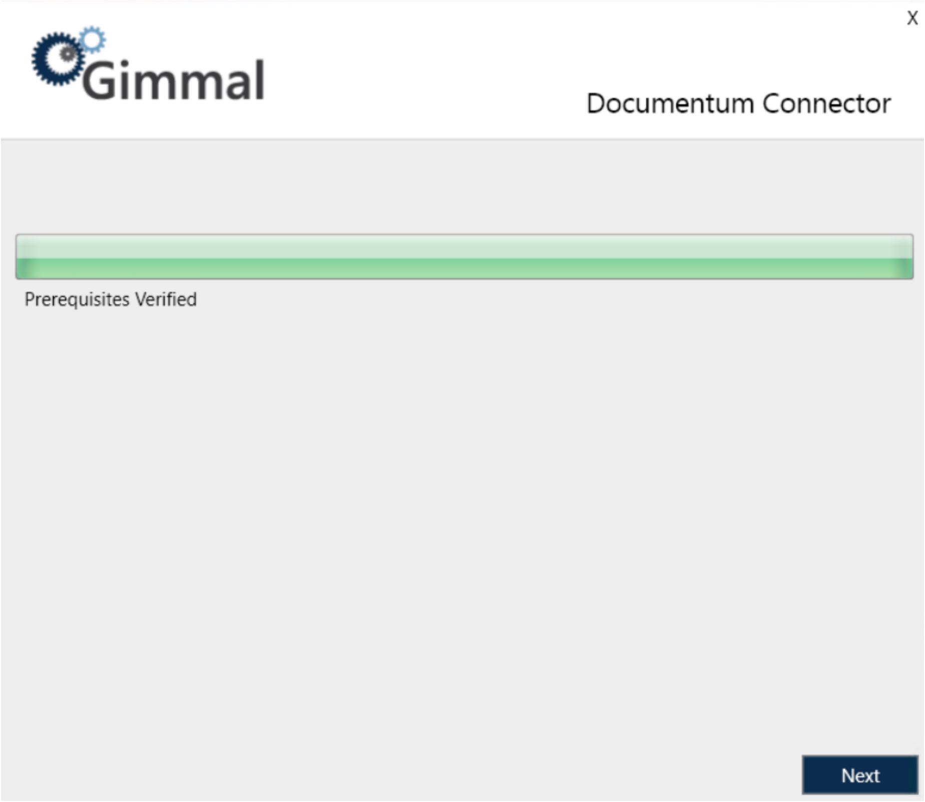
Installing the Documentum Connector

Before you install the Documentum Connector, verify the Connector system requirements(see page 253). This installation section also assumes that you have already installed the Records Management Core platform.

> ⓘ 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:

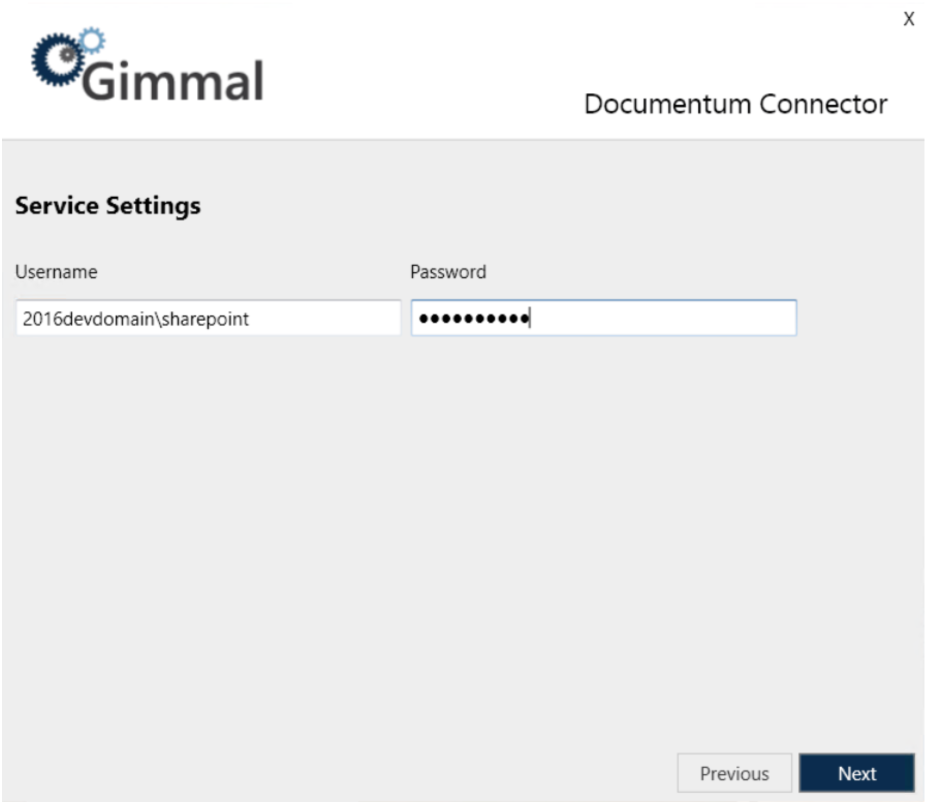
1. From the Records Management splash screen, click the **Install Documentum Connector** link and the User Account Control window opens.
2. Click Yes to allow the installer to make changes to your computer. The Documentum Connector installation window opens.
3. On the Documentum Connector installation 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



Prerequisites Verified

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.



Service Settings

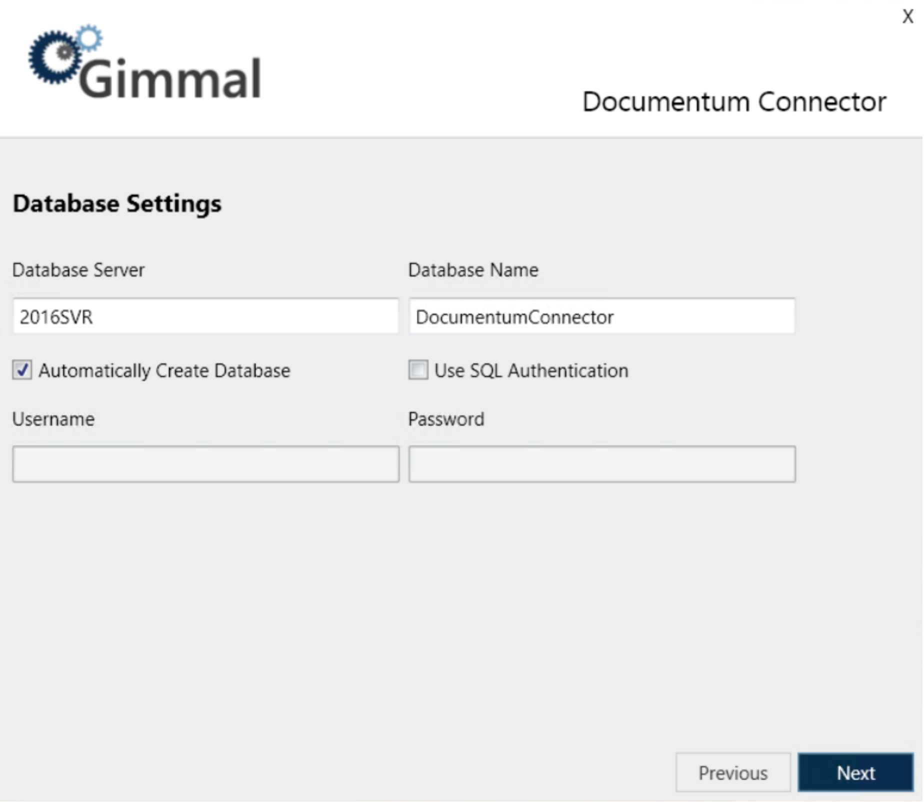
Username: 2016devdomain\sharepoint

Password: ●●●●●●●●●●

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.



Database Settings

Database Server: 2016SVR

Database Name: DocumentumConnector

☑ Automatically Create Database

□ Use SQL Authentication

Username:

Password:

> ⚠ 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:** he 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 **Gimmal Documentum Classification Service** and the **Gimmal 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 259).

7.10.9.5 Documentum Services Installation

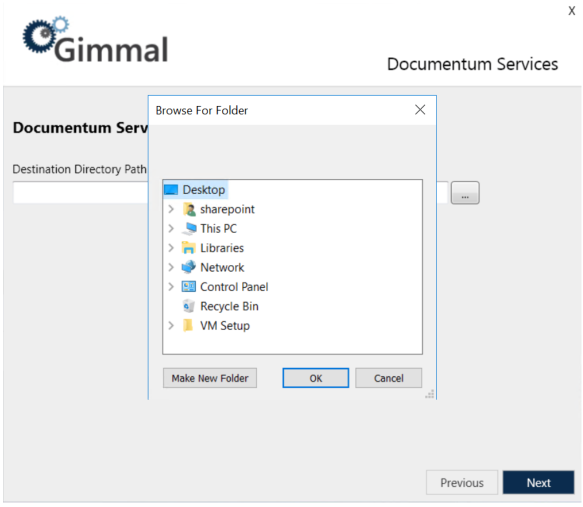
The Documentum Services component deploys required services and components to a Web Application Server that acts as a frontend to the Document Content Server. The Documentum Connector will leverage this server and the deployed services to communicate with Documentum. Specifically, a .WAR file*, which 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[51] settings
7. Start the Documentum Retention and Classification Windows services on the Documentum Connector server.

Deploying to a Non-Windows Documentum Web Application Server

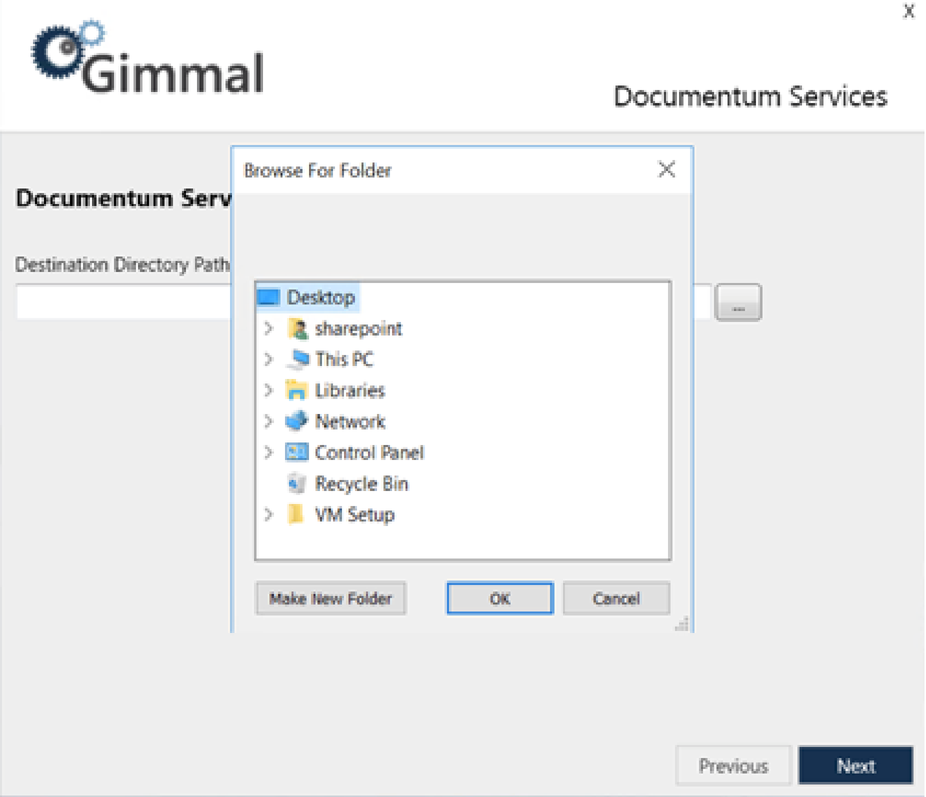
If desired, you can deploy the Documentum Connector .WAR file to a non-Windows Web Application Server*. To do so, perform the following steps on a Windows machine:

⚠ 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.

[51] https://docs.gimmal.com/rm/administrator-guide/connector-deployment/documentum-connector/applying-documentum-foundation-class-properties

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 ake 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[52] settings
8. Start the Documentum Retention and Classification Windows services on the Documentum Connector server.

7.10.9.6 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:

[52] https://docs.gimmal.com/rm/administrator-guide/connector-deployment/documentum-connector/applying-documentum-foundation-class-properties

#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:

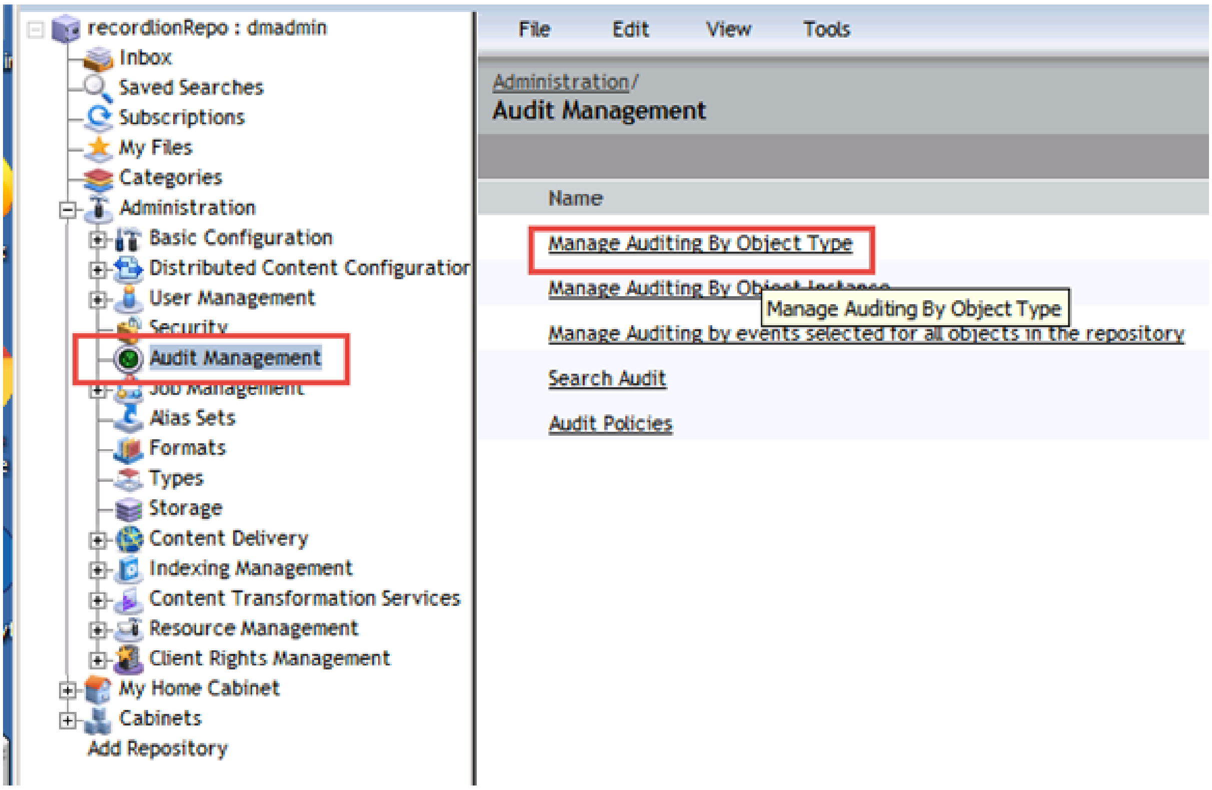
1. Copy the username and encrypted password for the global registry user from the **dfc.properties** file on the global registry Content Server host, or
2. Select another global registry user and encrypt the password using the following command:

   java -cp dfc.jar com.documentum.fc.tools.RegistryPasswordUtils <**password_to_be_encrypted**>

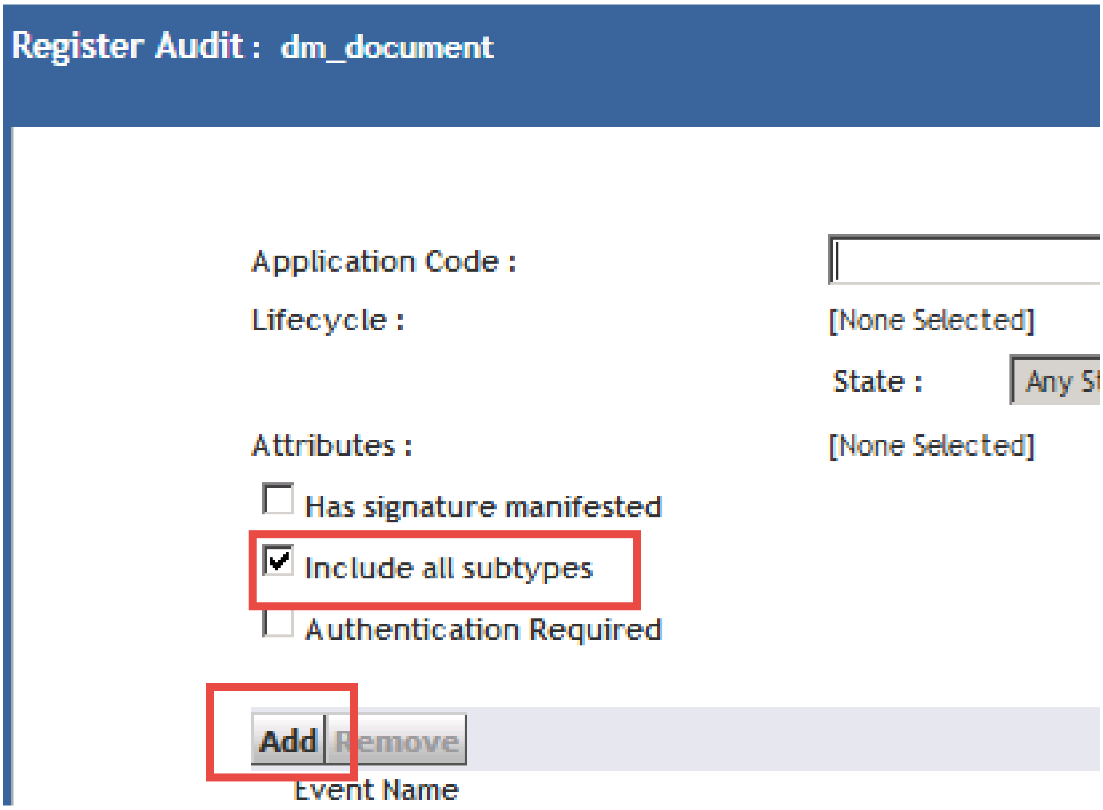
7.10.9.7 Enable Documentum Audit Events

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 : Any St

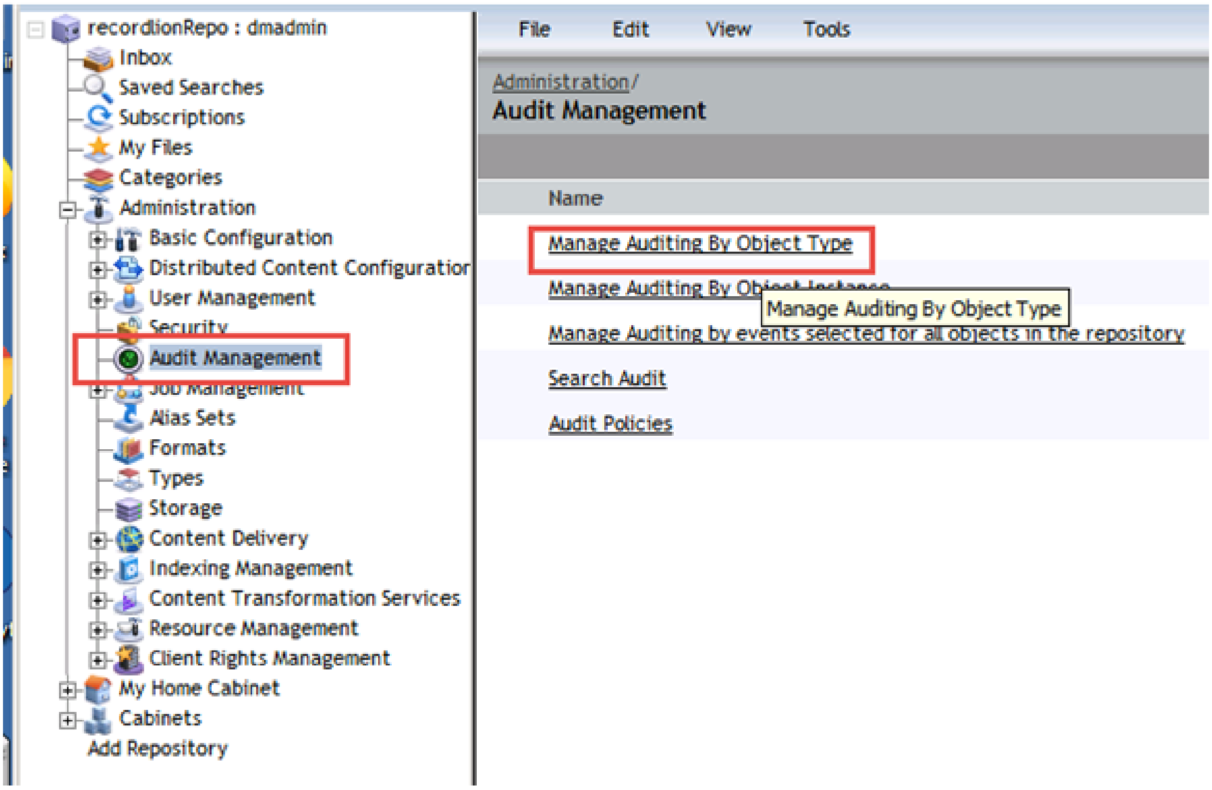
Attributes : [None Selected]

☐ Has signature manifested

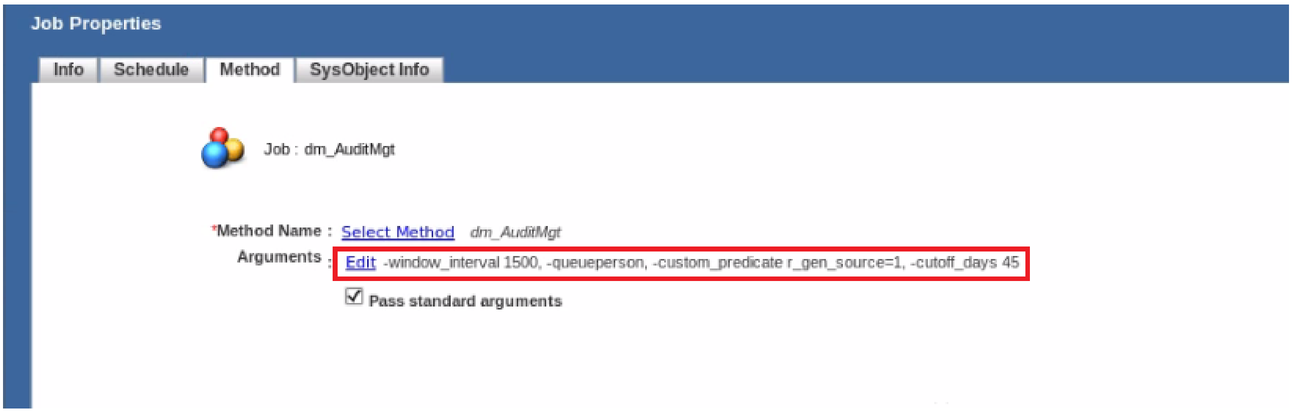
☑ Include all subtypes

☐ Authentication Required

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.



Job : dm_AuditMgt

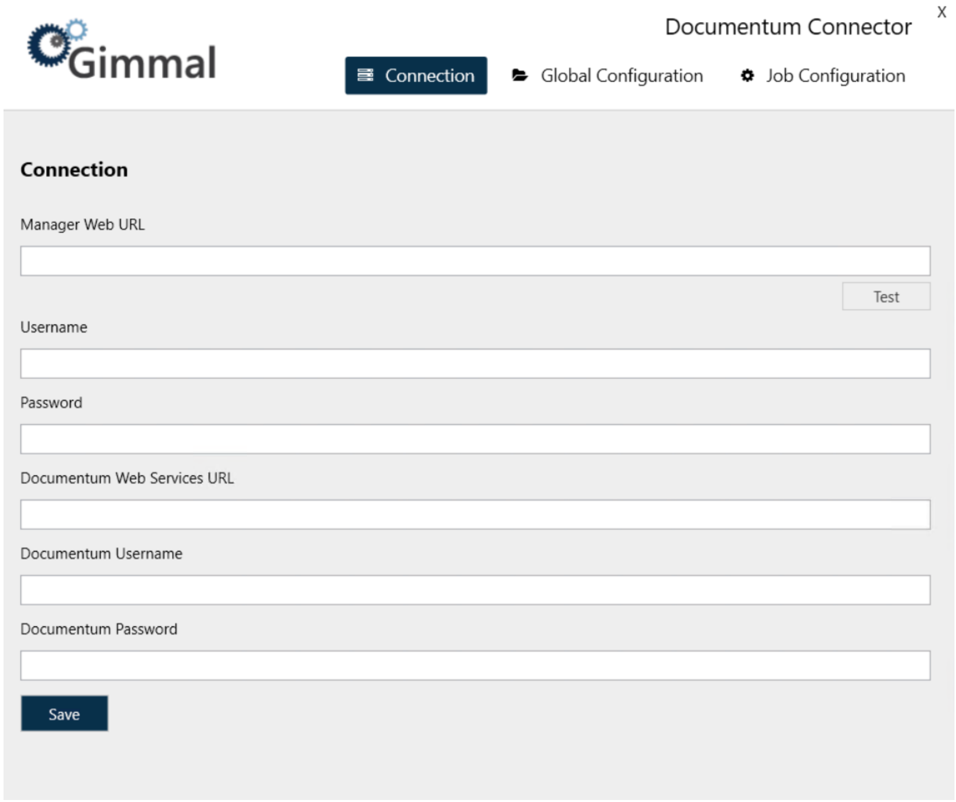
*Method Name : dm_AuditMgt

Arguments : -window_interval 1500, -queueperson, -custom_predicate r_gen_source=1, -cutoff_days 45

☑ Pass standard arguments

7.10.9.8 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.



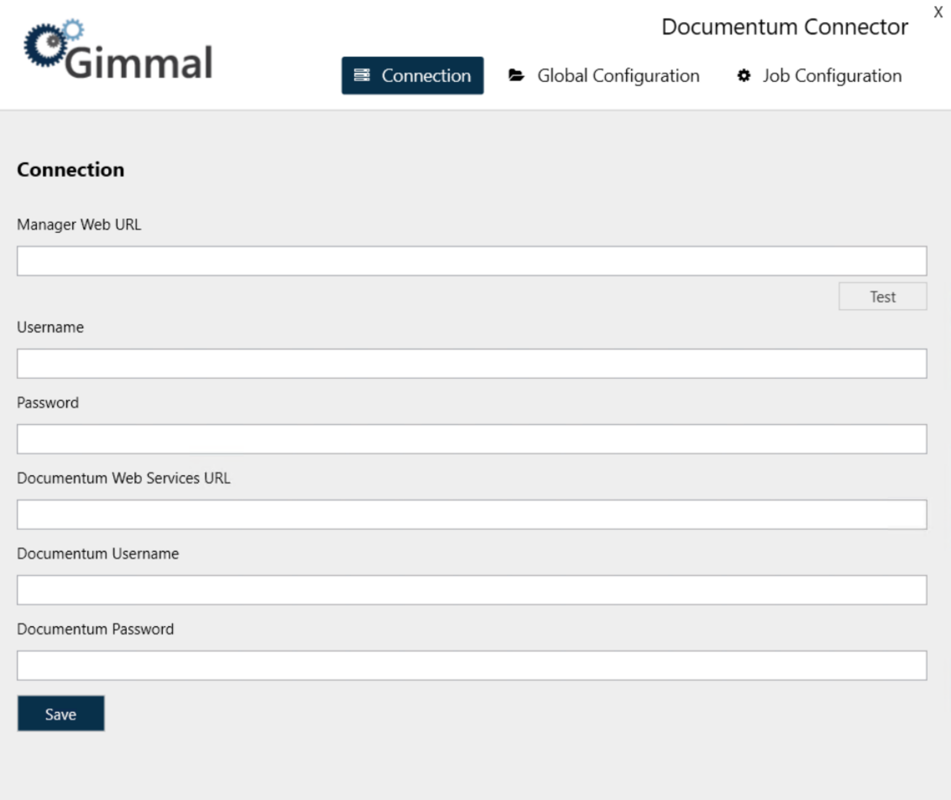
Configuring the Documentum Connection Settings

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.



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.

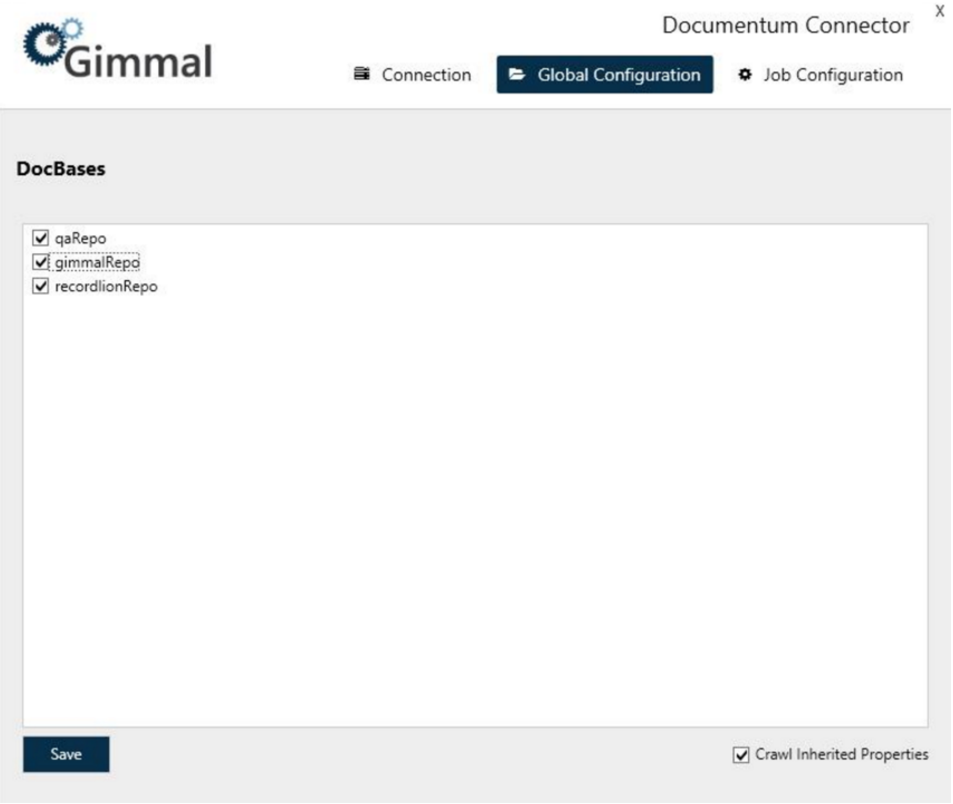
> ⓘ To ensure that all documents are entered into Records Management accurately, the DocBases you select on this tab must initially be crawled by the Custom Classification job described in Configuring the Documentum Job Configuration.

⚠ 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.



DocBases

☑ qaRepo
☑ gimmalRepo
☑ recordlionRepo

☑ Crawl Inherited Properties

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

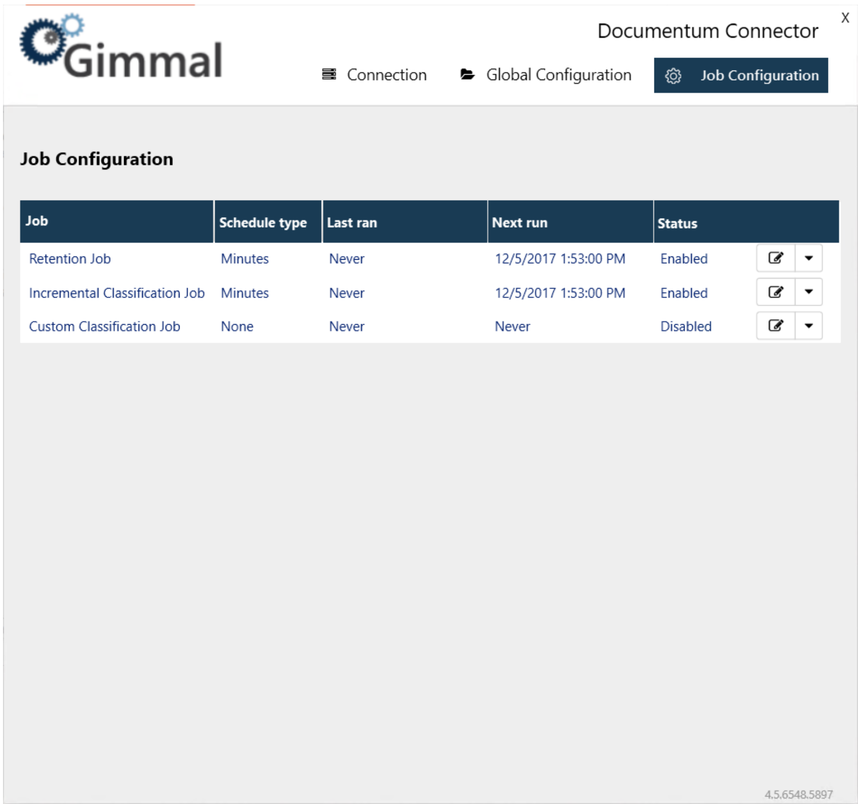
The Job Configuration dialog displays the retention and classification jobs included in the Documentum Connector, and enables you to either run the jobs immediately, or schedule how often you want the jobs to run. The jobs default to running every five minutes.

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.



Job Configuration

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

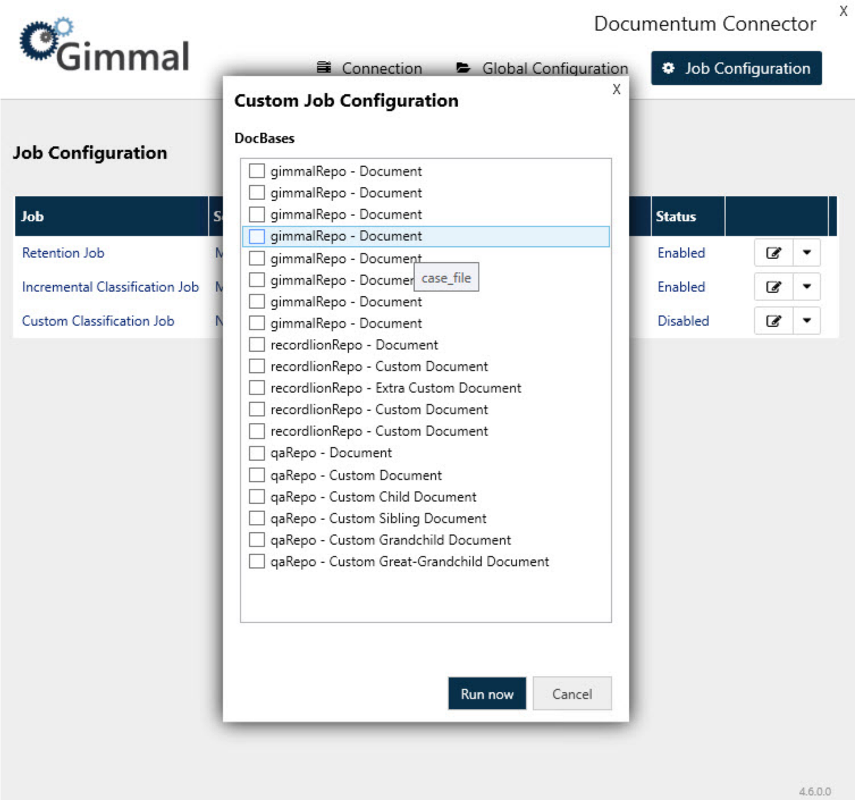
4.5.6548.5897

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 reenable 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.



Custom Job Configuration

DocBases

- □ gimmalRepo - Document
- □ gimmalRepo - Document
- □ gimmalRepo - Document
- □ gimmalRepo - Document
- □ gimmalRepo - Document
- □ gimmalRepo - Documer case_file
- □ gimmalRepo - Document
- □ gimmalRepo - Document
- □ recordlionRepo - Document
- □ recordlionRepo - Custom Document
- □ recordlionRepo - Extra Custom Document
- □ recordlionRepo - Custom Document
- □ recordlionRepo - Custom Document
- □ qaRepo - Document
- □ qaRepo - Custom Document
- □ qaRepo - Custom Child Document
- □ qaRepo - Custom Sibling Document
- □ qaRepo - Custom Grandchild Document
- □ qaRepo - Custom Great-Grandchild Document

Run now | Cancel

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
Gimmal 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.
Gimmal 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.

7.10.9.9 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 **Gimmal Documentum Connector** and double-click it. (You can also select Gimmal 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 Gimmal Documentum Classification Service and the Gimmal Documentum Retention Service no longer display in the Windows Services list.

7.10.9.10 Documentum Connector Upgrade from 5.1 to 5.1.1

Upgrade from version 5.1 to version 5.1.1

Prerequisites

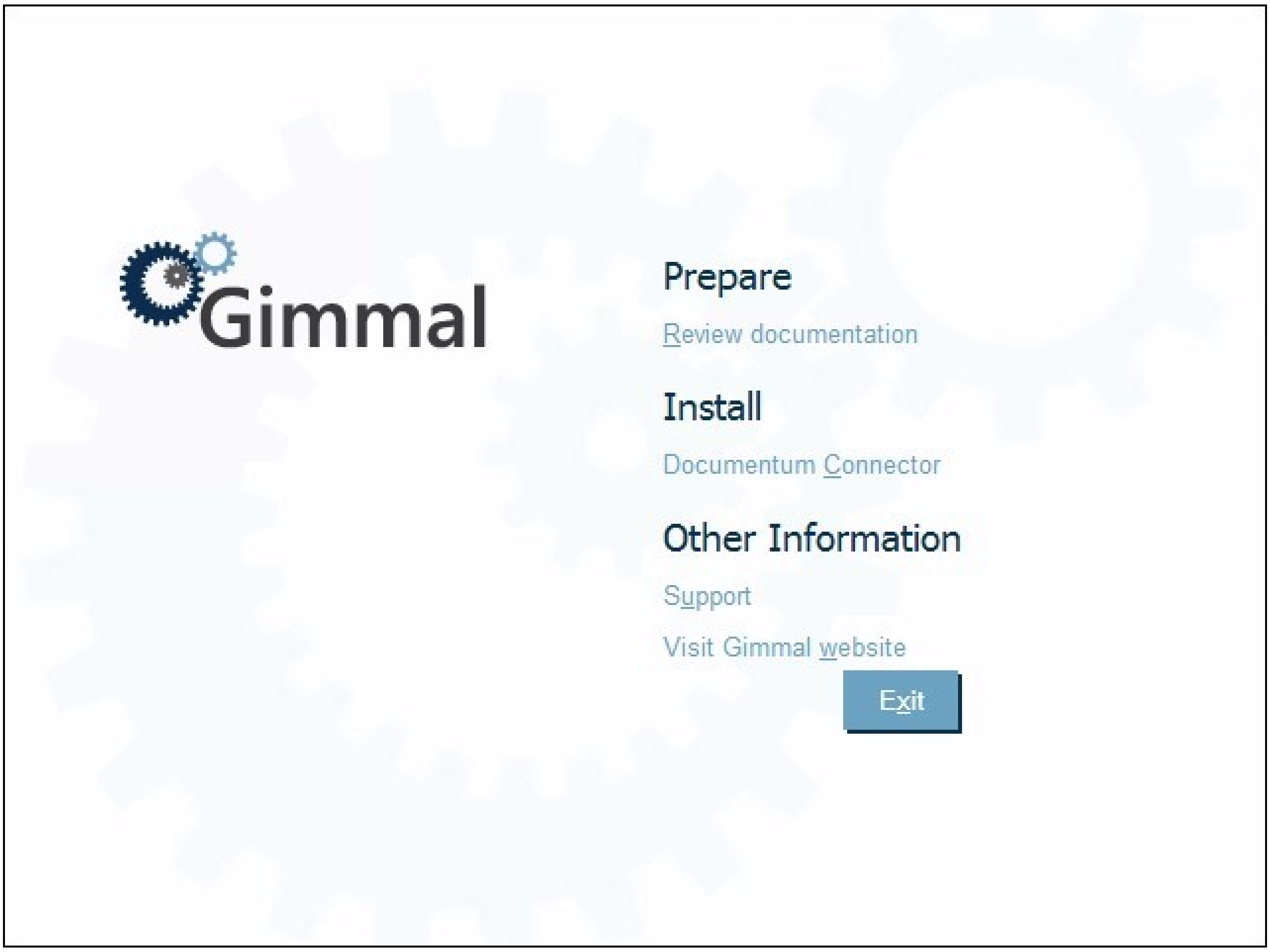
- The current user is a Local Administrator
- You have installed .NET Framework 4.5
- You have installed .NET Framework 3.5
- Connector system requirements[53].
- 100 MB of space available for the Documentum Connector
- A service account with Read / Write permissions to %Install path%\Logs

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:
   - Gimmal Documentum Classification Service
   - Gimmal Documentum Retention Service
3. Download the Documentum Connector ISO (Documentum Connector v5.1.1.iso) from the Gimmal Software Downloads[54] site. Once in the Gimmal 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 Gimmal Support[55].

Upon launching the Documentum Connector installer as the Local Administrator, the following screen displays:

[53] https://docs.gimmal.com/rm/5.1/Server/documentum-connector-system-requirements
[54] https://gimmal1.sharepoint.com/sites/EXT-Software/SitePages/Home.aspx
[55] https://support.gimmal.com



Upgrading the Documentum Connector

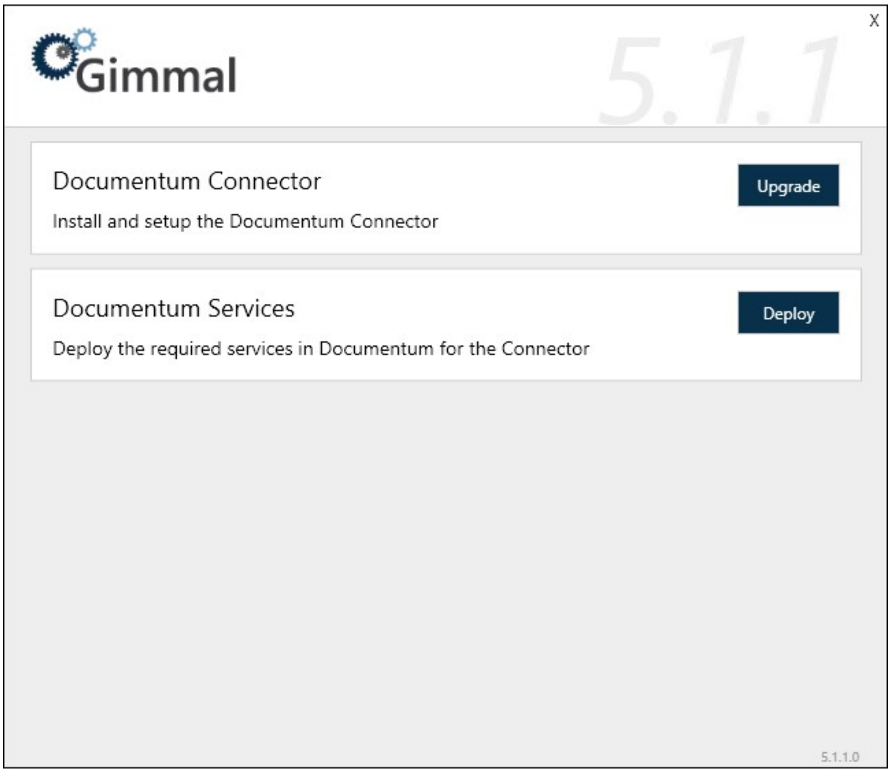
Before you upgrade the Documentum Connector, verify the Connector system requirements[56]. This upgrade section also assumes that you have already installed the Records Management Core platform.

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.

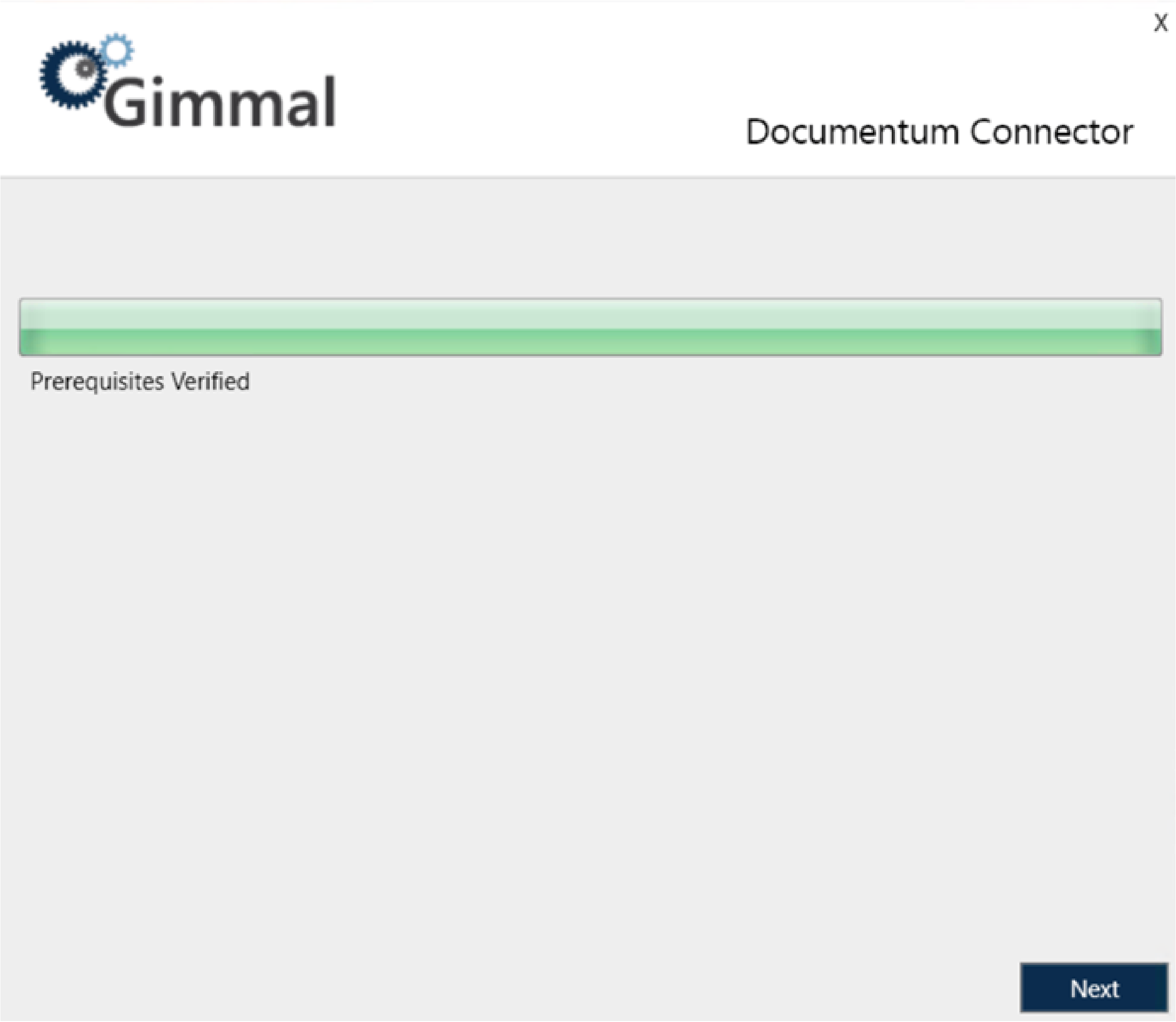
5. On the Documentum Connector installation screen, click **Upgrade** to the right of the Documentum Connector option. The first window that displays is the check for prerequisites.

[56] https://docs.gimmal.com/rm/5.1/Server/documentum-connector-system-requirements


X
Gimmal
5.1.1
Documentum Connector
Install and setup the Documentum Connector
Upgrade
Documentum Services
Deploy the required services in Documentum for the Connector
Deploy
5.1.1.0

This window validates the following information before allowing the installation to proceed:

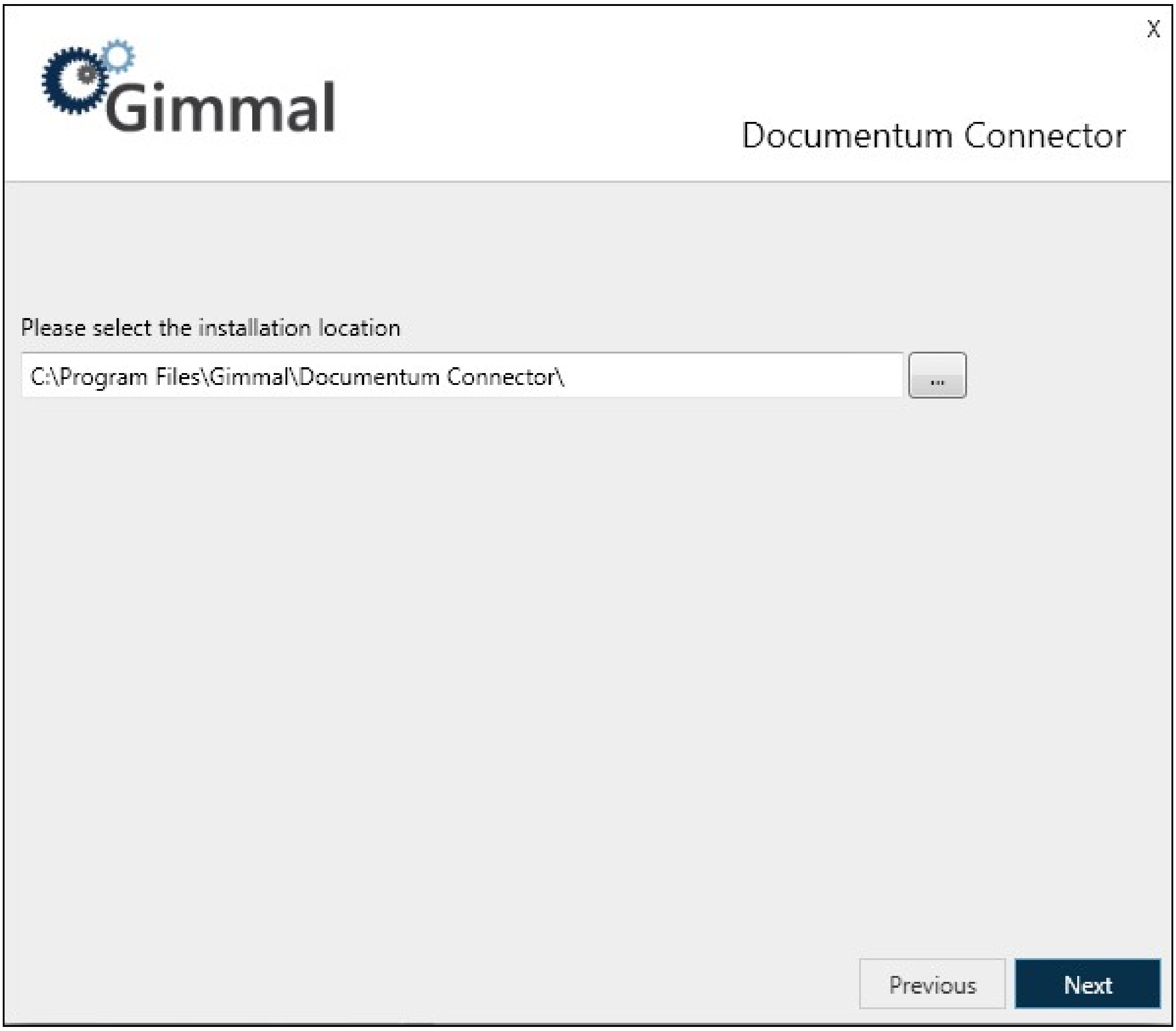
- The current user is a Local Administrator
- You have installed .NET Framework 4.5
- You have installed .NET Framework 3.5



Prerequisites Verified

6. Click **Next**. The installation location screen is displayed. This determines where the connector will be installed.

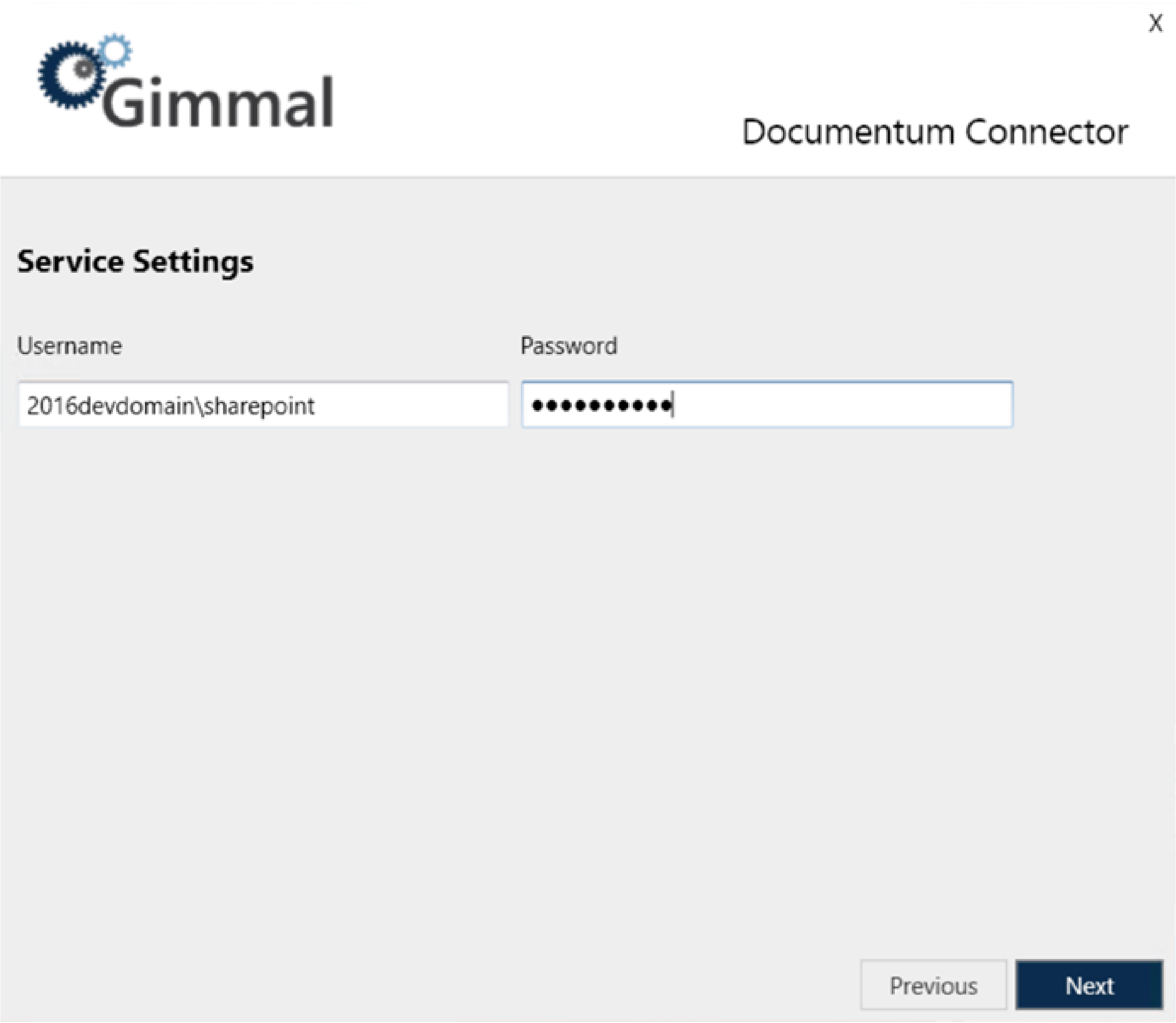
7. Leave the installation path as the default, or to change it, click the ... icon next to the installation location field, select the desired installation location, and then click **Next**.



Please select the installation location

C:\Program Files\Gimmal\Documentum Connector\

You must have at least 100MB of disk space available.



Service Settings

Username

2016devdomain\sharepoint

Password

●●●●●●●●●●●

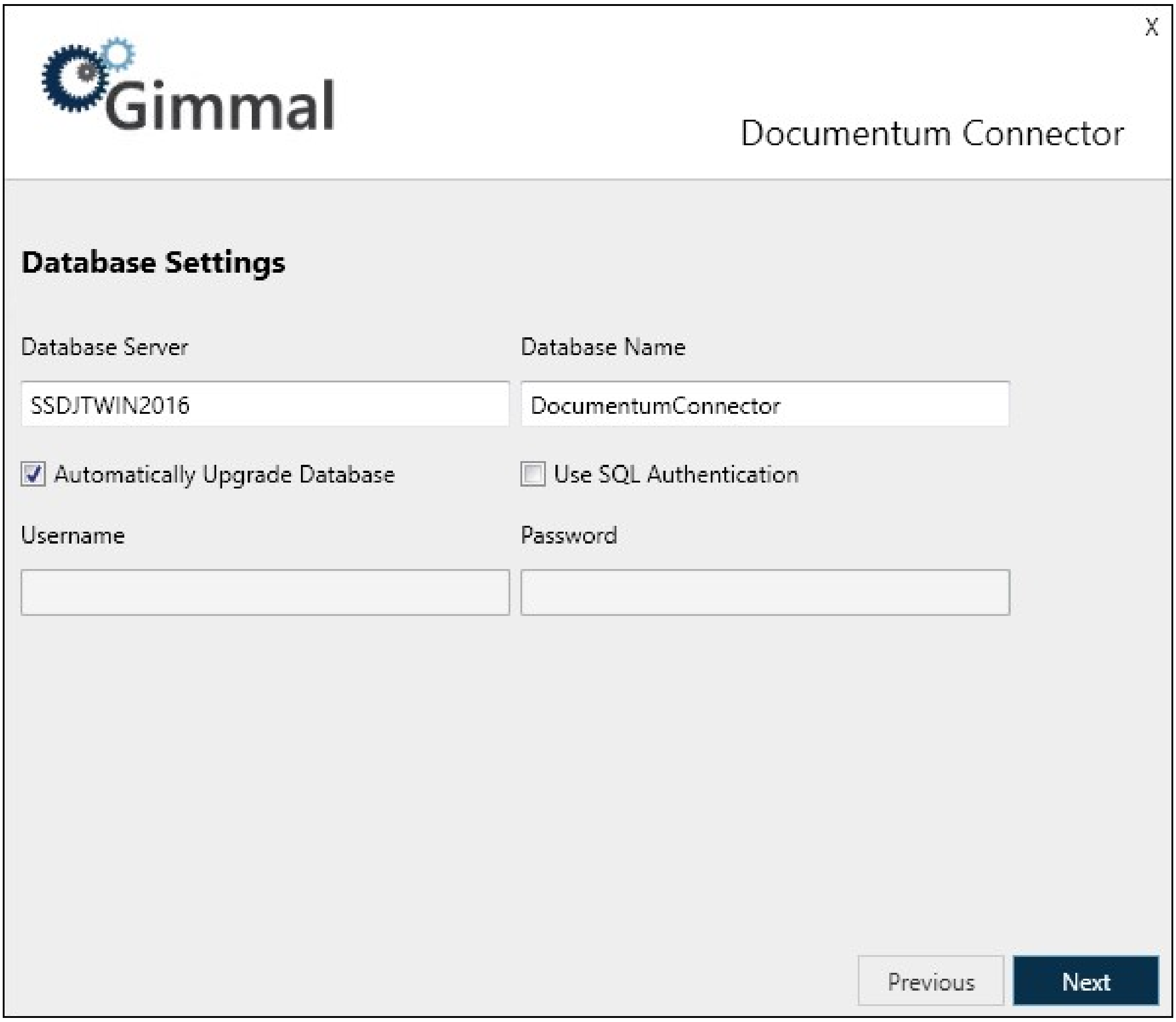
8. Enter the following required information to specify which user account to use when you run the Windows Services:

- **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

9. Click **Next**. The Database Settings screen displays.



Database Settings

Database Server: SSDJTWIN2016

Database Name: DocumentumConnector

☑ Automatically Upgrade Database

□ Use SQL Authentication

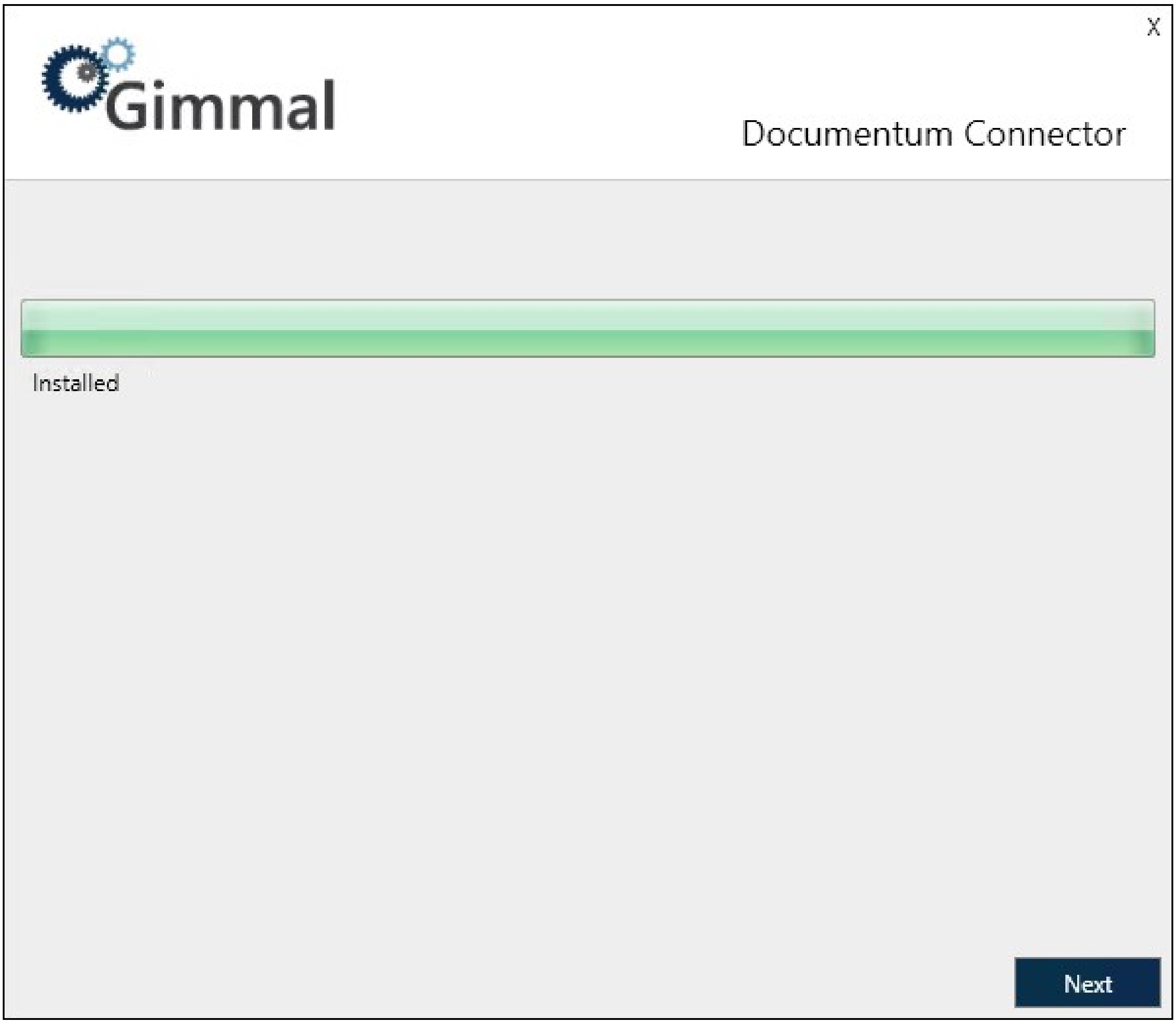
Username

Password

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.

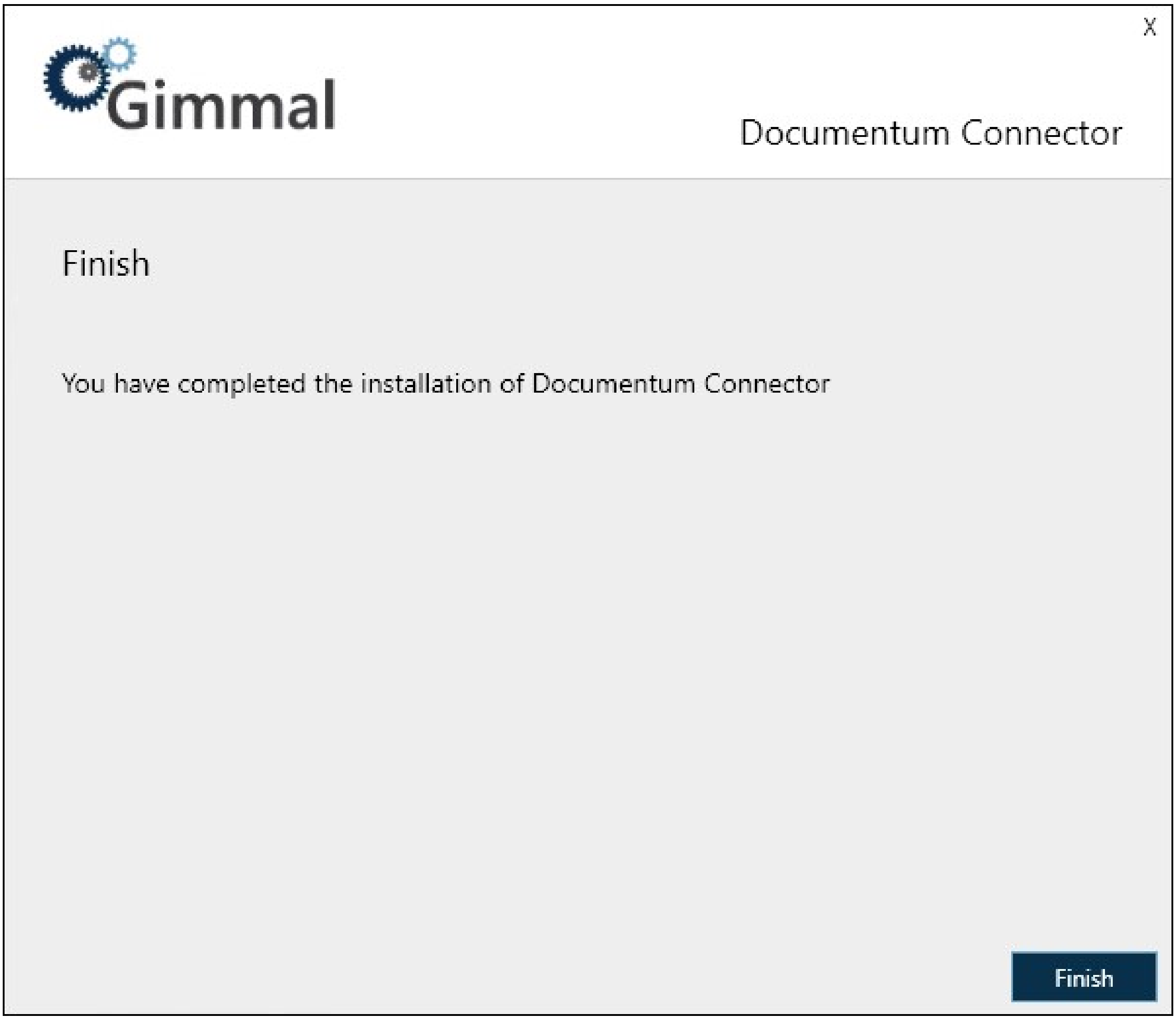
Click **Next** to perform the final installation using the database settings you specified above. The progress bar indicates the state of the installation

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).

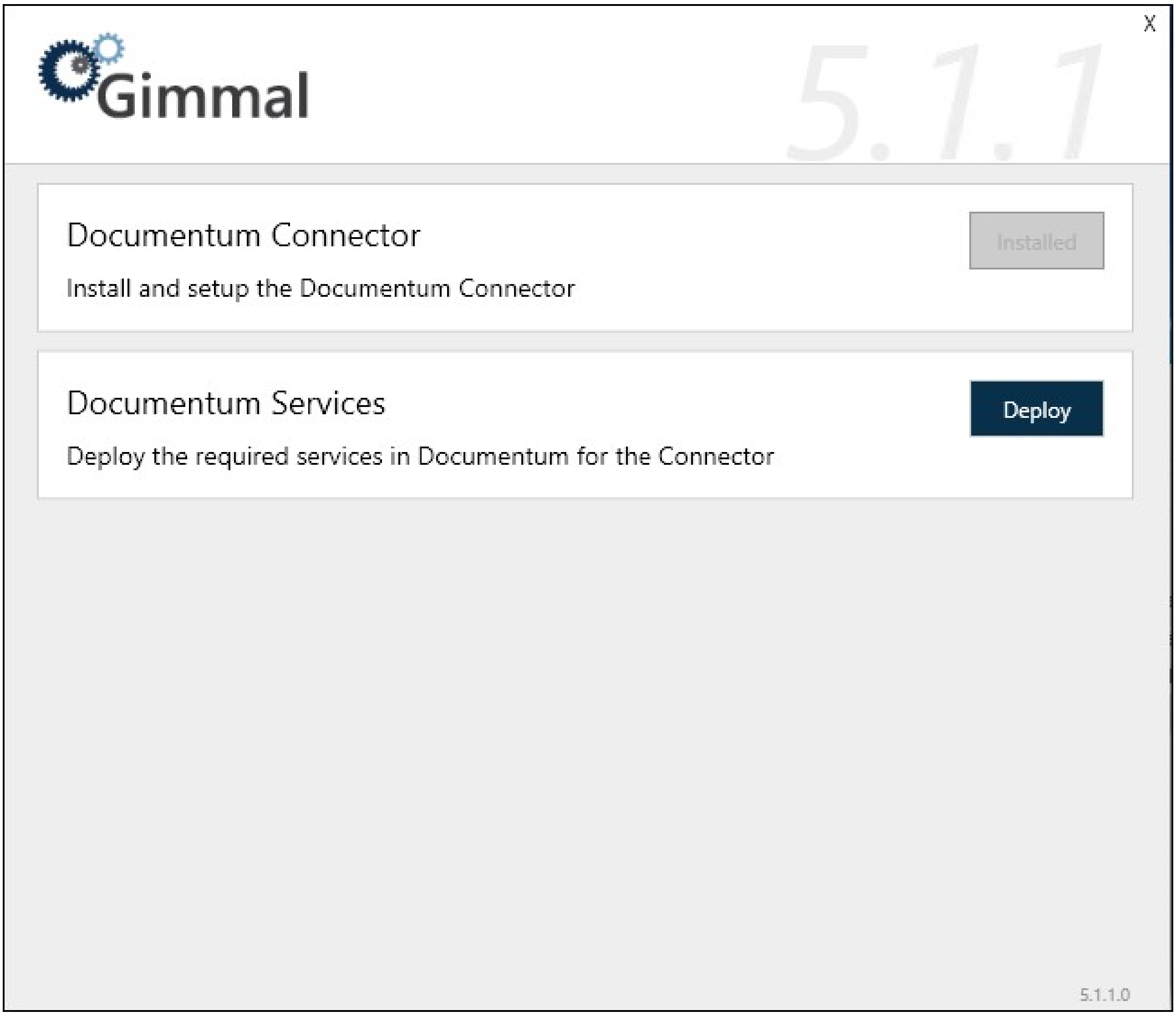
11. Click **Finish** to return to the main Setup screen, which should now indicate that the Documentum Connector was installed successfully.



Finish

You have completed the installation of Documentum Connector

12. After clicking Finish, you will see the initial installation screen showing that the Documentum Connector was installed.



Documentum Connector

Install and setup the Documentum Connector

Documentum Services

Deploy the required services in Documentum for the Connector

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.

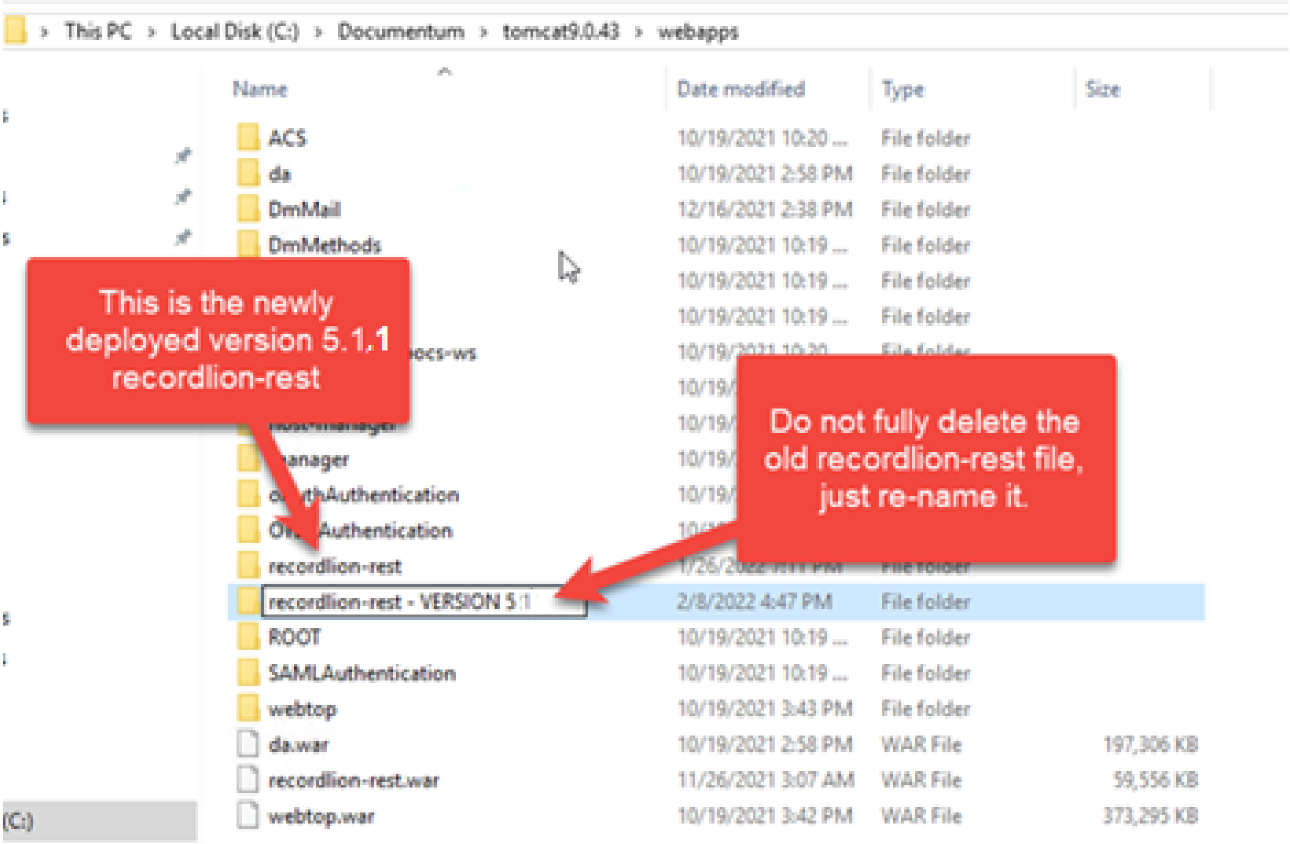
f. Expand the nodes: **DocumentumConnector** > **Security** > **Users**, and then verify that the Service/User account that was created during the installation steps above is listed and has the correct permissions.

15. Continue the installation process by installing the Documentum Services component. For information, see Installing Documentum Services[57].

16. Deploy the recordlion-rest war file by following these steps[58].

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.


This PC › Local Disk (C:) › Documentum › tomcat9.0.43 › webapps
(C:)

Name	Date modified	Type	Size
ACS	10/19/2021 10:20 ...	File folder	
da	10/19/2021 2:58 PM	File folder	
DmMail	12/16/2021 2:38 PM	File folder	
DmMethods	10/19/2021 10:19 ...	File folder	
[illegible]	10/19/2021 10:19 ...	File folder	
[illegible]	10/19/2021 10:19 ...	File folder	
[illegible]ocs-ws	10/19/2021 10:20	File folder	
[illegible]	10/19/[illegible]	[illegible]	
[illegible]	10/19/[illegible]	[illegible]	
[illegible]anager	10/19/[illegible]	[illegible]	
o[illegible]thAuthentication	10/19/[illegible]	[illegible]	
O[illegible] Authentication	10/[illegible]	[illegible]	
recordlion-rest	1/26/2022 [illegible] PM	File folder	
recordlion-rest - VERSION 5.1	2/8/2022 4:47 PM	File folder	
ROOT	10/19/2021 10:19 ...	File folder	
SAMLAuthentication	10/19/2021 10:19 ...	File folder	
webtop	10/19/2021 3:43 PM	File folder	
da.war	10/19/2021 2:58 PM	WAR File	197,306 KB
recordlion-rest.war	11/26/2021 3:07 AM	WAR File	59,556 KB
webtop.war	10/19/2021 3:42 PM	WAR File	373,295 KB

This is the newly deployed version 5.1.1 recordlion-rest

Do not fully delete the old recordlion-rest file, just re-name it.

17. Perform this step if you are deploying a new recordlion-net.war file in Step 16 above:

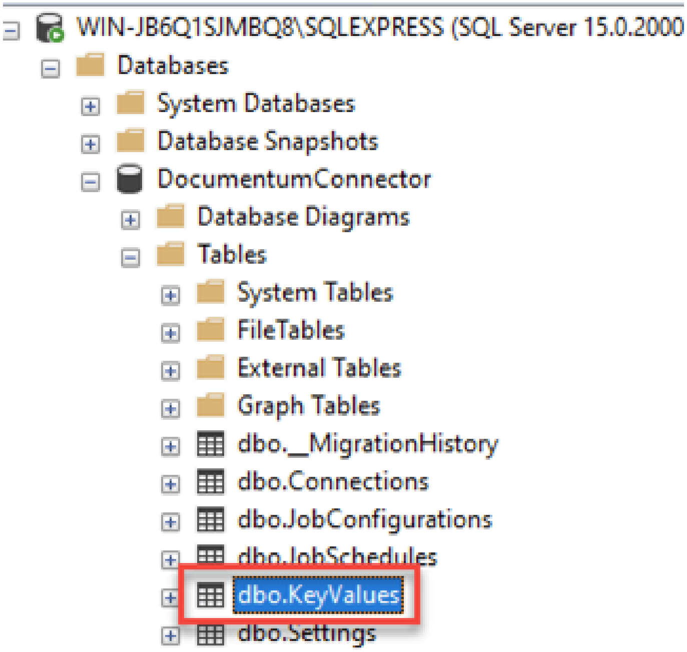
Update the **dfc.properties** file for the **recordlion-rest** by following these steps[59].

If you do not know where to find the dfc. properties, reference step 1 in the prerequisites.

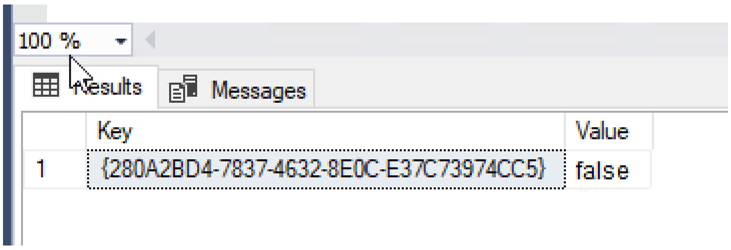
18. Confirm the KeyValue tables have been added to the **DocumentumConnector** table

o Expand the **DocumentumConnector** database in SQL Server Management Studio, then expand **Tables.** Then right-mouse-click on the KeyValues table and choose Select Top 1000 Rows…

[57] https://docs.gimmal.com/rm/5.1/Server/documentum-services-installation
[58] https://docs.gimmal.com/rm/5.1/Server/documentum-services-installation
[59] https://docs.gimmal.com/rm/5.1/Server/applying-documentum-foundation-class-properties

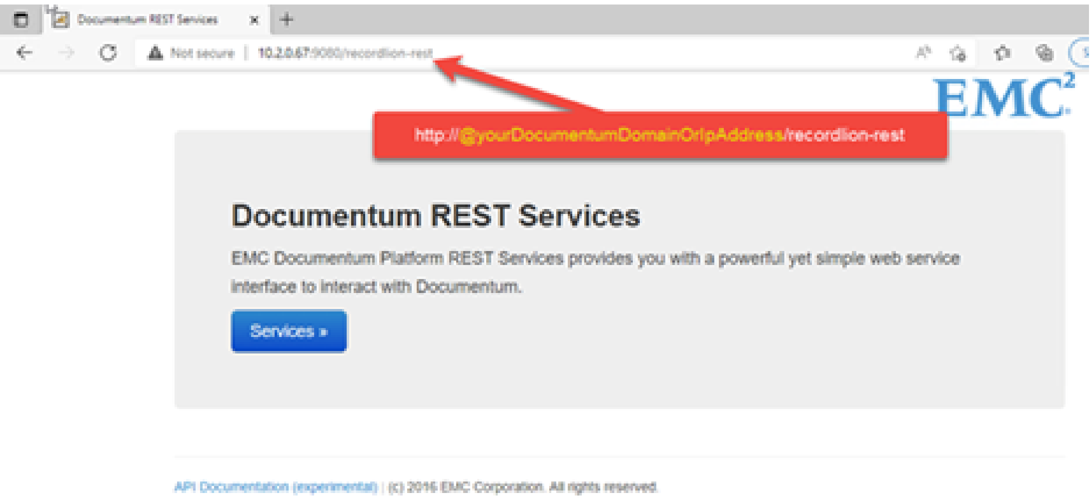


o Confirm that there is an entry in the **KeyValues** table that has a value of **false**



	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*[60]-, and confirm that the web page below renders.


Documentum REST Services
Not secure
10.2.0.67:9080/recordlion-rest
EMC²
http://@yourDocumentumDomainOrIpAddress/recordlion-rest
Services »

Documentum REST Services

EMC Documentum Platform REST Services provides you with a powerful yet simple web service interface to interact with Documentum.

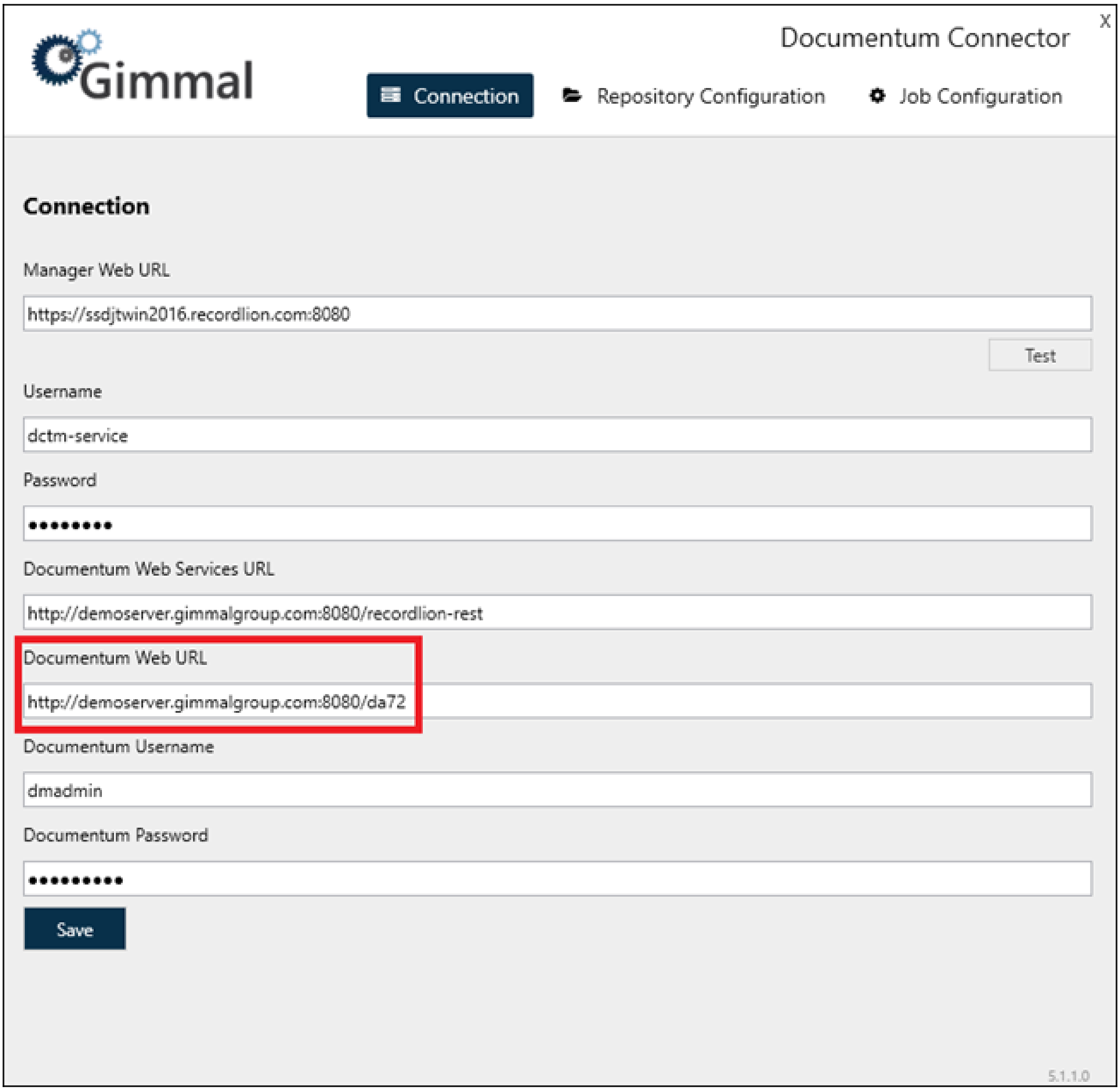
API Documentation (experimental) | (c) 2016 EMC Corporation. All rights reserved.

[60] http://yourdocumentumdomainoripaddress/recordlion-rest

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.



Connection

Manager Web URL

https://ssdjtwin2016.recordlion.com:8080

Username

dctm-service

Password

••••••••

Documentum Web Services URL

http://demoserver.gimmalgroup.com:8080/recordlion-rest

Documentum Web URL

http://demoserver.gimmalgroup.com:8080/da72

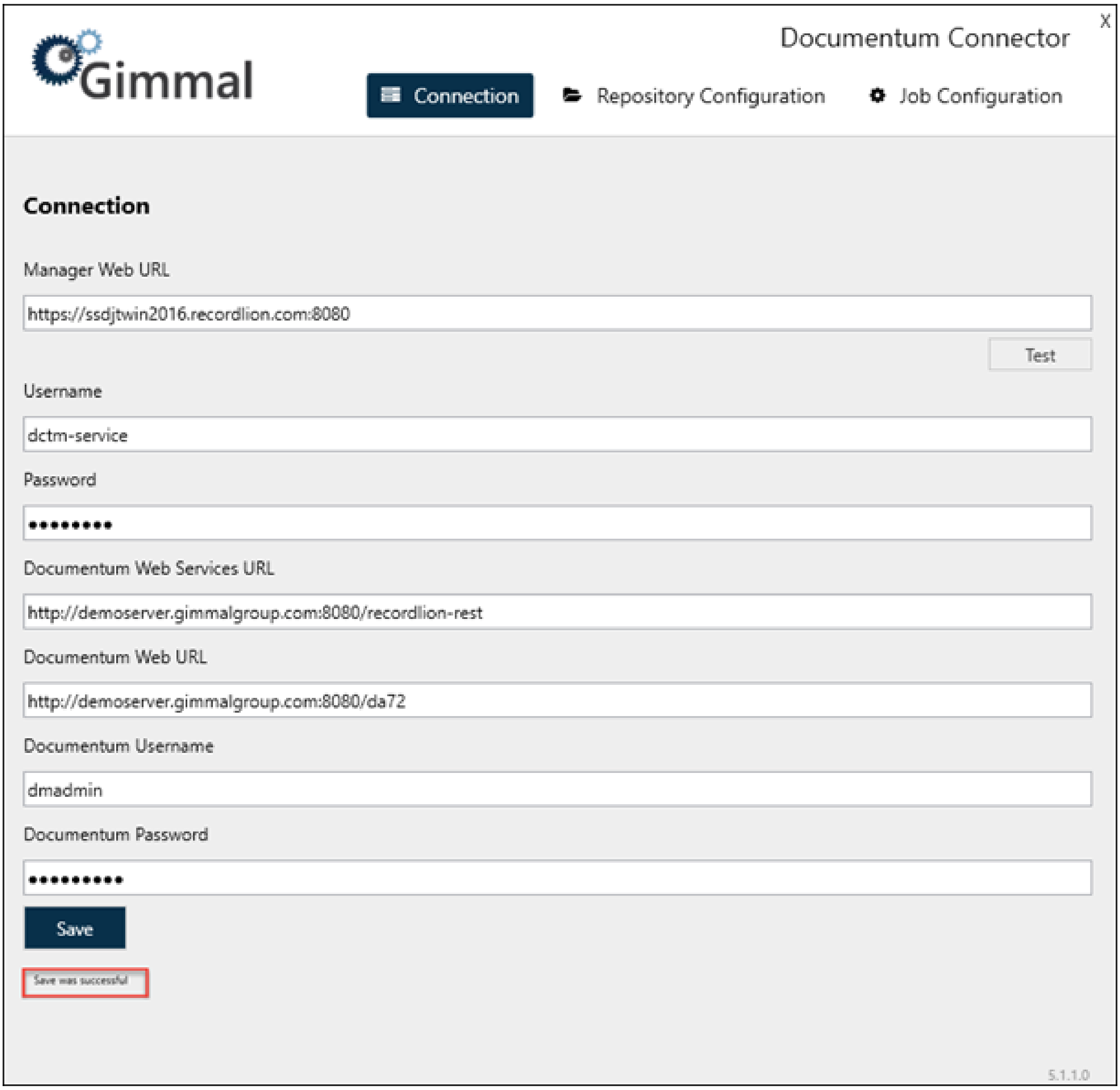
Documentum Username

dmadmin

Documentum Password

•••••••••

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.



Connection

Manager Web URL

https://ssdjtwin2016.recordlion.com:8080

Username

dctm-service

Password

••••••••

Documentum Web Services URL

http://demoserver.gimmalgroup.com:8080/recordlion-rest

Documentum Web URL

http://demoserver.gimmalgroup.com:8080/da72

Documentum Username

dmadmin

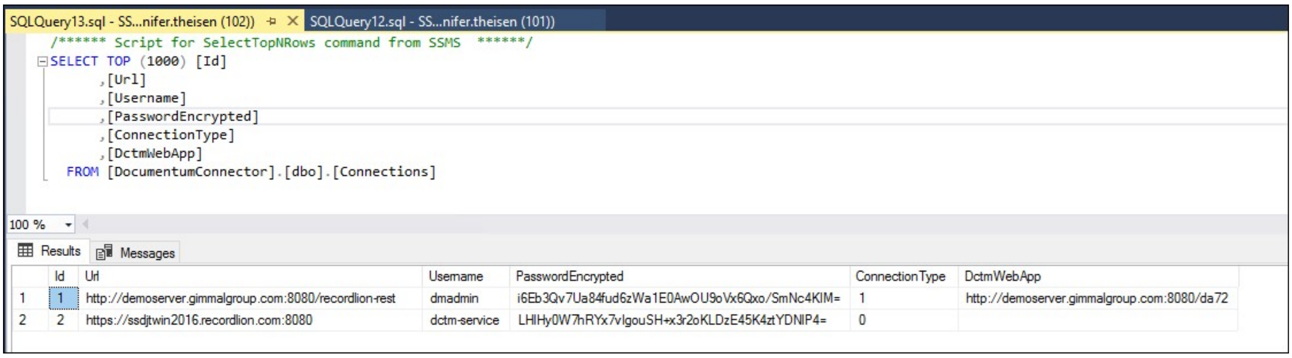
Documentum Password

•••••••••

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.

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:



SQLQuery13.sql - SS...nifer.theisen (102))
SQLQuery12.sql - SS...nifer.theisen (101))
100 %
Results
Messages

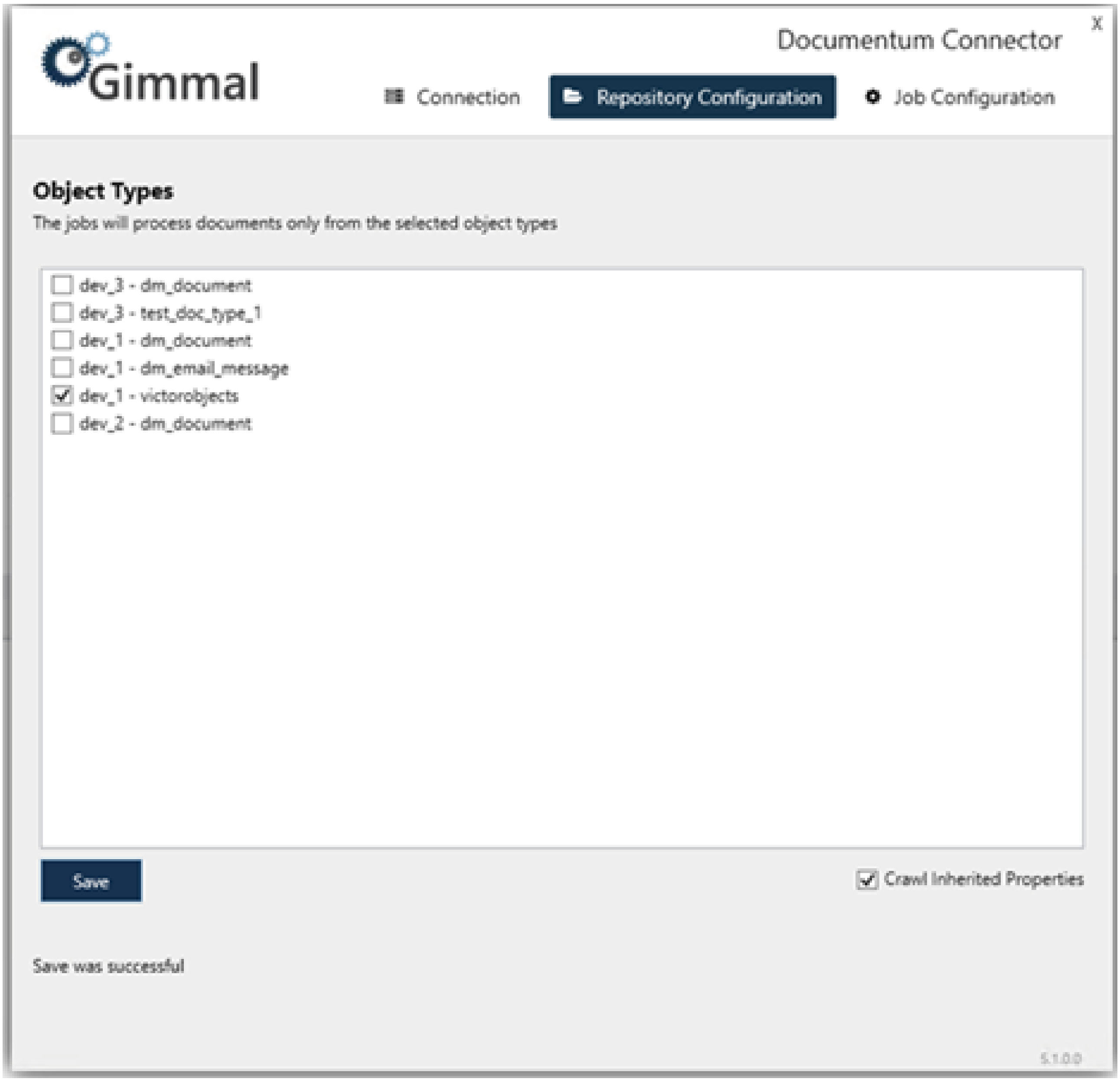
```
/****** Script for SelectTopNRows command from SSMS  ******/
SELECT TOP (1000) [Id]
      ,[Url]
      ,[Username]
      ,[PasswordEncrypted]
      ,[ConnectionType]
      ,[DctmWebApp]
  FROM [DocumentumConnector].[dbo].[Connections]
```

	Id	Url	Username	PasswordEncrypted	ConnectionType	DctmWebApp
1	1	http://demoserver.gimmalgroup.com:8080/recordlion-rest	dmadmin	i6Eb3Qv7Ua84fud6zWa1E0AwOU9oVx6Qxo/SmNc4KIM=	1	http://demoserver.gimmalgroup.com:8080/da72
2	2	https://ssdjtwin2016.recordlion.com:8080	dctm-service	LHIHy0W7hRYx7vIgouSH+x3r2oKLDzE45K4ztYDNIP4=	0	

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.



Documentum Connector

Object Types

The jobs will process documents only from the selected object types

- ☐ dev_3 - dm_document
- ☐ dev_3 - test_doc_type_1
- ☐ dev_1 - dm_document
- ☐ dev_1 - dm_email_message
- ☑ dev_1 - victorobjects
- ☐ dev_2 - dm_document

☑ Crawl Inherited Properties

Save was successful

8. Start Documentum Connector Services:

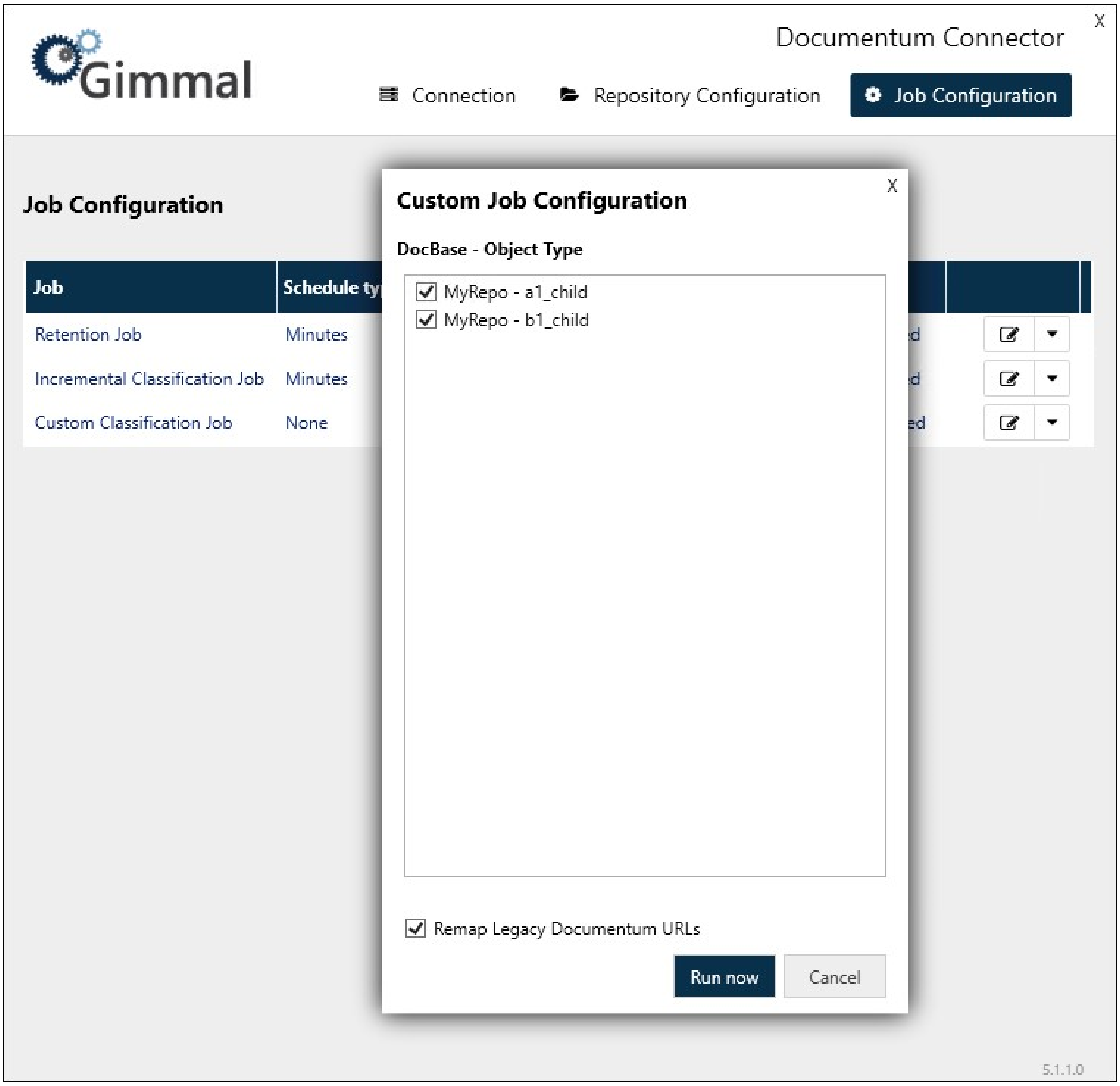
- Gimmal Documentum Classification Service
- Gimmal Documentum Retention Service

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-recordizing 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 ty		
Retention Job	Minutes	d	
Incremental Classification Job	Minutes	d	
Custom Classification Job	None	ed	

Custom Job Configuration

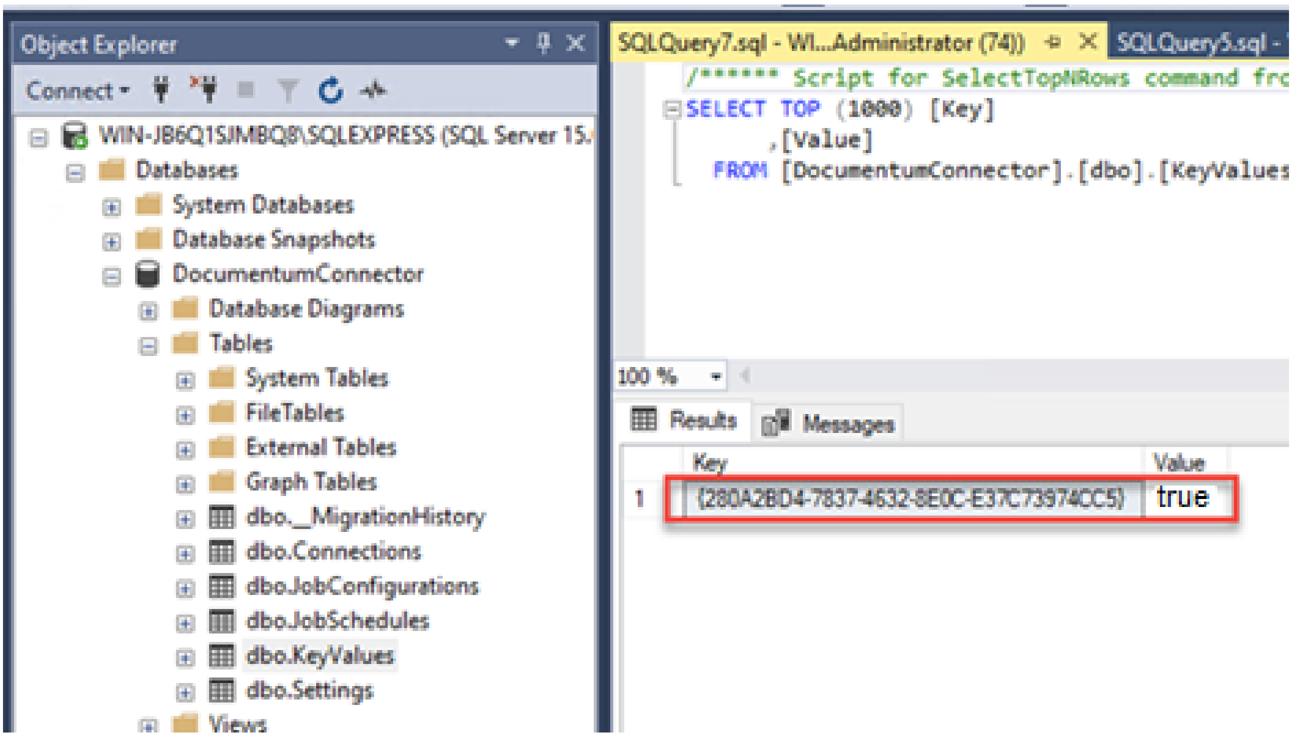
DocBase - Object Type

☑ MyRepo - a1_child
☑ MyRepo - b1_child

☑ Remap Legacy Documentum URLs

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.



```
/****** Script for SelectTopNRows command fro
SELECT TOP (1000) [Key]
      ,[Value]
  FROM [DocumentumConnector].[dbo].[KeyValues
```

	Key	Value
1	{280A2BD4-7837-4632-8E0C-E37C73974CC5}	true

12. The upgrade to version 5.1.1 is complete. Please re-enable retention and incremental classifications to proceed.

7.10.10 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.

7.10.10.7 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 Gimmal 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, Gimmal 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[61] To verify that your operating system supports TLS 1.2, read the Support for TLS 1.2 section of Microsoft's documentation[62].

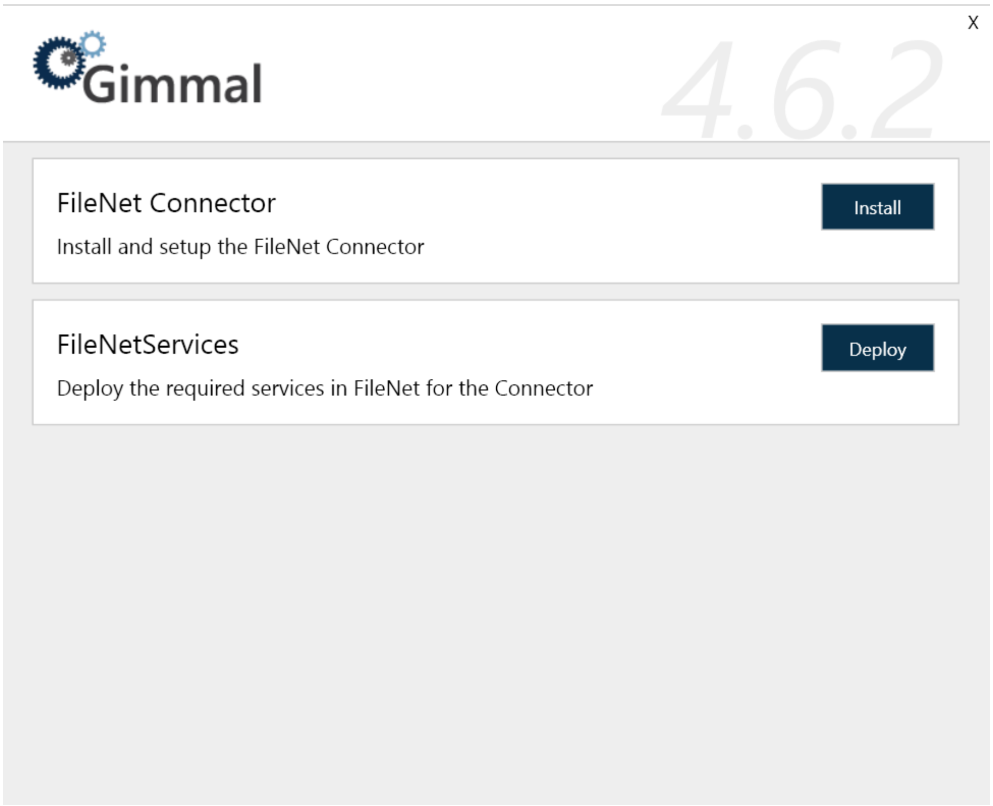
Database Server

- SQL Server 2016 or greater
- 100 MB for FileNet Database

7.10.10.8 FileNet Connector Installation

⚠ Ensure that you run the installer as the Local Administrator.

Upon launching the FileNet Connector installer, the following screen displays:



FileNet Connector

Install and setup the FileNet Connector

FileNetServices

Deploy the required services in FileNet for the Connector

[61] https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls#systemdefaulttlsversions
[62] https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls#support-for-tls-12

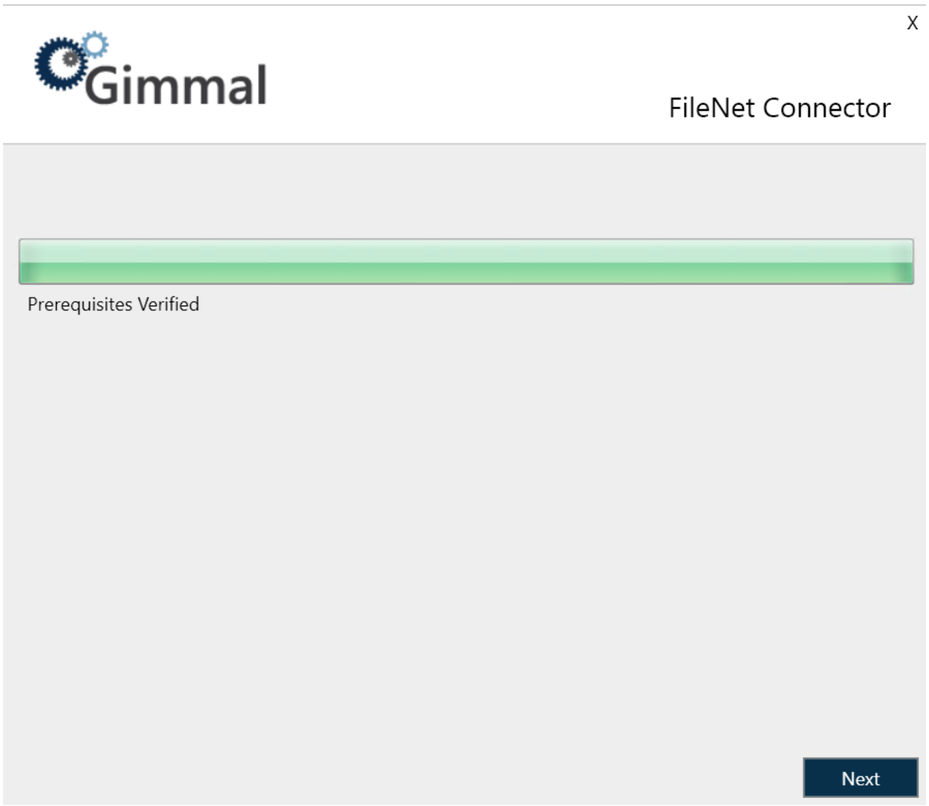
Installing the FileNet Connector

Before you install the FileNet Connector, verify the Connector system requirements.(see page 290) This installation section assumes that you have already installed the Records Management Core platform.

> When you install the FileNet Connector, a Configuration Application and two Records Management Windows Services are installed automatically as part of this process.

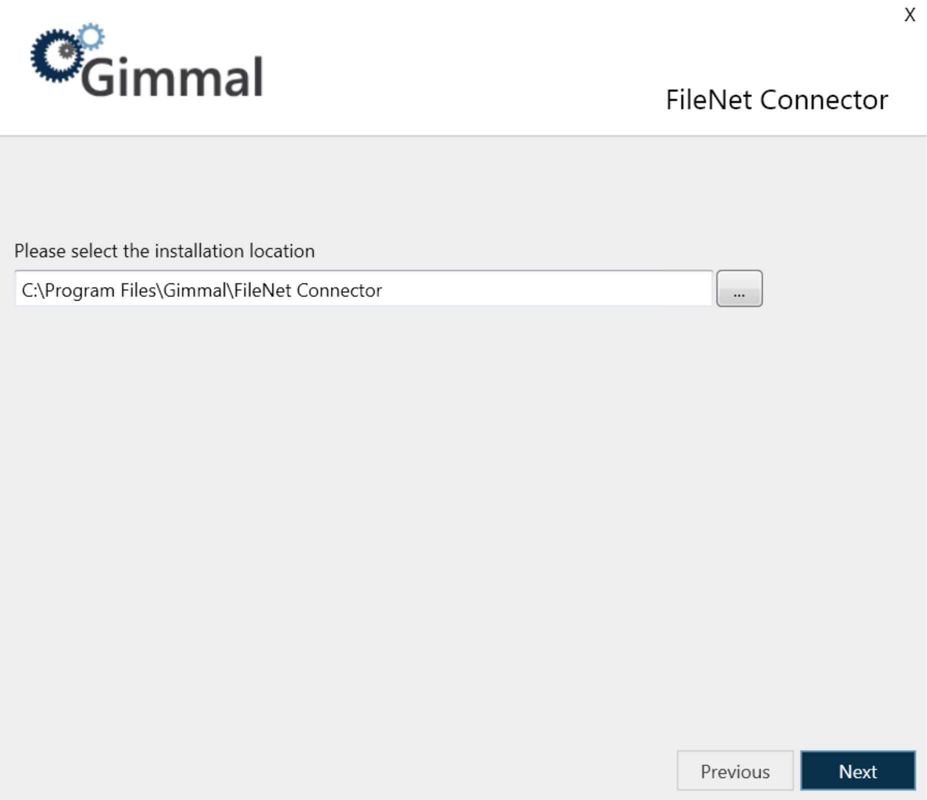
To install the FileNet Connector, perform the following steps:

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



Prerequisites Verified

4. Click **Next**. The installation location screen displays, which determines where the connector will be installed.

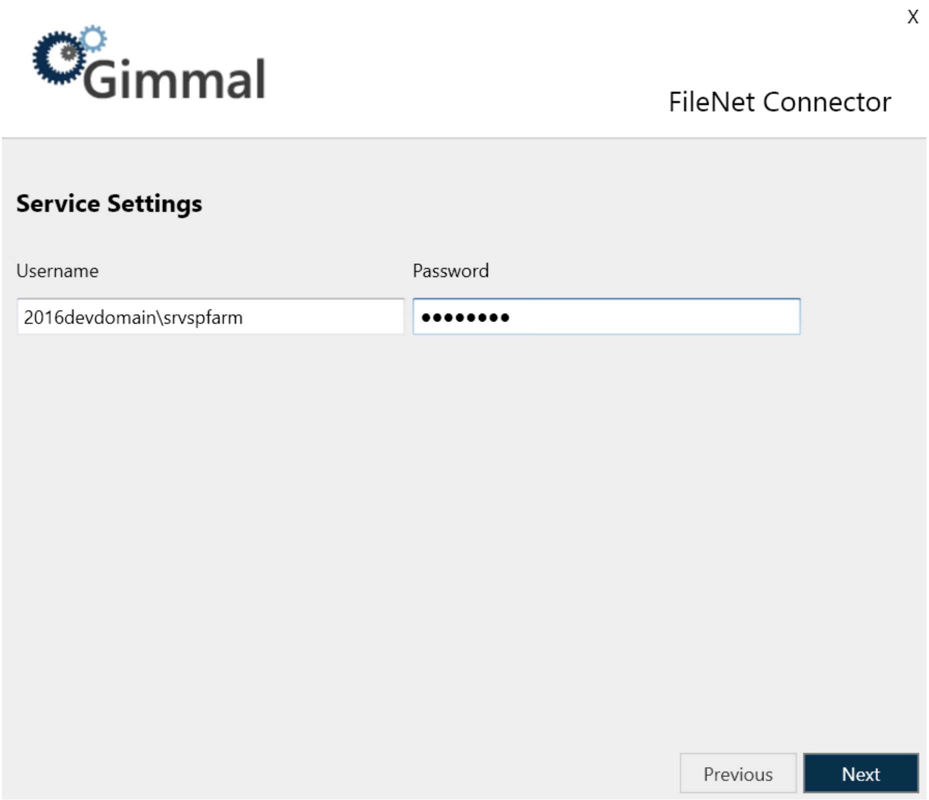


Please select the installation location

C:\Program Files\Gimmal\FileNet Connector

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.



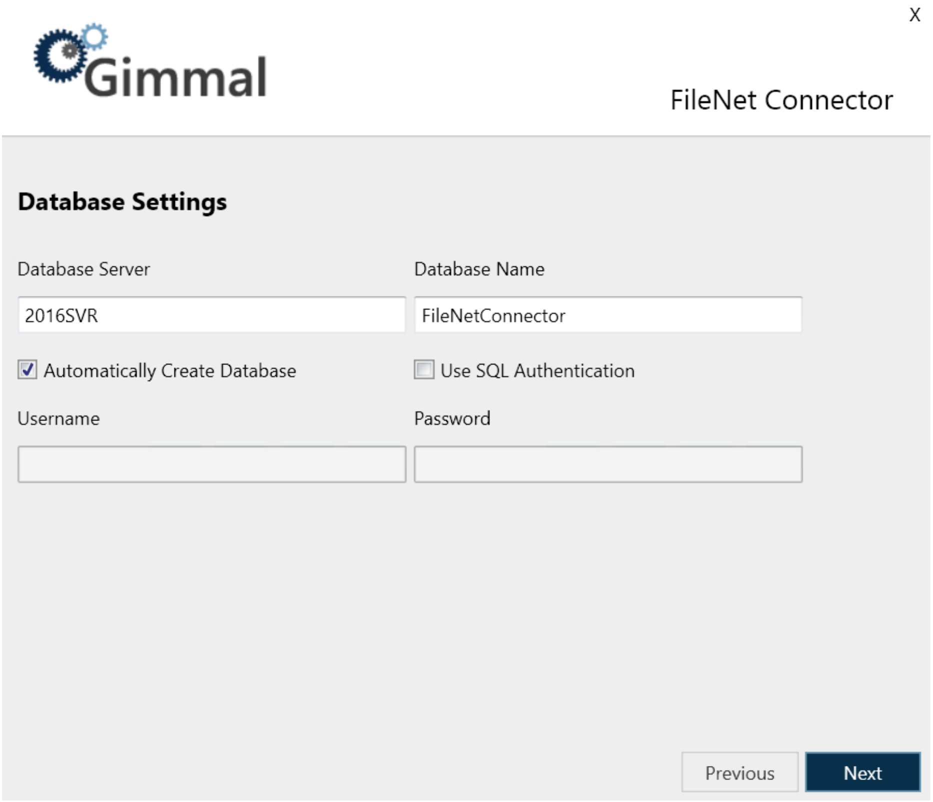
Service Settings

Username: 2016devdomain\srvspfarm

Password: ●●●●●●●●

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.



Database Settings

Database Server: 2016SVR

Database Name: FileNetConnector

☑ Automatically Create Database

□ Use SQL Authentication

Username:

Password:

⚠ 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 **Gimmal FileNet Classification Service** and the **Gimmal 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[63].

7.10.10.9 FileNet Services Installation

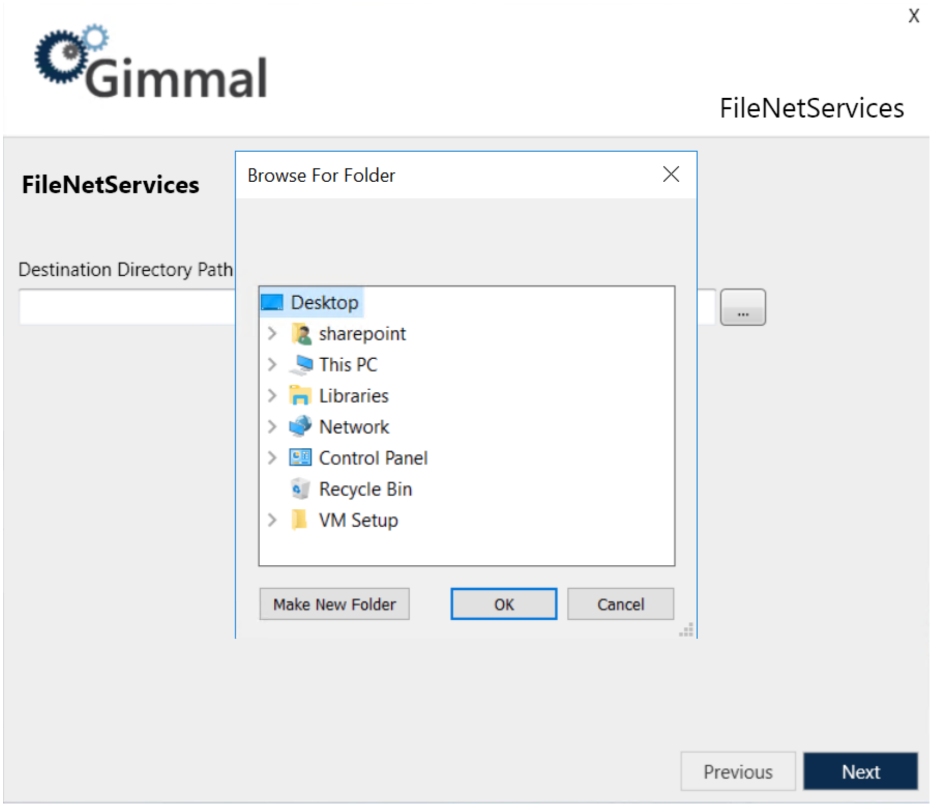
The FileNet Services component deploys required services and components into the FileNet Server, which the FileNet Connector will leverage to communicate with FileNet. Additionally, a .WAR file*, which contains the services that are deployed to the FileNet farm, is deployed. The FileNet Connector uses 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.

[63] http://docs.gimmal.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[64]. 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.

[64] http://docs.gimmal.com/en/14452-installing-filenet-services.html

7.10.10.10 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 &lt;TOMCAT INSTALLATION DIRECTORY&gt;\webapps\filenet-rest\WEB-INF\classes, and edit the file. The following section lists the properties and values.

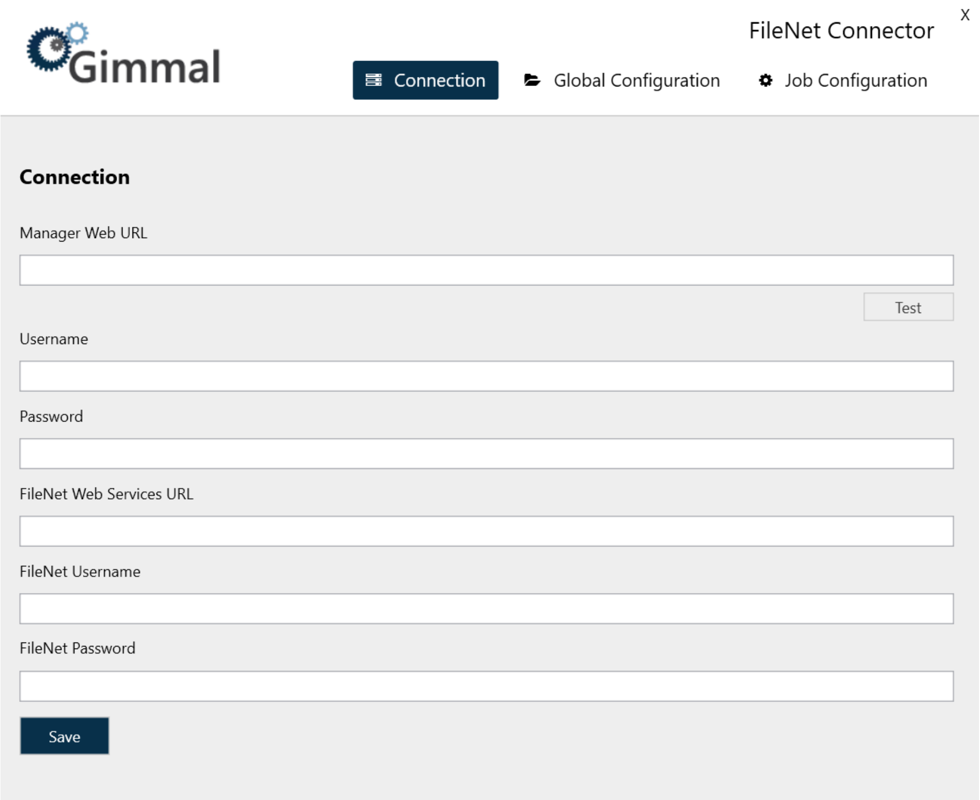
Application.Properties File Properties and Values

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.)

7.10.10.11 FileNet Connector Configuration

he 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.



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 Gimmal

1. Launch the Gimmal 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 multipleFileNet 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

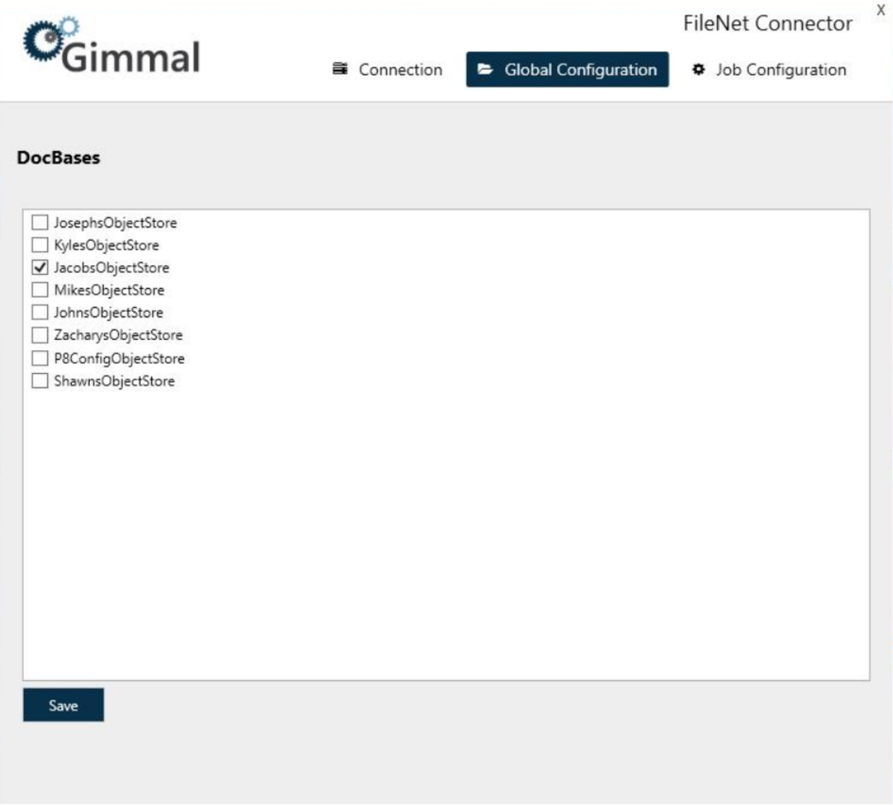
The Global Configuration dialog enables you to select which Libraries you would like to classify and apply retention actions to. Different Libraries support different users, departments, operations, etc.

> ⚠ 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.)

> ⓘ 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.



DocBases

☐ JosephsObjectStore
☐ KylesObjectStore
☑ JacobsObjectStore
☐ MikesObjectStore
☐ JohnsObjectStore
☐ ZacharysObjectStore
☐ P8ConfigObjectStore
☐ ShawnsObjectStore

2. Select the desired Library(s).
3. Click **Save**.
4. Continue with the next section

Configuring the FileNet Job Configuration

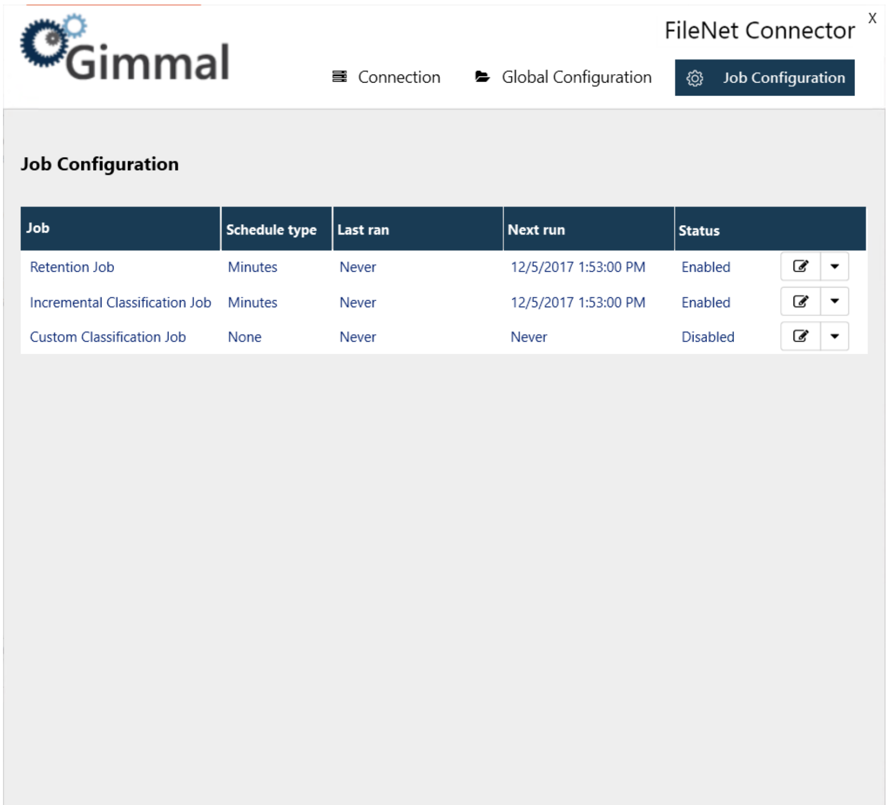
The Job Configuration dialog displays the retention and classification jobs included in the FileNet Connector, and enables you to either run the jobs immediately, or schedule how often you want the jobs to run. The jobs default to running every five minutes.

> ⚠ 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.



Job Configuration

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**
Gimmal FileNet Classification Service	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. **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.
Gimmal FileNet 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.

7.10.10.12 Uninstall FileNet Connector

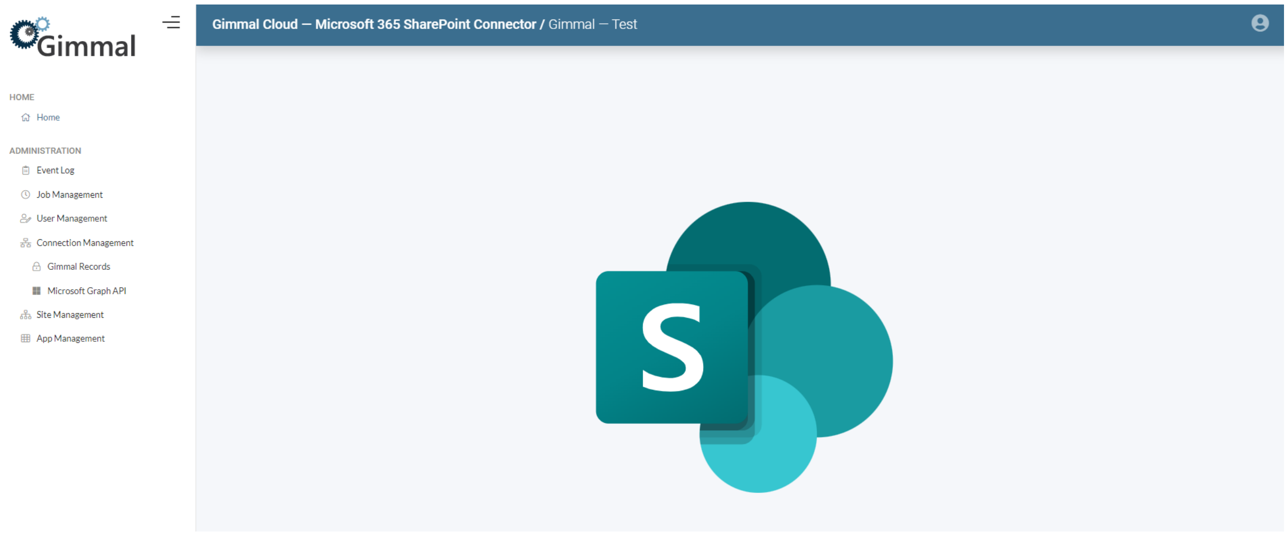
To uninstall the FileNet Connector, perform the following steps:

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 **Gimmal FileNet Connector** and double-click it. (You can also select Gimmal 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 Gimmal FileNet Classification Service and the Gimmal 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.

7.10.11 Microsoft 365 SharePoint Connector

The Microsoft 365 SharePoint Connector integrates with Gimmal Records SaaS, Gimmal Archive, and SharePoint Online to create, store, and manage preservation copy records in Azure Storage.



7.10.11.1 Quick Start Guide

Quick-start list of steps for connection configuration, user creation, adding a new site, and enabling preservation!

Connect to Gimmal Archive

Work with your Microsoft 365 Azure Administrator to authorize Gimmal Archive with your Azure Blog Storage.

- From the Stratus application landing page, click **Archive**.
- Click **Connection Management**.
- Enter your Blob Connection Settings as detailed in Create Azure Blog Connection Settings(see page 304).

Connect to Gimmal Records SaaS

Work with your Gimmal Records System Administrator to authorize the Microsoft 365 SharePoint Connector with your Gimmal Records SaaS environment.

- From the Stratus application landing page, click **Microsoft 365 SharePoint Connector**.
- Click **Gimmal Records** underneath the **Connection Management**
- Enter your Gimmal Records Connection Settings as detailed in Create Gimmal Records Connection Settings(see page 305).

Connect to Microsoft Graph API

Work with your Microsoft 365 Azure Administrator to authorize the Microsoft 365 SharePoint Connector with your Microsoft Graph API.

- From the Stratus application landing page, click **Microsoft 365 SharePoint Connector**.
- Click **Microsoft Graph API** underneath the **Connection Management**

- Enter your Microsoft Graph API Connection Settings and upload your certificate as detailed in Create Microsoft Graph API Connection Settings(see page 306).

Create a User

Add users to administer the Microsoft 365 Connector.

- From the Stratus application landing page, click **Microsoft 365 SharePoint Connector**.
- Click **User Management**.
- Create a new user as detailed in User Management.

Manage a New SharePoint Site

Add SharePoint sites to be managed by the Microsoft 365 Connector.

- From the Stratus application landing page, click **Microsoft 365 SharePoint Connector**.
- Click **Site Management**.
- Add a new site as detailed in Site Management.

Enable Preservation Copies

Work with your Gimmal Records Administrator to enable Preservation Copy functionality.

- See Preservation Copies for details.

7.10.11.2 Create Azure Blob Connection Settings

Work with Microsoft 365 Azure Administrator to authorize Gimmal Archive with your Azure Blog Storage.

Prerequisites

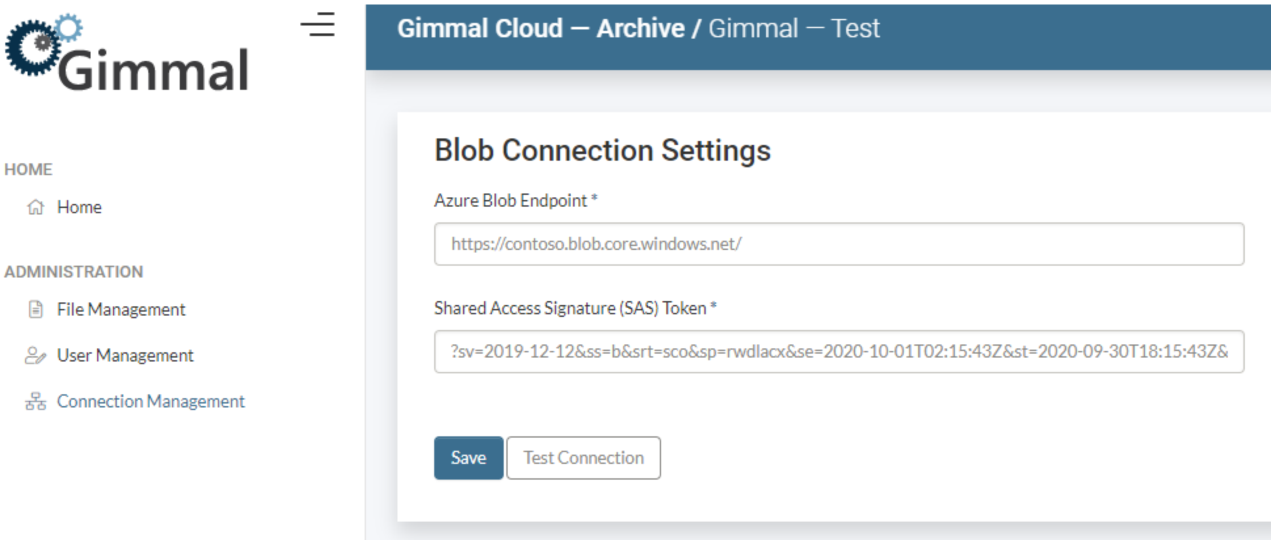
- Azure Blob Storage[65]

Blob Connection Settings

From the Stratus application landing page, click **Archive**.

Click **Connection Management**.

[65] https://azure.microsoft.com/en-us/services/storage/blobs/#overview



Blob Connection Settings

Azure Blob Endpoint *

https://contoso.blob.core.windows.net/

Shared Access Signature (SAS) Token *

?sv=2019-12-12&ss=b&srt=sco&sp=rwdlacx&se=2020-10-01T02:15:43Z&st=2020-09-30T18:15:43Z&

Enter your Blob Connection Settings:

- Azure Blob Endpoint[66]
- Shared Access Signature (SAS) Token[67]

Click **Test Connection** to test that the values are valid.

Click **Create** to save your settings.

7.10.11.3 Create Gimmal Records Connection Settings

Work with your Gimmal Records System Administrator to authorize the Microsoft 365 SharePoint Connector with your Gimmal Records SaaS environment.

Prerequisites

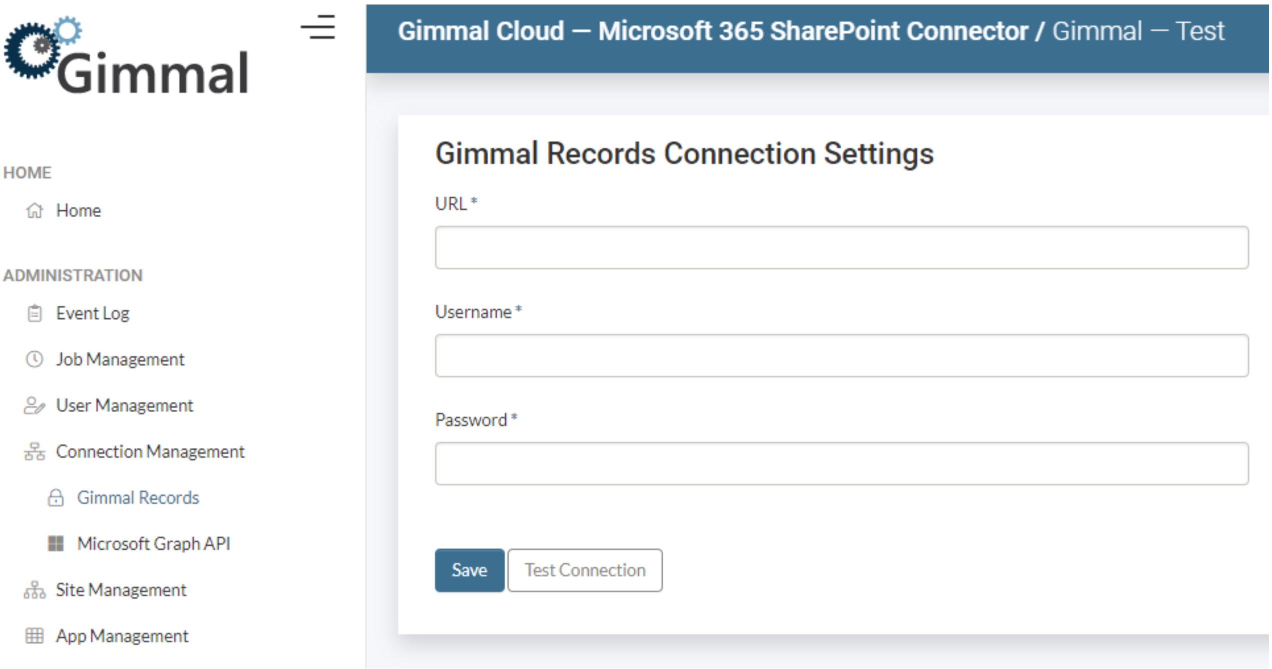
- Gimmal Records SaaS Tenant[68]

Gimmal Records Connection Settings

From the Stratus application landing page, click **Microsoft 365 SharePoint Connector**.

Click **Gimmal Records** underneath the **Connection Management** header.

[66] https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blobs-introduction#blob-storage-resources
[67] https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview#how-a-shared-access-signature-works
[68] https://records.gimmal.cloud/



Gimmal Records Connection Settings

URL *

Username *

Password *

Enter your Gimmal Records Connection Settings:

- URL
  - Enter https://records.gimmal.cloud/ for Gimmal Records SaaS Production Tenant.
- Username
  - Create a Service Account[69] in Gimmal Records for the M365 SharePoint Connector.
- Password
  - Enter the password for the Service Account created above.

Click **Test Connection** to test that the values are valid.

Click **Create** to save your settings.

7.10.11.4 Create Microsoft Graph API Connection Settings

Work with your Microsoft 365 Azure Administrator to authorize the Microsoft 365 SharePoint Connector with your Microsoft Graph API.

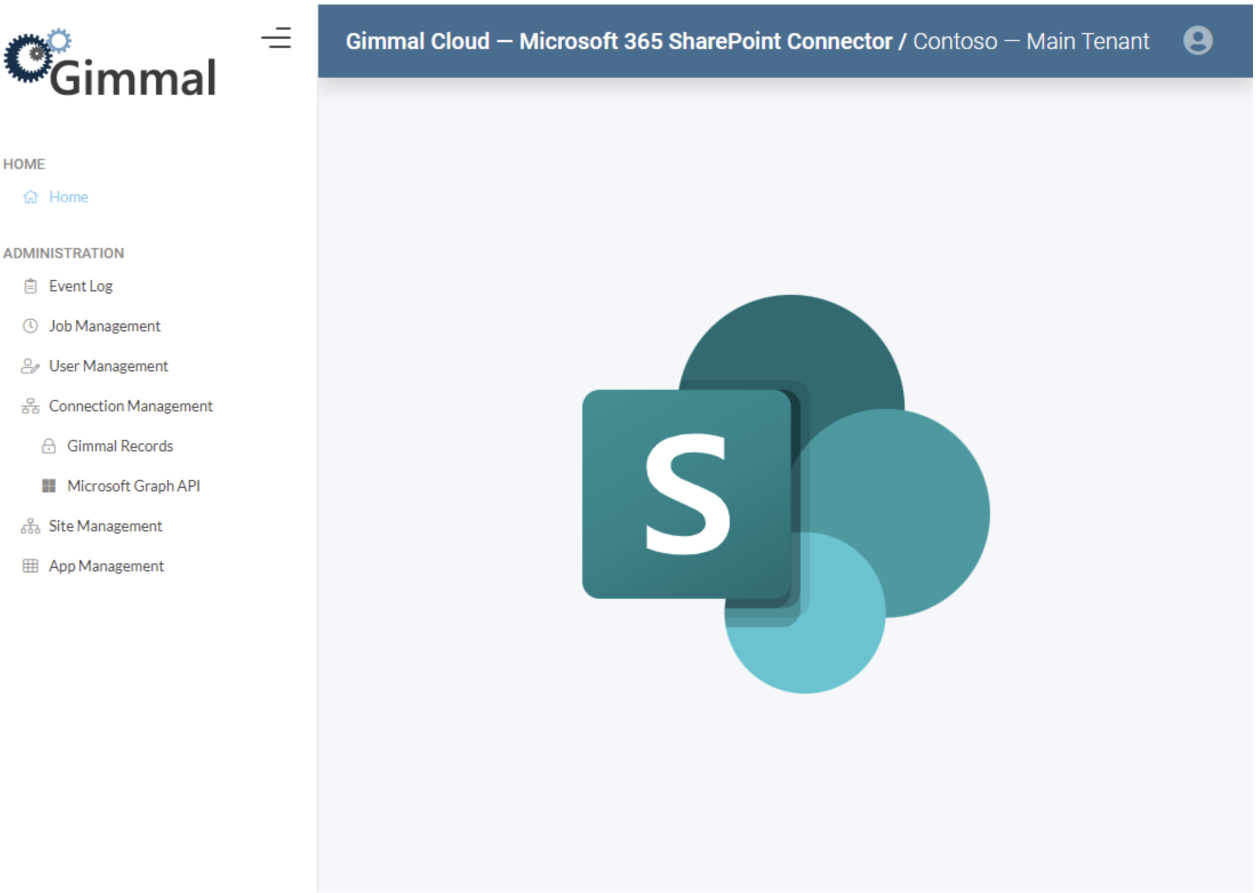
Prerequisites

- Configuring Graph API[70]
- For production environments, please acquire a certificate from a public Certificate Authority.
- For non-production environments please follow the Instructions from Microsoft to generate a self-signed certificate[71]
- Configure Azure App Registration(see page 311)

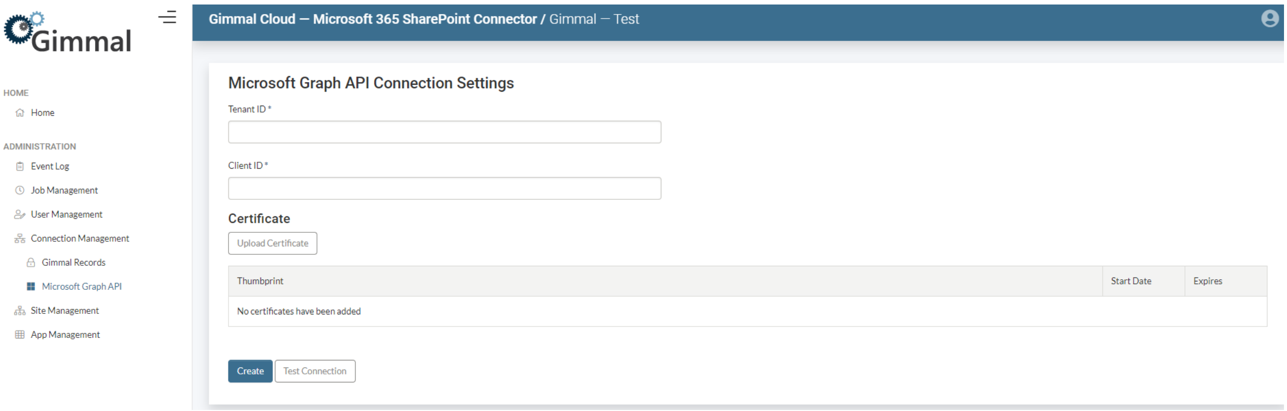
[69] https://docs.gimmal.com/rm/latest/server/administrator-guide/managing-security/creating-a-service-account
[70] https://docs.gimmal.com/cdz/administrator-guide/authentication-management/configuring-graph-api
[71] https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-self-signed-certificate

Microsoft Graph API Connection Settings

From the Stratus application landing page, click **Microsoft 365 SharePoint Connector**.



Click **Microsoft Graph API** underneath the **Connection Management** header.



Microsoft Graph API Connection Settings

Tenant ID *

Client ID *

Certificate

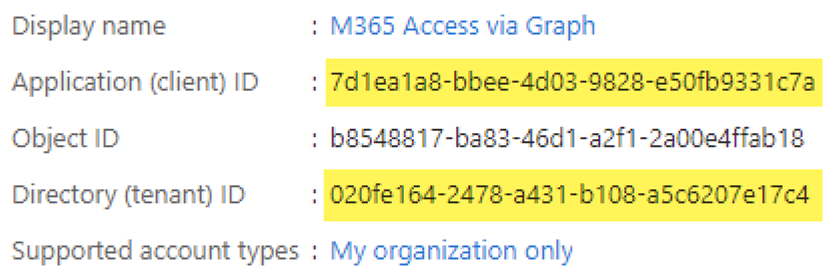
Upload Certificate

Thumbprint	Start Date	Expires
No certificates have been added		

Create   Test Connection

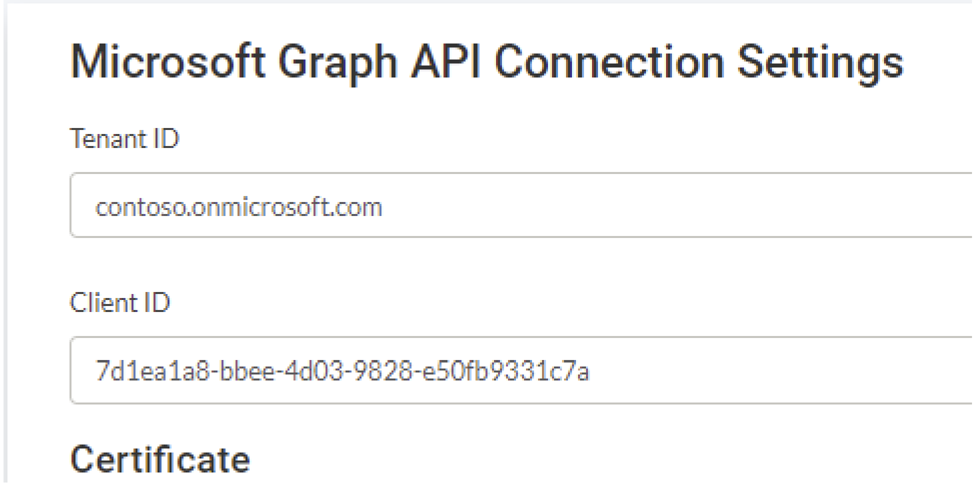
Create Connection

Enter your Microsoft Graph API Connection Settings:



Display name	:	M365 Access via Graph
Application (client) ID	:	7d1ea1a8-bbee-4d03-9828-e50fb9331c7a
Object ID	:	b8548817-ba83-46d1-a2f1-2a00e4ffab18
Directory (tenant) ID	:	020fe164-2478-a431-b108-a5c6207e17c4
Supported account types	:	My organization only

- Tenant ID
    - Also referred to as “Directory (tenant) ID”
- Client ID
    - Also referred to as “Application (client) ID”



Microsoft Graph API Connection Settings

Tenant ID: contoso.onmicrosoft.com

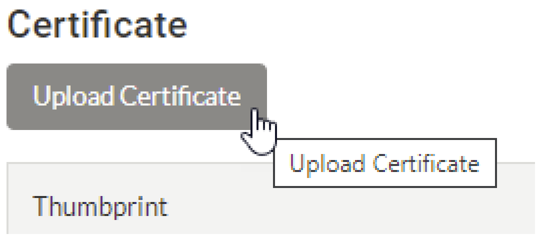
Client ID: 7d1ea1a8-bbee-4d03-9828-e50fb9331c7a

Click **Create** to save your settings.

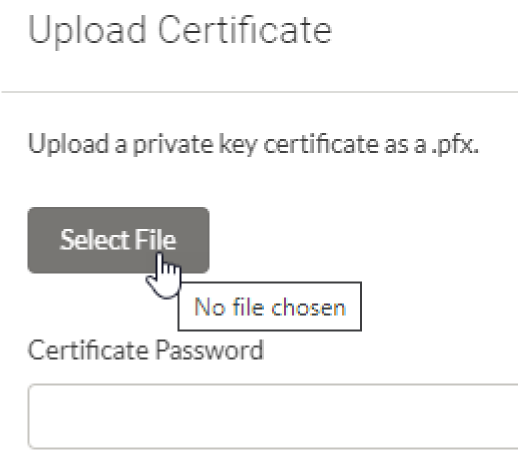
Upload Certificate

Go back to **Microsoft Graph API** underneath the **Connection Management** header.

Click **Upload Certificate**.



Click **Select File**.



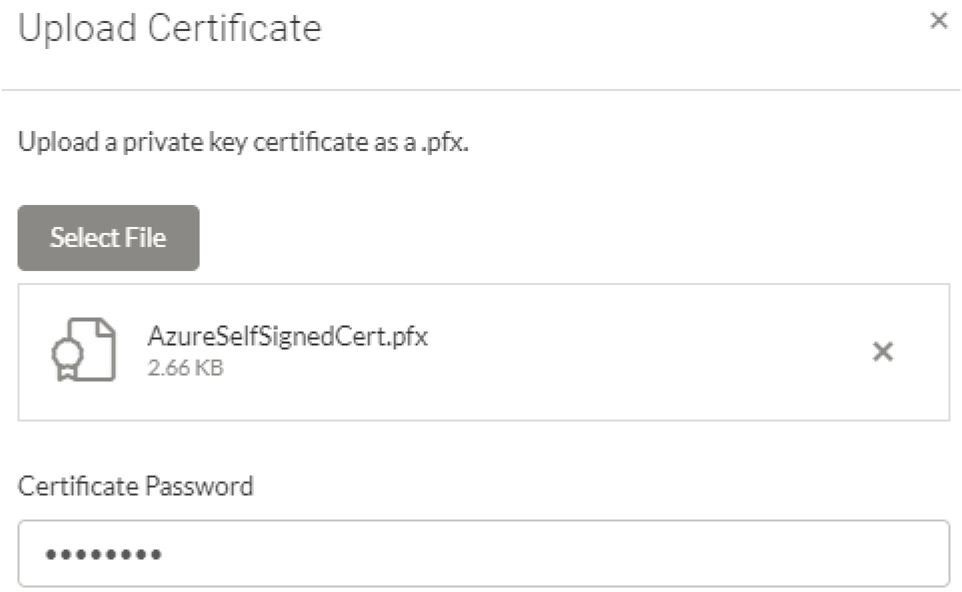
Upload Certificate

Upload a private key certificate as a .pfx.

Certificate Password

Select the .pfx file that was created in Generate Self-Signed Certificate(see page 310).

Enter the Certificate Password used in Generate Self-Signed Certificate(see page 310).



Upload Certificate

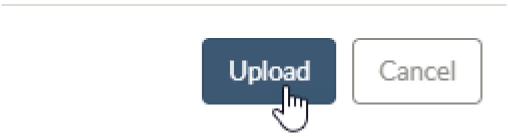
Upload a private key certificate as a .pfx.

AzureSelfSignedCert.pfx
2.66 KB

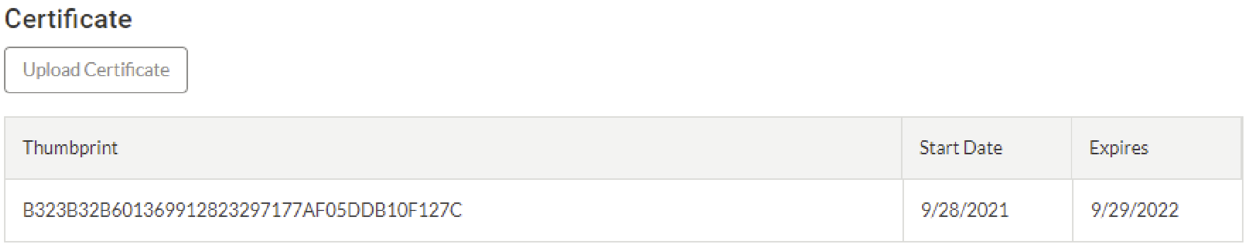
Certificate Password

••••••••

Click **Upload**.



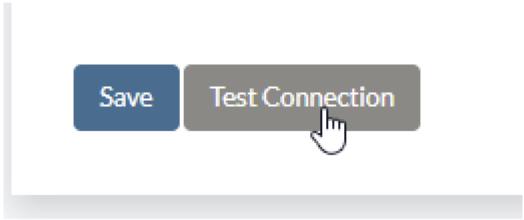
Verify the Thumbprint, Start Date, and Expires.



Certificate

Thumbprint	Start Date	Expires
B323B32B601369912823297177AF05DDB10F127C	9/28/2021	9/29/2022

Click **Test Connection**.



You should see a success notification in the upper-right stating “The values are valid”.

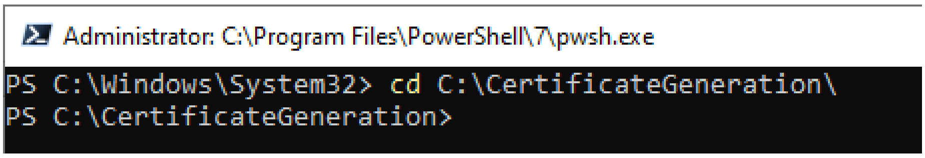
Click **Save** again.

Generate Self-Signed Certificate

Generate a self-signed certificate used when creating the Microsoft Graph API Connection Settings.

Download Create-SelfSignedCert.ps1[72] and ensure that the file is unblocked.

Open PowerShell and cd to the downloaded location of the .ps1.



```
PS C:\Windows\System32> cd C:\CertificateGeneration\
PS C:\CertificateGeneration>
```

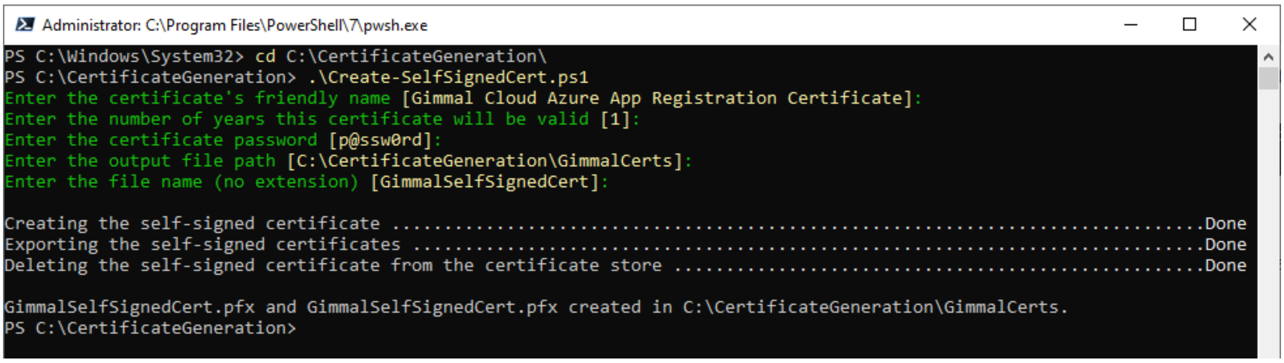
Type **.\Create-SelfSignedCert.ps1** and press ENTER.

Enter the required information. If the default value (between brackets in yellow) is acceptable, just press ENTER.

- **Certificate Friendly Name**: The friendly name of the certificate. (**Default**: Gimmal Cloud Azure App Registration Certificate)
- **Number of Years**: The number of years before the certificate will expire. (**Default**: 1)
- **Certificate Password**: The password used to secure the certificate. **DO NOT LOSE THIS** (**Default**: p@ssw0rd)
- **Output File Path**: The directory where the certificates will be saved. (**Default**: Current Directory + \GimmalCerts)
- **File Name (no extension)**: The file name of the certificates. (**Default**: GimmalSelfSignedCert)

The script will generate two files and inform you of the saved location.

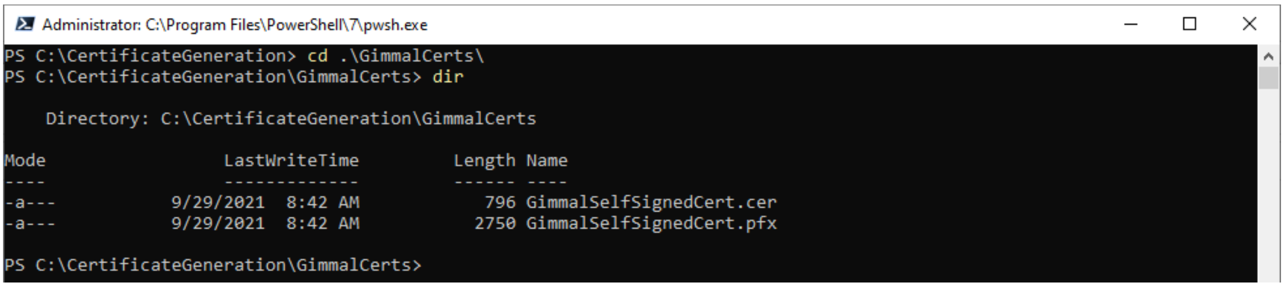
[72] https://dev.azure.com/gimmal1/99a0cbfa-e43a-448c-9093-49af255ebb1c/_apis/git/repositories/c4b0a8b3-d78c-44bf-bf48-848cf106bee1/Items?path=/.attachments/Create-SelfSignedCert-1917f250-907d-4bec-9199-0ddbcb098b77.ps1&download=false&resolveLfs=true&%24format=octetStream&api-version=5.0-preview.1&sanitize=true&versionDescriptor.version=wikiMaster



Administrator: C:\Program Files\PowerShell\7\pwsh.exe

```
PS C:\Windows\System32> cd C:\CertificateGeneration\
PS C:\CertificateGeneration> .\Create-SelfSignedCert.ps1
Enter the certificate's friendly name [Gimmal Cloud Azure App Registration Certificate]:
Enter the number of years this certificate will be valid [1]:
Enter the certificate password [p@ssw0rd]:
Enter the output file path [C:\CertificateGeneration\GimmalCerts]:
Enter the file name (no extension) [GimmalSelfSignedCert]:

Creating the self-signed certificate ..........................................................Done
Exporting the self-signed certificates ........................................................Done
Deleting the self-signed certificate from the certificate store ...............................Done

GimmalSelfSignedCert.pfx and GimmalSelfSignedCert.pfx created in C:\CertificateGeneration\GimmalCerts.
PS C:\CertificateGeneration>
```

It is highly recommended you make copies of the .pfx and .crt file. **DO NOT LOSE THEM**.



Administrator: C:\Program Files\PowerShell\7\pwsh.exe

```
PS C:\CertificateGeneration> cd .\GimmalCerts\
PS C:\CertificateGeneration\GimmalCerts> dir

    Directory: C:\CertificateGeneration\GimmalCerts

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a---           9/29/2021  8:42 AM            796 GimmalSelfSignedCert.cer
-a---           9/29/2021  8:42 AM           2750 GimmalSelfSignedCert.pfx

PS C:\CertificateGeneration\GimmalCerts>
```

Configure Azure App Registration

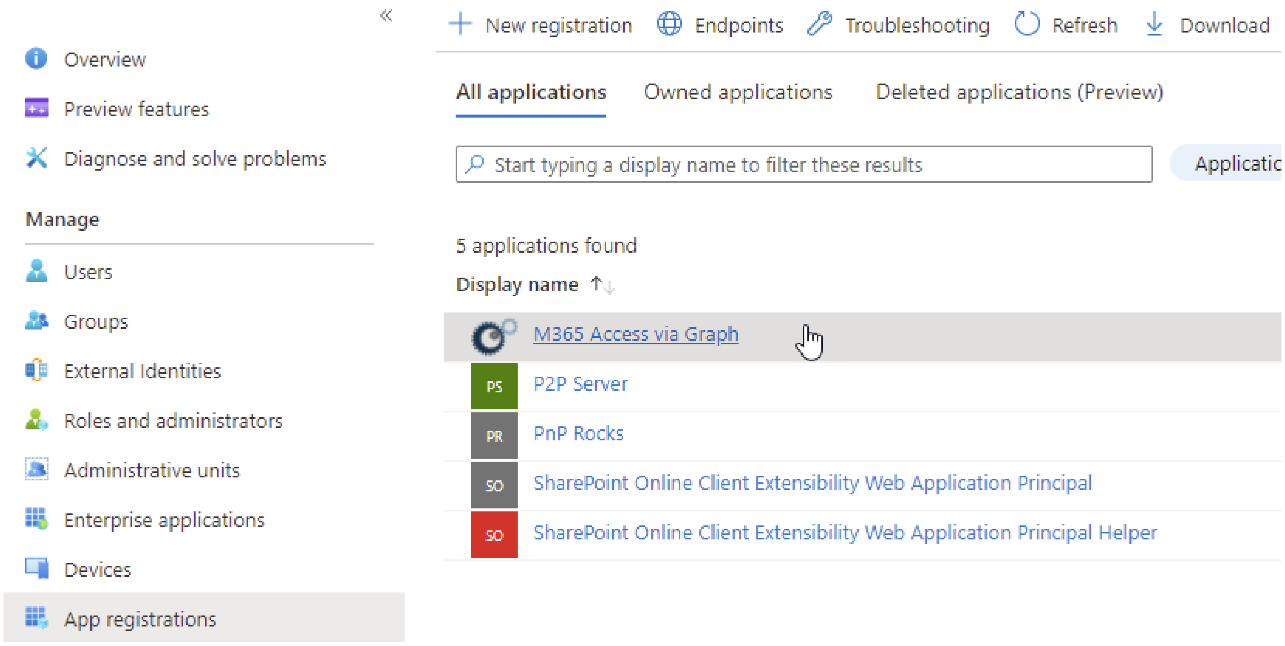
Login to your Azure Portal[73].

Navigate to **Azure Active Directory** and click **App Registrations**.

Select the app registration used for Gimmal Cloud connectivity (possibly named M365 Access via Graph).

- You may need to select **All applications**.
- If one has not been created, please follow Configuring Graph API[74].

[73] https://portal.azure.com/
[74] https://docs.gimmal.com/cdz/administrator-guide/authentication-management/configuring-graph-api

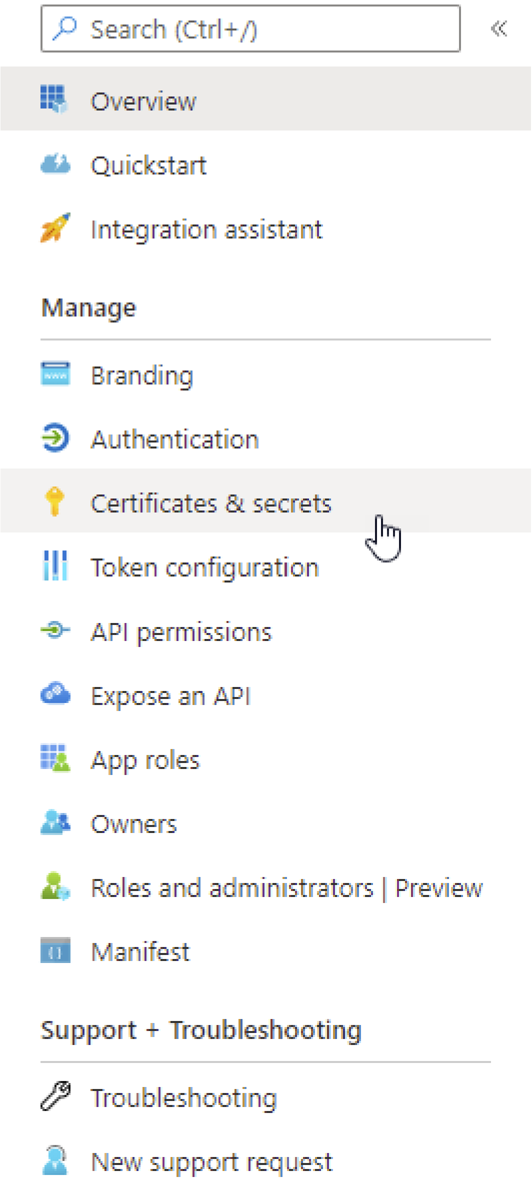


5 applications found

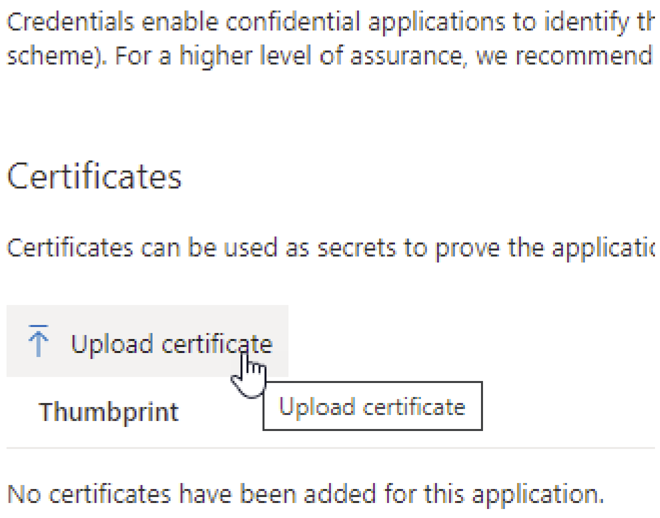
Display name ↑↓
M365 Access via Graph
PS P2P Server
PR PnP Rocks
SO SharePoint Online Client Extensibility Web Application Principal
SO SharePoint Online Client Extensibility Web Application Principal Helper

Upload Certificate

Click **Certificates & secrets** in the left navigation.



Click **Upload certificate**.



Credentials enable confidential applications to identify th
scheme). For a higher level of assurance, we recommend

Certificates

Certificates can be used as secrets to prove the applicati

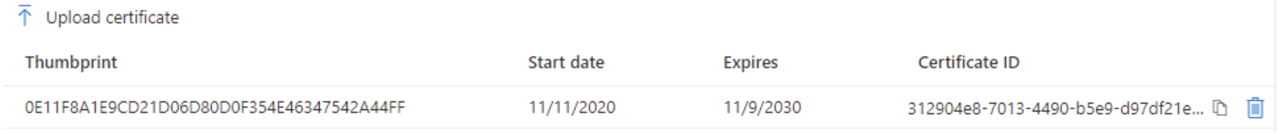
No certificates have been added for this application.

In the right drawer, click **Select a file**.

Select the .crt file that was created in Generate Self-Signed Certificate(see page 310).

Click **Add**.

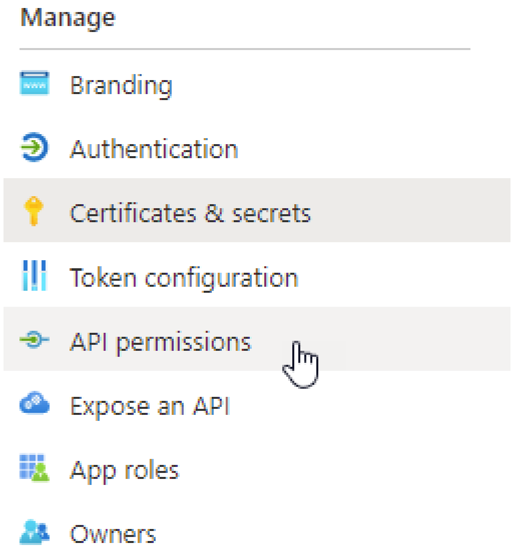
Verify the Thumbprint, Start date, and Expires.



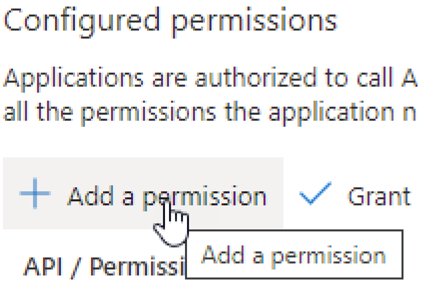
Thumbprint	Start date	Expires	Certificate ID
0E11F8A1E9CD21D06D80D0F354E46347542A44FF	11/11/2020	11/9/2030	312904e8-7013-4490-b5e9-d97df21e...

Configure Permissions

Click **API permissions** in the left navigation.



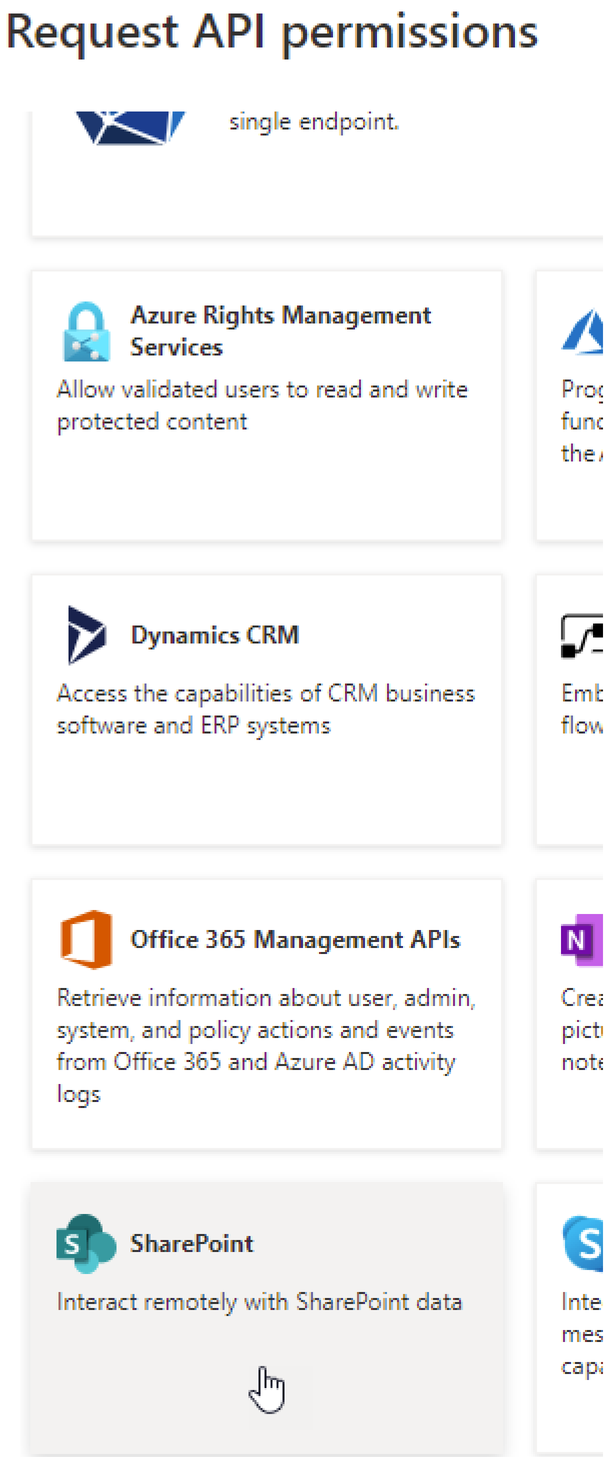
Click **Add a permission**.



Configured permissions

Applications are authorized to call A
all the permissions the application n

In the right drawer, click **SharePoint**.



Request API permissions

single endpoint.

Azure Rights Management Services

Allow validated users to read and write protected content

Dynamics CRM

Access the capabilities of CRM business software and ERP systems

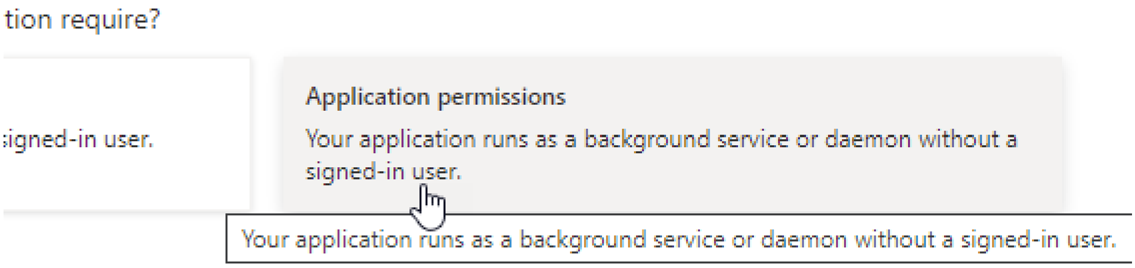
Office 365 Management APIs

Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity logs

SharePoint

Interact remotely with SharePoint data

Click **Application permissions**.



tion require?

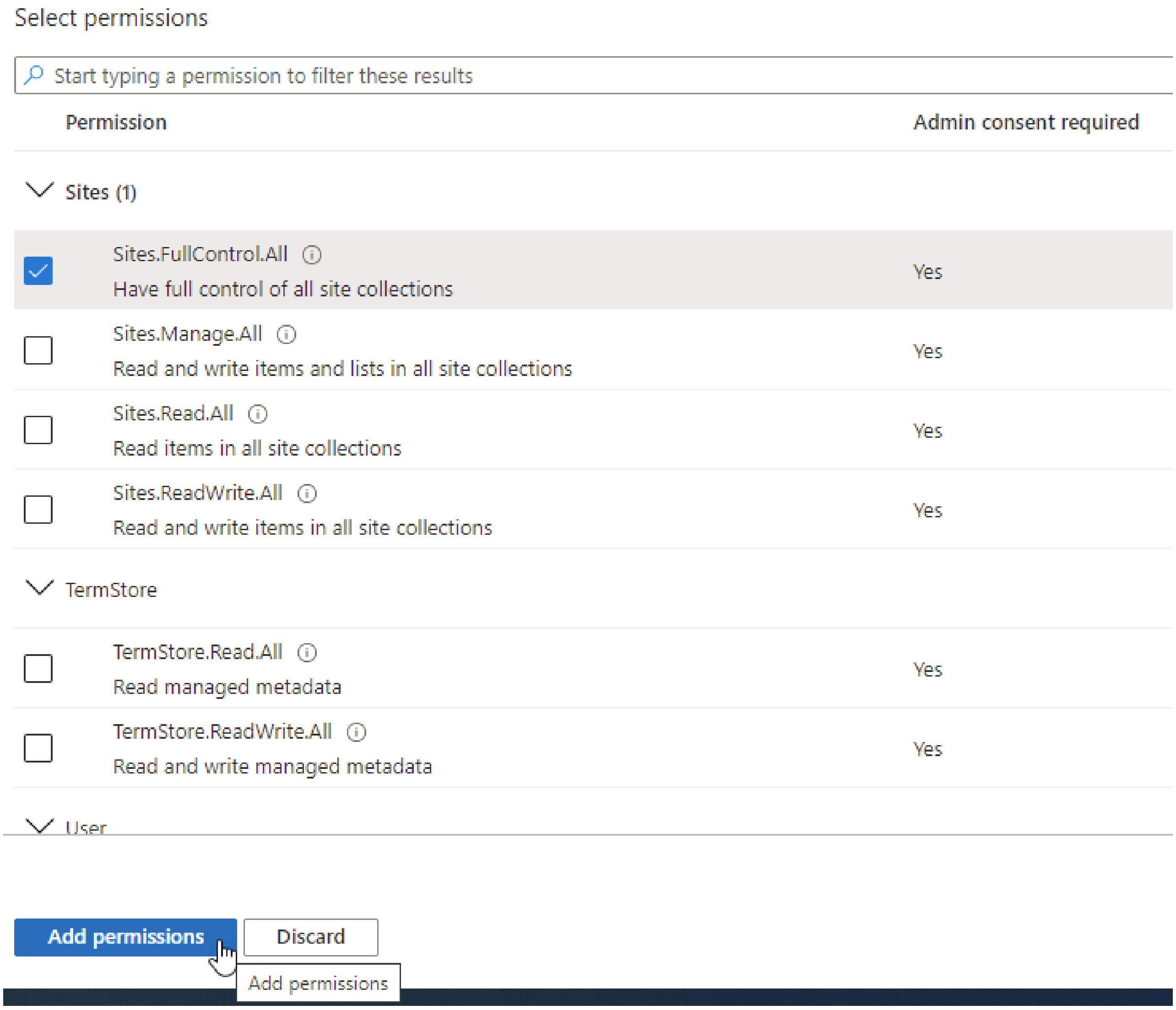
igned-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Your application runs as a background service or daemon without a signed-in user.

Select **Sites.FullControl.All**, then click **Add permissions**.

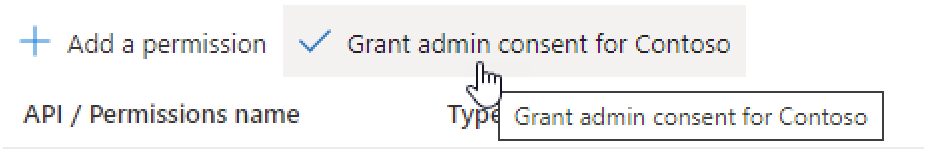


Select permissions

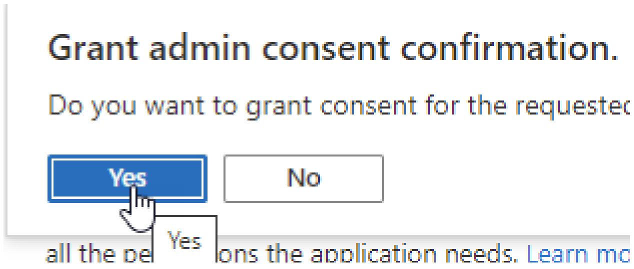
Start typing a permission to filter these results

	Permission	Admin consent required
	Sites (1)	
☑	Sites.FullControl.All ⓘ Have full control of all site collections	Yes
□	Sites.Manage.All ⓘ Read and write items and lists in all site collections	Yes
□	Sites.Read.All ⓘ Read items in all site collections	Yes
□	Sites.ReadWrite.All ⓘ Read and write items in all site collections	Yes
	TermStore	
□	TermStore.Read.All ⓘ Read managed metadata	Yes
□	TermStore.ReadWrite.All ⓘ Read and write managed metadata	Yes
	User	

Click **Grant admin consent for {Your Tenant}**.

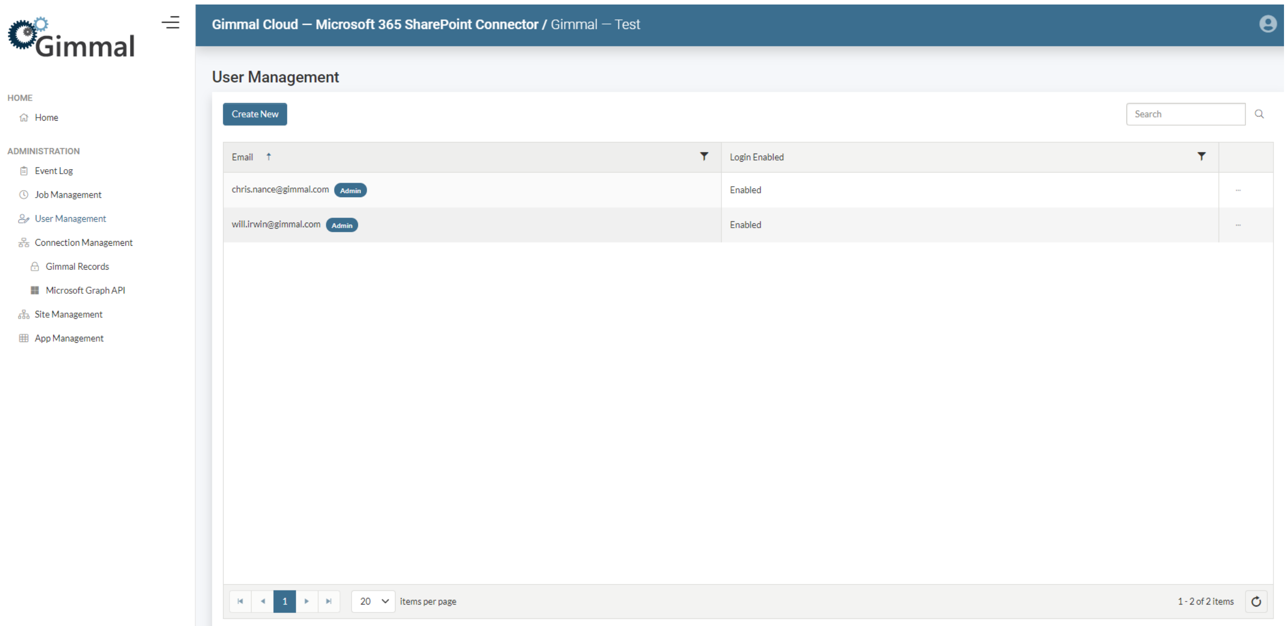

+ Add a permission
✓ Grant admin consent for Contoso
API / Permissions name
Type
Grant admin consent for Contoso

Click **Yes**.


Grant admin consent confirmation.
Do you want to grant consent for the requestec
Yes
No
all the pe
Yes
ons the application needs. Learn mo

7.10.11.5 User Management

Microsoft 365 SharePoint Connector users can be added, viewed, edited, and deleted.



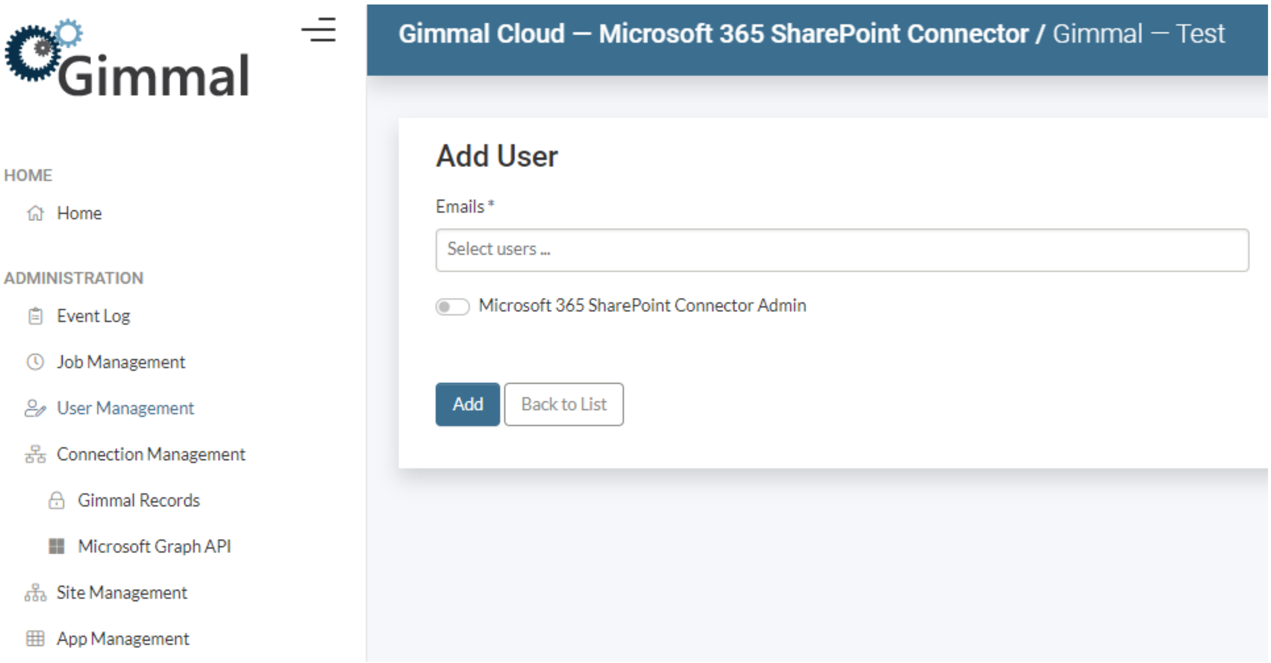
Email	Login Enabled
chris.nance@gimmal.com Admin	Enabled
will.irwin@gimmal.com Admin	Enabled

Add a User

Click **Create New** button.

Begin typing the email of the user to be added. Select the correct user, then decide if the user should be a Microsoft 365 SharePoint Connector Admin.

Click **Add** to add the user to Microsoft 365 SharePoint Connector.


Gimmal Cloud — Microsoft 365 SharePoint Connector / Gimmal — Test

Add User

Emails *

Select users ...

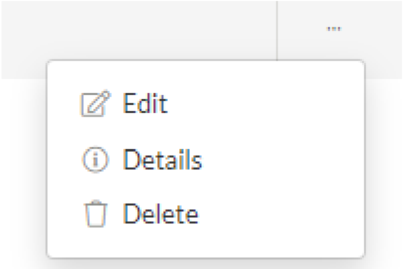
Microsoft 365 SharePoint Connector Admin

NOTE – to add a user to the Microsoft 365 SharePoint Connector that user must first have access to the Gimmal Cloud tenant hosting the Microsoft 365 SharePoint Connector.

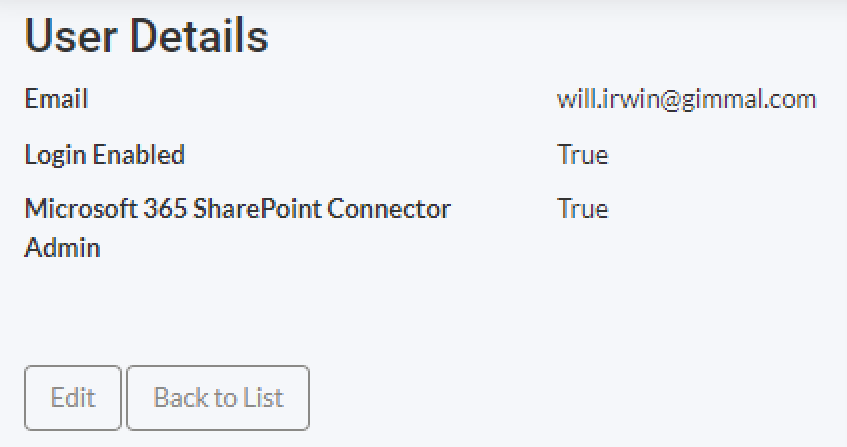
1. Navigate to https://manage.gimmal.cloud/<tenant name goes here>
2. Select **Invite User**
3. Enter the user's email address and select the appropriate tenant to provide access.
4. Select **Invite** to send the invitation.

View User Details

Click the ellipses button (…) for the user that you want to view, then click **Details**.



The User Details will display. Click **Edit** to edit the user or click **Back to List** to return to list of users.

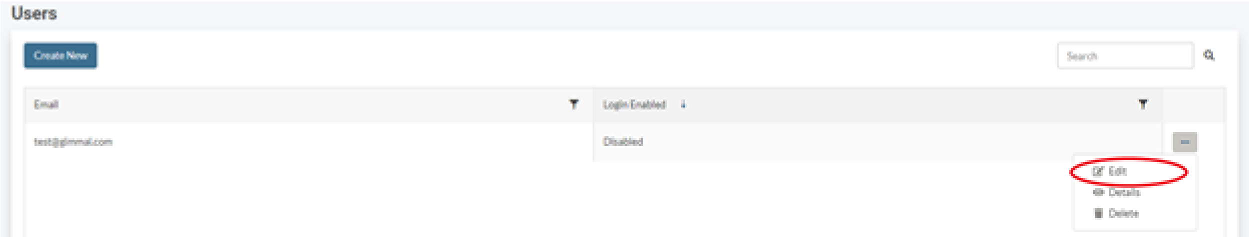


User Details

Email	will.irwin@gimmal.com
Login Enabled	True
Microsoft 365 SharePoint Connector Admin	True

Edit a User

Click the ellipses button (…) for the user that you want to edit, then click **Edit**.

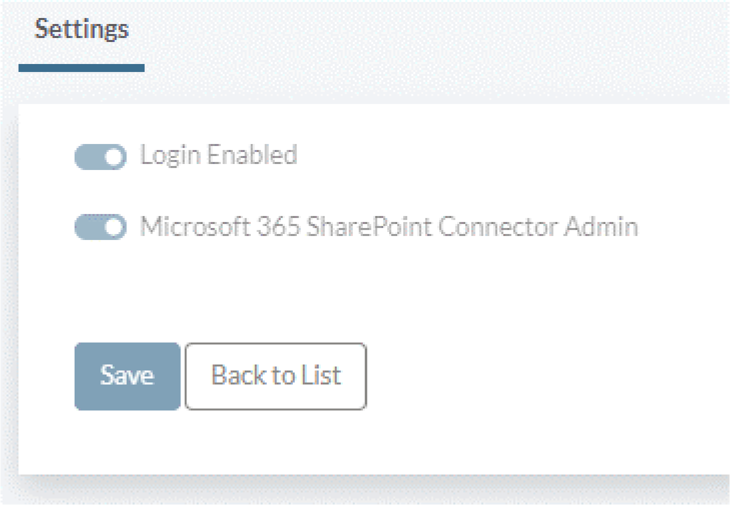


Users

Email	Login Enabled
test@gimmal.com	Disabled

Under the **Settings** tab a few options can be toggled:

- **Login Enabled** – allows the user to log in to the Microsoft 365 SharePoint Connector.
- **Microsoft 365 SharePoint Connector Admin** – gives the user admin privileges in the Microsoft 365 SharePoint Connector.



Settings

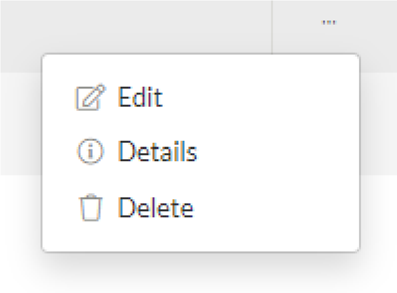
Login Enabled

Microsoft 365 SharePoint Connector Admin

Click **Save** to save the changes made to the user or click **Back to List** to return without saving the changes.

Delete a User

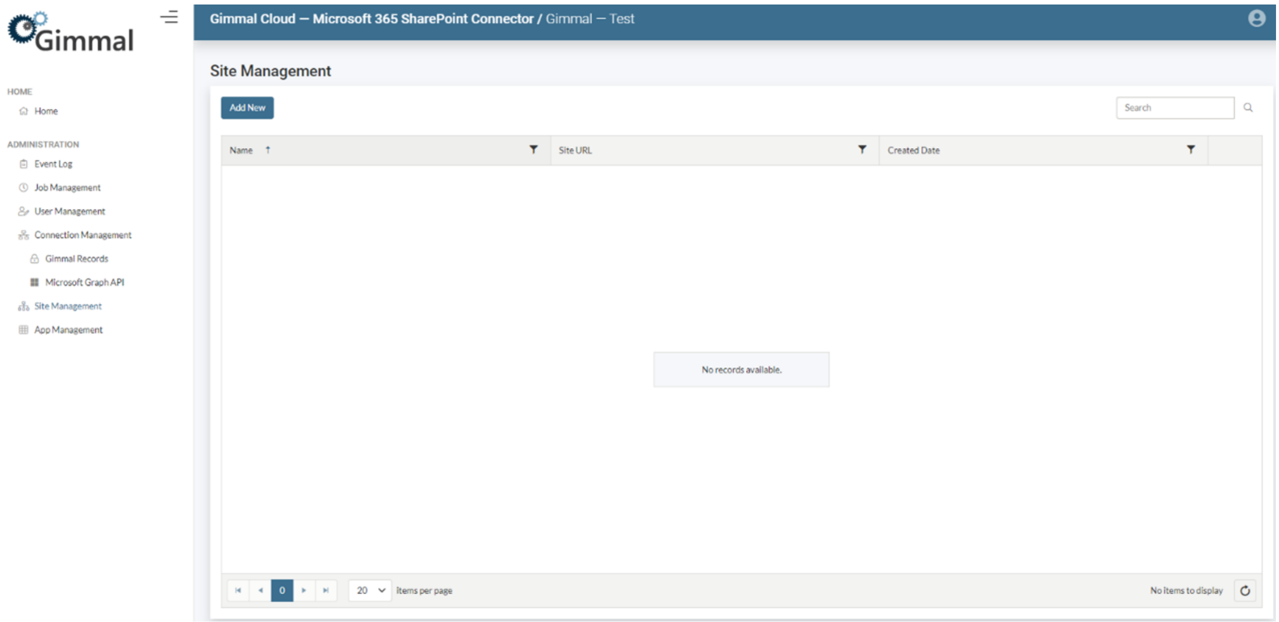
Click the ellipses button (…) for the user to delete, then click **Delete**.



On the next screen, clicking Delete confirms and removes the User from the Microsoft 365 SharePoint Connector. **Back to List** exits without deleting the user.

7.10.11.6 Site Management

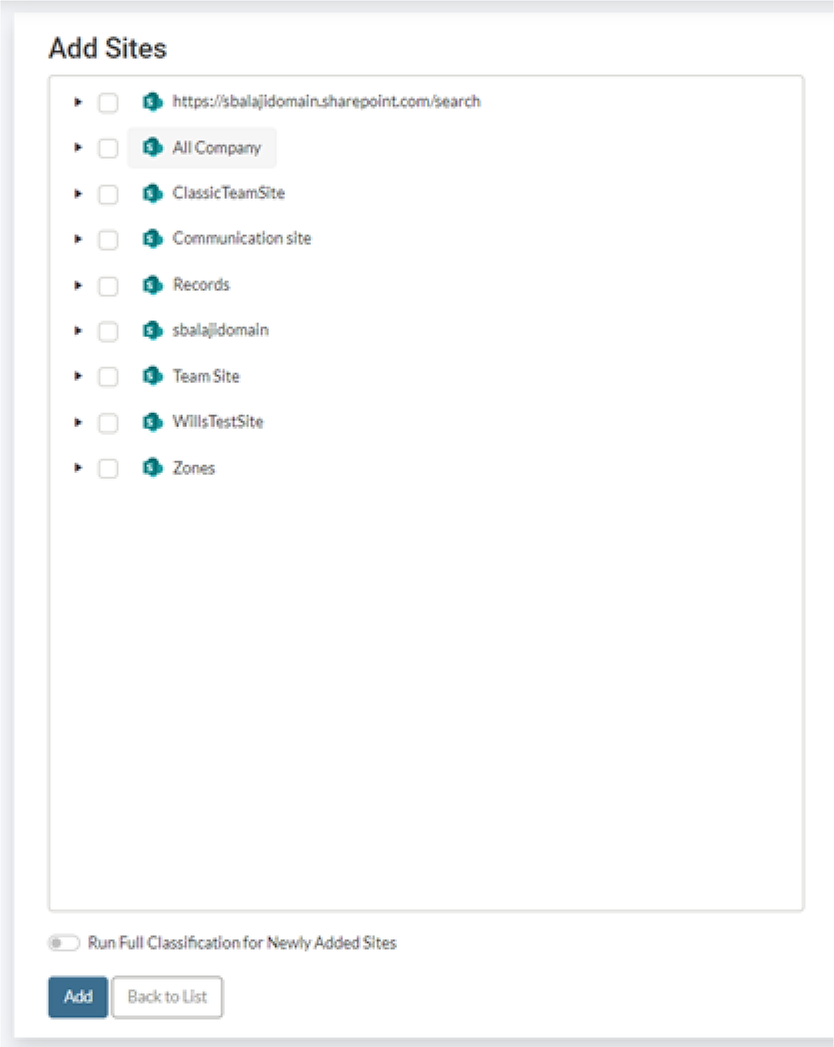
Microsoft 365 SharePoint Connector sites can be added, viewed, and deleted.



Add a Site

Click **Add New**.

The list of available sites to add is displayed.



Add Sites

- □ https://sbalajidomain.sharepoint.com/search
- □ All Company
- □ ClassicTeamSite
- □ Communication site
- □ Records
- □ sbalajidomain
- □ Team Site
- □ WillsTestSite
- □ Zones

○ Run Full Classification for Newly Added Sites

Select the checkbox for the site(s) you want to add.

Select the drop-down arrow next to a site to display a list of available subsites.

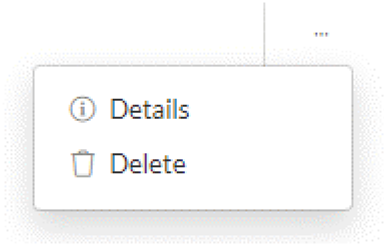
Enable **Run Full Classification for Newly Added Sites** if you want the Microsoft 365 SharePoint Connector to crawl the newly added site(s) and immediately start managing content.

NOTE – you can manually run Full Classification from Job Management(see page 323).

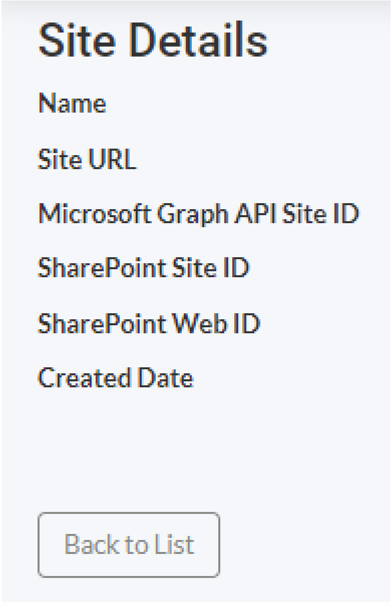
Click **Add** to add the selected site(s) to the Microsoft 365 SharePoint Connector.

View Site Details

Click the ellipses button (…) for the site that you want to view, then click **Details**.



The Site Details will display. Click **Back to List** to return to list of sites.


Site Details

Name

Site URL

Microsoft Graph API Site ID

SharePoint Site ID

SharePoint Web ID

Created Date

Delete a Site

Click **Delete** in the Site Management list to remove the site entry from the database.

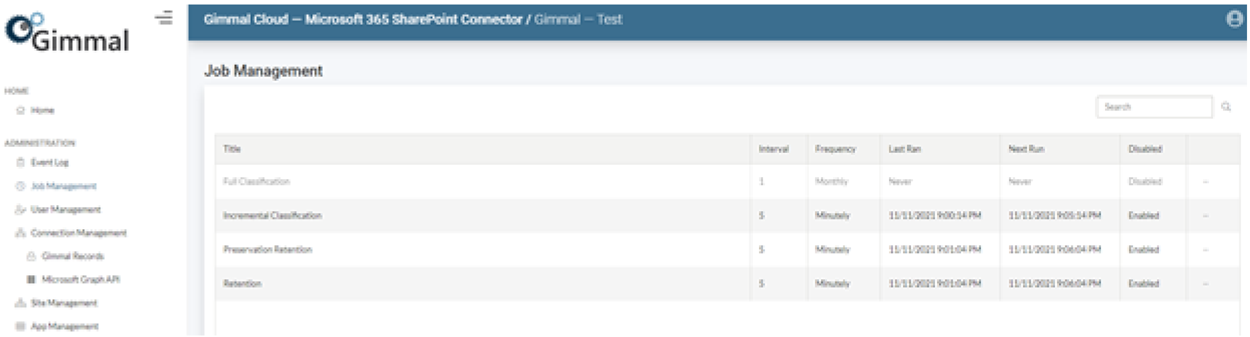
> **NOTE** – do not add/delete/add/delete site entries in quick succession.

Gimmal Records will delete the record entries for content residing in the removed site.

> **NOTE** – Gimmal Records can take possibly up to 30+ minutes to delete records.
>
> **NOTE** – be careful when removing managed sites because Gimmal Records does **not** remove a **preserved** record when a site is removed. Therefore, Gimmal Records now has a record that the Microsoft 365 SharePoint Connector is no longer managing or knows about – essentially orphaning that record.

7.10.11.7 Job Management

The following timer jobs are necessary for the Microsoft 365 SharePoint Connector to manage content.



Gimmal Cloud – Microsoft 365 SharePoint Connector / Gimmal – Test

Job Management

Title	Interval	Frequency	Last Ran	Next Run	Disabled	
Full Classification	1	Monthly	Never	Never	Disabled	–
Incremental Classification	5	Minutely	11/11/2021 9:00:54 PM	11/11/2021 9:05:54 PM	Enabled	–
Preservation Retention	5	Minutely	11/11/2021 9:01:04 PM	11/11/2021 9:06:04 PM	Enabled	–
Retention	5	Minutely	11/11/2021 9:01:04 PM	11/11/2021 9:06:04 PM	Enabled	–

Timer Jobs

Full Classification – the Full Classification job crawls every file contained within SharePoint Online sites that were added to Site Management(see page 321), and notifies Gimmal Records of their existence. This job is typically executed upon initial addition of a new site. It is disabled by default, but it can be scheduled to run on a regular basis.

> **NOTE** – scheduling Full Classification to run on a regular basis can put considerable strain on the system.

Incremental Classification – the Incremental Classification job synchronizes all file changes that have occurred within SharePoint Online sites that were added to Site Management(see page 321).

Preservation Retention – the Preservation Retention job processes approved retention actions for SharePoint Online items with Preservation enabled.

Retention – the Retention job processes approved retention actions for SharePoint Online items after they have been approved from Gimmal Records. As the Retention job completes the processing of retention actions, it notifies Gimmal Records of the completion status. The job's status is shown in the Pending Automation section.

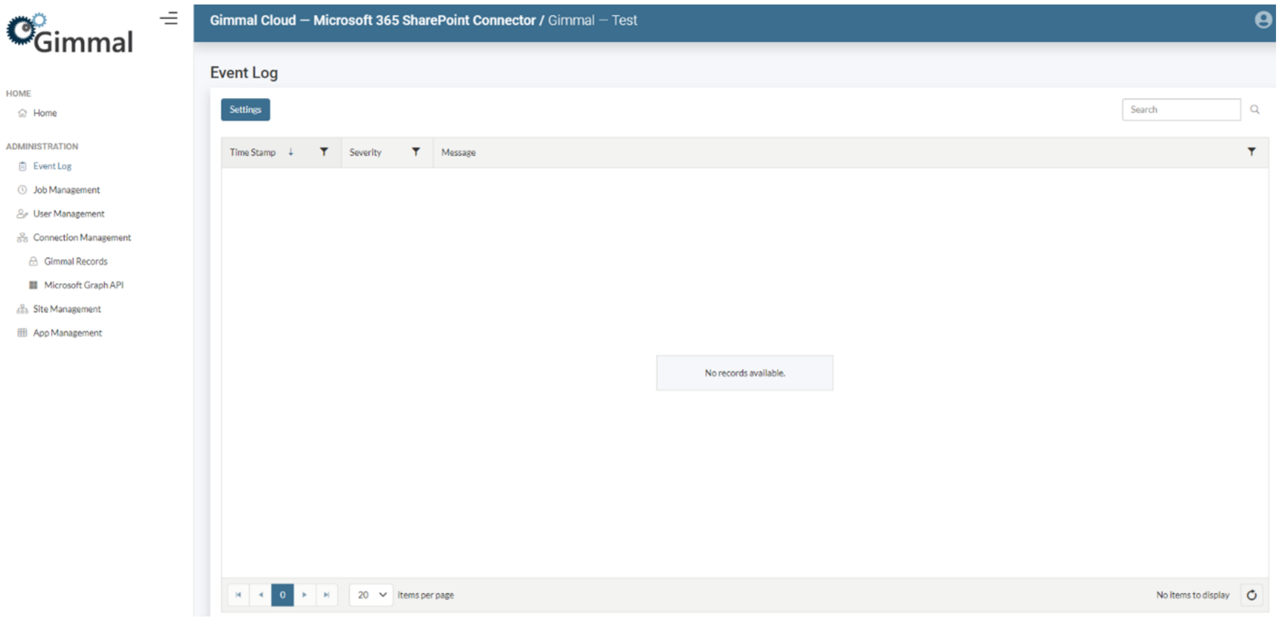
Default Timer Job Schedules

These job schedules are the optimized intervals for this timer job and changing them could affect the overall performance of Gimmal Records functions.

Job	Schedule
Full Classification	Monthly (Disabled)
Incremental Classification	Every 5 Minutes
Preservation Retention	Every 5 Minutes
Retention	Every 5 Minutes

7.10.11.8 Event Logs

Microsoft 365 SharePoint Connector event log can be viewed and exported.



Gimmal Cloud – Microsoft 365 SharePoint Connector / Gimmal – Test

Event Log

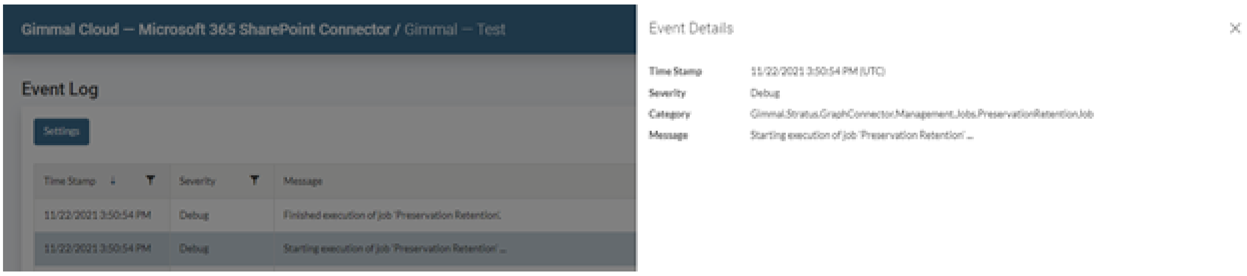
Time Stamp	Severity	Message

No records available.

No items to display

Event Details

Select an event from the log to view Event Details.



Gimmal Cloud – Microsoft 365 SharePoint Connector / Gimmal – Test

Event Log

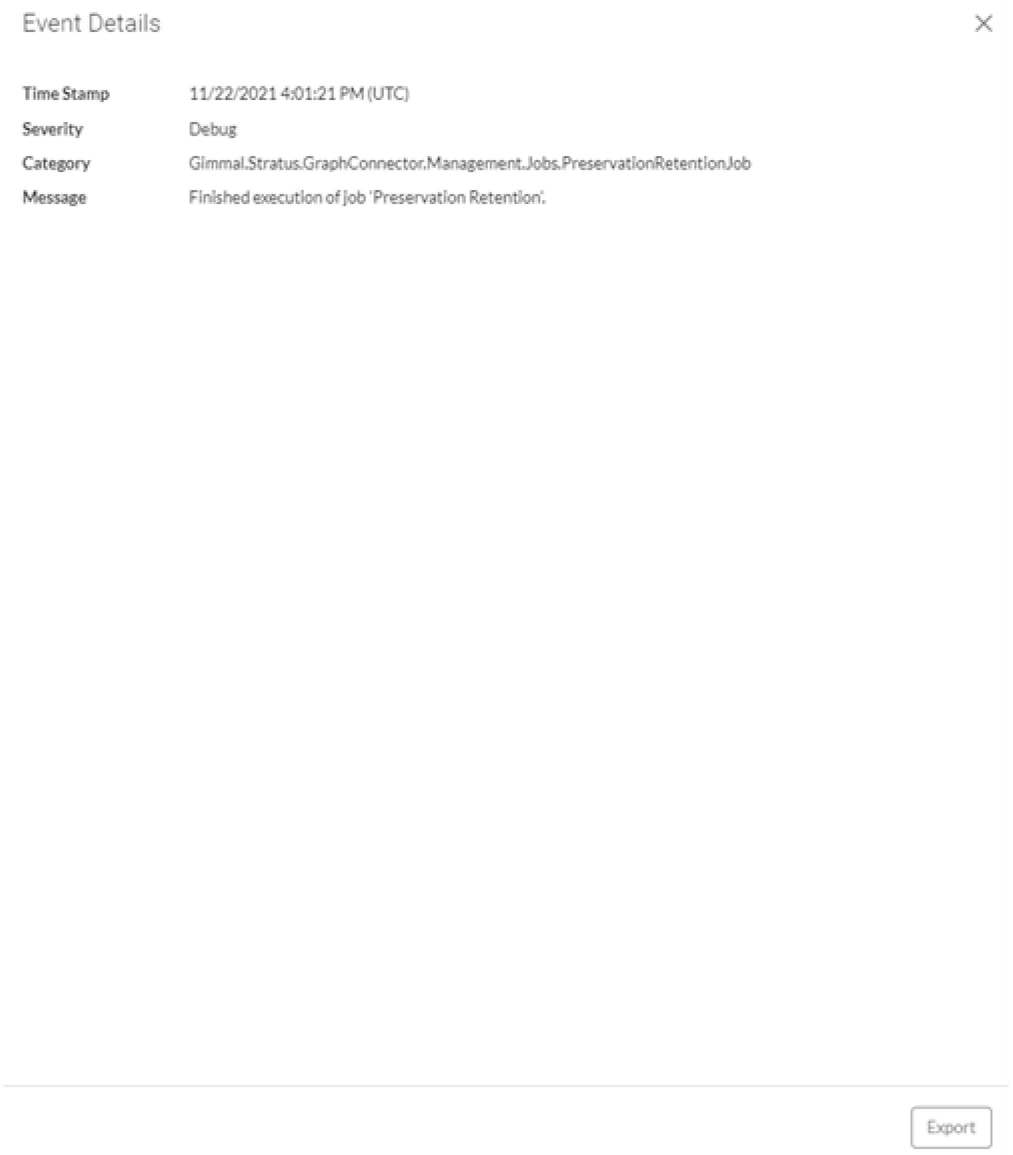
Time Stamp	Severity	Message
11/22/2021 3:50:54 PM	Debug	Finished execution of job 'Preservation Retention'.
11/22/2021 3:50:54 PM	Debug	Starting execution of job 'Preservation Retention' ...

Event Details

Time Stamp	11/22/2021 3:50:54 PM (UTC)
Severity	Debug
Category	Gimmal.Stratus.GraphConnector.Management.Jobs.PreservationRetentionJob
Message	Starting execution of job 'Preservation Retention' ...

Export Event Details

Click **Export** to export Event Details.



Time Stamp 11/22/2021 4:01:21 PM (UTC)

Severity Debug

Category Gimmal.Stratus.GraphConnector.Management.Jobs.PreservationRetentionJob

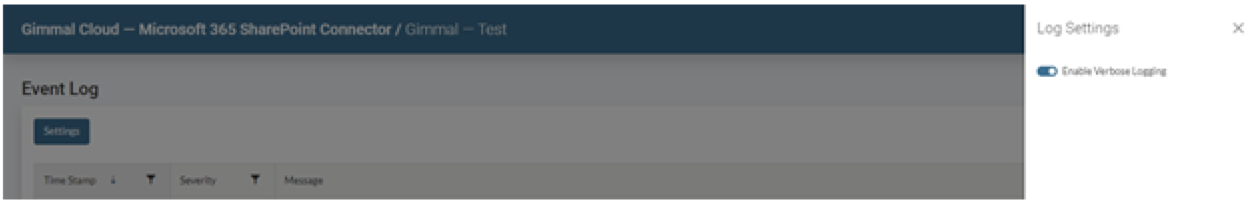
Message Finished execution of job 'Preservation Retention'.

Enable Verbose Logging

Click **Settings** to view Log Settings.

Select the slider to enable or disable **Verbose Logging**.

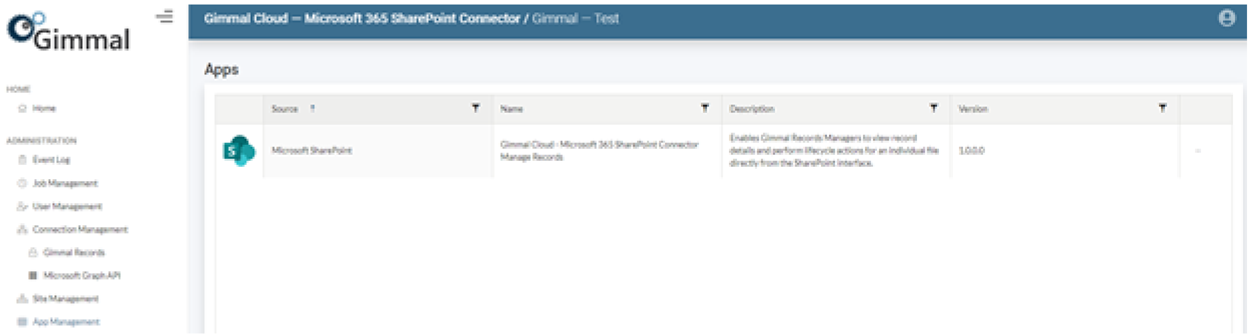
Click **Save** to save settings.



7.10.11.9 App Management

The **App Management** page is where administrators can download the Manage Record app.

The **Manage Record** option enables Gimmal Records Managers to view record details and perform lifecycle actions for an individual file directly from the SharePoint interface.

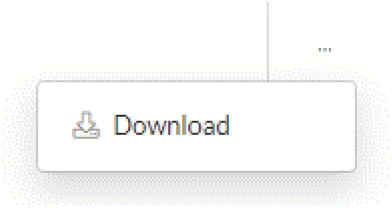


	Source	Name	Description	Version	
	Microsoft SharePoint	Gimmal Cloud - Microsoft 365 SharePoint Connector Manage Records	Enables Gimmal Records Managers to view record details and perform lifecycle actions for an individual file directly from the SharePoint interface.	1.0.0.0	...

Implement App Management

Navigate to **App Management** within the Microsoft 365 SharePoint Connector.

Click the ellipses button (…) for the app, then click **Download**.



An .sppkg file will appear in your **Downloads** folder in File Explorer.

Login to your SharePoint Admin Center[75].

Navigate to the **App Catalog** by selecting **More features** on the left navigation menu and click **Apps**.

Click **App Catalog**.

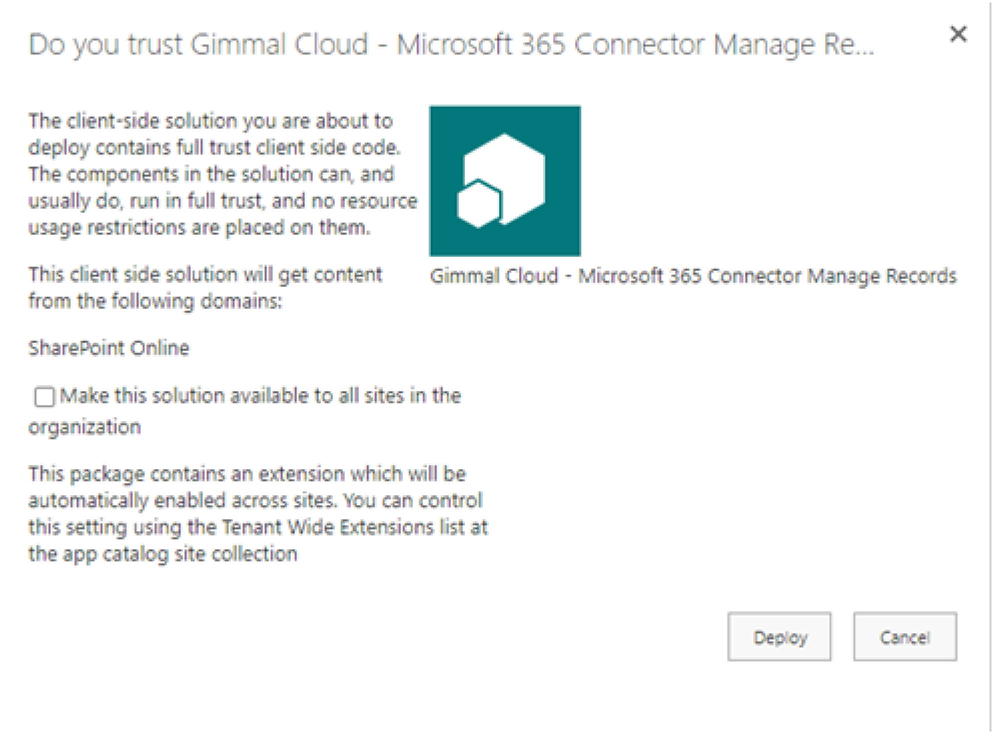
Click **Apps for SharePoint**.

Click **Upload**, choose the .sppkg file previously downloaded from the Microsoft 365 SharePoint Connector App Management page, and click **OK**.

Click **Deploy** to deploy the Manage Record functionality to the SharePoint Online App Catalog.

> **NOTE** – Select **Make this solution available to all sites in the organization** to automatically add the app to all new and existing sites in the organization.

[75] https://admin.microsoft.com/sharepoint?page=home&modern=true



Do you trust Gimmal Cloud - Microsoft 365 Connector Manage Re...

The client-side solution you are about to deploy contains full trust client side code. The components in the solution can, and usually do, run in full trust, and no resource usage restrictions are placed on them.

Gimmal Cloud - Microsoft 365 Connector Manage Records

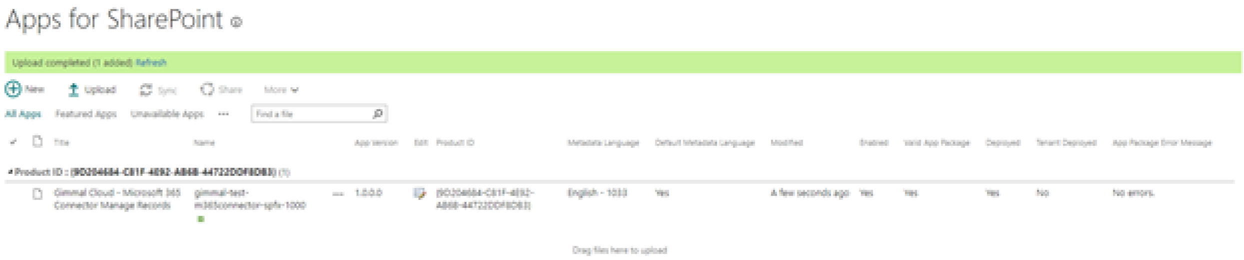
This client side solution will get content from the following domains:

SharePoint Online

☐ Make this solution available to all sites in the organization

This package contains an extension which will be automatically enabled across sites. You can control this setting using the Tenant Wide Extensions list at the app catalog site collection

Verify that the app is deployed to the SharePoint Online App Catalog.



Apps for SharePoint

Upload completed (1 added) Refresh

Product ID : {9D204684-C81F-4E92-AB6B-44722DDF8D83} (1)

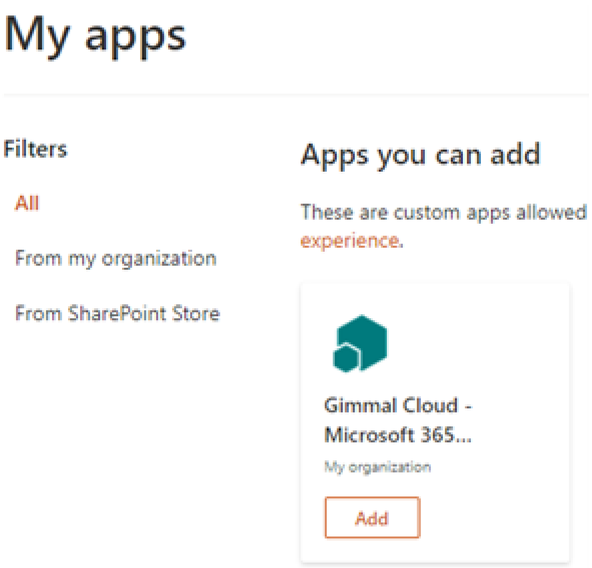
Title	Name	App Version	Edit	Product ID	Metadata Language	Default Metadata Language	Modified	Enabled	Valid App Package	Deployed	Tenant Deployed	App Package Error Message
Gimmal Cloud - Microsoft 365 Connector Manage Records	gimmal-test-m365connector-spfx-1000	1.0.0.0		{9D204684-C81F-4E92-AB6B-44722DDF8D83}	English - 1033	Yes	A few seconds ago	Yes	Yes	Yes	No	No errors.

Drag files here to upload

Manually add the app to a SharePoint site by navigating to a SharePoint site and click **Site Contents**.

Click **(+) New** and select **App**.

Select the **Gimmal Cloud – Microsoft 365 Connector Manage Records** app and click **Add**.



My apps

Filters

- All
- From my organization
- From SharePoint Store

Apps you can add

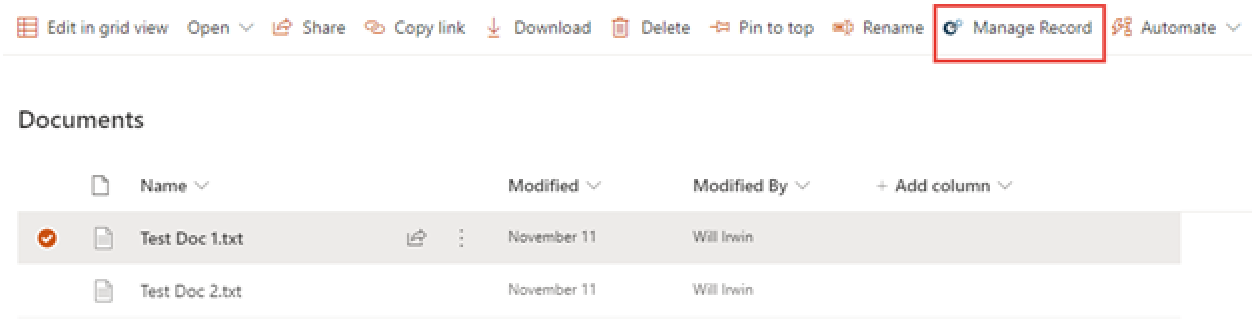
These are custom apps allowed experience.

Gimmal Cloud - Microsoft 365...

My organization

Verify the **Gimmal Cloud – Microsoft 365 Connector Manage Records** app is added to Site Contents.

The Gimmal Manage Record button will now appear for documents being managed by Gimmal Records.



Documents

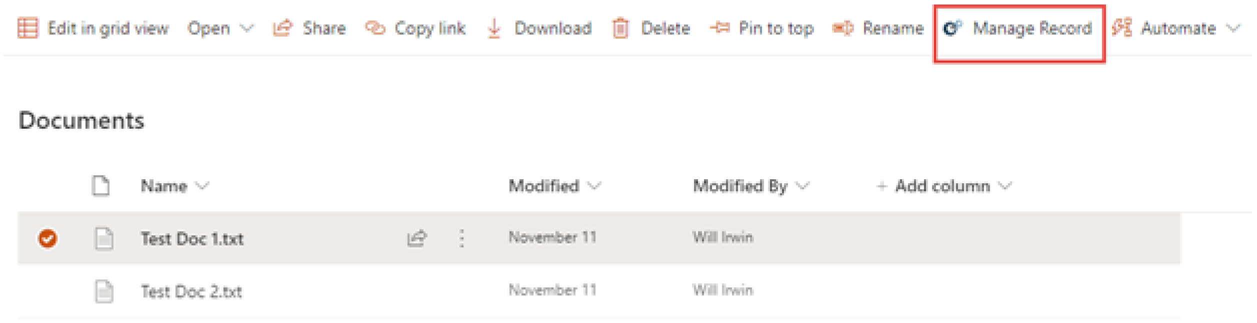
	Name	Modified	Modified By	+ Add column
✓	Test Doc 1.txt	November 11	Will Irwin	
	Test Doc 2.txt	November 11	Will Irwin	

7.10.11.10 Manage Records

The **Manage Record** option enables Gimmal Records Managers to view record details and perform lifecycle actions for an individual file directly from the SharePoint interface.

Select a single file in a Document Library.

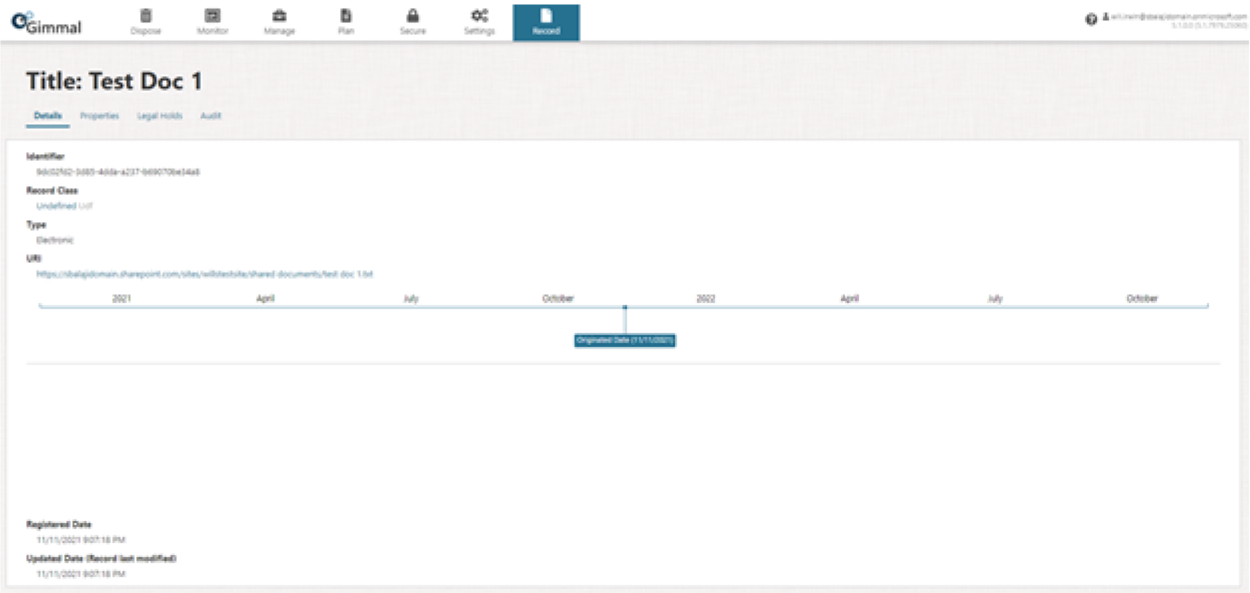
Click the **Manage Record** button.



Documents

	Name	Modified	Modified By	+ Add column
✓	Test Doc 1.txt	November 11	Will Irwin	
	Test Doc 2.txt	November 11	Will Irwin	

Gimmal Records will open in a new web browser tab and the **Record Overview** tab will display record details.



Title: Test Doc 1

Details Properties Legal Holds Audit

Identifier
9dc02fd2-3d85-4dda-a237-b690706e34a8

Record Class
Undefined UDF

Type
Electronic

URI
https://sbalajidomain.sharepoint.com/sites/willstestsite/shared documents/test doc 1.txt

Registered Date
11/11/2021 9:07:18 PM

Updated Date (Record last modified)
11/11/2021 9:07:18 PM

7.10.11.11 Preservation

Gimmal's Microsoft 365 SharePoint Connector allows for the creation of preservation copies. Enable the **Preserve** setting on a Record Class in Gimmal Records to preserve content, leaving content in place, that uses a connected Azure Blog Storage for preservation.

Enable Preservation

Preservation Copies are enabled within the Gimmal Records Manager Web.

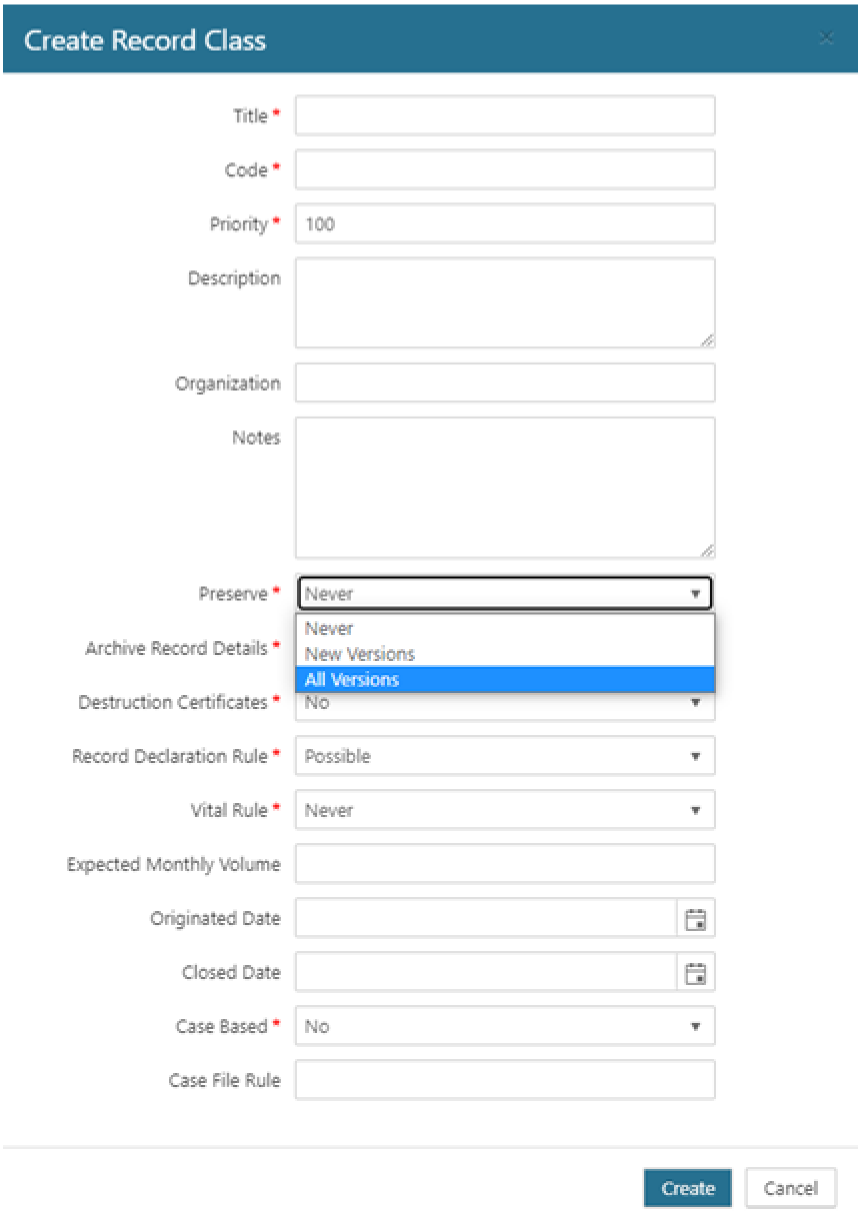
Create or edit a Record Class.

For **Preserve**, select **New Versions** or **All Versions**.

- **New Versions** – this option will retain all new versions of a document, as well as the current version.
  - For sources with versioning, this would create a preservation copy for the current version and every new version created.
  - For sources without versioning, or versioning turned off, this will create a new preservation copy every time the content or metadata is changed.
- **All Versions** – this option will retain all previous versions and all new versions of a document.
  - For sources with versioning, this would create a preservation copy for every version already existing and for every new version.
  - For sources without versioning, or versioning turned off, this will create a new preservation copy every time the content or metadata is changed.

NOTE – see Preservation Copy Creation and Behavior sections below for more detail.

Click **Create** or **Save** to save the Record Class.



Create Record Class

Title *

Code *

Priority * 100

Description

Organization

Notes

Preserve * Never

Archive Record Details *

Destruction Certificates * No

Record Declaration Rule * Possible

Vital Rule * Never

Expected Monthly Volume

Originated Date

Closed Date

Case Based * No

Case File Rule

All records that get classified to this record class will now have a preservation copy created based on the chosen configuration setting.

Preservation Copy Creation

Preservation Copy Setting	**SharePoint Versioning**	**Scenario**	**Preservation Copy Created?**

Preserve All Versions	Major Versions	‘Create major versions’ is enabled on a Document Library that contains records configured for *Preserve all versions.*	**Yes** – a preservation copy is created for each existing major version and every new major version.
	Major and Minor (Draft) Versions	‘Create major and minor (draft) versions’ is enabled on a Document Library that contains records configured for *Preserve all versions.*	**Yes** – a preservation copy is created for each existing major and minor version, and every new major and minor version.
	No Versioning	‘No versioning’ is enabled on a Document Library that contains records configured for *Preserve all versions.*	**Yes** – adhere to Preservation Copy Settings and create a preservation copy for current version and each time the incremental classification job notices a change for the file.
Preserve New Versions	Major Versions	‘Create major versions’ is enabled on a Document Library that contains records configured for *Preserve new versions.*	**Yes** – a preservation copy is created for each new major version, as well as the current version.
	Major and Minor (Draft) Versions	‘Create major and minor (draft) versions’ is enabled on a Document Library that contains records configured for *Preserve new versions.*	**Yes** – a preservation copy is created for each new major and minor version, as well as the current version.
	No Versioning	‘No versioning’ is enabled on a Document Library that contains records configured for *Preserve new versions.*	**Yes** – adhere to Preservation Copy Settings and create a preservation copy for current version and each time the incremental classification job notices a change for the file.
Never (Disabled)	Major Versions	‘Create major versions’ is enabled on a Document Library that contains records *NOT* configured for Preservation.	**No** – a preservation copy is not created.
	Major and Minor (Draft) Versions	‘Create major and minor (draft) versions’ is enabled on a Document Library that contains records *NOT* configured for Preservation.	**No** – a preservation copy is not created.

	No Versioning	‘No versioning’ is enabled on a Document Library that contains records *NOT* configured for Preservation.	**No** – a preservation copy is not created.
Any Configuration Option	**Any Configuration Option**	A Record Manager **declares a record** (either manually or through a lifecycle action).	**No** – a preservation copy is not created. **Note** – M365 Connector will successfully “complete” the retention declare / undeclare action but does not lock / unlock the item in SharePoint Online, unless the Gimmal "Locked Record" M365 Retention Label is created and published.
Any Configuration Option	**Any Configuration Option**	A Record Manager applies a **legal hold** (either manually or through a classification rule).	**Yes** – a preservation copy is created for each existing version and every new version for all documents under that legal hold. (Behaves like “All Versions” being preserved)

Preservation Copy Behavior

Site Registration

Preservation Setting	**Scenario**	**Preservation Copy Behavior**	**Gimmal Records Behavior**
Enabled (Preserve All or New Versions)	1. Site is added in M365 Connector. 2. Crawls the newly added site and adds records to Gimmal Records. 3. Classifies newly crawled records to a Record Class with preservation enabled. 4. Preservation copies are created in Archive. 5. Unregister the newly added site in M365 Connector.	Preservation copies remain in Archive.	Preserved records remain in Gimmal Records. **Note** – re-registering a site that was unregistered will sync back to the same records that remain in Gimmal Records (no duplicate record entries).

Never (Disabled)	1. Site is added in M365 Connector. 2. Crawls the newly added site and adds records to Gimmal Records. 3. Classifies newly crawled records to a Record Class with preservation disabled. 4. No preservation copies are created in Archive. 5. Unregister the newly added site in M365 Connector.	No preservation copies in Archive.	Records are removed from Gimmal Records.

Changing the Preserve Setting on a Record Class

Original Preservation Setting	**New Preservation Setting**	**Scenario**	**Preservation Copy Behavior**
Preserve All Versions	**Preserve New Versions**	The preservation setting on a Record Class is changed from Preserve All Versions to Preserve New Versions.	Existing preservation copies are unchanged; however, now only new versions will be retained as preservation copies.
Preserve New Versions	**Preserve All Versions**	The preservation setting on a Record Class is changed from Preserve New Versions to Preserve All Versions.	Existing preservation copies are unchanged; however, all versions will **not** be retained as preservation copies. **NOTE** - at this time, changing the original preservation setting will not preserve earlier versions.
Enabled (Preserve All or New Versions)	**Disabled**	The preservation setting on a Record Class is changed from being enabled to disabled.	Existing preservation copies are unchanged; however, no new preservation copies will be created.

Applying a Legal Hold

Preservation Setting	**Legal Hold Setting**	**Scenario / Preservation Copy Behavior**

Preserve New Versions	1 legal hold applied, then removed	1. A record exists in a Record Class with preservation set to “Preserve New Versions”. a. Preservation copy is created based on Preservation Copy Creation matrix above for “Preserve New Versions”. 2. Apply 1 legal hold. a. Additional preservation copies created because legal holds will behave like “Preserve All Versions” setting. 3. Remove the legal hold. a. Preservation copies remain in Archive, but now only new versions will be retained.
Preserve All Versions	1 legal hold applied, then removed	1. A record exists in a Record Class with preservation set to “Preserve All Versions”. a. Preservation copy is created based on Preservation Copy Creation matrix above for “Preserve All Versions”. 2. Apply 1 legal hold. a. No new preservation copy is created because they all already exist for this record because preservation was set to “Preserve All Versions”. 3. Remove the legal hold. a. Preservation copies remain in Archive.
Never (Disabled)	1 legal hold applied, then removed	1. A record exists in a Record Class with preservation disabled. 2. Apply 1 legal hold. a. Preservation copy is created (behaves like “Preserve All Versions” setting). 3. Remove the legal hold. a. Preservation copy created when legal hold was applied will remain in Archive until record is disposed in Gimmal Records, but no new preservation copies will be created because preservation setting is disabled.

Deleting the Source Item

Preservation Setting	**Scenario**	**Preservation Copy Behavior**	**Gimmal Records Behavior**

Enabled (Preserve All or New Versions)	The source item is deleted in the repository. (SharePoint Online) **Note** – this scenario is a user deleting a file in SharePoint and not through the official Gimmal Record disposition process.	Existing preservation copies will remain.	Gimmal Records that have preservation copies enabled will not be deleted when the source item is deleted. The Record will remain in Gimmal Records until disposition occurs.
Never (Disabled)	The source item is deleted in the repository. (SharePoint Online)	No preservation copies in Archive.	Records are removed from Gimmal Records.

Gimmal Records Disposition

Scenario	**Preservation Copy Behavior**
The record is disposed using Gimmal Records based on retention rules and lifecycle settings.	Existing preservation copies are deleted.

7.10.11.12 Record Locking with Microsoft 365 Retention Labels

The Microsoft 365 SharePoint Connector supports the option to perform record locking using M365 Retention Labels for customers wanting to lock records when declared, when on legal hold, etc.

NOTE – when using M365 Retention Labels for record locking, SharePoint Site users will still have the ability to modify the labeled document and edit its properties, but not delete the document.

Create Microsoft 365 Retention Label for Record Locking

Navigate to your SharePoint Admin Center.

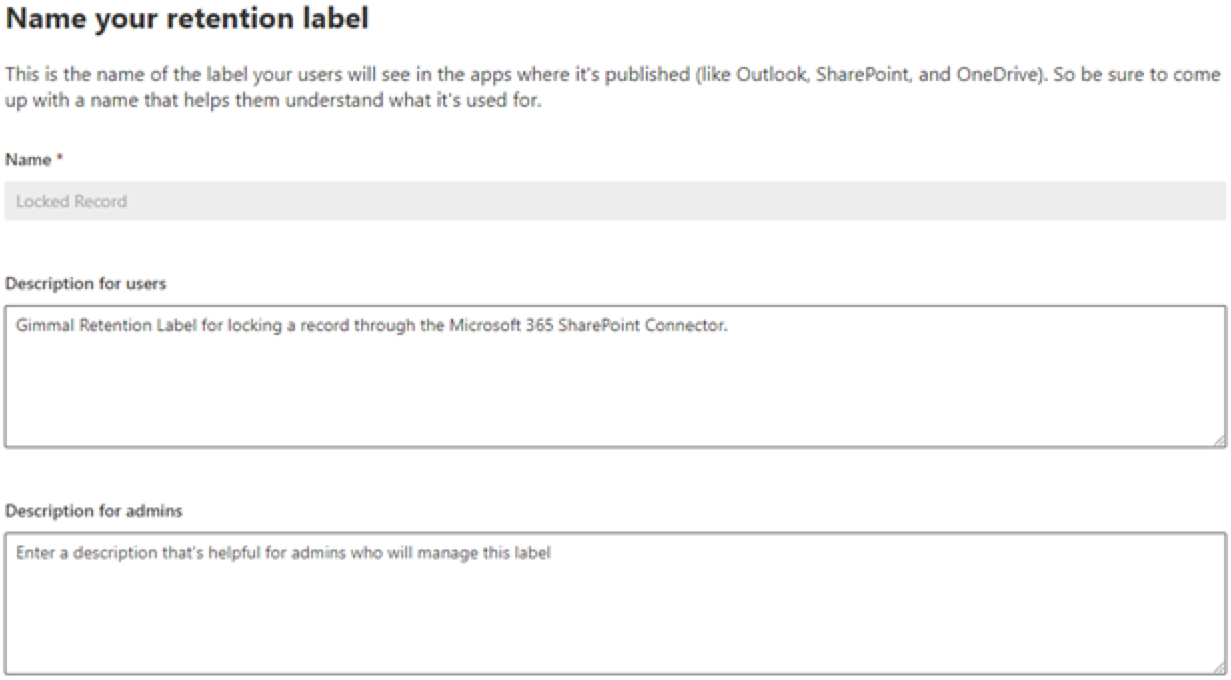
Click **Compliance** in the left navigation.

Click **Records Management** in the left navigation.

Select **File Plan** from the top navigation.

Click **Create a label**.

- **Name** – must be named “**Locked Record**”.
    - **NOTE** – The Microsoft 365 SharePoint Connector is looking for a retention label titled “Locked Record”, naming this something different will results in no record locking.
- **Description** – optional
    - “Gimmal Retention Label for locking a record through the Microsoft 365 SharePoint Connector.”
- **Description for admins** – optional



Name your retention label

This is the name of the label your users will see in the apps where it's published (like Outlook, SharePoint, and OneDrive). So be sure to come up with a name that helps them understand what it's used for.

Name *

Locked Record

Description for users

Gimmal Retention Label for locking a record through the Microsoft 365 SharePoint Connector.

Description for admins

Enter a description that's helpful for admins who will manage this label

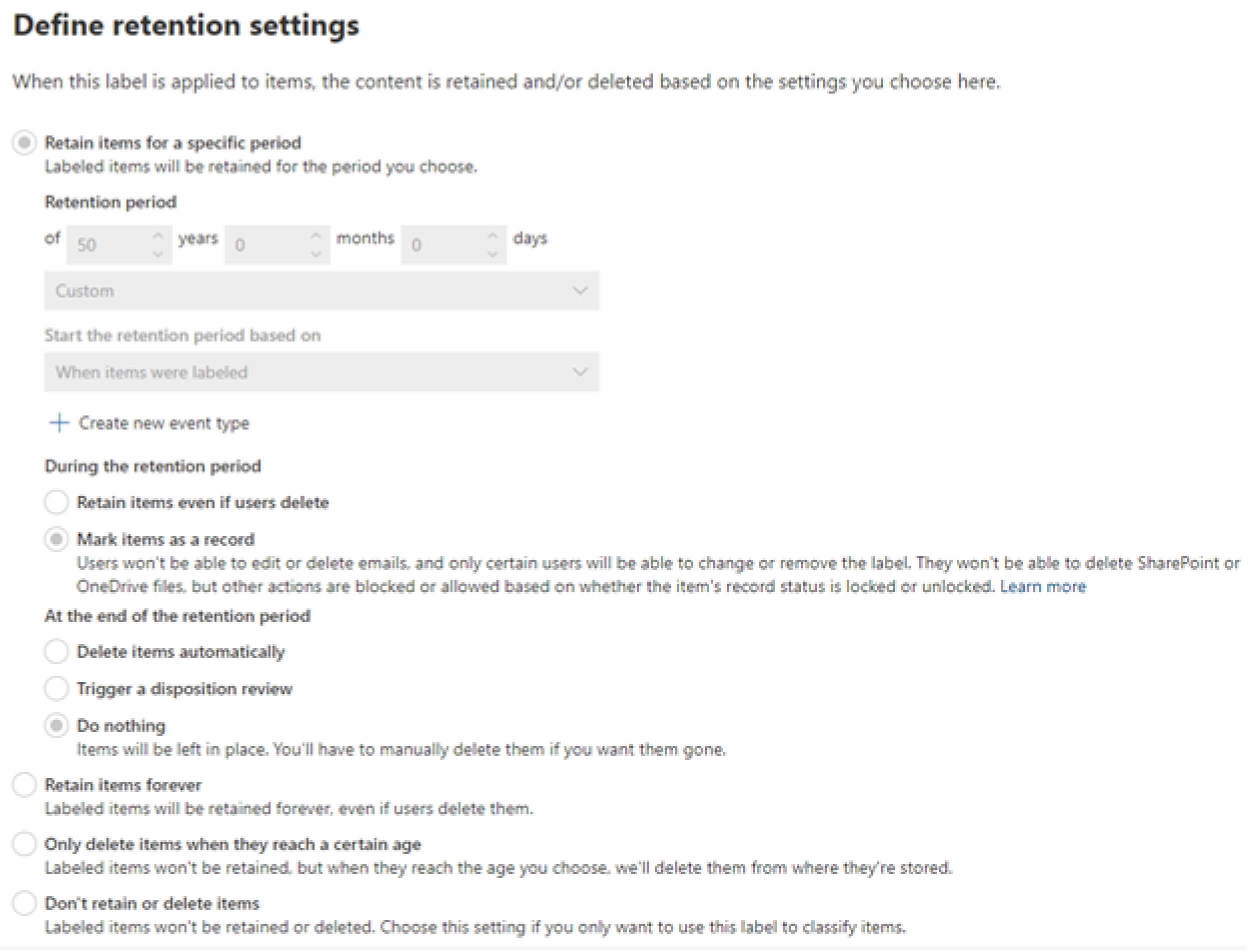
Click **Next**.

File plan descriptors are optional.

Click **Next**.

Retention Settings:

- Retain items for a specific period:
    - Select a **Retention Period of 50 Years**.
- **Mark items as a record**
- Set **Do nothing** for end of retention period.



Define retention settings

When this label is applied to items, the content is retained and/or deleted based on the settings you choose here.

● Retain items for a specific period
Labeled items will be retained for the period you choose.

Retention period

of 50 years 0 months 0 days

Custom

Start the retention period based on

When items were labeled

+ Create new event type

During the retention period

○ Retain items even if users delete

● Mark items as a record
Users won't be able to edit or delete emails, and only certain users will be able to change or remove the label. They won't be able to delete SharePoint or OneDrive files, but other actions are blocked or allowed based on whether the item's record status is locked or unlocked. Learn more

At the end of the retention period

○ Delete items automatically

○ Trigger a disposition review

● Do nothing
Items will be left in place. You'll have to manually delete them if you want them gone.

○ Retain items forever
Labeled items will be retained forever, even if users delete them.

○ Only delete items when they reach a certain age
Labeled items won't be retained, but when they reach the age you choose, we'll delete them from where they're stored.

○ Don't retain or delete items
Labeled items won't be retained or deleted. Choose this setting if you only want to use this label to classify items.

Review and finish. Click **Create**.

Select **Publish This Label**.

Creating the Policy:

- Ensure your new label is the one being published – click **Next**.
- Can leave as default or select **let me choose** and only select SharePoint site – click **Next**.
- Pick a name for the policy – name isn't important, but required – click **Next**.
- Review your settings and submit.
- **NOTE** – publishing the label can take up to one (1) day to show up in SharePoint.

7.10.12 SharePoint Online Connector

The SharePoint Online Connector enables content in your SharePoint Online tenant to be manged by Gimmal 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 340)
- 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)

7.10.12.1 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 Gimmal.

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 Gimmal Records. You would want to enable this feature for your Site before registering and configuring the SharePoint Online Connector.
> Please contact your SharePoint system administrator for help enabling the “In Place Records Management” feature.

> Before installing the SharePoint Online Connector a SharePoint Administrator must run from PowerShell
>
> **Disable Custom App Authentication**
>
> ```
> set-spotenant -DisableCustomAppAuthentication $false
> ```

on the SharePoint Online tenant. Please refer to this Microsoft documentation: https://docs.microsoft.com/en-us/sharepoint/dev/solution-guidance/security-apponly-azureacs

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 Gimmal 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 Gimmal with channels within Microsoft Teams:

Declaring content as a record or adding content to a legal hold in a Teams channel folder	The content will be successfully locked but Gimmal Records Management will not be able to delete it at the end of the lifecycle due to the Channel folder behavior. **Workaround**: Manually un-declare the record within SharePoint before the disposition phase.
Declaring a record using In Place Record Management	Gimmal strongly discourages you from using the user interface in SharePoint to declare a record using "In Place Records Management" while using Gimmal Records Management. If content is declared using "In Place Records Management", Gimmal Records Management will not be able to delete it at the end of the lifecycle due to the separate hold. **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.

Gimmal recommends that when using Records Management with Microsoft Teams to not declare records or create legal holds on items within Microsoft Team channels.

7.10.12.2 Prepare to use the SharePoint Online Connector

These instructions are provided for convenience. Registering the SharePoint App and creating the catalog are out of scope for Gimmal Support. Please contact your SharePoint Online or Microsoft 365 administrator for help completing these tasks.

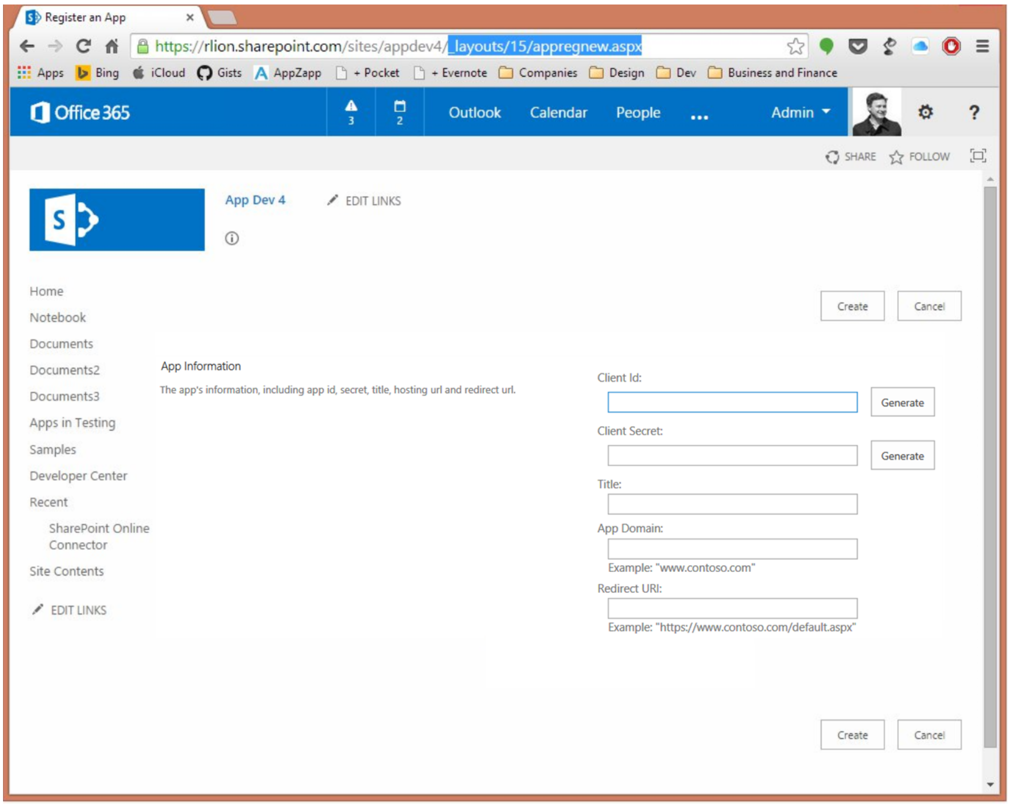
⚠ You cannot configure the SharePoint Online Connector app (effectively the same O365 tenant) to work with two different instances of Records Management. You must provide distinct Microsoft 365 tenants to accomplish this requirement. For example, https://test-company.sharepoint.com is registered to https://records.gimmal.build and https://company.sharepoint.com is registered to https://records.gimmal.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.



App Information

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

Client Id:

Client Secret:

Title:

App Domain:

Example: "www.contoso.com"

Redirect URI:

Example: "https://www.contoso.com/default.aspx"

- **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.com[76]:8084. If you are using the

[76] http://spoc.domain.com

default HTTPS port (443) for your connector web, then you can omit it from the App Domain; for example, spoc.domain.com[77].

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** Gimmal Cloud service customers (pre-Feb. 27th, 2021) should continue to use the existing URLs.
New Gimmal 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[78]):
  App Domain: test-conn-spo.recordlion.net[79]
  Redirect URL: https://test-conn-spo.recordlion.net[80]
- Your SPOC app should be configured in O365 exactly as follows for a PRODUCTION tenant (https://app.recordlion.net[81]):
  App Domain: app-conn-spo.recordlion.net[82]
  Redirect URL: https://app-conn-spo.recordlion.net[83]

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[84]):
  App Domain: testuk-conn-spo.recordlion.net[85]
  Redirect URL: https://testuk-conn-spo.recordlion.net[86]
- Your SPOC app should be configured in O365 exactly as follows for a PRODUCTION tenant (https://uk.recordlion.net[87]):

[77] http://spoc.domain.com
[78] https://testuk.recordlion.net
[79] http://testuk-conn-spo.recordlion.net
[80] https://testuk-conn-spo.recordlion.net
[81] https://uk.recordlion.net
[82] http://uk-conn-spo.recordlion.net
[83] https://uk-conn-spo.recordlion.net
[84] https://test.recordlion.net
[85] http://test-conn-spo.recordlion.net
[86] https://test-conn-spo.recordlion.net
[87] https://app.recordlion.net

App Domain: uk-conn-spo.recordlion.net[88]
Redirect URL: https://uk-conn-spo.recordlion.net[89]

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.gimmal.build):
  App Domain: spo-records.gimmal.build[90]
  Redirect URL: https://spo-records.gimmal.build
- Your SPOC app should be configured in O365 exactly as follows for a PRODUCTION tenant (https://records.gimmal.cloud):
  App Domain: spo-records.gimmal.cloud[91]
  Redirect URL: https://spo-records.gimmal.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.gimmal.build):
  App Domain: spo-records.uk.gimmal.build[92]
  Redirect URL: https://spo-records.uk.gimmal.build
- Your SPOC app should be configured in O365 exactly as follows for a PRODUCTION tenant (https://records.uk.gimmal.cloud):
  App Domain: spo-records.uk.gimmal.cloud[93]
  Redirect URL: https://spo-records.uk.gimmal.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.gimmal.cloud):
  App Domain: spo-records-ca.gimmal.cloud[94]
  Redirect URL: https://spo-records-ca.gimmal.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.

[88] http://app-conn-spo.recordlion.net
[89] https://app-conn-spo.recordlion.net
[90] https://spo-records.gimmal.build
[91] https://spo-records.gimmal.cloud
[92] https://spo-records.uk.gimmal.build
[93] https://spo-records.uk.gimmal.cloud
[94] https://spo-records-ca.gimmal.cloud

> ⓘ 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.

7.10.12.3 SharePoint Online Connector On-Premise Only

> ⚠ If you are setting up the SharePoint Online Connector using the Gimmal Cloud platform, skip the topics for SharePoint Online Connector On-Premise.

The SharePoint Online Connector enables Gimmal Records Management to manage the lifecycle of documents stored in SharePoint Online. It consists of the following components:

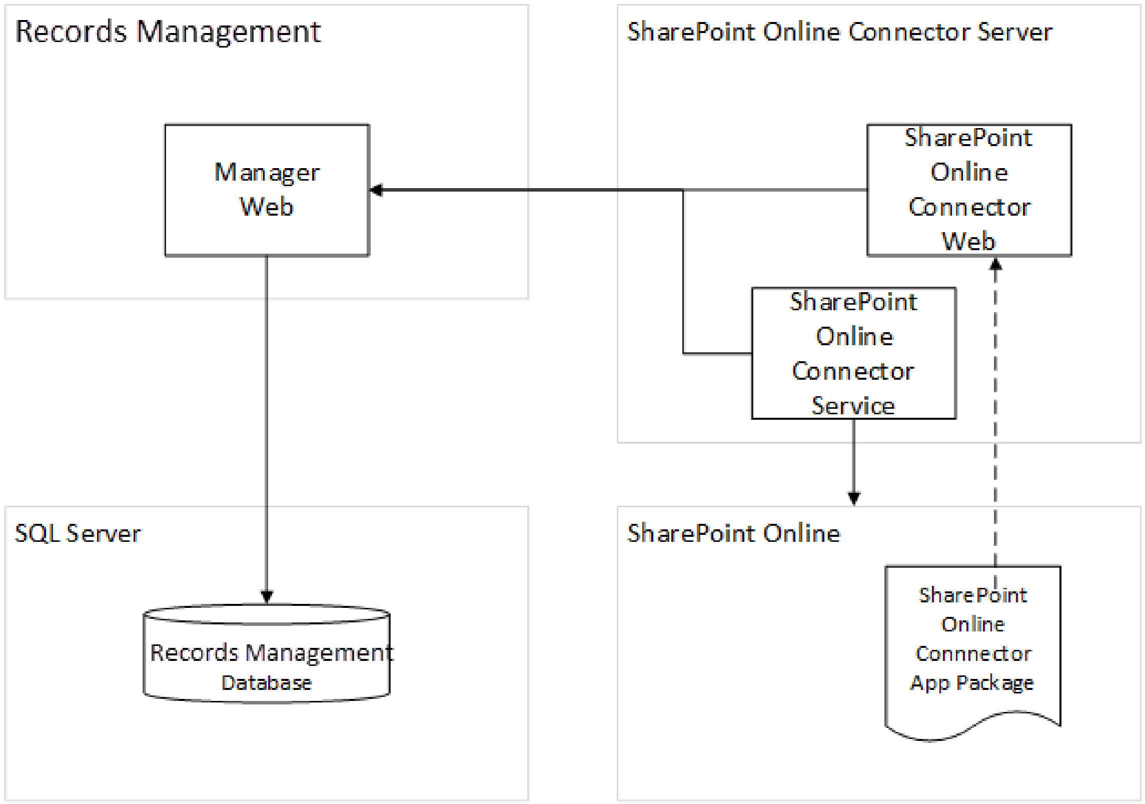
SharePoint Online Connector Web

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


Records Management
Manager Web
SharePoint Online Connector Server
SharePoint Online Connector Web
SharePoint Online Connector Service
SQL Server
Records Management Database
SharePoint Online
SharePoint Online Connnector App Package

Scalability

SharePoint Online Connector Web	
What comprises the solution...	• SharePoint App model • 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...	• 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...	• 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[95].
As a security best practice when using the .NET Framework, Gimmal 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[96] To verify that your operating system supports TLS 1.2, read the Support for TLS 1.2 section of Microsoft's documentation[97].

Database Server

- SQL Server 2016 or greater

[95] https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls#systemdefaulttlsversions
[96] https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls#systemdefaulttlsversions
[97] https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls#support-for-tls-12

SharePoint Online Connector On-Premise Installation

Pre-Installation

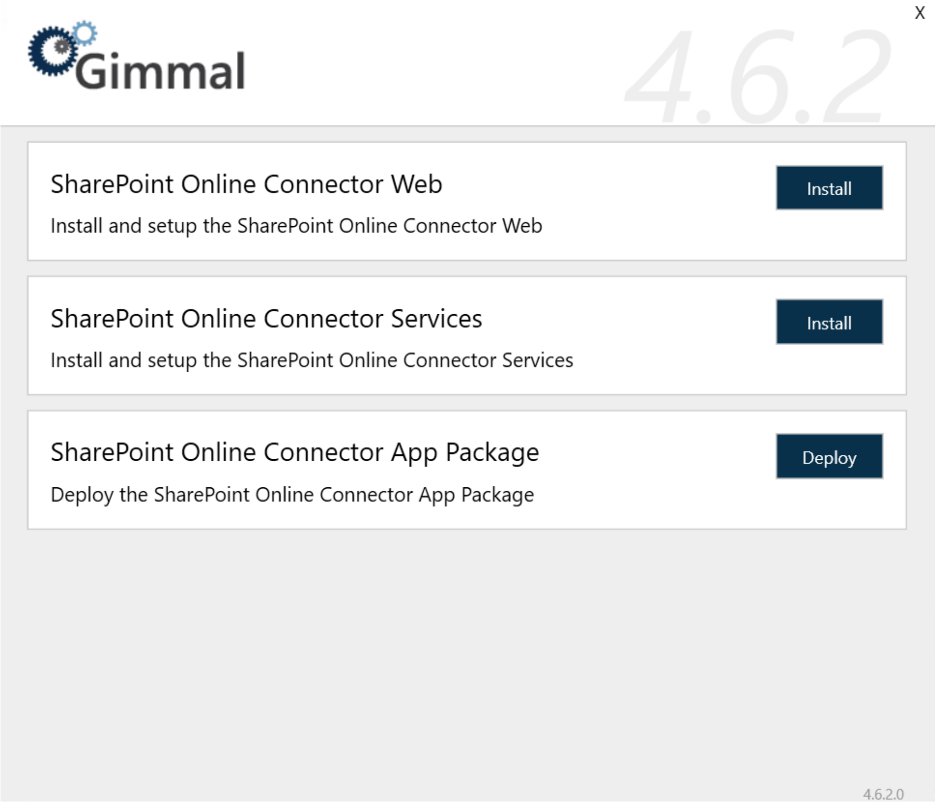
Configure Windows Roles and Features as follows:

- 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:



SharePoint Online Connector Web

Install and setup the SharePoint Online Connector Web

SharePoint Online Connector Services

Install and setup the SharePoint Online Connector Services

SharePoint Online Connector App Package

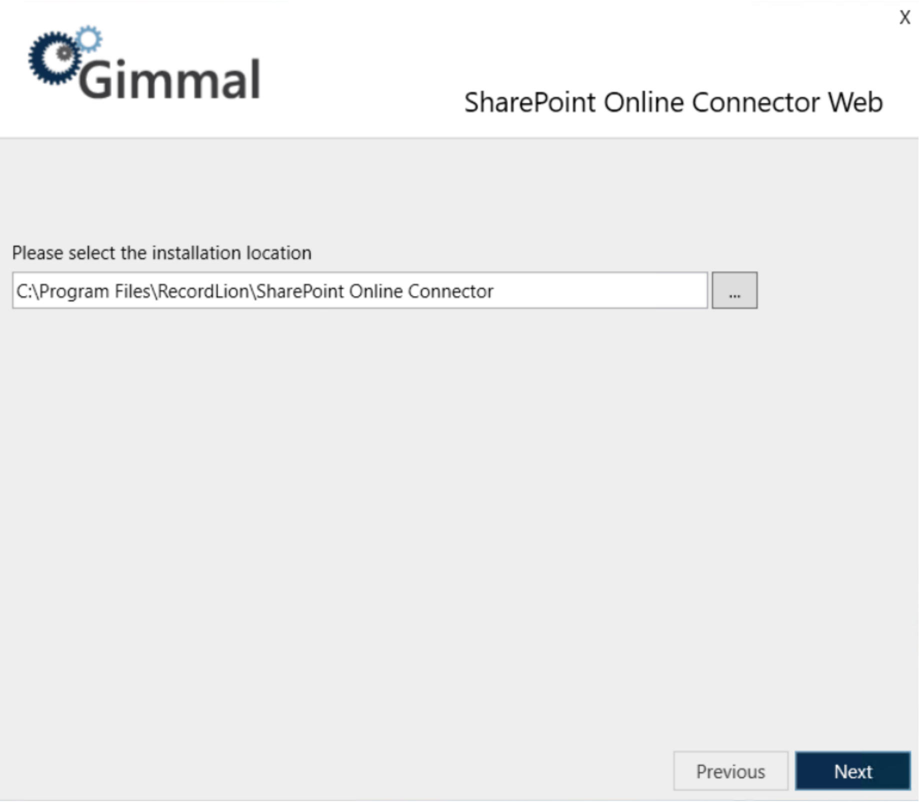
Deploy the SharePoint Online Connector App Package

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:

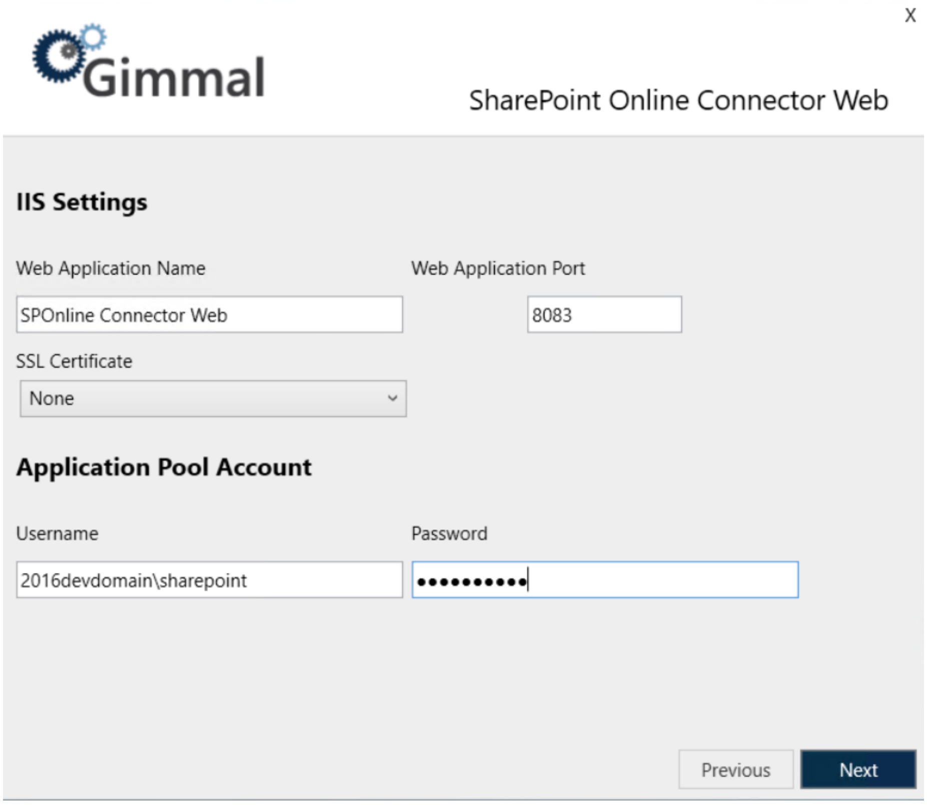
1. On the SharePoint Online Connector installer, click **Install** to the right of the SharePoint Online Connector Web option. The first screen that displays is the Check for Prerequisites. This screen validates the following information before allowing the installation to proceed:
   - Current User is Local Administrator
   - IIS 7+ is Installed
2. Click **Next**. The installation location screen displays, which determines where the connector will be installed.



Please select the installation location

C:\Program Files\RecordLion\SharePoint Online Connector

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.



SharePoint Online Connector Web

IIS Settings

Web Application Name: SPOnline Connector Web

Web Application Port: 8083

SSL Certificate: None

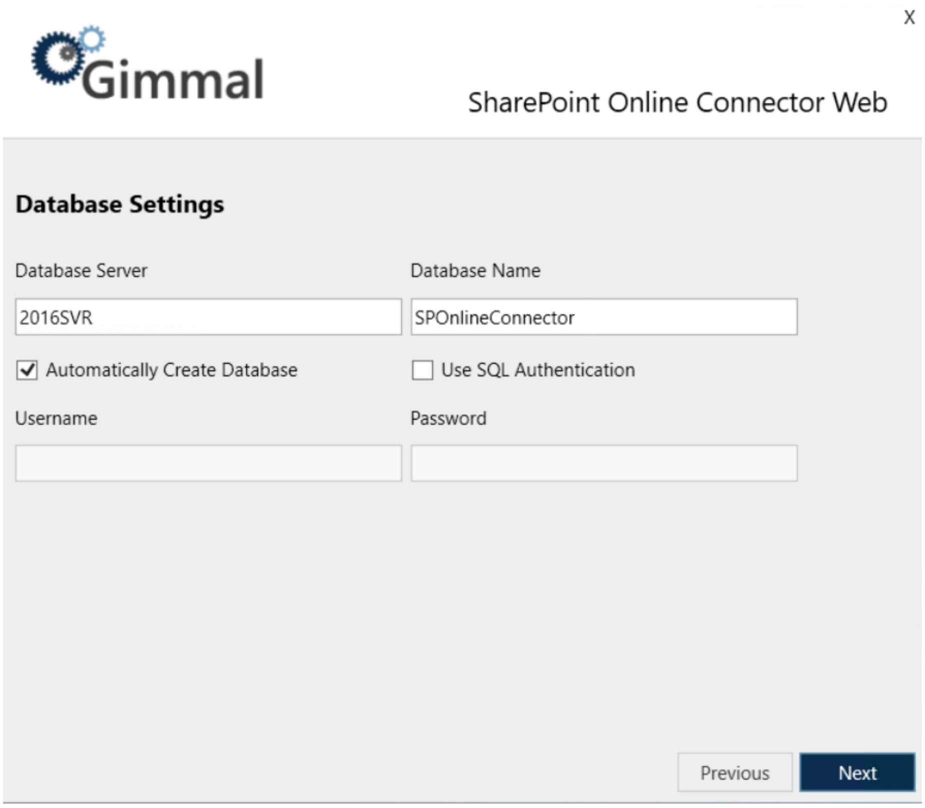
Application Pool Account

Username: 2016devdomain\sharepoint

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.



Database Settings

Database Server: 2016SVR

Database Name: SPOnlineConnector

☑ Automatically Create Database

□ Use SQL Authentication

Username:

Password:

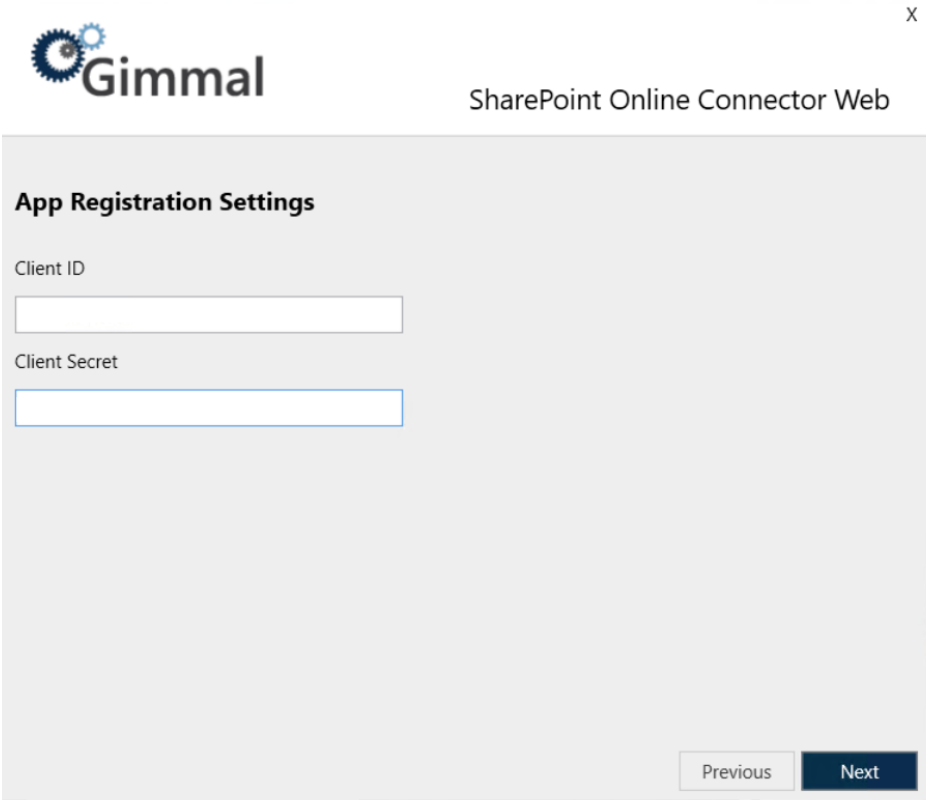
6. Enter the following information to determine the connection information that will be used by the SharePoint Online Connector to connect to SQL Server:
    - **Database Server:** The name of the SQL Server Install (ex. SERVERNAME\InstanceName)
    - **Database Name:** The name of the actual SQL Server 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

7. 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 340).



8. 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.
9. Click **Next**. The Installation screen displays. The progress bar indicates the current state of the installation.
10. When the application is finished installing, click **Next**. The Finish screen indicates that everything installed successfully.
11. Click **Finish** to close the installer.

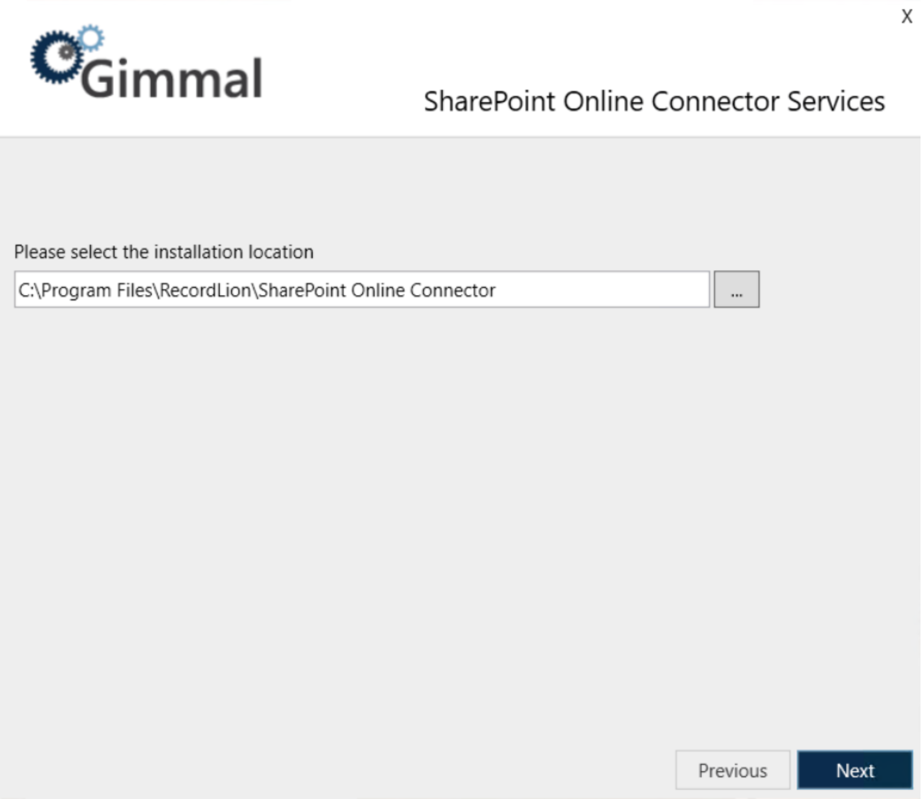
Continue to the next topic to install the SharePoint Online Connector Service:

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:

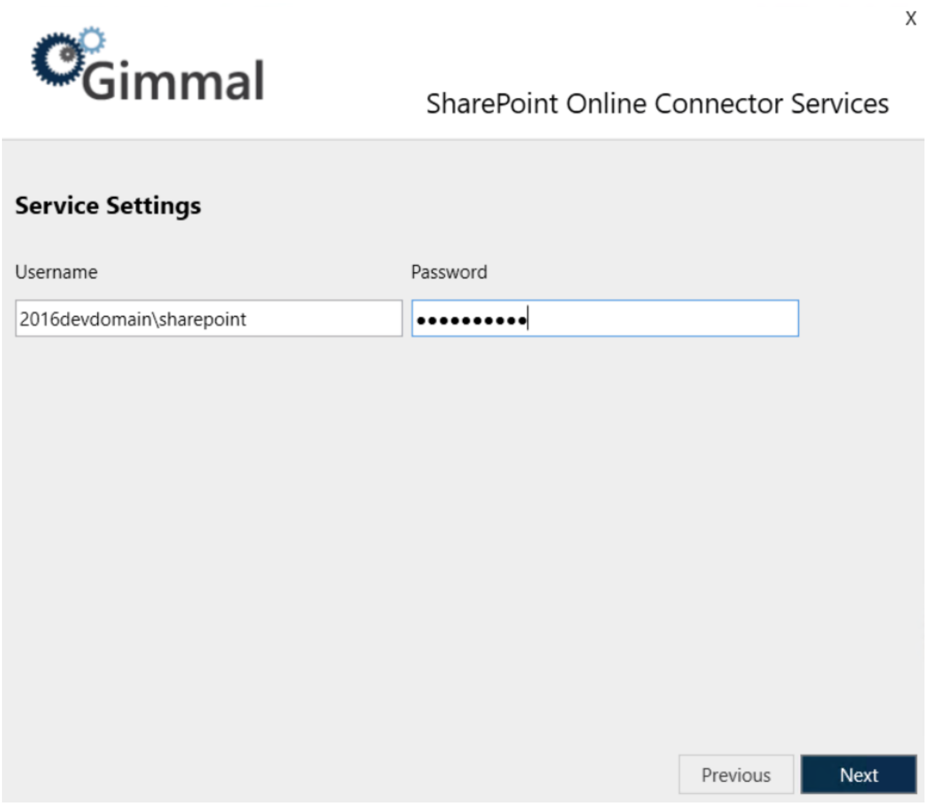
1. On the SharePoint Online Connector installer, click **Install** to the right of the SharePoint Online Connector Services option. The first screen that displays is the Check for Prerequisites. This screen validates the following information before allowing the installation to proceed:
2. Click **Next**. The installation location screen displays, which determines where the connector will be installed.



Please select the installation location

C:\Program Files\RecordLion\SharePoint Online Connector

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.



Service Settings

Username: 2016devdomain\sharepoint

Password: ●●●●●●●●●●

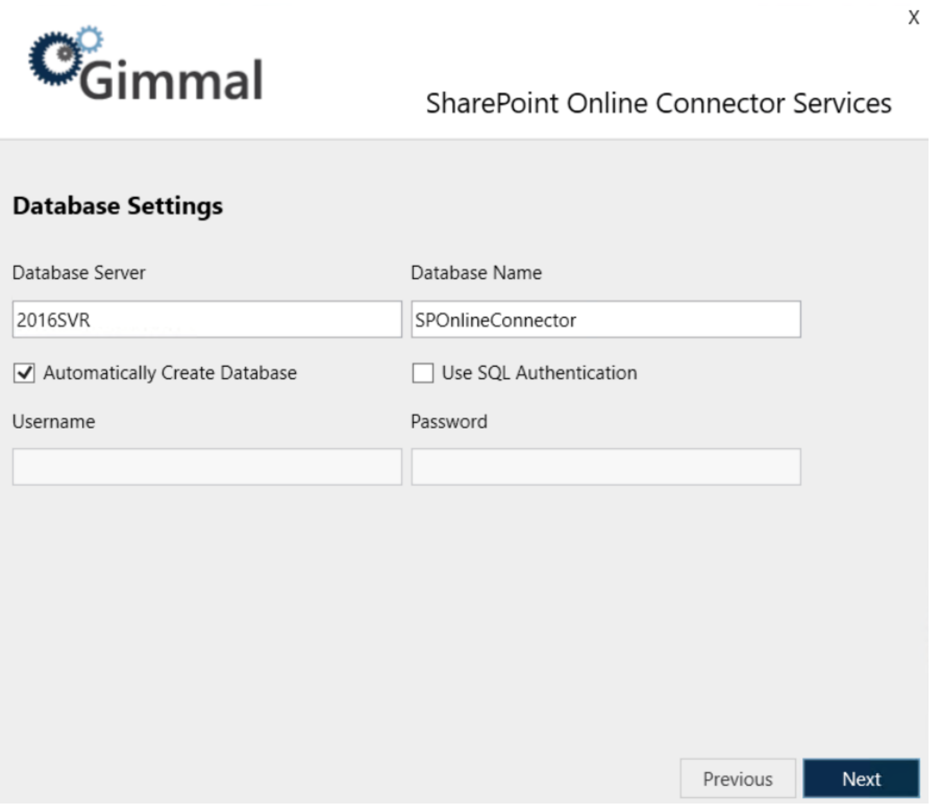
When SharePoint Online Connector Services is installed, a Windows Service is created. The following settings specify which user account to use to execute this Windows Service.

- **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.



SharePoint Online Connector Services

Database Settings

Database Server: 2016SVR

Database Name: SPOnlineConnector

☑ Automatically Create Database

☐ Use SQL Authentication

Username:

Password:

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

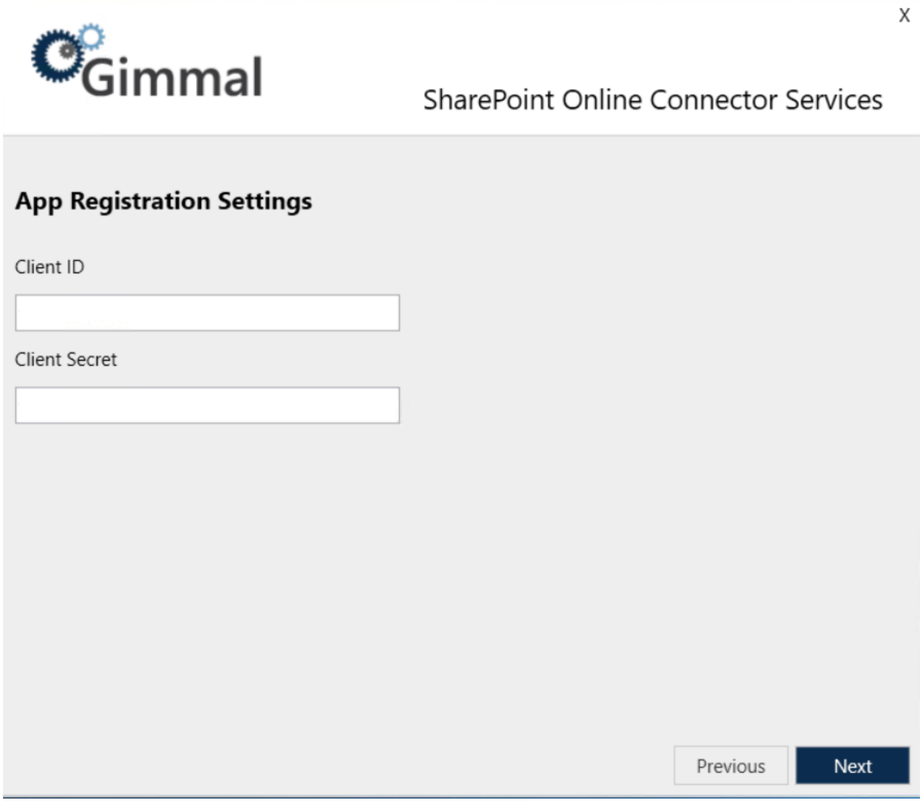
   If SQL Authentication is not specified, the connection information will use Windows Authentication by specifying a trusted connection. This means that the Service account will be used to connect to SQL Server, therefore, this account will need the following database permissions. If SQL Authentication 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.


x
Gimmal
SharePoint Online Connector Services
App Registration Settings
Client ID
Client Secret
Previous
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.

7.10.12.4 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

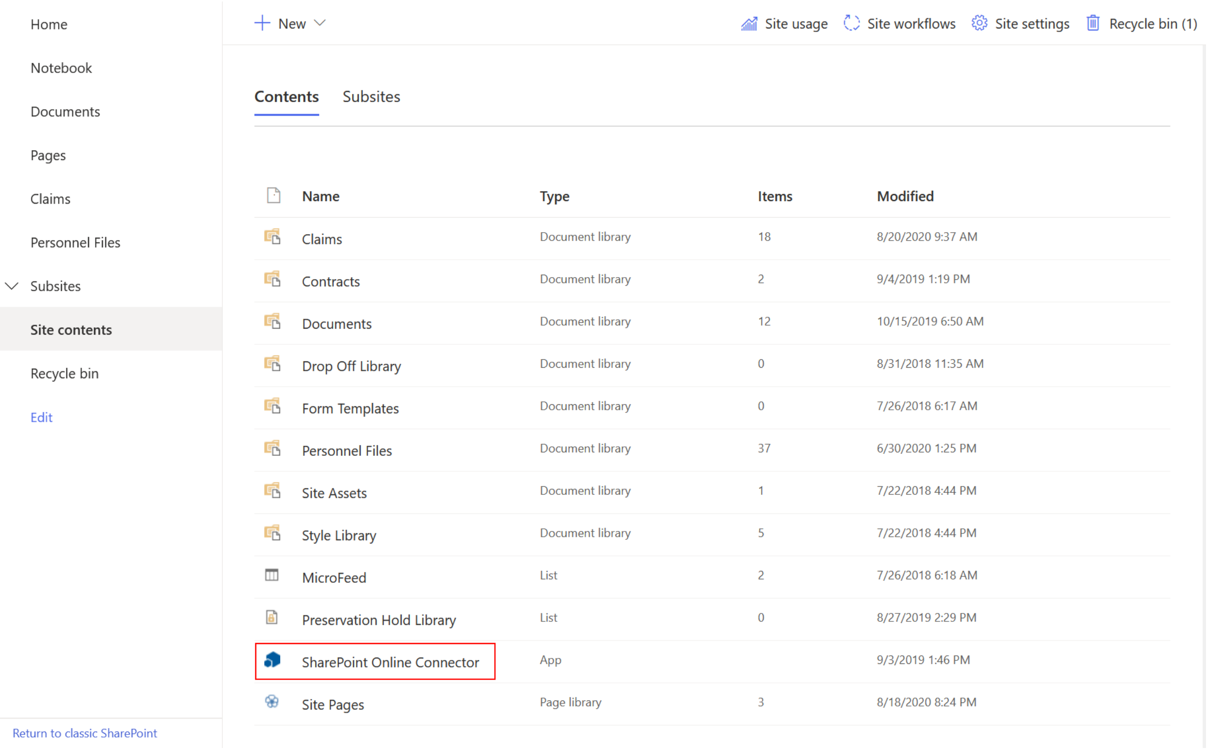
2. Click **Next**. The App Package will be uploaded to the SharePoint Online App Catalog you specified above.

7.10.12.5 SharePoint Online Connector Configuration

Connection

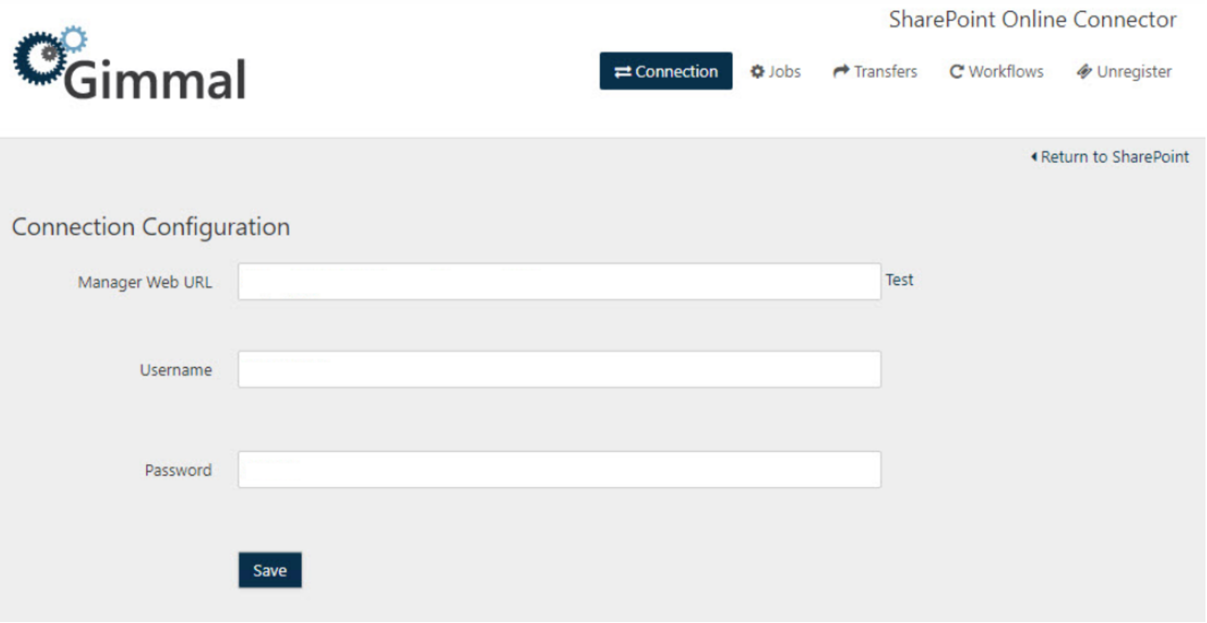
Once you install the SharePoint Online Connector, you must direct the Connector to the location of Records Management. To do so, perform the following steps:

1. Browse to a SharePoint Site that has the connector installed and open the Site Contents page.



Name	Type	Items	Modified
Claims	Document library	18	8/20/2020 9:37 AM
Contracts	Document library	2	9/4/2019 1:19 PM
Documents	Document library	12	10/15/2019 6:50 AM
Drop Off Library	Document library	0	8/31/2018 11:35 AM
Form Templates	Document library	0	7/26/2018 6:17 AM
Personnel Files	Document library	37	6/30/2020 1:25 PM
Site Assets	Document library	1	7/22/2018 4:44 PM
Style Library	Document library	5	7/22/2018 4:44 PM
MicroFeed	List	2	7/26/2018 6:18 AM
Preservation Hold Library	List	0	8/27/2019 2:29 PM
SharePoint Online Connector	App		9/3/2019 1:46 PM
Site Pages	Page library	3	8/18/2020 8:24 PM

2. Select the SharePoint Online Connector to open the SharePoint Online Connector Web and ensure that you're on the **Connection** tab.



3. Enter the URL to the Manager Web.
4. Enter the Username* of the Service Account(see page 221) created in Records Management.
5. Enter Password of the Service Account(see page 221) created in Records Management. (The password has a maximum length of 18 characters)
6. Click **Save.**

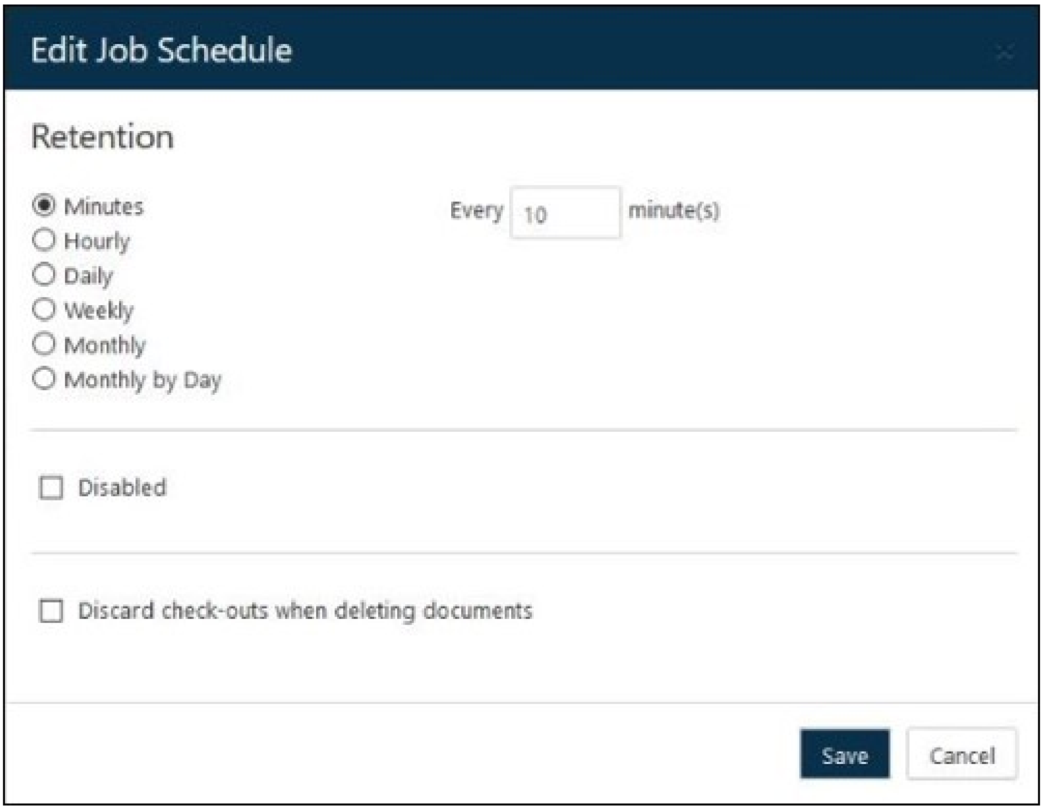
> ⚠ The Service Account username format depends on whether or not you are connecting to the Gimmal Cloud for Records Management. If the Gimmal Cloud is being used, the username format is: {service account name}@{tenant domain} (e.g. spocservice@gimmal.com[98], or fscservice@companyname.com[99]), otherwise, 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.

[98] mailto:spocservice@gimmal.com
[99] mailto:fscservice@companyname.com

Timer Job Type	Description
Gimmal Full Classification Job	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. 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. 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.
Gimmal Incremental Classification Job	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.

Timer Job Type	Description
Gimmal Retention Job	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.  Edit Job Schedule Retention ● Minutes ○ Hourly ○ Daily ○ Weekly ○ Monthly ○ Monthly by Day Every 10 minute(s) □ Disabled □ Discard check-outs when deleting documents *Discard Check-outs When Deleting Documents* 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.

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.

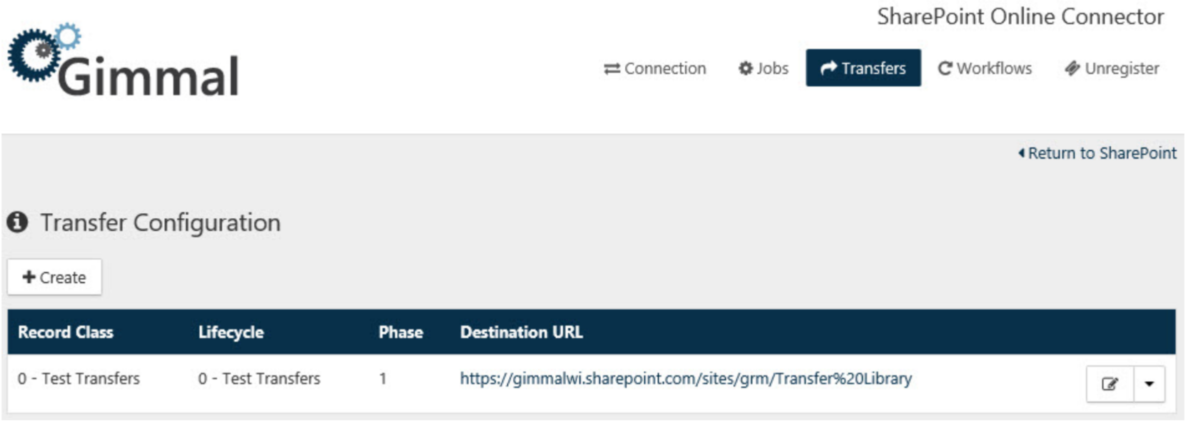
Job	Schedule
Gimmal Full Classification Job	Monthly
Gimmal Incremental Classification Job	Every 5 Minutes

Job	Schedule
Gimmal Retention Job	Every 5 Minutes

Transfer

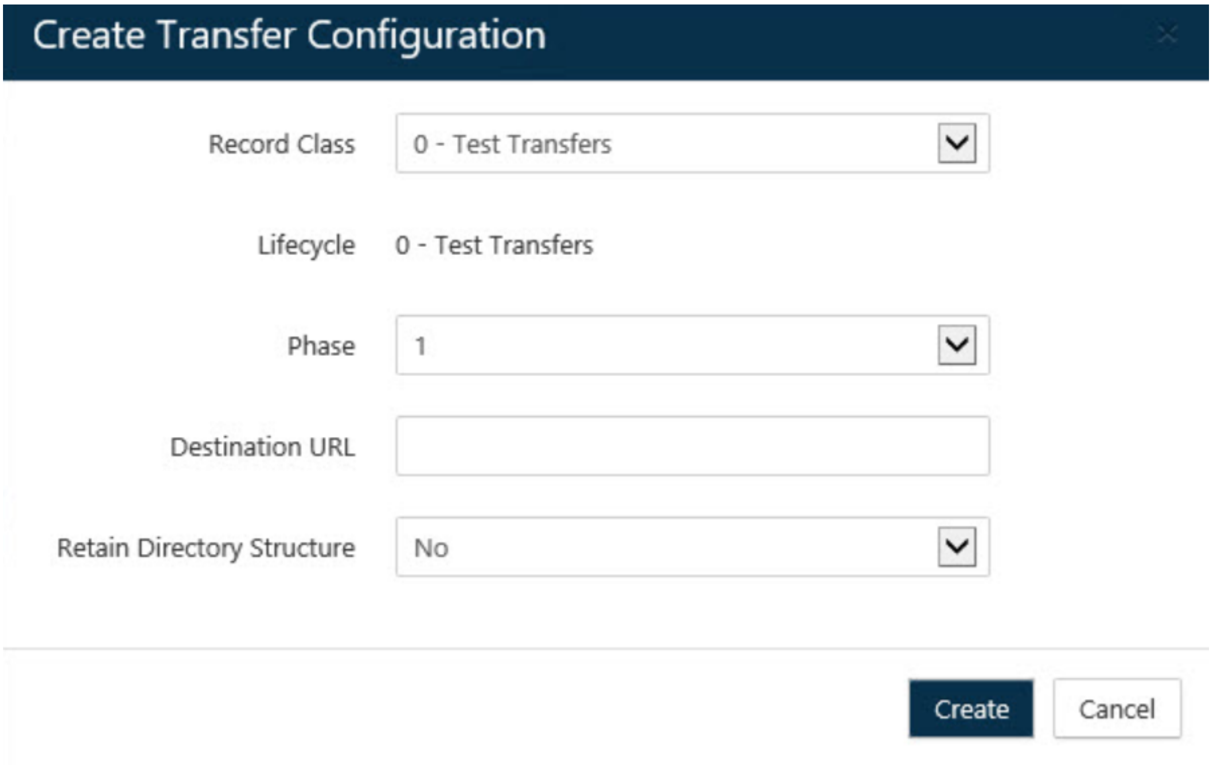
When a lifecycle in Records Management contains a Transfer Action, the SharePoint Online Connector requires that an Administrator configure the repository-specific destination of the transfer for items contained within the repository. This tells the Connector where to put the files when it sees that 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.
2. Click **Transfers**



Record Class	Lifecycle	Phase	Destination URL
0 - Test Transfers	0 - Test Transfers	1	https://gimmalwi.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: 0 - Test Transfers

Lifecycle: 0 - Test Transfers

Phase: 1

Destination URL:

Retain Directory Structure: No

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**

ⓘ 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.

Workflow

ⓘ Workflow Actions are not supported in SharePoint Online. They are supported in SharePoint on-premises only.

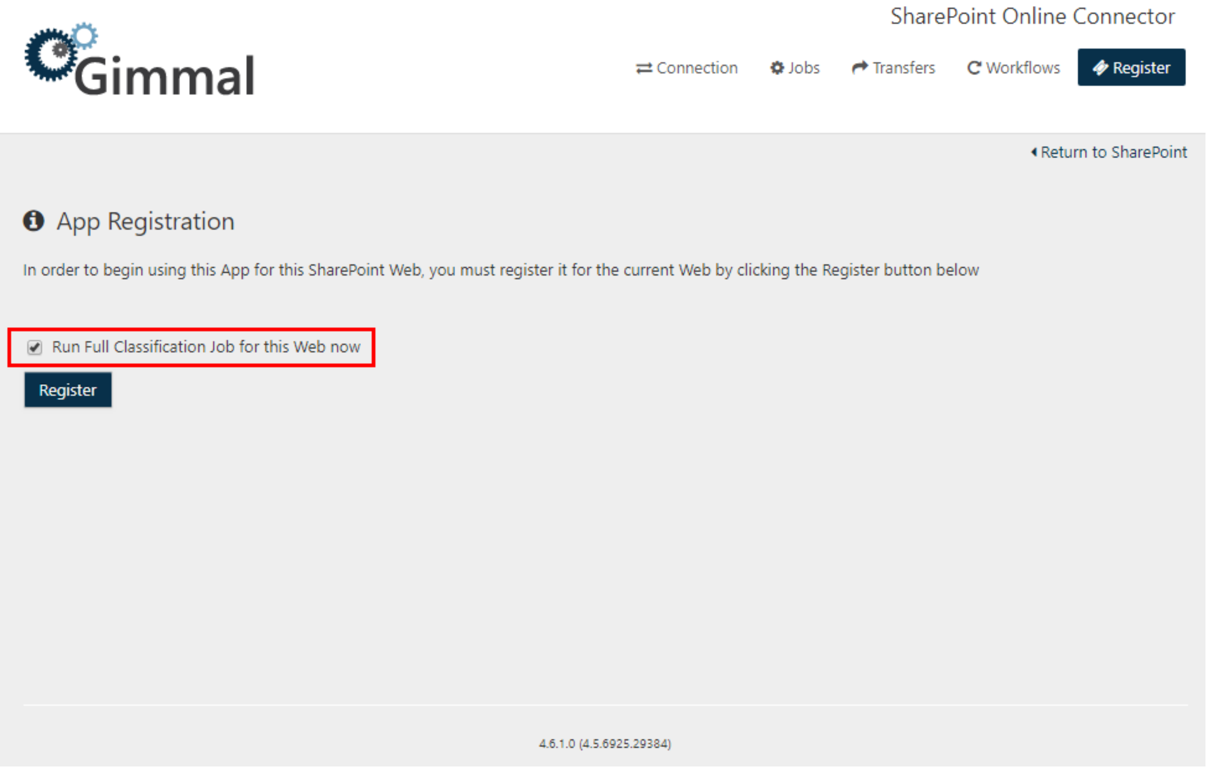
Register

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.



App Registration

In order to begin using this App for this SharePoint Web, you must register it for the current Web by clicking the Register button below

☑ Run Full Classification Job for this Web now

> ⓘ If you need to unregister a Web (Site), follow the directions on the topic Unregistering a SharePoint App from an Individual Web(see page 363).

7.10.12.6 Renewing a Client Secret

Microsoft provides documentation for replacing an expiring or expired client secret in a SharePoint Add-ins[100], 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[101] since this entire process is controlled by Microsoft and Gimmal 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 Gimmal Cloud versions of the SharePoint Online Connector.

[100] https://docs.microsoft.com/en-us/sharepoint/dev/sp-add-ins/replace-an-expiring-client-secret-in-a-sharepoint-add-in
[101] https://docs.microsoft.com/en-us/sharepoint/dev/sp-add-ins/replace-an-expiring-client-secret-in-a-sharepoint-add-in

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
```

Gimmal Cloud

To renew a client secret for SharePoint Online Connector in the Gimmal 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[102] 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 Gimmal Support ticket[103], providing the Client Secret value that you generated in step 1. (Gimmal 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 Gimmal Extend Client Secret Script, see the following Knowledge Base article[104] located at the Gimmal Support site.

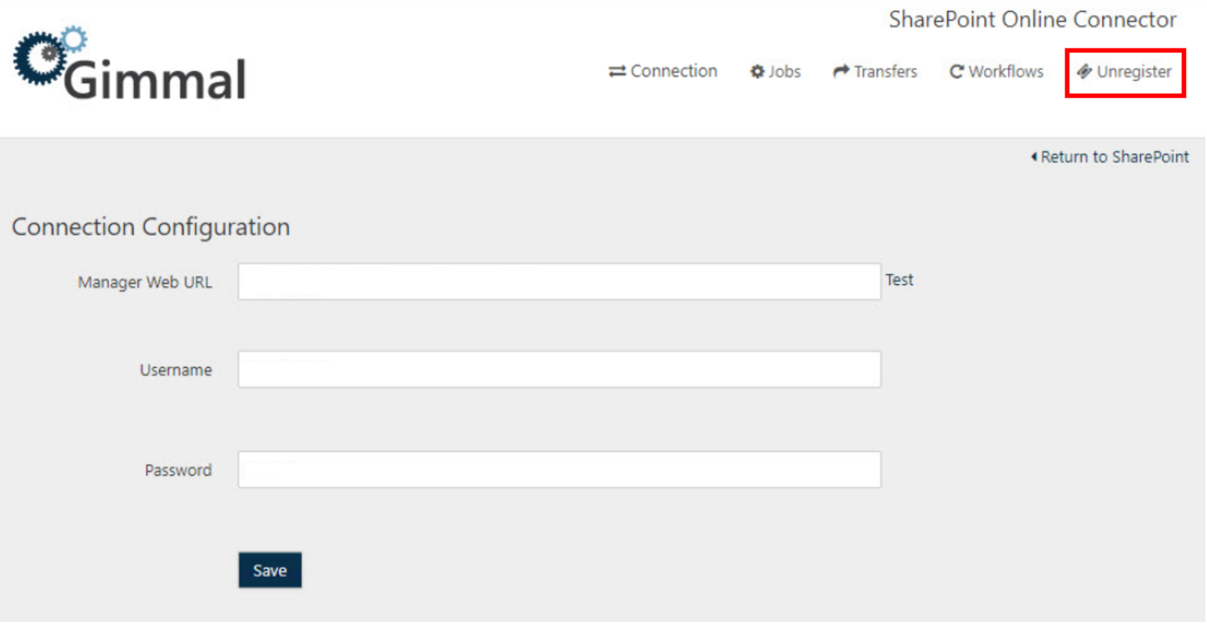
7.10.12.7 Unregistering a SharePoint App from an Individual Web

If you plan on removing a SharePoint app from an individual Web, Gimmal 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.

[102] https://docs.microsoft.com/en-us/sharepoint/dev/sp-add-ins/replace-an-expiring-client-secret-in-a-sharepoint-add-in
[103] https://support.gimmal.com/hc/en-us
[104] https://support.gimmal.com/hc/en-us/articles/360022551712-Extending-Expired-Client-Secret-for-SharePoint-Online-Add-Ins



Connection Configuration

Manager Web URL Test

Username

Password

2. Click **Unregister**. The app is now unregistered from the Web

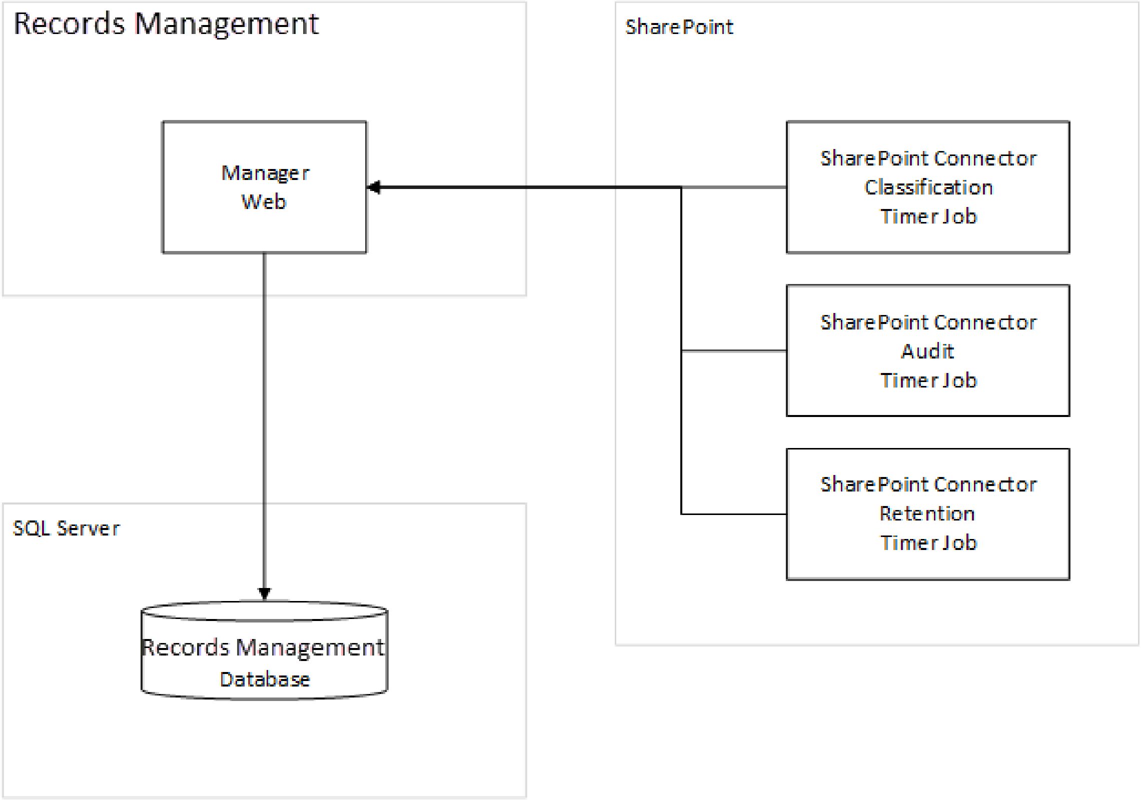
7.10.13 SharePoint Server Connector

The SharePoint Connector enables Records Management to manage the lifecycle of documents stored in on-premise SharePoint 2010, SharePoint 2013 and SharePoint 2016.

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.

7.10.13.1 Architecture


Records Management
Manager Web
SharePoint
SharePoint Connector Classification Timer Job
SharePoint Connector Audit Timer Job
SharePoint Connector Retention Timer Job
SQL Server
Records Management Database

7.10.13.2 Scalability

What comprises the solution...	• .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...	• Multiple instances of SharePoint can be load balanced • Will scale in accordance with the scaling of the SharePoint farm
When to scale...	• Scale SharePoint farm according to Microsoft Recommended Guidelines and your unique environment needs
General Sizing Guidelines...	• Follow Microsoft capacity planning guidelines for SharePoint https://technet.microsoft.com/en-us/library/ff758645(v=office.15).aspx

7.10.13.3 Additional Topics

SharePoint Server Connector Requirements

SharePoint Server Connector Installation

Configure SharePoint Server

SharePoint Server Connector Configuration

7.10.13.4 SharePoint Server Connector Requirements

Before you install the Records Management SharePoint Connector, verify that your system meets or exceeds the following requirements.

SharePoint

- SharePoint Server 2013 + .NET 4.8
- 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

7.10.13.5 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 2010, SharePoint 2013, or SharePoint 2016. The Connector also integrates with the SharePoint user interface to allow direct interaction with Records Management as though it were a part of SharePoint.

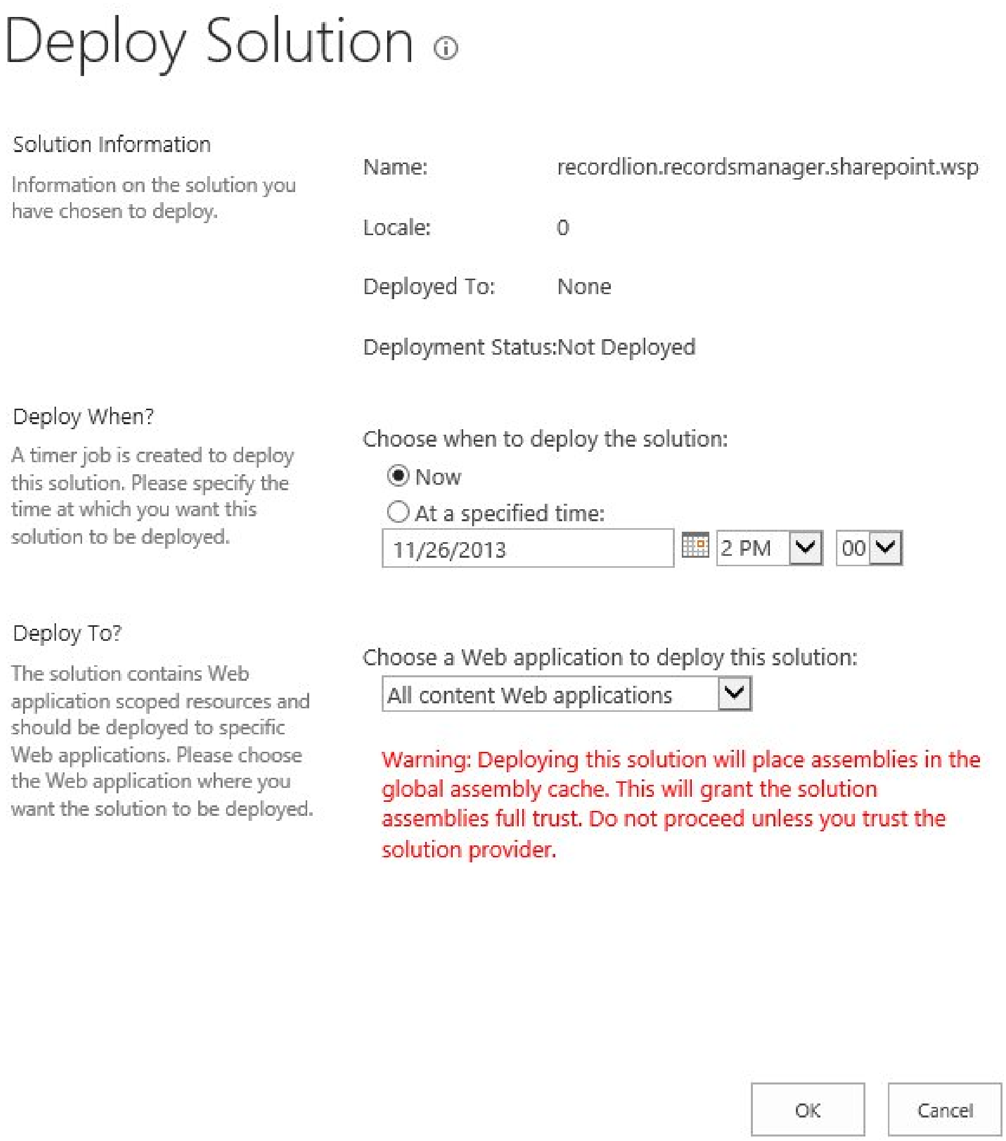
To install the SharePoint Connector, perform these steps:

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.

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.

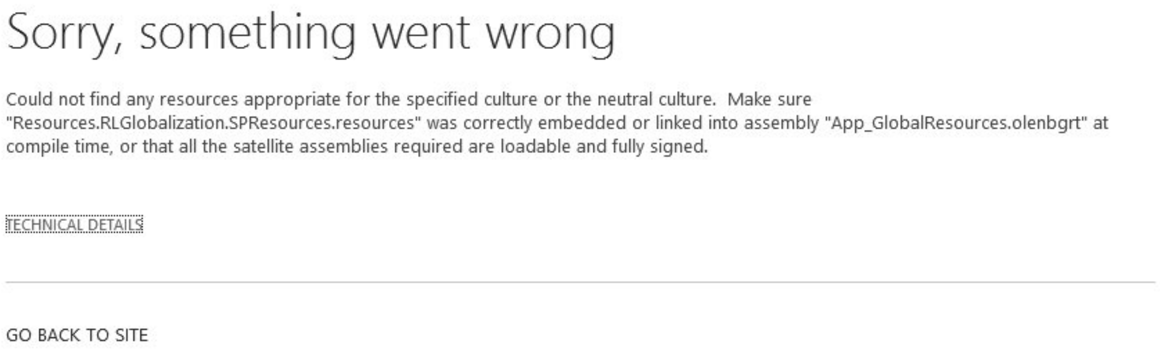
The **first workaround** is to grant the farm account membership to the local machine administrators group for each Central Administration or web front end server in the farm. This workaround is only necessary during the deployment phase of the installation. The **second workaround** requires the use 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.

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:

Configure SharePoint Server(see page 369)

SharePoint Server Connector Configuration(see page 373)

7.10.13.6 Configure SharePoint Server

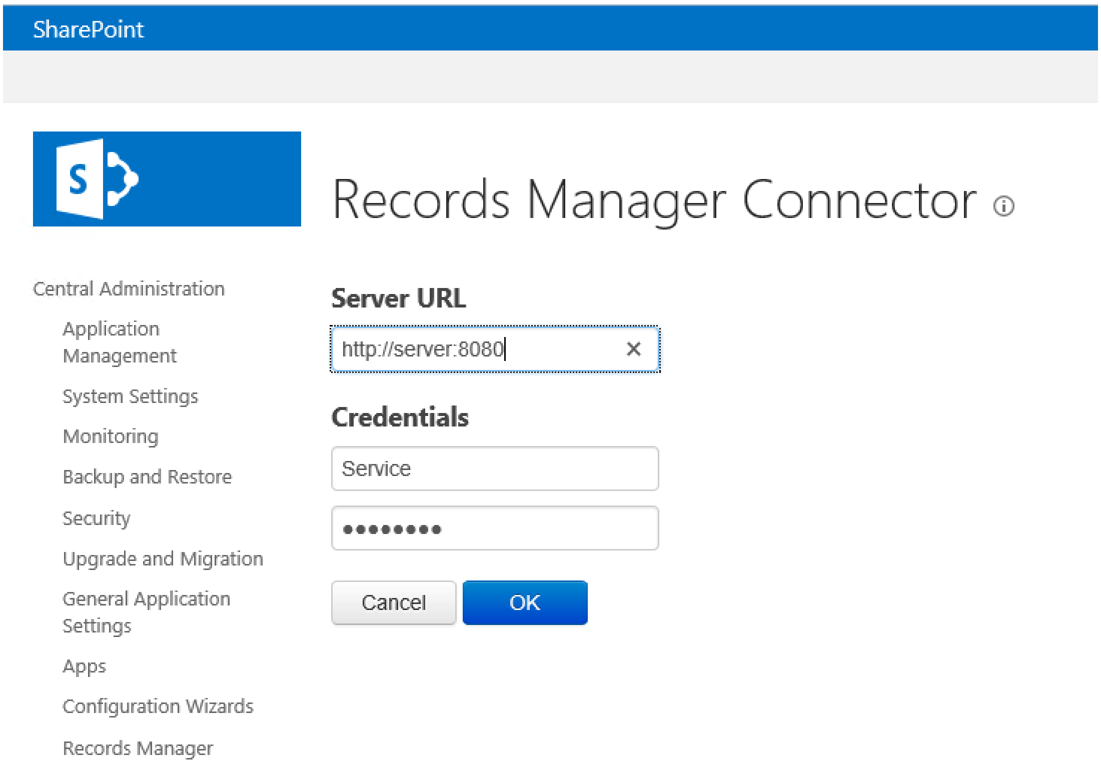
Configure for SharePoint 2010

⚠ This section is only for SharePoint 2010, skip this section if you are running SharePoint 2013 or later.

To finish installing the SharePoint Connector for SharePoint 2010, after the solution has been deployed, you must configure the SharePoint Connector to communicate with Records Management. To do this, perform the following steps:

1. Open **Central Administration**.
2. Navigate to **Central Administration** > **SharePoint Connector** > **Configure Connector**.
3. Enter the following information:
    - URL to Records Management (ex. https://server:8080)
    - Records Management Service Account (Service accounts are created in Records Management Core(see page 228))

- Password for Service Account



Records Manager Connector

Server URL

http://server:8080

Credentials

Service

••••••••

4. Click **OK**

Proceed to Enabling a Site Collection for Records Management to[105] configure the connector, and continue with the remaining topics in the Configuring section.

Configure for SharePoint 2013/2016

> ⚠ This section is only for SharePoint 2013 and later. Skip this section if you are running earlier versions of SharePoint.

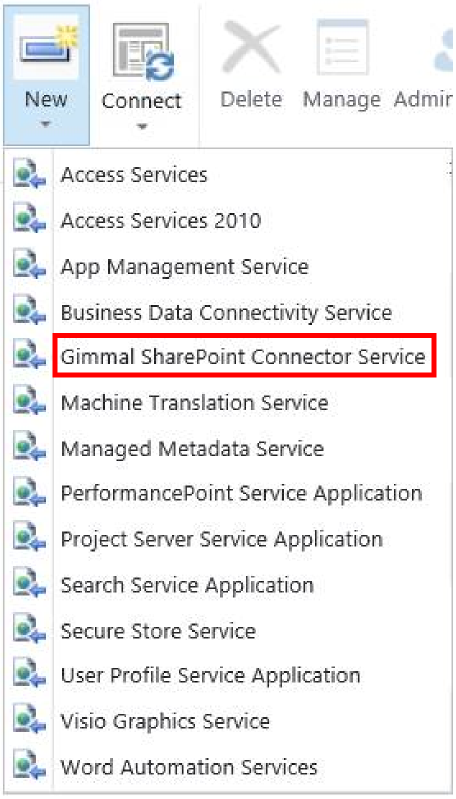
To finish installing the SharePoint Connector, you must perform the following steps:

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**.

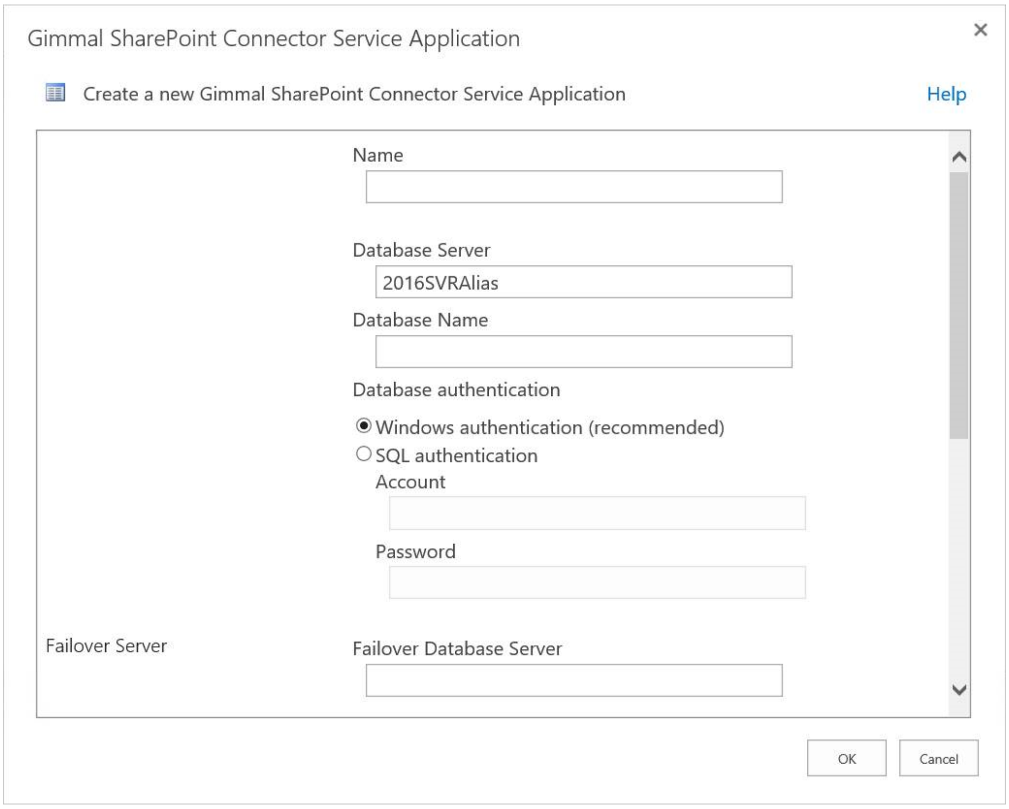
2. Next, you must create a Gimmal SharePoint Connector Service Application. To do this, perform the following steps:
   - **Open Central Administration**.

[105] http://docs.gimmal.com/en/14472-configure-sharepoint-connector.html

- Navigate to **Central Administration** > **Application Management** > **Manage Service Applications**.
- From the **New** option in the ribbon, choose **Gimmal SharePoint Connector Service**.


New
Connect
Delete
Manage
Admir
Access Services
Access Services 2010
App Management Service
Business Data Connectivity Service
Gimmal SharePoint Connector Service
Machine Translation Service
Managed Metadata Service
PerformancePoint Service Application
Project Server Service Application
Search Service Application
Secure Store Service
User Profile Service Application
Visio Graphics Service
Word Automation Services

- Provide the requested information to create the Service Application. (**Important!** A unique name is required for the **Database Name** setting.)



Gimmal SharePoint Connector Service Application

Create a new Gimmal SharePoint Connector Service Application

Name

Database Server: 2016SVRAlias

Database Name

Database authentication

● Windows authentication (recommended)

○ SQL authentication

Account

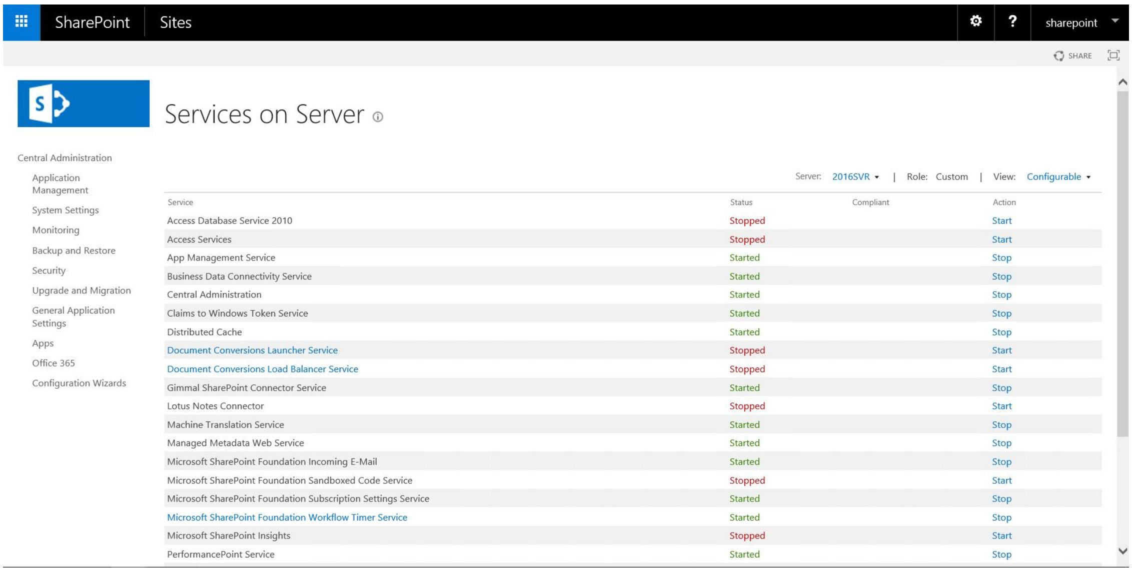
Password

Failover Server

Failover Database Server

- Click **OK**.

3. After you create the Gimmal SharePoint Connector Service Application, you must start the Gimmal SharePoint Connector Service on each SharePoint Server that should process Gimmal 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 Gimmal SharePoint Connector Service.



Services on Server

Server: 2016SVR | Role: Custom | View: Configurable

Service	Status	Compliant	Action
Access Database Service 2010	Stopped		Start
Access Services	Stopped		Start
App Management Service	Started		Stop
Business Data Connectivity Service	Started		Stop
Central Administration	Started		Stop
Claims to Windows Token Service	Started		Stop
Distributed Cache	Started		Stop
Document Conversions Launcher Service	Stopped		Start
Document Conversions Load Balancer Service	Stopped		Start
Gimmal SharePoint Connector Service	Started		Stop
Lotus Notes Connector	Stopped		Start
Machine Translation Service	Started		Stop
Managed Metadata Web Service	Started		Stop
Microsoft SharePoint Foundation Incoming E-Mail	Started		Stop
Microsoft SharePoint Foundation Sandboxed Code Service	Stopped		Start
Microsoft SharePoint Foundation Subscription Settings Service	Started		Stop
Microsoft SharePoint Foundation Workflow Timer Service	Started		Stop
Microsoft SharePoint Insights	Stopped		Start
PerformancePoint Service	Started		Stop

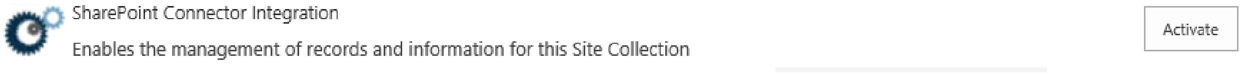
4. After starting the Gimmal SharePoint Connector Service, you must configure the Connector to communicate with Information Lifecycle. To do this, perform the following steps:
   - **Open Central Administration**.
   - Navigate to **Central Administration** > **Application Management** > **Manage Service 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 228))
     - Password for Service Account
   - Click **OK**.

7.10.13.7 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



SharePoint Connector Integration

Enables the management of records and information for this Site Collection

⚠ 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	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. 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. When enabling a new site for Records Management, at that time you will want to run the Full Classification Job.
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 Gimmal 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

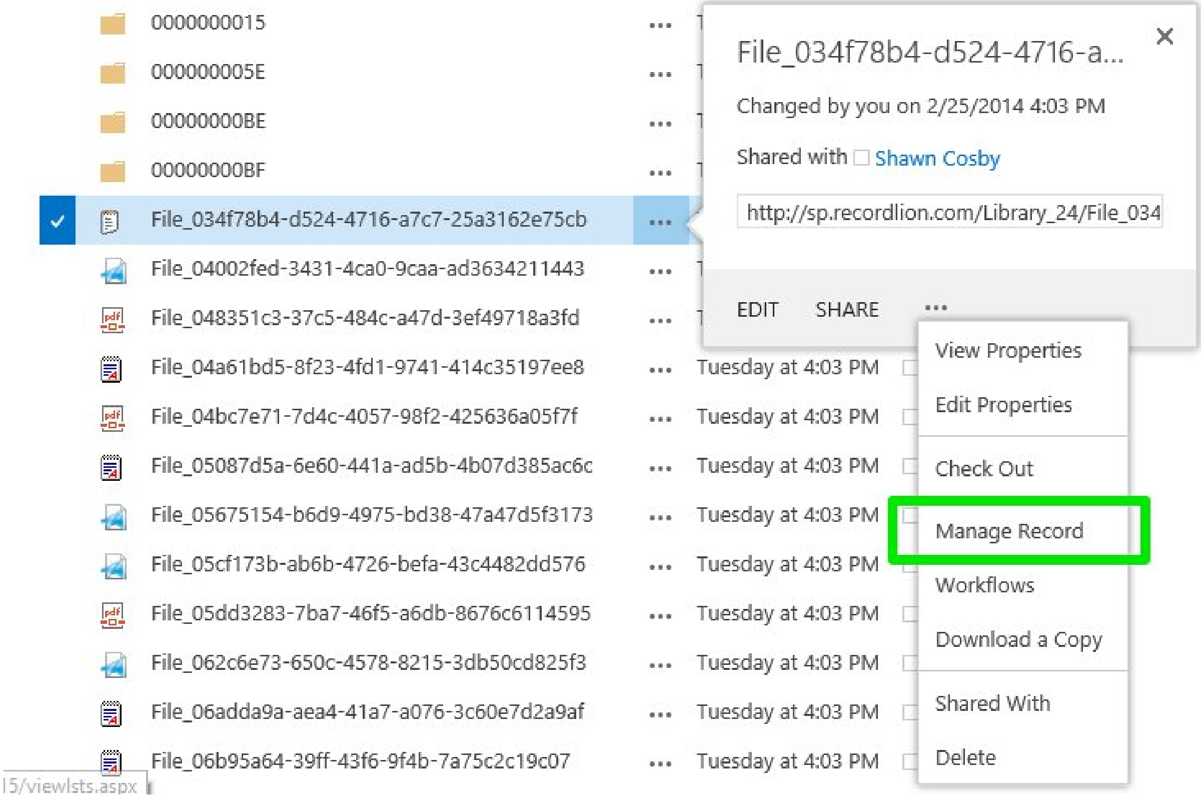
Enabling UI Integration with Records Management

> ⓘ 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.



0000000015	•••	T
000000005E	•••	T
00000000BE	•••	T
00000000BF	•••	T
File_034f78b4-d524-4716-a7c7-25a3162e75cb	•••	
File_04002fed-3431-4ca0-9caa-ad3634211443	•••	T
File_048351c3-37c5-484c-a47d-3ef49718a3fd	•••	T
File_04a61bd5-8f23-4fd1-9741-414c35197ee8	•••	Tuesday at 4:03 PM
File_04bc7e71-7d4c-4057-98f2-425636a05f7f	•••	Tuesday at 4:03 PM
File_05087d5a-6e60-441a-ad5b-4b07d385ac6c	•••	Tuesday at 4:03 PM
File_05675154-b6d9-4975-bd38-47a47d5f3173	•••	Tuesday at 4:03 PM
File_05cf173b-ab6b-4726-befa-43c4482dd576	•••	Tuesday at 4:03 PM
File_05dd3283-7ba7-46f5-a6db-8676c6114595	•••	Tuesday at 4:03 PM
File_062c6e73-650c-4578-8215-3db50cd825f3	•••	Tuesday at 4:03 PM
File_06adda9a-aea4-41a7-a076-3c60e7d2a9af	•••	Tuesday at 4:03 PM
File_06b95a64-39ff-43f6-9f4b-7a75c2c19c07	•••	Tuesday at 4:03 PM

File_034f78b4-d524-4716-a...

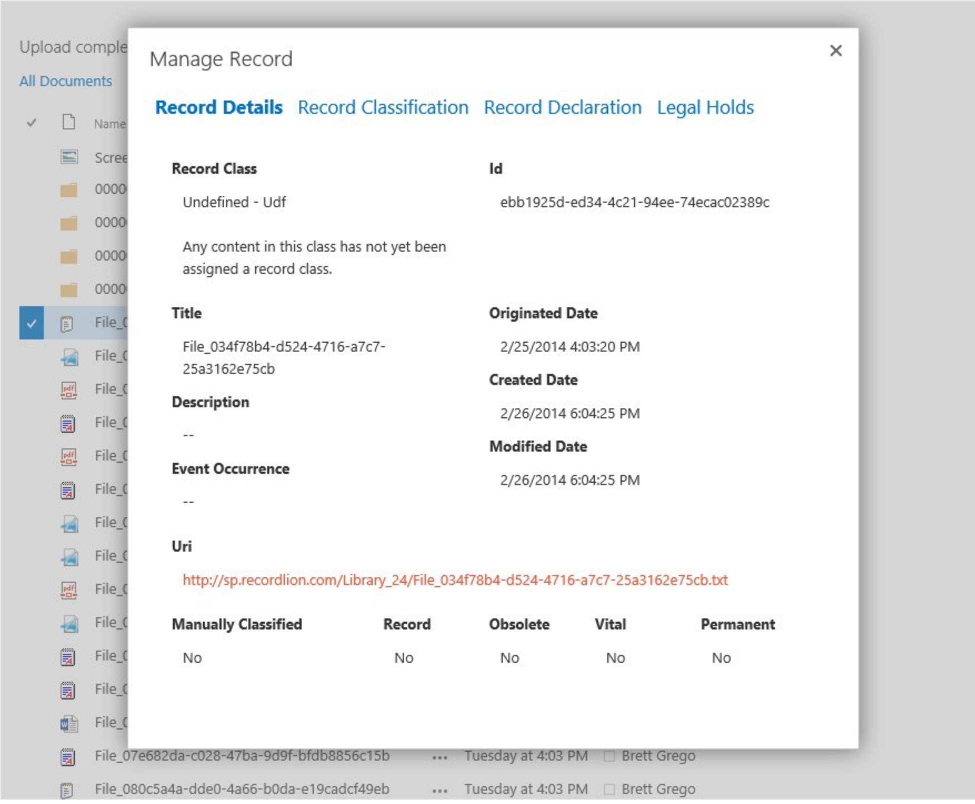
Changed by you on 2/25/2014 4:03 PM

Shared with □ Shawn Cosby

http://sp.recordlion.com/Library_24/File_034

l5/viewlsts.aspx

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.



Manage Record

Record Class

Undefined - Udf

Any content in this class has not yet been assigned a record class.

Id

ebb1925d-ed34-4c21-94ee-74ecac02389c

Title

File_034f78b4-d524-4716-a7c7-25a3162e75cb

Description

--

Event Occurrence

--

Originated Date

2/25/2014 4:03:20 PM

Created Date

2/26/2014 6:04:25 PM

Modified Date

2/26/2014 6:04:25 PM

Uri

http://sp.recordlion.com/Library_24/File_034f78b4-d524-4716-a7c7-25a3162e75cb.txt

Manually Classified	Record	Obsolete	Vital	Permanent
No	No	No	No	No

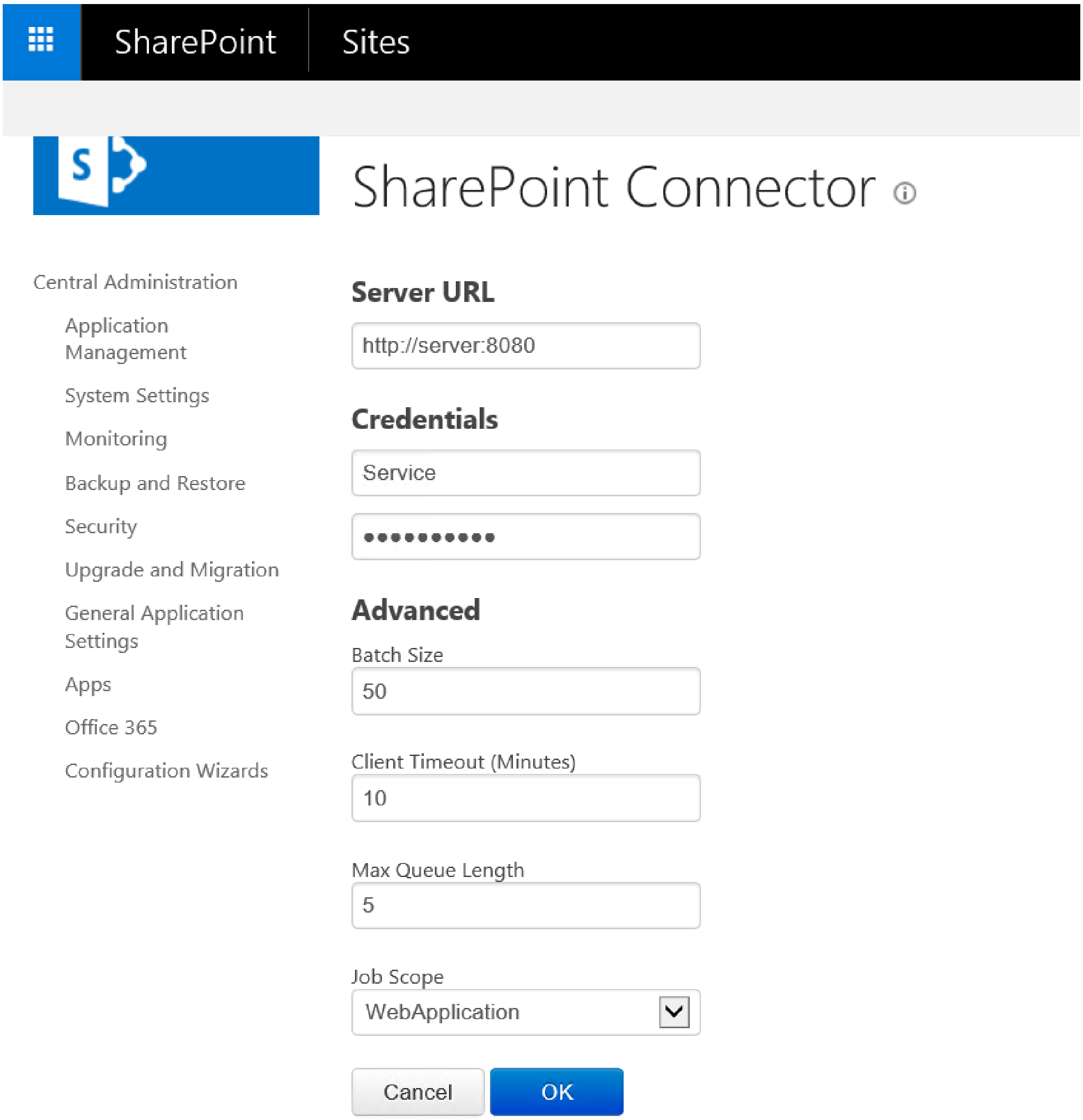
File_07e682da-c028-47ba-9d9f-bfdb8856c15b ··· Tuesday at 4:03 PM □ Brett Grego

File_080c5a4a-dde0-4a66-b0da-e19cadcf49eb ··· Tuesday at 4:03 PM □ Brett Grego

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.
- For **SharePoint 2010:** Select **Gimmal Records Management** from the Main Menu. For **SharePoint 2013/2016:** Go to **Manage Service Applications** > **Gimmal SharePoint Connector**.
- Select Configure Connection.



Server URL

http://server:8080

Credentials

Service

●●●●●●●●●●●

Advanced

Batch Size: 50

Client Timeout (Minutes): 10

Max Queue Length: 5

Job Scope: WebApplication

- Enter the following information:
  - Server URL to Information Lifecycle Manager Web (ex. http://server:8080)
  - Username* for the Service Account[106] (Service Account is created in Records Management)
  - Password for the Service Account[107]
  - Batch Size
  - Client Timeout in minutes.
  - Max Queue Length
  - Job Scope
- Click OK. (Credentials will be validated.)

[106] http://docs.gimmal.com/en/3517-creating-a-service-account.html

[107] http://docs.gimmal.com/en/3517-creating-a-service-account.html

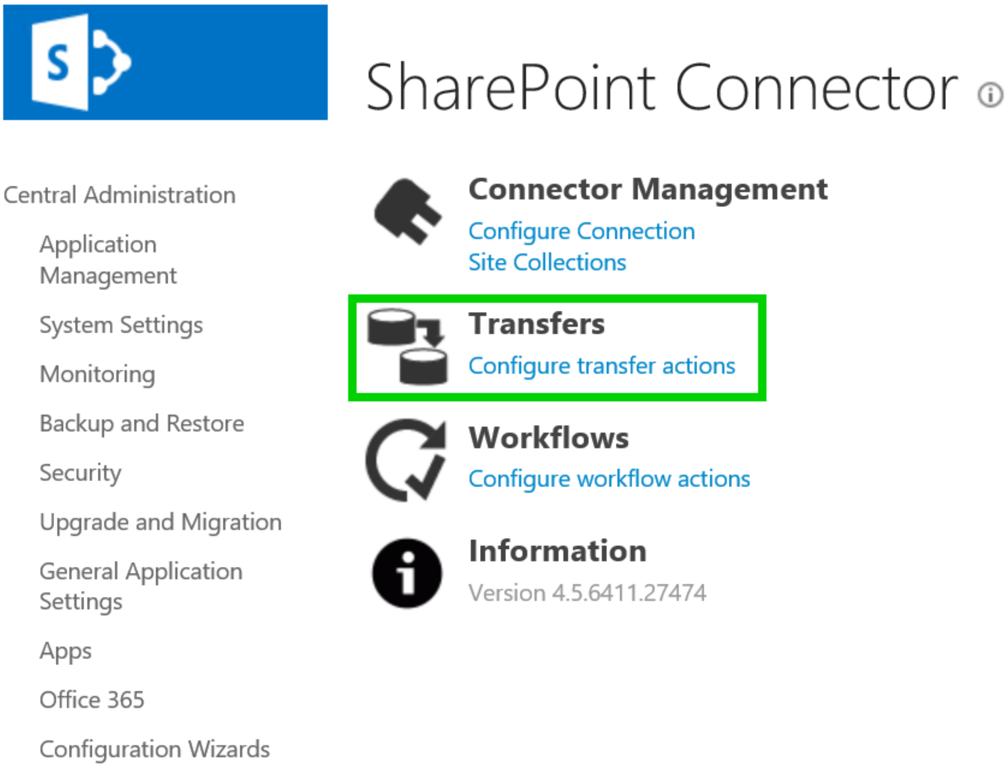
> ⓘ The Service Account username format depends on whether or not you are connecting to the Gimmal Cloud for Records Management. If the Gimmal Cloud is being used, the username format is: {service account name}@{tenant domain} (e.g. spocservice@gimmal.com[108], or fscservice@companyname.com[109]), otherwise, 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:

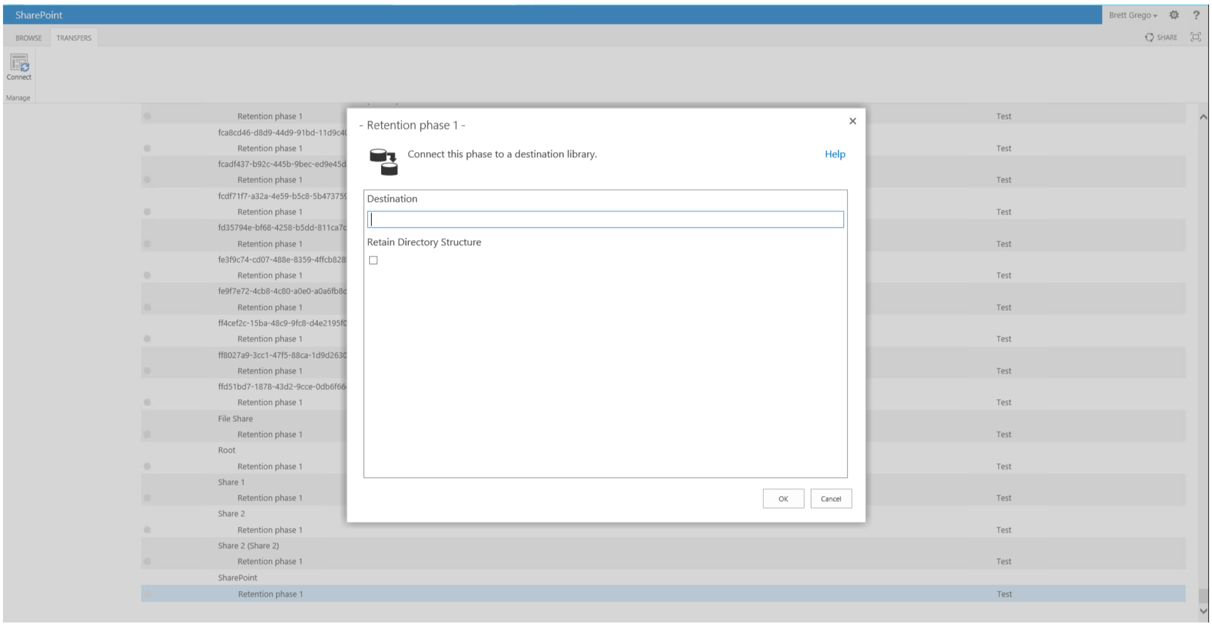
1. Open SharePoint Central Administration.
2. From the Application Management section, click **Manage Service Applications** > **Gimmal SharePoint Connector.**
3. On the SharePoint Connector page, click **Configure transfer actions** from the Transfers section.



4. Select the Retention Phase for the Record Class in which you would like to configure the transfer destination.

[108] mailto:spocservice@gimmal.com
[109] mailto:fscservice@companyname.com

5. Click **Connect** from the ribbon.



- Retention phase 1 -

Connect this phase to a destination library.

Destination

Retain Directory Structure

□

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.

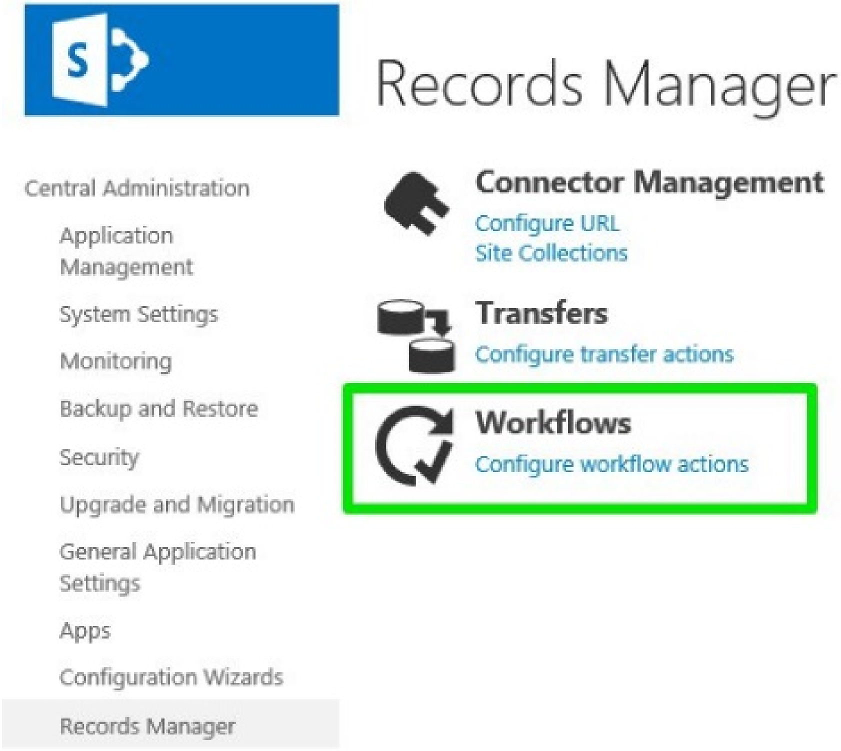
Configuring Workflow Actions

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.

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 **Gimmal Records Management** menu option.
3. Select **Configure Workflow Actions** from the Workflows section.



Records Manager

Central Administration

Application Management

System Settings

Monitoring

Backup and Restore

Security

Upgrade and Migration

General Application Settings

Apps

Configuration Wizards

Records Manager

Connector Management

Configure URL

Site Collections

Transfers

Configure transfer actions

Workflows

Configure workflow actions

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

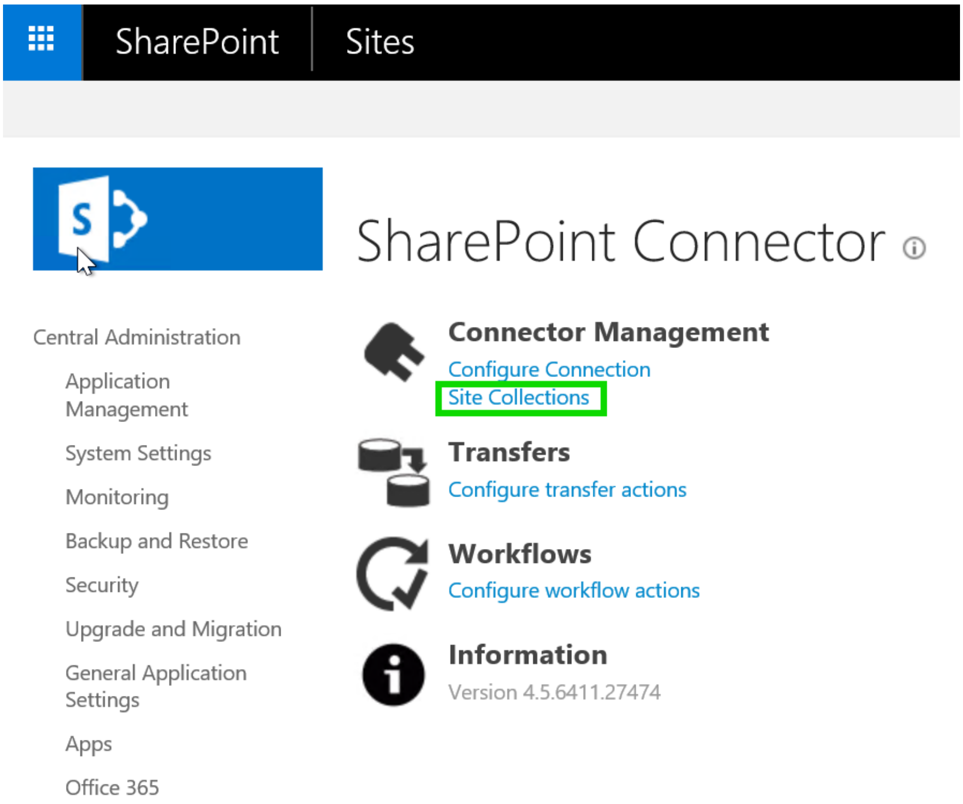
Configuring a New Site Collection

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.

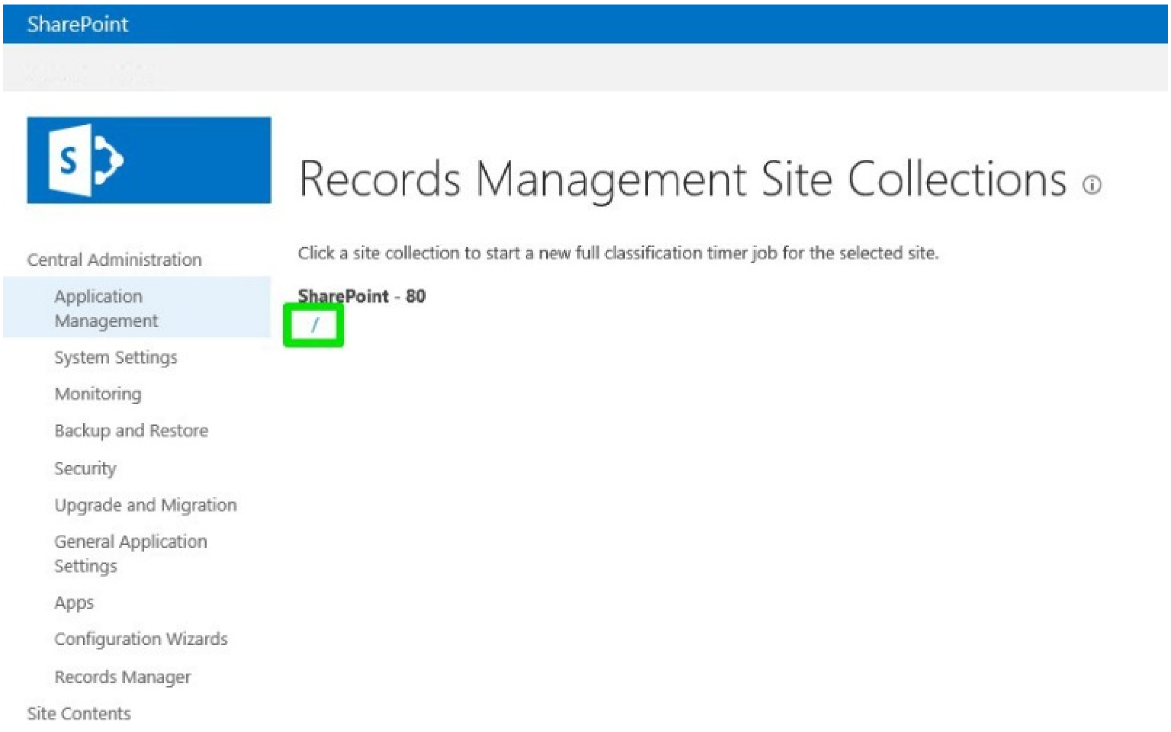
> ⓘ Manually running any of these timer jobs does not affect the run schedule already set.

To do a full crawl on a newly enabled site collection, perform the following steps:

1. Open SharePoint Central Administration.
2. For **SharePoint 2010:** Select **Gimmal Records Management** from Main Menu. For **SharePoint 2013/2016:** Go to **Manage Service Applications** > **Gimmal SharePoint Connector.**
3. Select Site Collections from the Connector Management section.



4. Click the Site Collection that you would like to submit to the full crawl.



Records Management Site Collections

Click a site collection to start a new full classification timer job for the selected site.

SharePoint - 80

/

Uninstall SharePoint Server Connector

To ensure a clean uninstall of the SharePoint Connector, perform the following steps depending on the version of SharePoint Server.

SharePoint 2010

1. Open **Central Administration**.
2. Navigate to **Central Administration** > **System Settings** > **Manage Farm Solutions**.
3. Click recordsmanager.sharepoint.wsp.
4. Select **Retract Solution** and click **OK.**
5. Click recordsmanager.sharepoint.wsp.
6. Select **Remove Solution** and click **OK.**
7. Open Services MMC.
8. Right-click **SharePoint Timer Service** and choose **Restart**.
9. Right-click **App Fabric Caching Service** and choose **Restart**.
10. Open a command prompt.
11. Execute command IIS Reset.
12. Open directory %windir%\assembly.
13. Delete any assemblies beginning with RecordLion.RecordsManager…"
14. Open directory %windir%\Microsoft.NET\assembly.
15. Delete any assemblies beginning with RecordLion.RecordsManager…”

SharePoint 2013 and above

1. Open SharePoint Management Shell.
2. Import the Gimmal SharePoint Connector PowerShell Module (see PowerShell Section).
3. Execute Remove-RecordsManagerServices to delete and unregister any Gimmal SharePoint Connector Service Applications.
4. Open **Central Administration**.
5. Navigate to **Central Administration** > **System Settings** > **Manage Farm Features**.
6. Deactivate the **Gimmal SharePoint Connector** feature.
7. Navigate to **Central Administration** > **System Settings** > **Manage Farm Solutions**.
8. Click recordsmanager.sharepoint.wsp.
9. Select **Retract Solution** and click **OK**.
10. Click recordsmanager.sharepoint.wsp.
11. Select **Remove Solution** and click **OK**.

For steps 12-21, please execute these steps on all SharePoint servers.

12. Open Services MMC

13. Right-click **SharePoint Timer Service** and choose **Restart**.

14. Right-click **App Fabric Caching Service** and choose **Restart**

15. Open a command prompt.

16. Execute command IIS Reset\

17. Open directory %windir%\assembly

18. Delete any assemblies beginning with RecordLion.RecordsManager…”

19. If the delete option was unavailable in step 18, remove the assemblies from the GAC by doing the following

a. Open a RUN command window and enter "C:\Windows\Assembly\GAC_MSIL"

b. Delete any assemblies here beginning with RecordLion.RecordsManager…”.

20. Open directory %windir%\Microsoft.NET\assembly

21. Delete any assemblies beginning with RecordLion.RecordsManager…”.

7.10.14 Universal File Share Connector

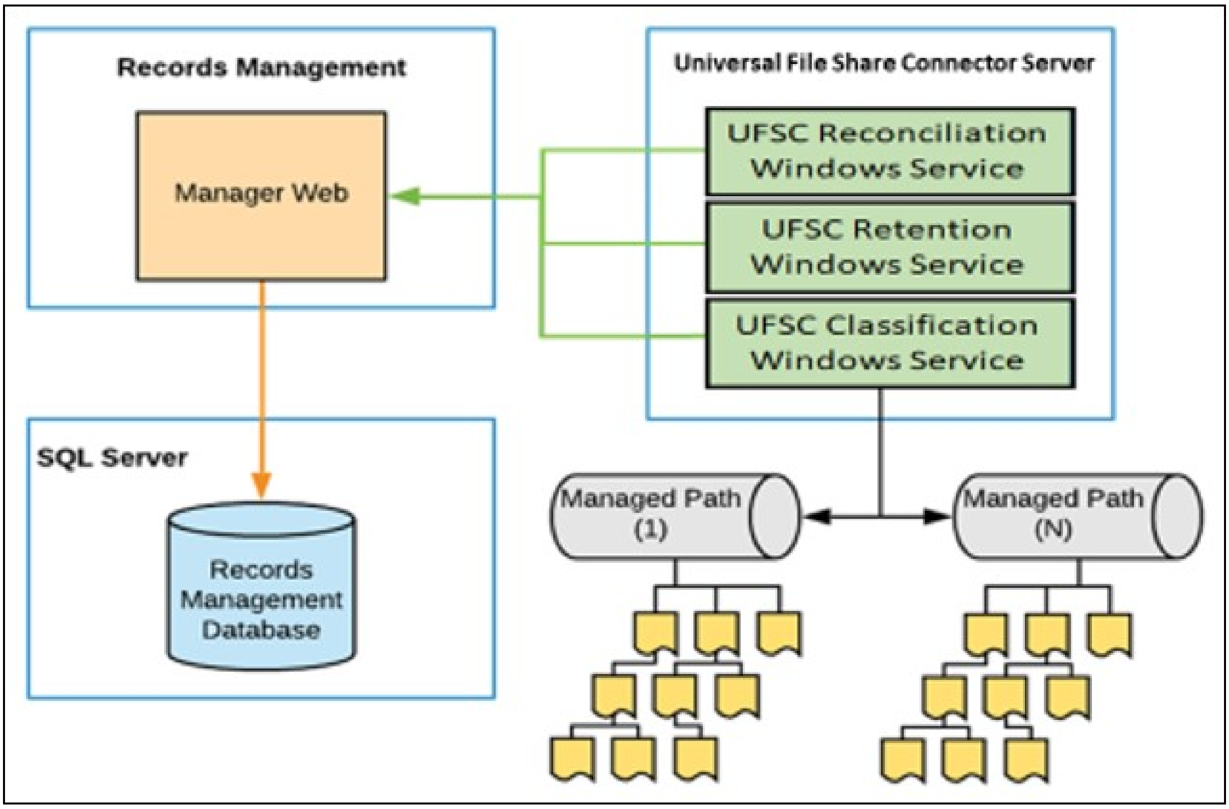
The Universal File Share Connector enables Records Management to manage the lifecycle of documents stored on network file shares.

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 Gimmal 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.

7.10.14.1 Universal File Share Connector Architecture


Records Management
Manager Web
SQL Server
Records Management Database
Universal File Share Connector Server
UFSC Reconciliation Windows Service
UFSC Retention Windows Service
UFSC Classification Windows Service
Managed Path (1)
Managed Path (N)

7.10.14.2 Scalability

What comprises the solution...	• .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
How scaling works...	• 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
When to scale...	• 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...	• (Total # Files / 10,000,000) = # Managed Paths • Ceiling(# Managed Paths / 10) = # Servers

7.10.14.3 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 Core 3.1
- 100 MB Disk Space for Software

Database Server

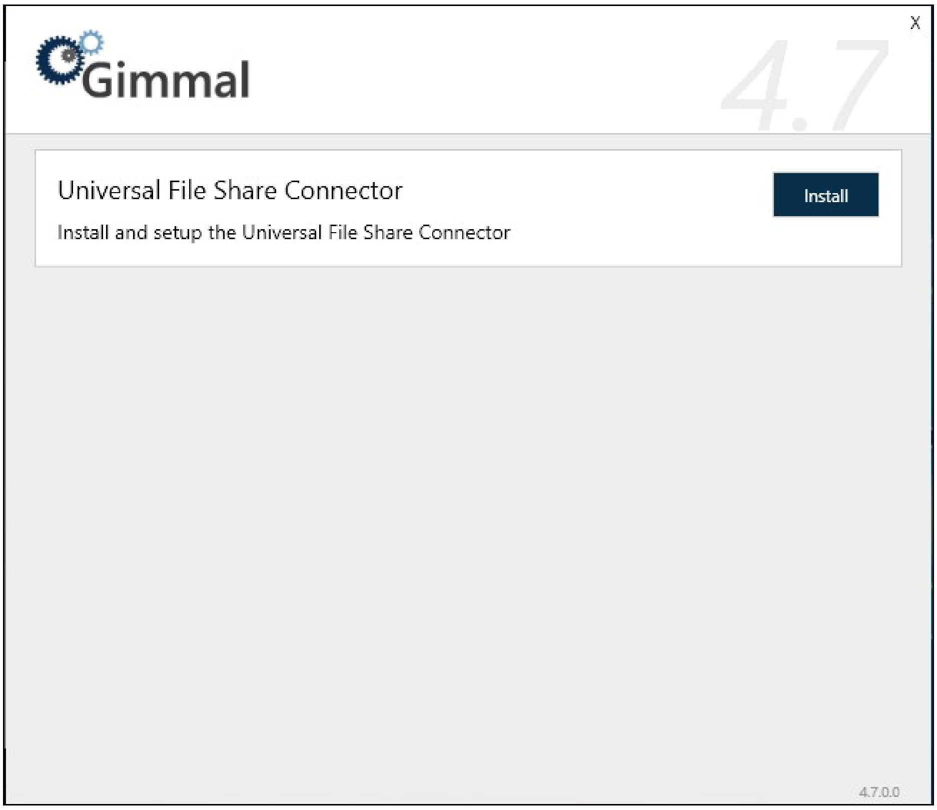
- SQL Server 2016 or greater
- 100 MB for File Share Connector Database

> ⓘ As a security best practice when using the .NET Framework, Gimmal 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[110] To verify that your operating system supports TLS 1.2, read the Support for TLS 1.2 section of Microsoft's documentation[111].

7.10.14.4 Universal File Share Connector Installation

Upon starting the Universal File Share Connector, the following screen displays:



Universal File Share Connector

Install and setup the Universal File Share Connector

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:

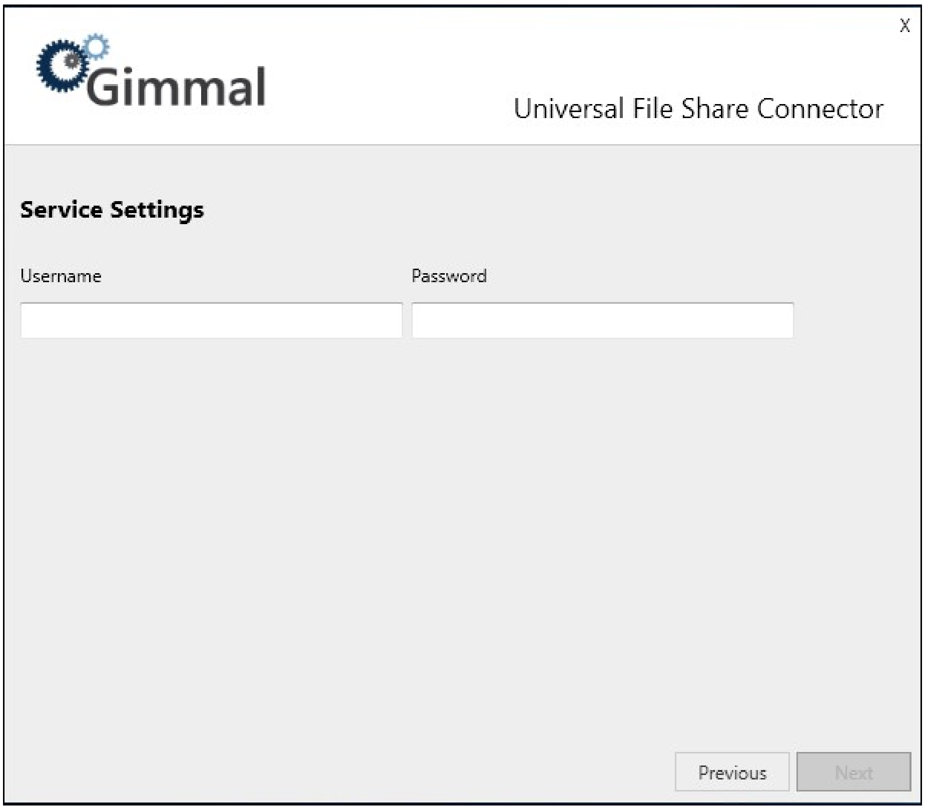
1. From the Records Management splash screen, click the **Install Universal File Share Connector** link. The Universal File Share Connector installation screen displays.
2. Click **Install** to the right of the Universal File Share Connector option. The first screen that displays is the check for prerequisites. This screen validates that .NET Core 3.1 is installed and the Current User is Local Administrator before allowing the installation to proceed.

   ⚠ The Universal File Share Connector requires that .NET Core Desktop Runtime 3.1 is installed.

[110] https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls#systemdefaulttlsversions
[111] https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls#support-for-tls-12

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 Core Desktop Runtime 3.1.

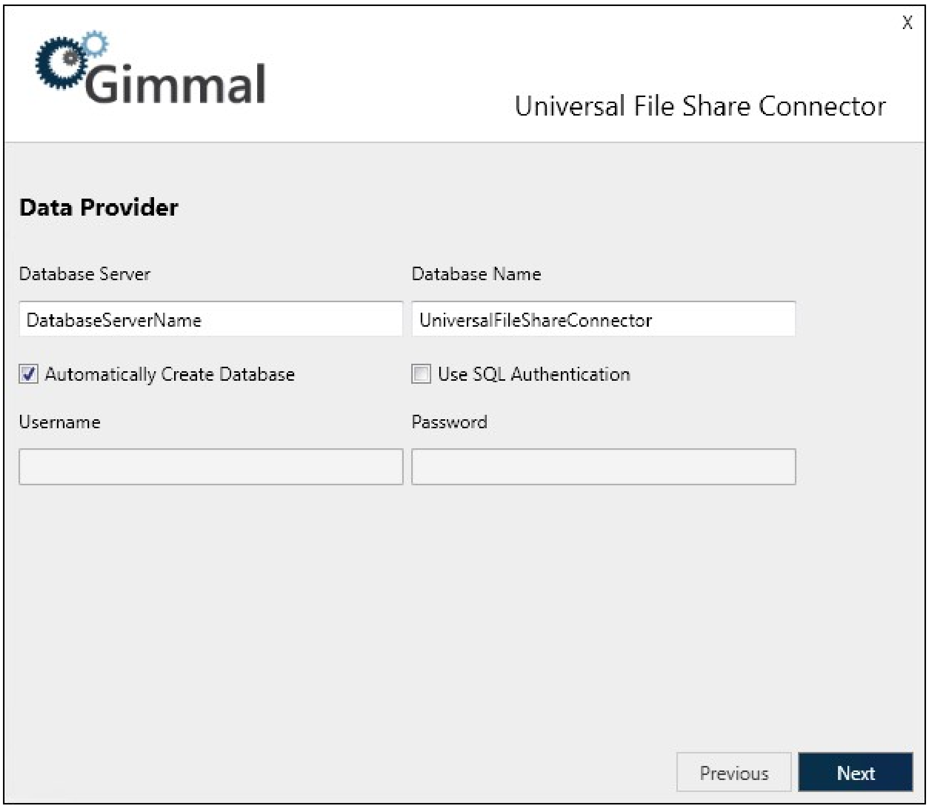
3. Click **Next**. The installation location screen displays, which determines where the connector will be installed.
4. Leave the installation path as the default, or to change it to the desired installation location, and click **Next**. The Service Settings screen displays, where you will configure the settings for the Universal File Share Connector Services.



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.



Data Provider

Database Server: DatabaseServerName

Database Name: UniversalFileShareConnector

☑ Automatically Create Database

□ Use SQL Authentication

Username:

Password:

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

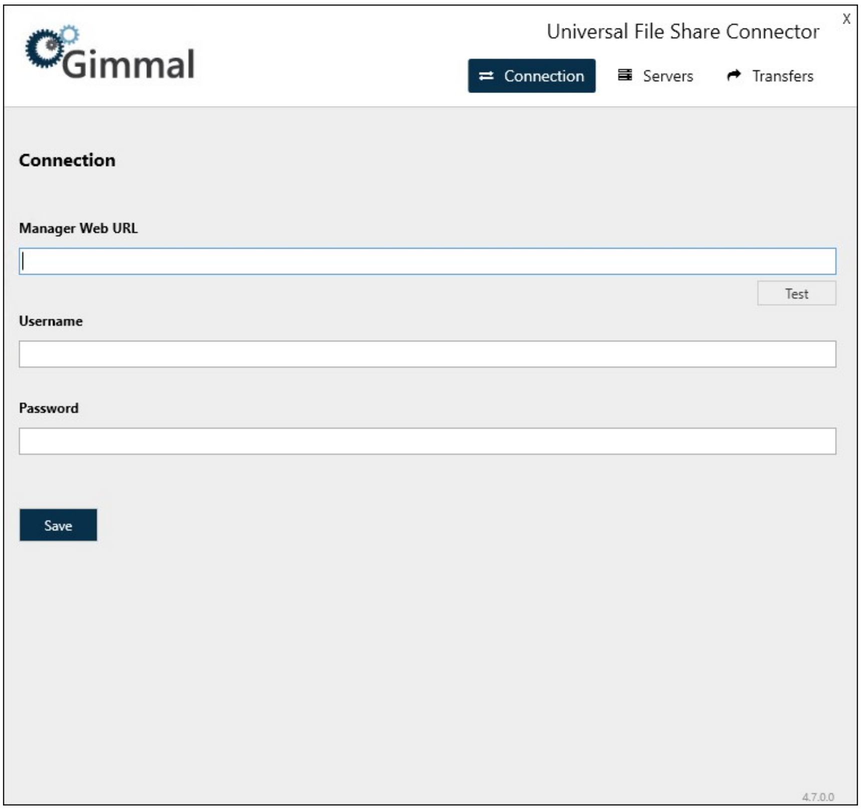
6. Click **Next** and then Finish to continue through the remaining screens and complete the installation.

7.10.14.5 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

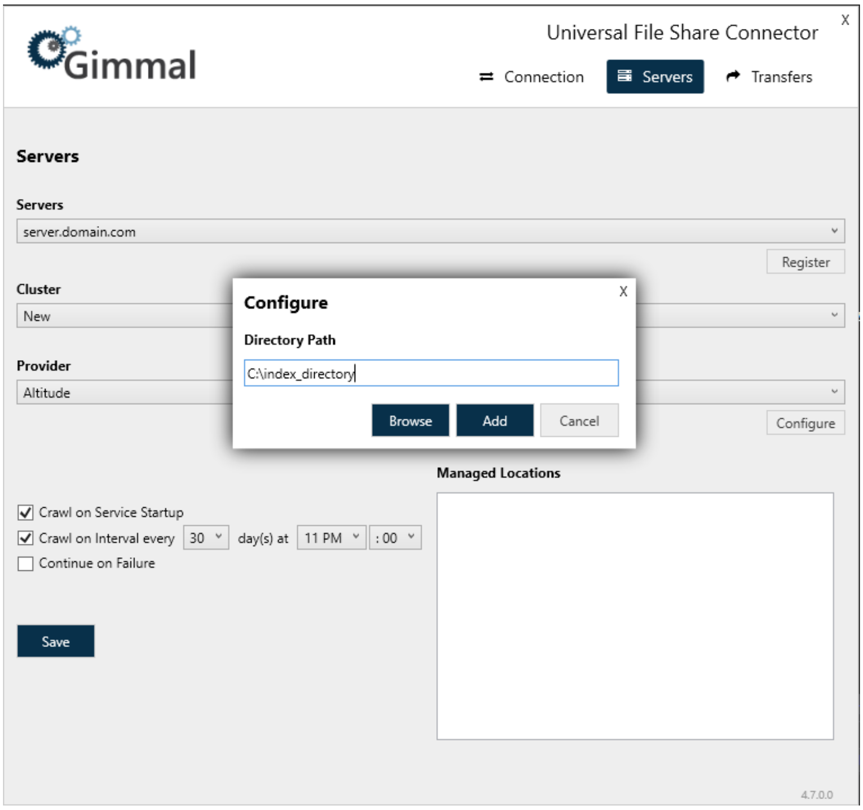


1. Enter the URL to the Records Management Manager Web.
2. Enter the Username* of the Universal File Share Connector Service Account created in Records Management Manager Web.
3. Enter the Password of the Universal File Share Connector Service Account created in Records Management Manager Web.

> ⚠ 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.com[112], or fscservice@companyname.com[113]), otherwise, the format is just: {service account name}.

[112] mailto:spocservice@gimmal.com
[113] mailto:fscservice@companyname.com

Servers



Servers

Servers: server.domain.com

Cluster: New

Provider: Altitude

Configure

Directory Path: C:\index_directory

Managed Locations

☑ Crawl on Service Startup

☑ Crawl on Interval every 30 day(s) at 11 PM :00

□ Continue on Failure

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 Gimmal Altitude Connector
If records are to be managed by Gimmal Records Management after they have been transferred, the index must be regenerated in Gimmal 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 Gimmal 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**
Gimmal 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.
Gimmal Universal File Share Reconciliation Service	This service is responsible for performing reconciliation actions for records in Records Management.

Gimmal 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.

ⓘ 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.

7.10.14.6 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.

7.11 Physical Records Management Deployment

7.11.1 Physical Records Management Configuration

7.11.2 Physical Records Management Configuration

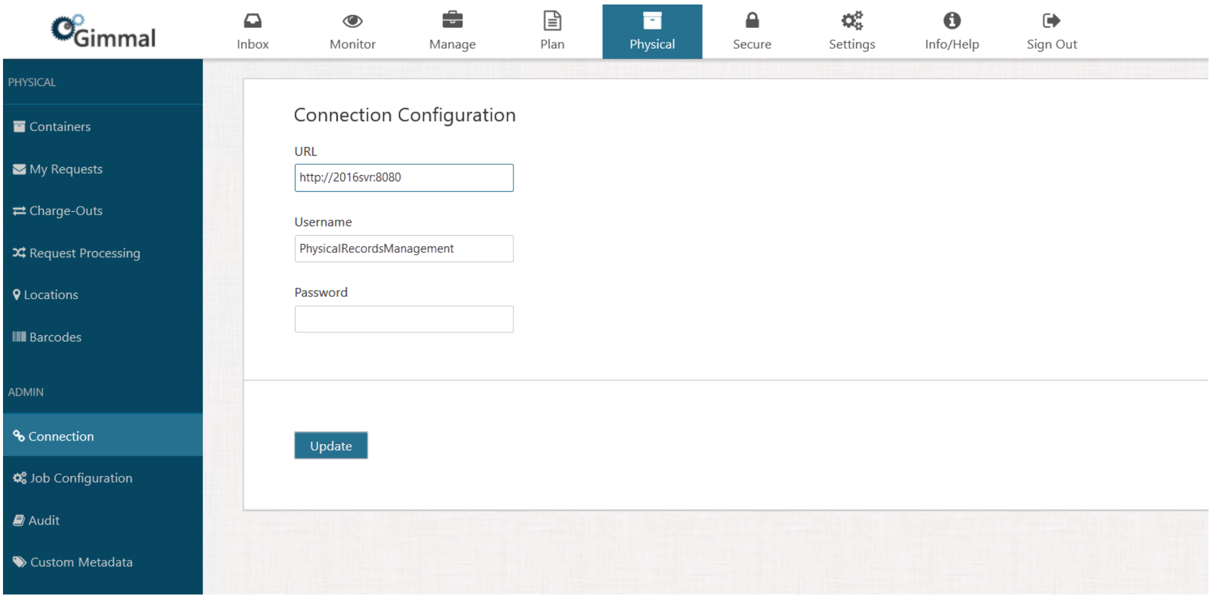
1. Log into Records Management Manager Web using your Master ("Administrator") account, and verify that the Physical Records Management Service Account has been created. (For more information, see Creating a Service Account[114].)

   ⚠ **Gimmal Cloud**

   If you are using Records Management on the Gimmal Cloud, you must create the Service Account (referenced in step 1 above) as a user with “System Admin” access. Then, configure the Physical Records Management Connection (see remaining steps) as a user with “Physical Administrator” access. (This may be the same user with both permissions.)

2. Click **Physical** on the Main Menu, and then click **Connection** on the left Navigation Menu. The Connection Configuration page displays.

[114] http://docs.gimmal.com/en/3517-creating-a-service-account.html



Connection Configuration

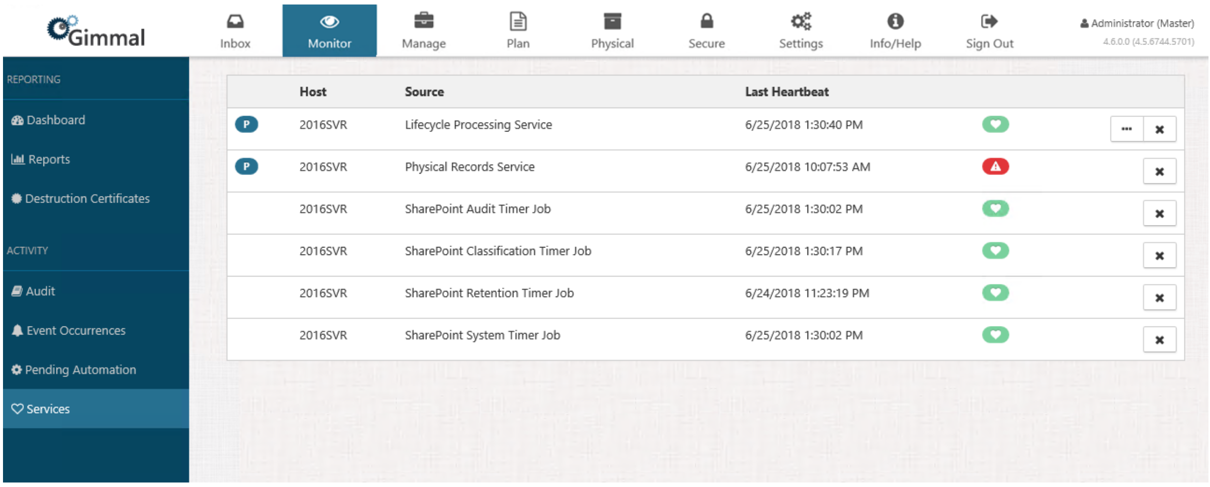
URL
http://2016svr:8080

Username
PhysicalRecordsManagement

Password

Update

3. Enter the connection URL
4. Enter the Service Account [115]**Username** and the Service Account **Password**.
5. Click **Update**. (This button will display **Save** if this is the first time configuring the connection)
6. Start the **Gimmal 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		
P	2016SVR	Lifecycle Processing Service	6/25/2018 1:30:40 PM	♥	··· ✖
P	2016SVR	Physical Records Service	6/25/2018 10:07:53 AM	⚠	✖
	2016SVR	SharePoint Audit Timer Job	6/25/2018 1:30:02 PM	♥	✖
	2016SVR	SharePoint Classification Timer Job	6/25/2018 1:30:17 PM	♥	✖
	2016SVR	SharePoint Retention Timer Job	6/24/2018 11:23:19 PM	♥	✖
	2016SVR	SharePoint System Timer Job	6/25/2018 1:30:02 PM	♥	✖

⚠ **Existing Gimmal 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

[115] http://docs.gimmal.com/en/3515-account-types---permission-oververview.html

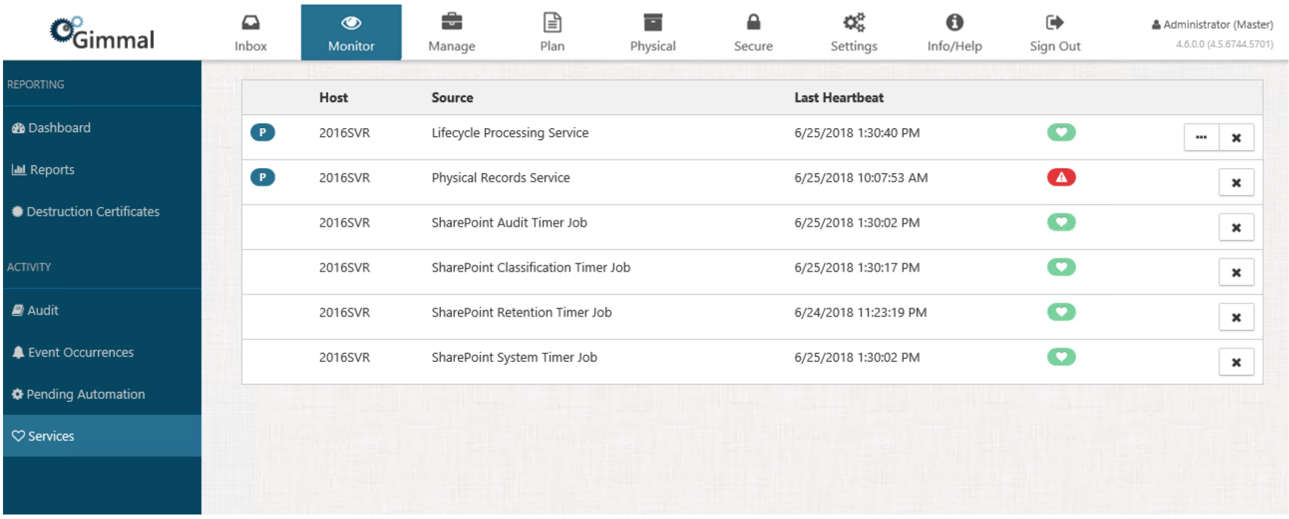
New Gimmal Cloud service customers (post-Feb. 27th, 2021) should use the new URLs.

- US Test - https://records.gimmal.build
- US Production - https://records.gimmal.cloud
- UK Test - https://records.uk.gimmal.build
- UK Production - https://records.uk.gimmal.cloud
- CAN Production - https://records-ca.gimmal.cloud/

NOTE: Existing customers already using the existing URL should not change to the new URLs as this may cause issues.

7.12 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.



	Host	Source	Last Heartbeat		
P	2016SVR	Lifecycle Processing Service	6/25/2018 1:30:40 PM	♥	··· ✖
P	2016SVR	Physical Records Service	6/25/2018 10:07:53 AM	⚠	✖
	2016SVR	SharePoint Audit Timer Job	6/25/2018 1:30:02 PM	♥	✖
	2016SVR	SharePoint Classification Timer Job	6/25/2018 1:30:17 PM	♥	✖
	2016SVR	SharePoint Retention Timer Job	6/24/2018 11:23:19 PM	♥	✖
	2016SVR	SharePoint System Timer Job	6/25/2018 1:30:02 PM	♥	✖

7.12.1 Heartbeat Icon Legend

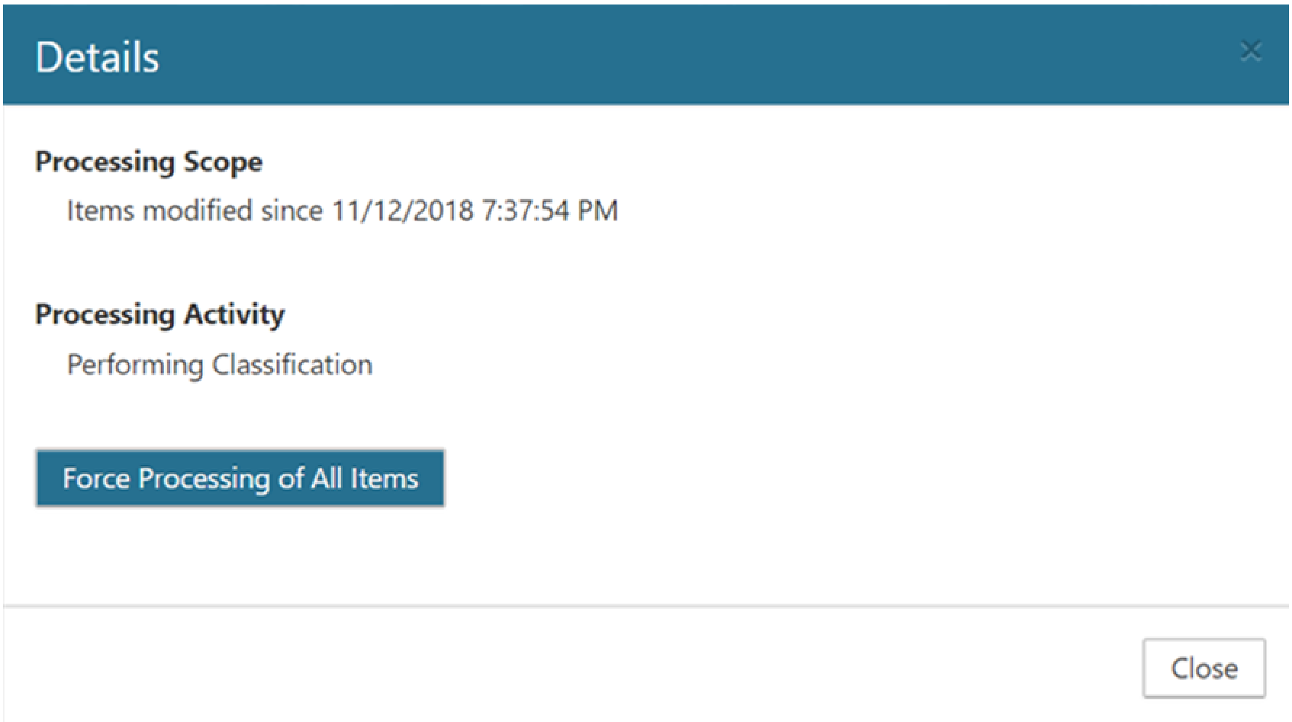
The heartbeat icon to the right of the **Last Heartbeat** column in the preceding screenshot indicates the status of each service. See the following legend for the time thresholds corresponding to service status and icon color:

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**.

Icon Color	Service Status
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**.

7.12.2 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

ⓘ *Do **NOT** click the **Force Processing of All Items** button on the Details dialog unless directed to do so by a member of Gimmal'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.

7.12.3 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.

7.13 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.

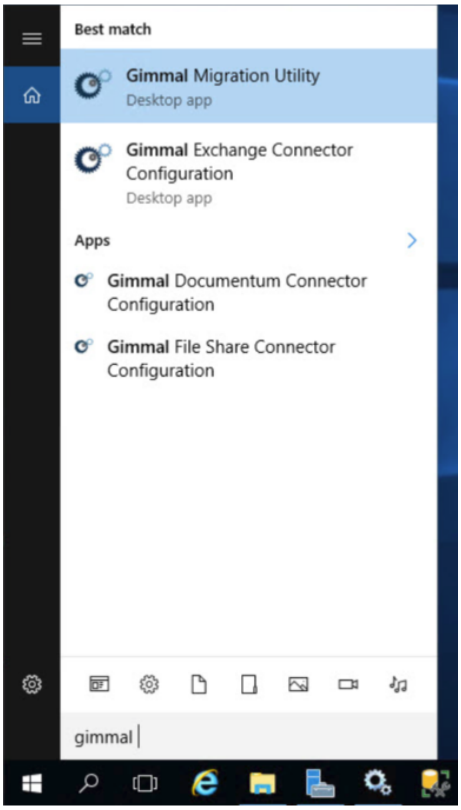
7.13.1 Running the Migration Utility

7.13.1.1 Open the Migration Utility

Open the Migration UtilityTo 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**.



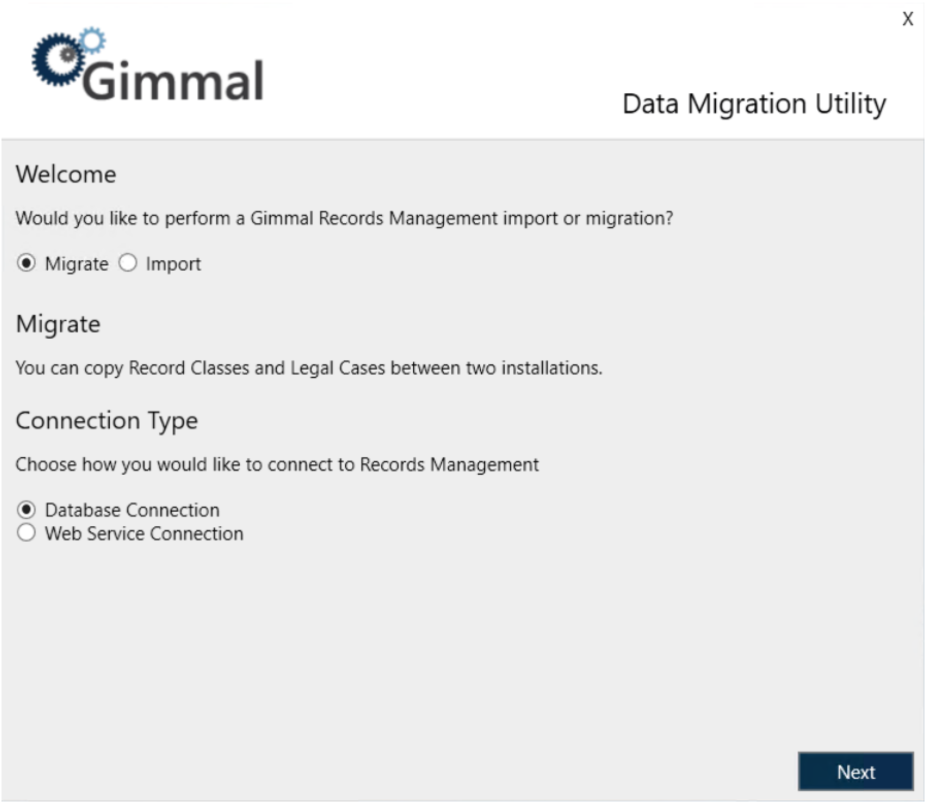
Best match
Gimmal Migration Utility
Desktop app
Gimmal Exchange Connector Configuration
Desktop app
Apps
Gimmal Documentum Connector Configuration
Gimmal File Share Connector Configuration
gimmal

7.13.1.2 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 407)
2. Import(see page 399)



Welcome

Would you like to perform a Gimmal 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

7.13.2 Import

Select **Import** from the Welcome screen, this section will guide you through the wizard.

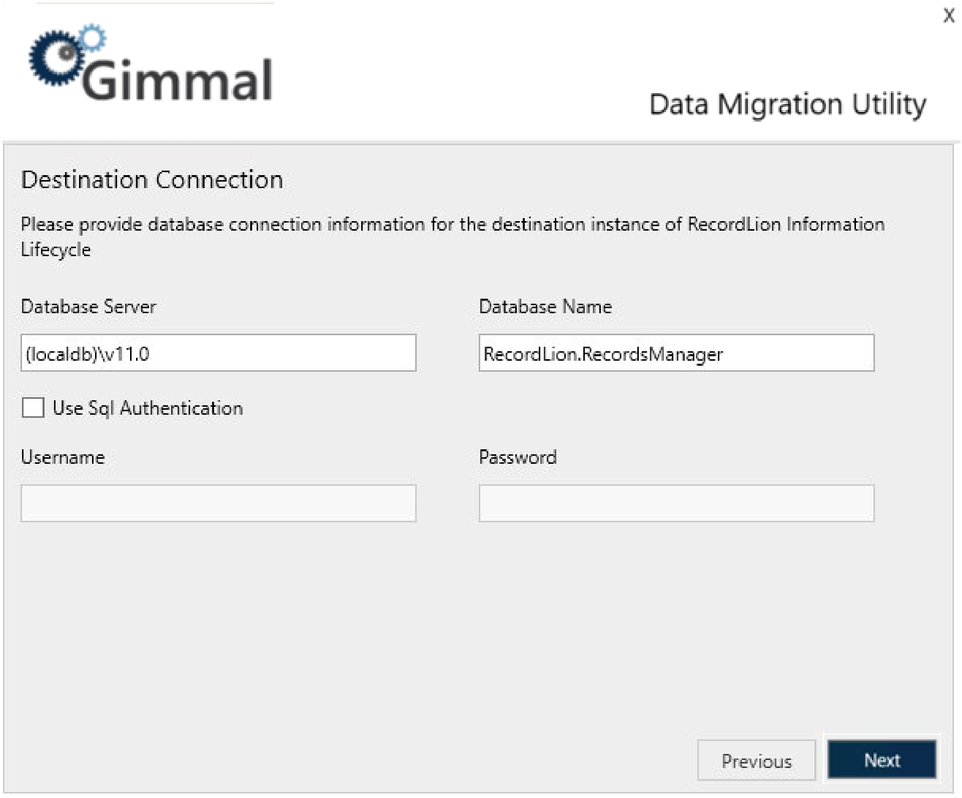
7.13.2.1 Import Configuration

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.

7.13.2.2 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

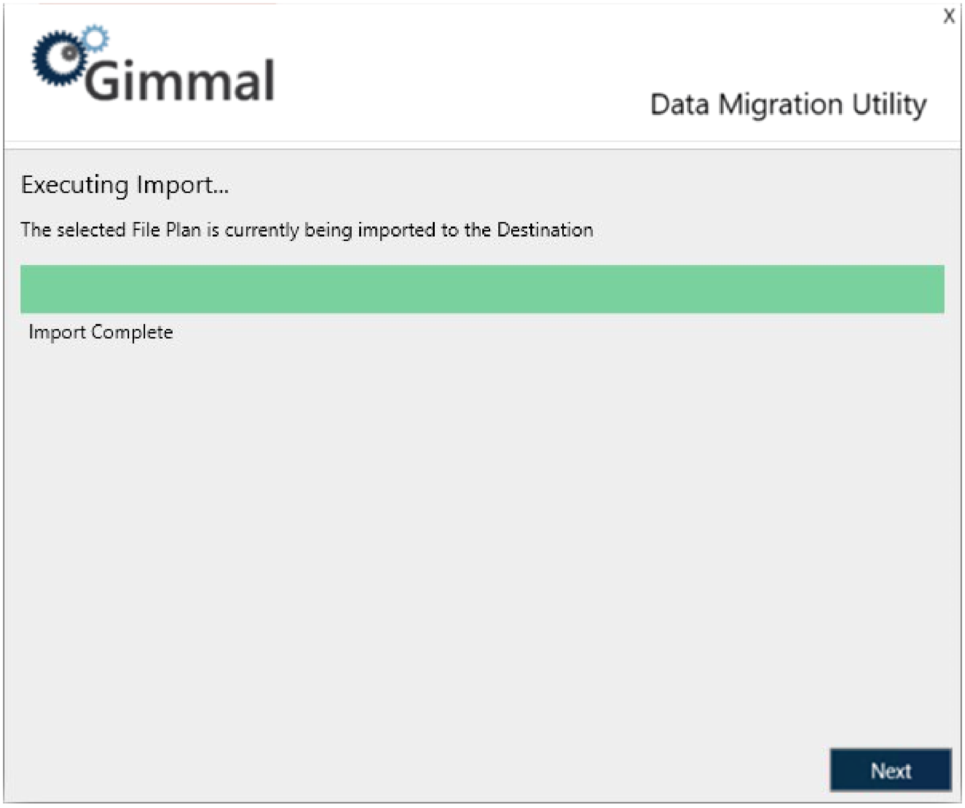
Username:

Password:

7.13.2.3 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.



Executing Import...

The selected File Plan is currently being imported to the Destination

Import Complete

7.13.2.4 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.gimmal.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
```

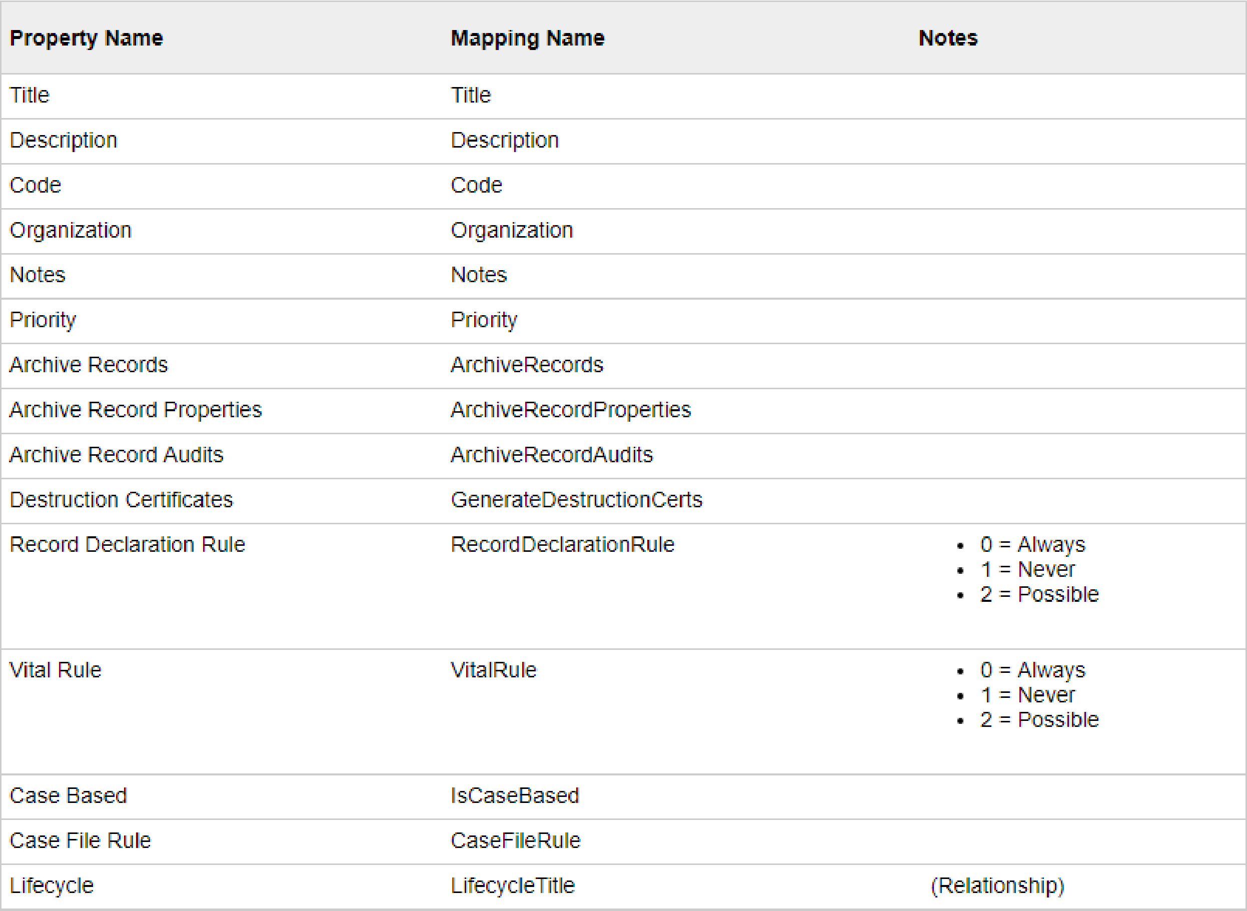
```
                    [Excel Column] some conditions
            ]]>
          </mapping>
          <levels>
            <level>
              <mapping>
                <![CDATA[
                    SELECT
                        [Excel Column] AS [Record Class Property],
                        ...
                    FROM
                        [Worksheet$]
                    WHERE
                        [Excel Column] = '{Title}' AND
                        [Excel Column] some conditions
                ]]>
              </mapping>
              <levels>
                <level>...
              </levels>
            </level>
            <level>...
          </levels>
        </level>
        <level>...
    </recordClasses>
    <lifecycles>
        <lifecycle>
            <mapping>
                <![CDATA[
                    SELECT
                        [Excel Column] AS [Lifecycle Property],
                        ...
                    FROM
                        [Worksheet$]
                    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>
    <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>
```

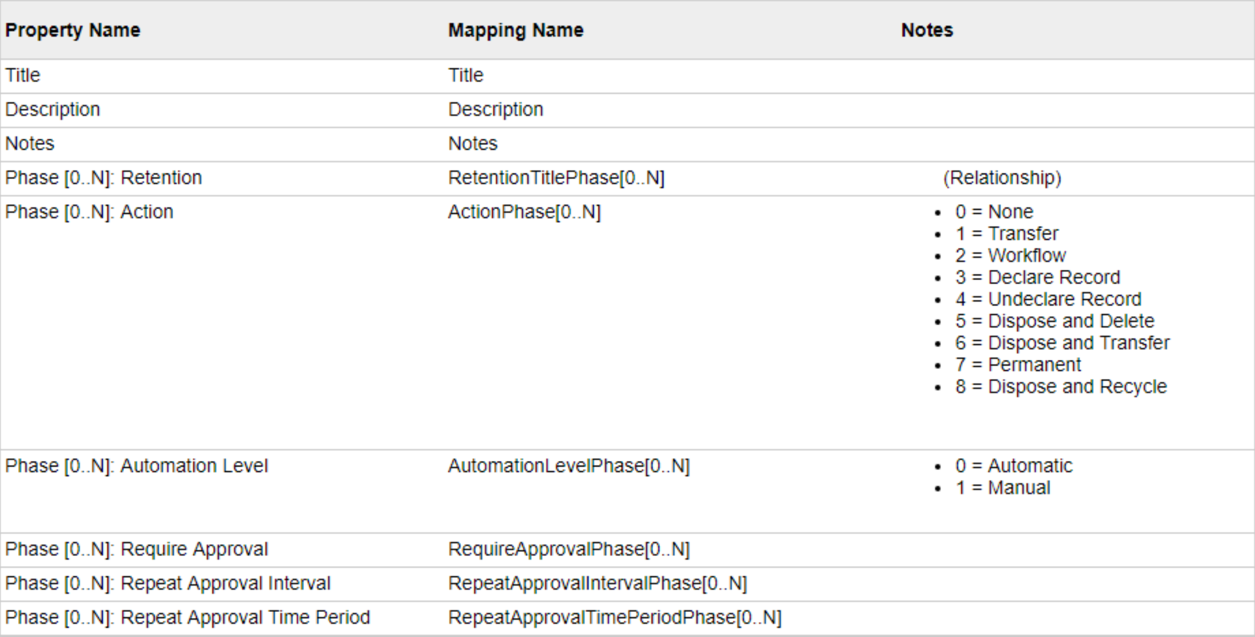
7.13.2.5 Object Schema for Import Mapping

Record Class



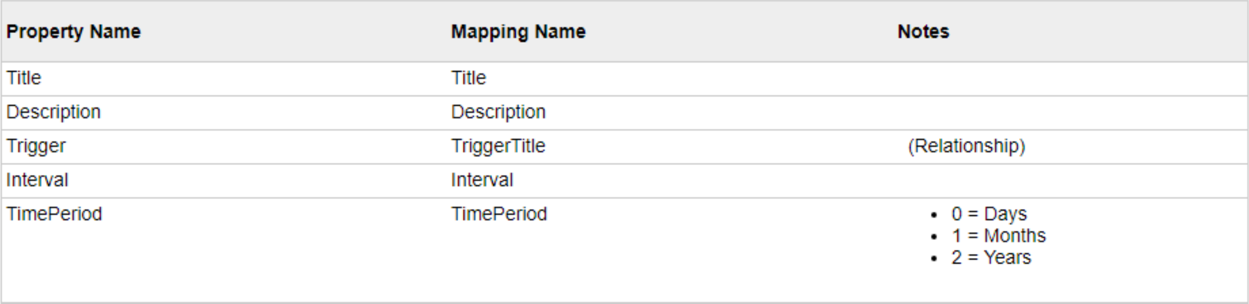
Property Name	Mapping Name	Notes
Title	Title	
Description	Description	
Code	Code	
Organization	Organization	
Notes	Notes	
Priority	Priority	
Archive Records	ArchiveRecords	
Archive Record Properties	ArchiveRecordProperties	
Archive Record Audits	ArchiveRecordAudits	
Destruction Certificates	GenerateDestructionCerts	
Record Declaration Rule	RecordDeclarationRule	• 0 = Always • 1 = Never • 2 = Possible
Vital Rule	VitalRule	• 0 = Always • 1 = Never • 2 = Possible
Case Based	IsCaseBased	
Case File Rule	CaseFileRule	
Lifecycle	LifecycleTitle	(Relationship)

Lifecycle



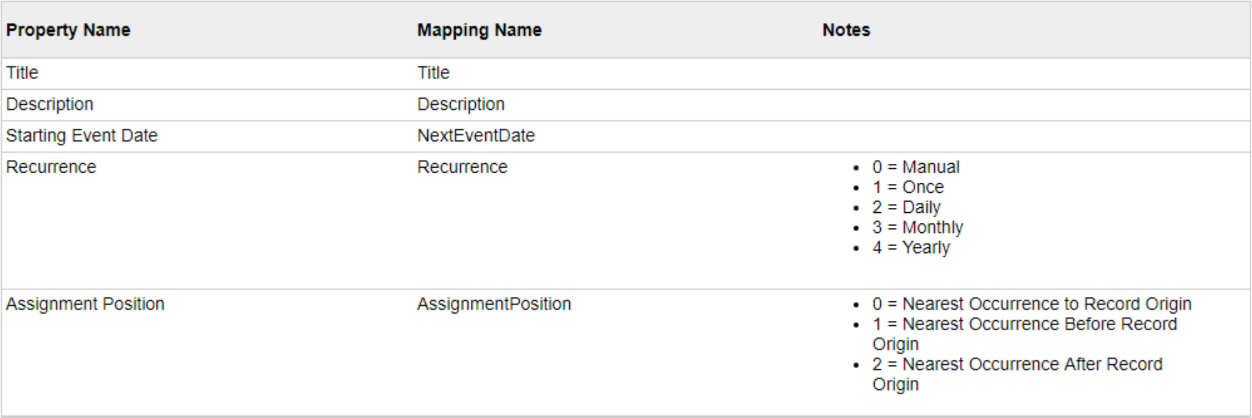
Property Name	Mapping Name	Notes
Title	Title	
Description	Description	
Notes	Notes	
Phase [0..N]: Retention	RetentionTitlePhase[0..N]	(Relationship)
Phase [0..N]: Action	ActionPhase[0..N]	• 0 = None • 1 = Transfer • 2 = Workflow • 3 = Declare Record • 4 = Undeclare Record • 5 = Dispose and Delete • 6 = Dispose and Transfer • 7 = Permanent • 8 = Dispose and Recycle
Phase [0..N]: Automation Level	AutomationLevelPhase[0..N]	• 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



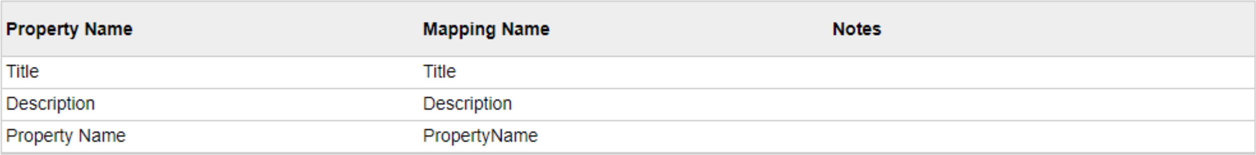
Property Name	Mapping Name	Notes
Title	Title	
Description	Description	
Trigger	TriggerTitle	(Relationship)
Interval	Interval	
TimePeriod	TimePeriod	• 0 = Days • 1 = Months • 2 = Years

Event Trigger



Property Name	Mapping Name	Notes
Title	Title	
Description	Description	
Starting Event Date	NextEventDate	
Recurrence	Recurrence	• 0 = Manual • 1 = Once • 2 = Daily • 3 = Monthly • 4 = Yearly
Assignment Position	AssignmentPosition	• 0 = Nearest Occurrence to Record Origin • 1 = Nearest Occurrence Before Record Origin • 2 = Nearest Occurrence After Record Origin

Date Property Trigger



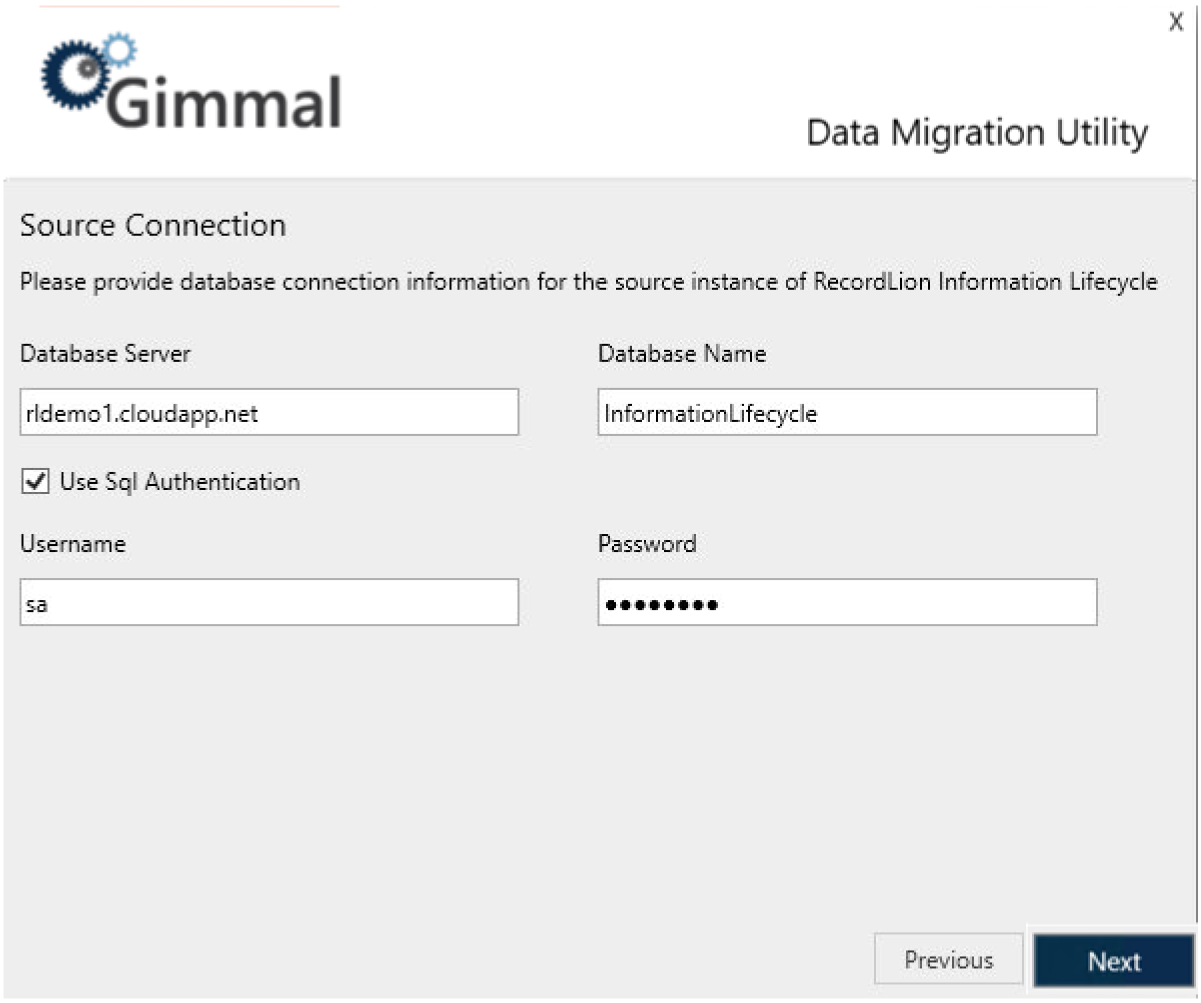
Property Name	Mapping Name	Notes
Title	Title	
Description	Description	
Property Name	PropertyName	

7.13.3 Migrate

If you selected Migrate from the Welcome screen, this section will guide you through the wizard.

7.13.3.1 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**.



Source Connection

Please provide database connection information for the source instance of RecordLion Information Lifecycle

Database Server: rldemo1.cloudapp.net

Database Name: InformationLifecycle

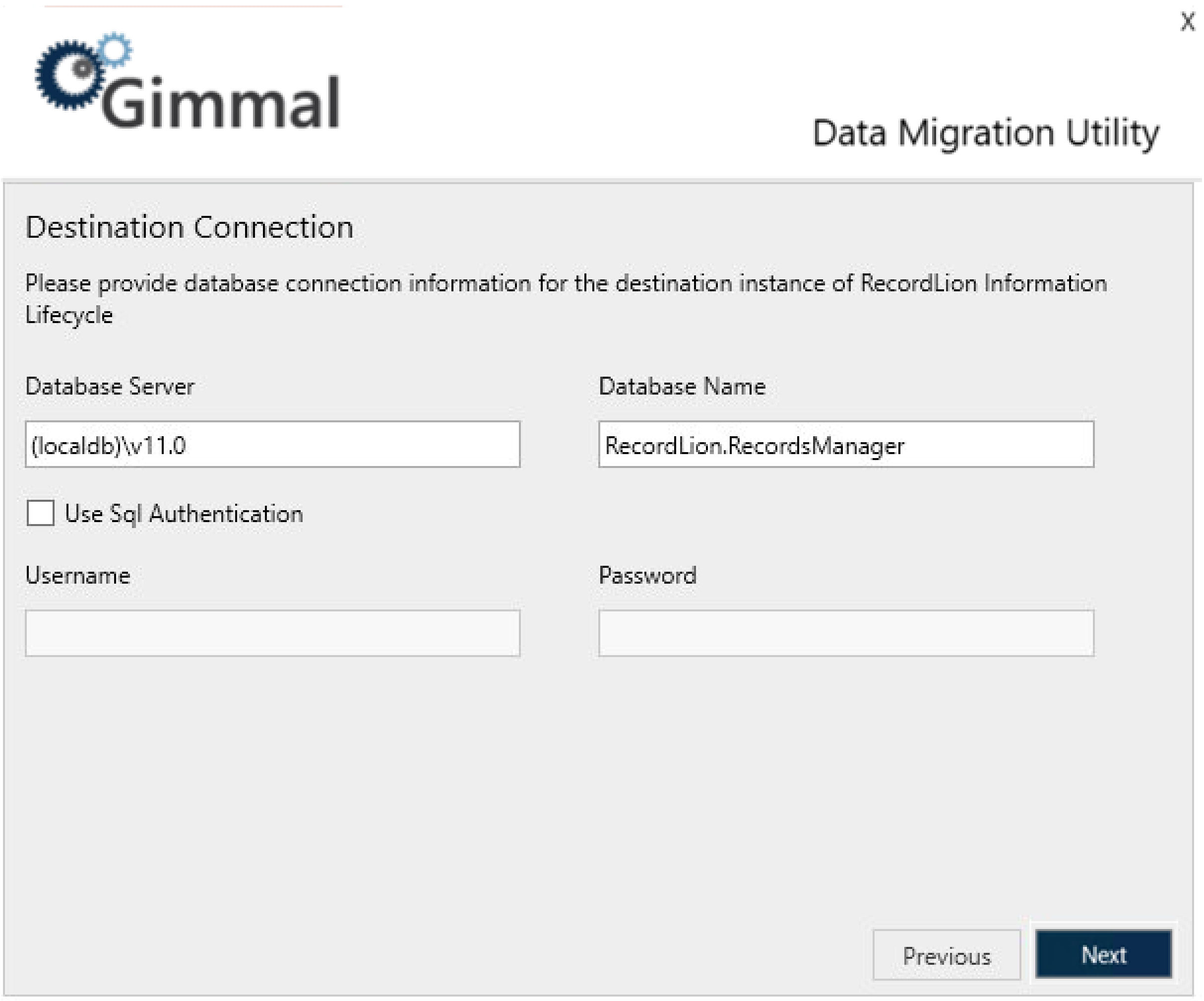
☑ Use Sql Authentication

Username: sa

Password: ●●●●●●●●●

7.13.3.2 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

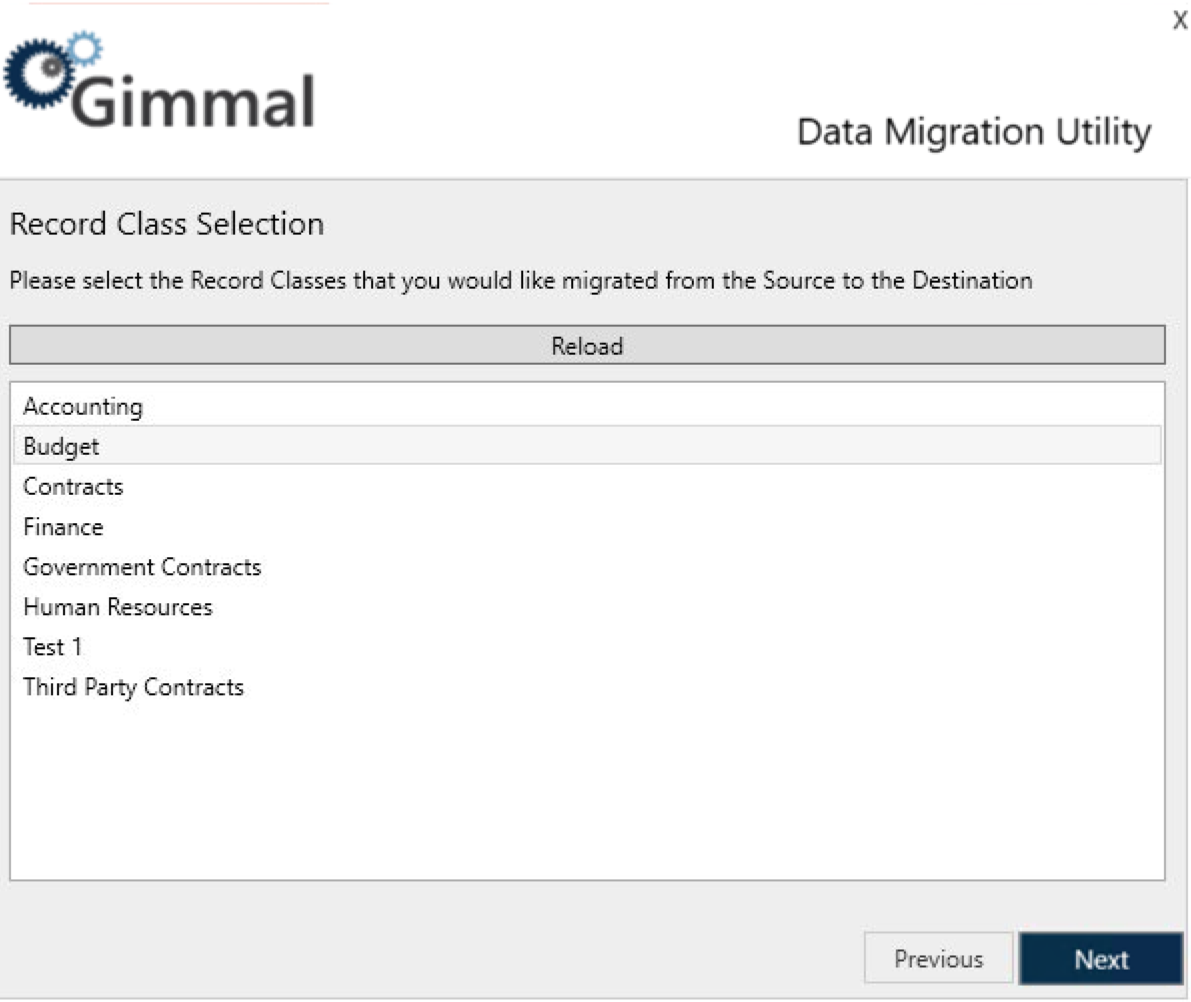
□ Use Sql Authentication

Username

Password

7.13.3.3 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**.



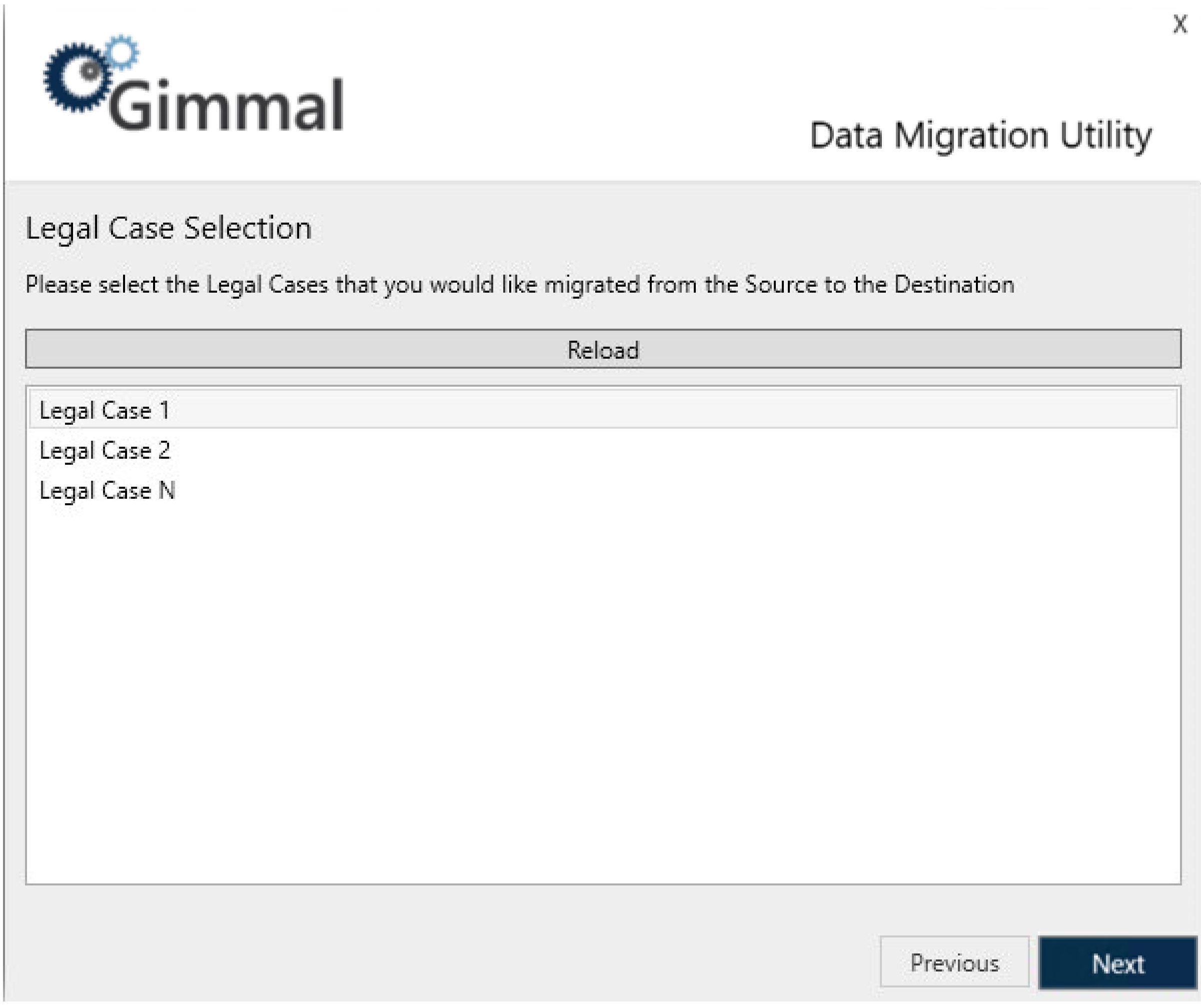
Record Class Selection

Please select the Record Classes that you would like migrated from the Source to the Destination

Accounting
Budget
Contracts
Finance
Government Contracts
Human Resources
Test 1
Third Party Contracts

7.13.3.4 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**.



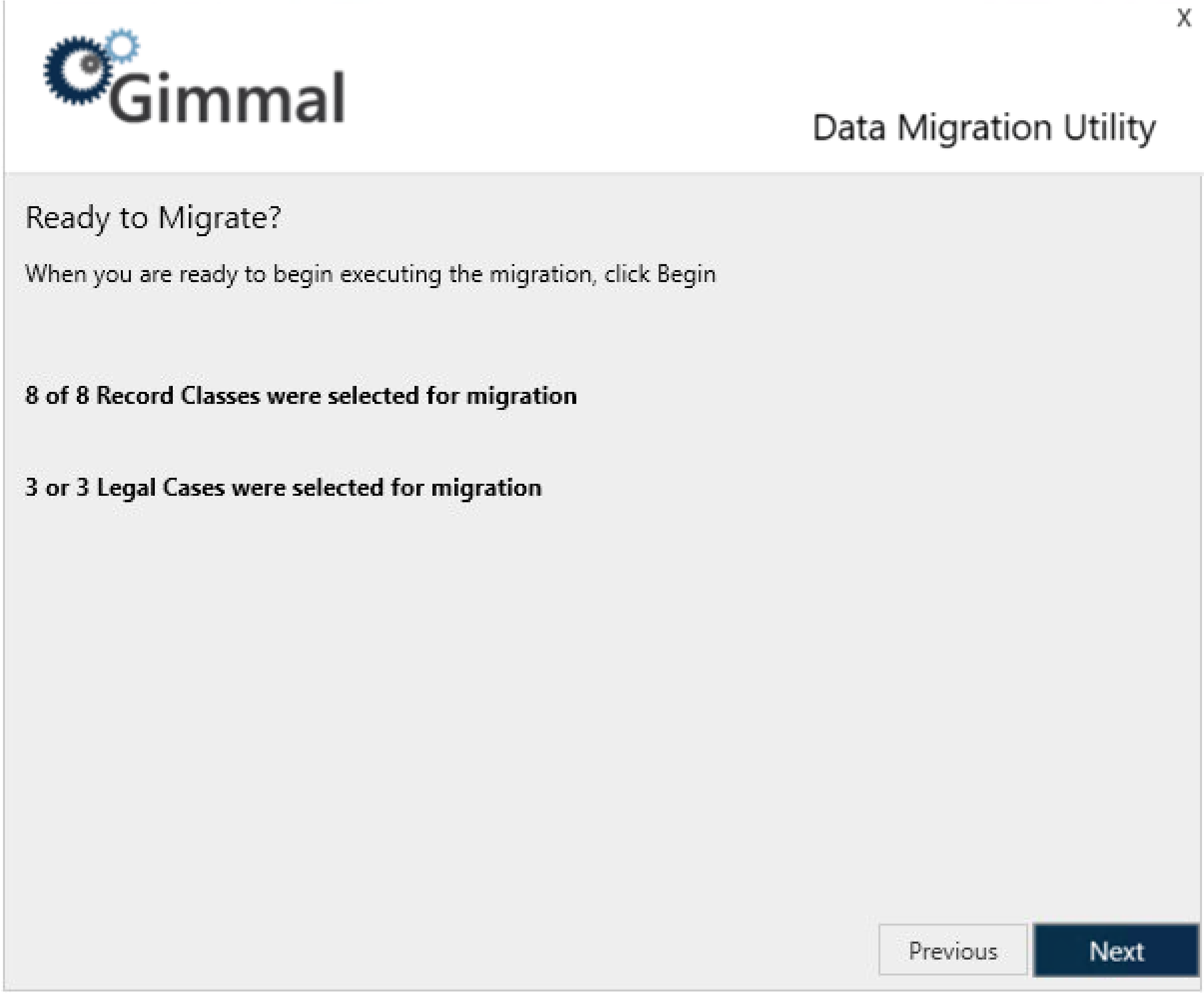
Legal Case Selection

Please select the Legal Cases that you would like migrated from the Source to the Destination

Legal Case 1
Legal Case 2
Legal Case N

7.13.3.5 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.



Ready to Migrate?

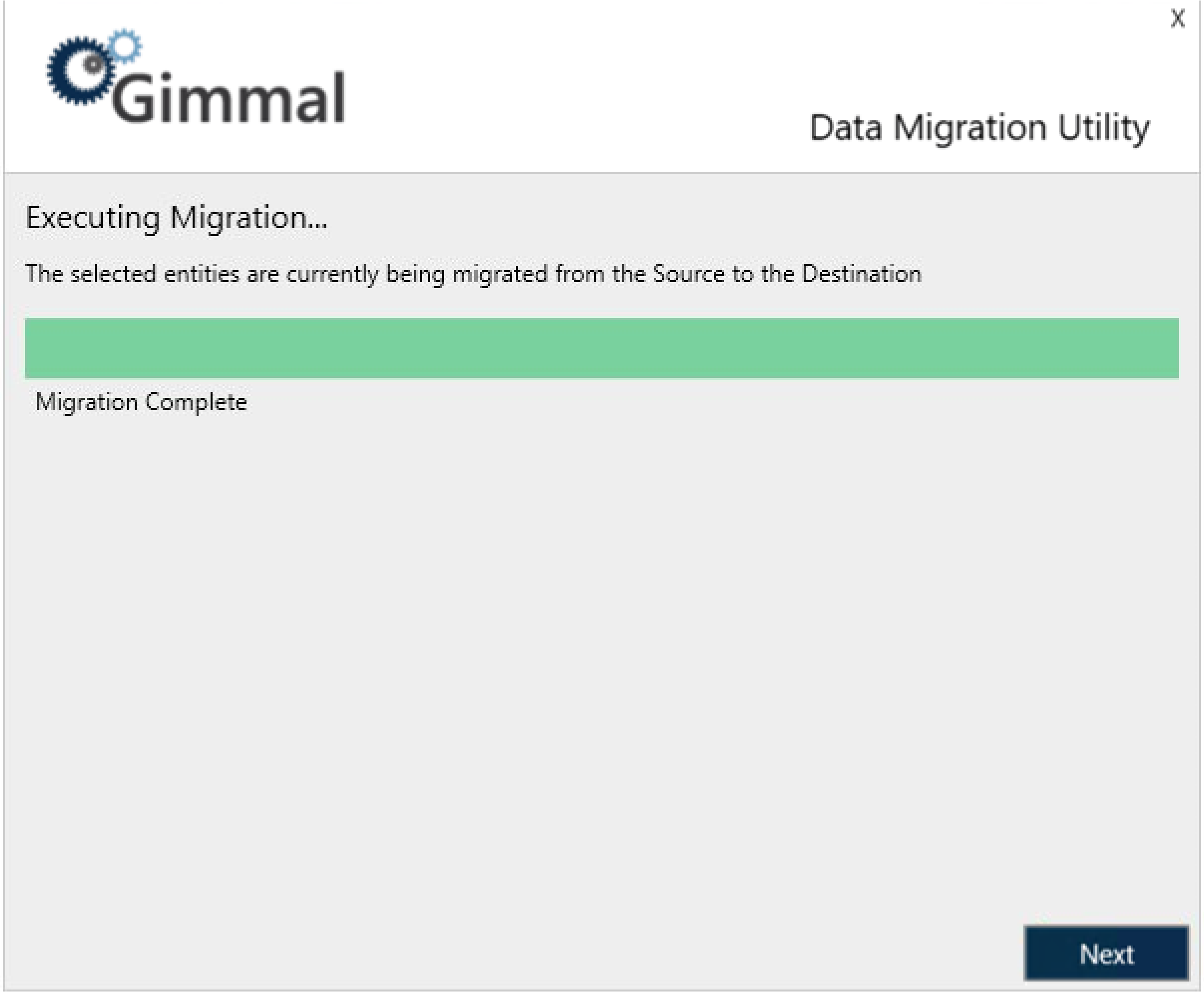
When you are ready to begin executing the migration, click Begin

8 of 8 Record Classes were selected for migration

3 or 3 Legal Cases were selected for migration

7.13.3.6 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**.



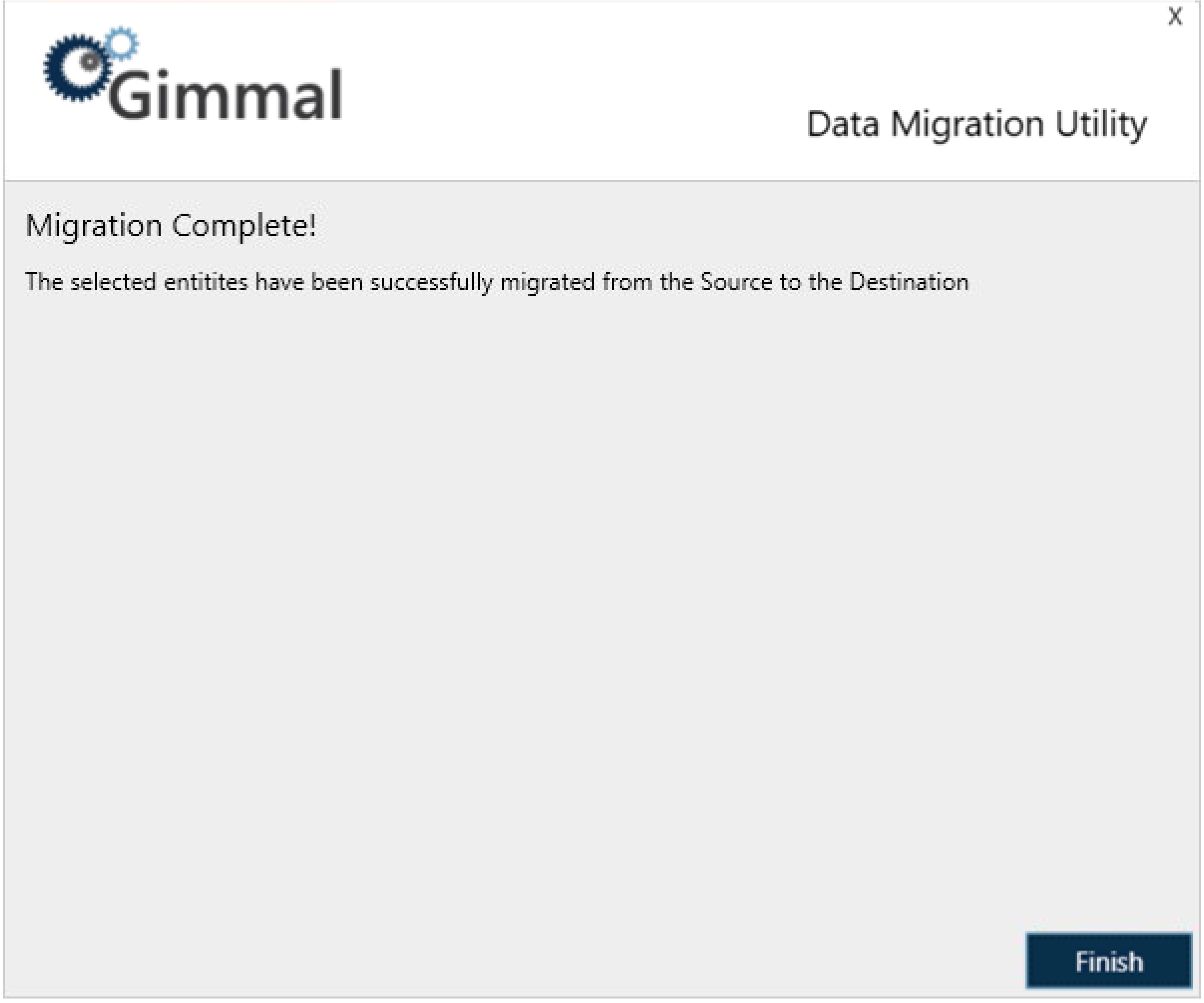
Executing Migration...

The selected entities are currently being migrated from the Source to the Destination

Migration Complete

7.13.3.7 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.



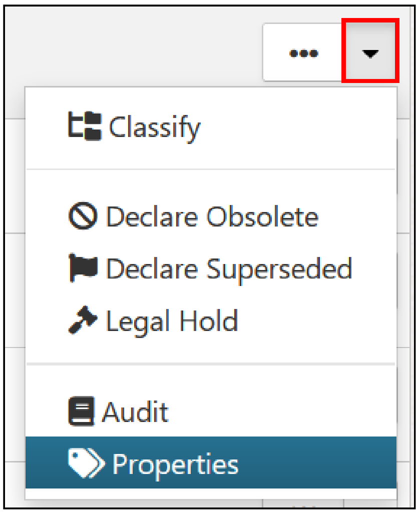
Migration Complete!

The selected entitites have been successfully migrated from the Source to the Destination

7.14 Filtering Records by Rules and Metadata

Gimmal 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 415)
- Creating Record Filters(see page 419)
- Adding Filters to Record Classes(see page 421)

7.14.1 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.

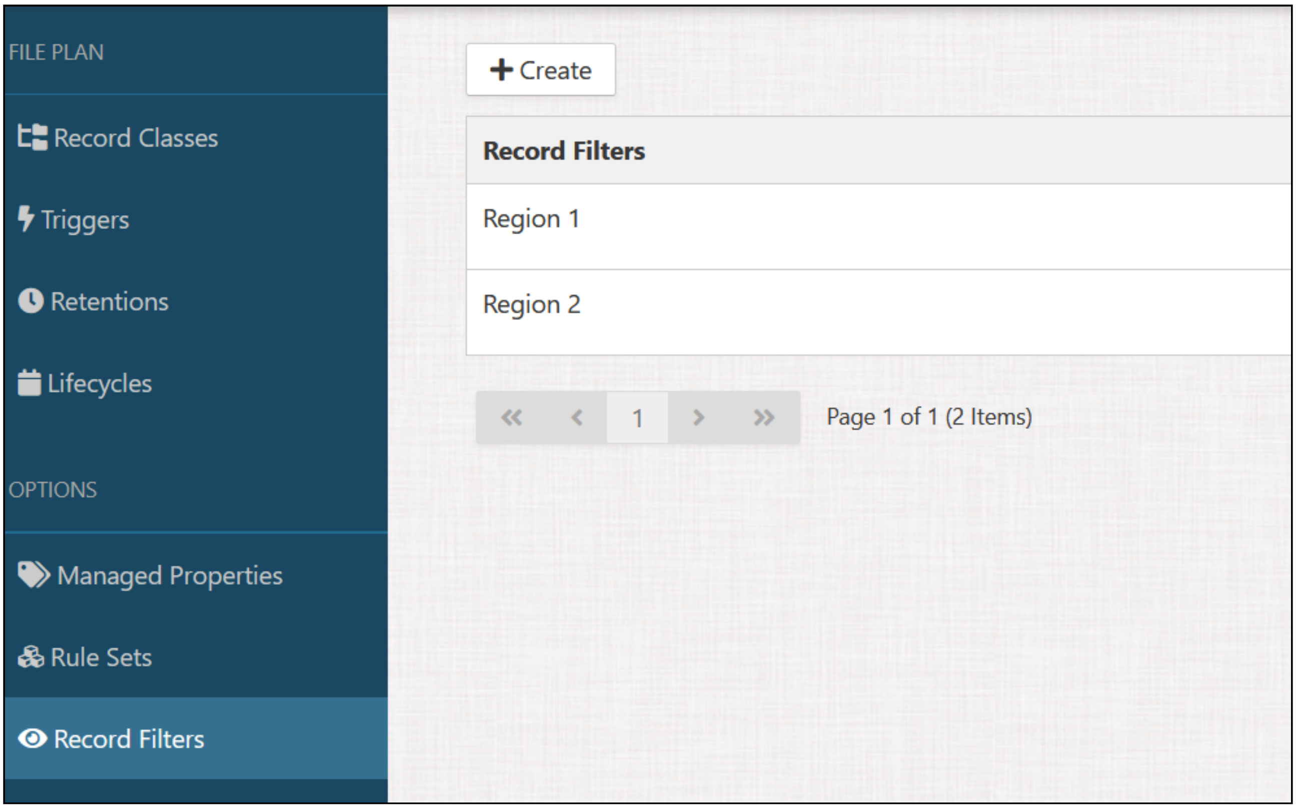
7.14.1.1 Record Filters in Practice

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.

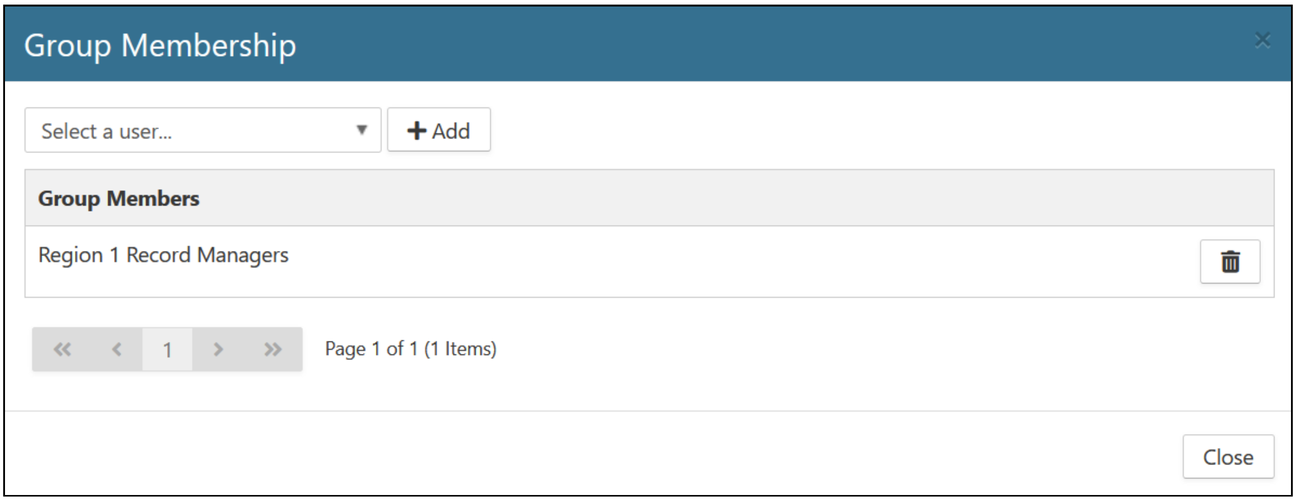
Two Record Filters would be created, Region 1 and Region 2:



Record Filters
Region 1
Region 2

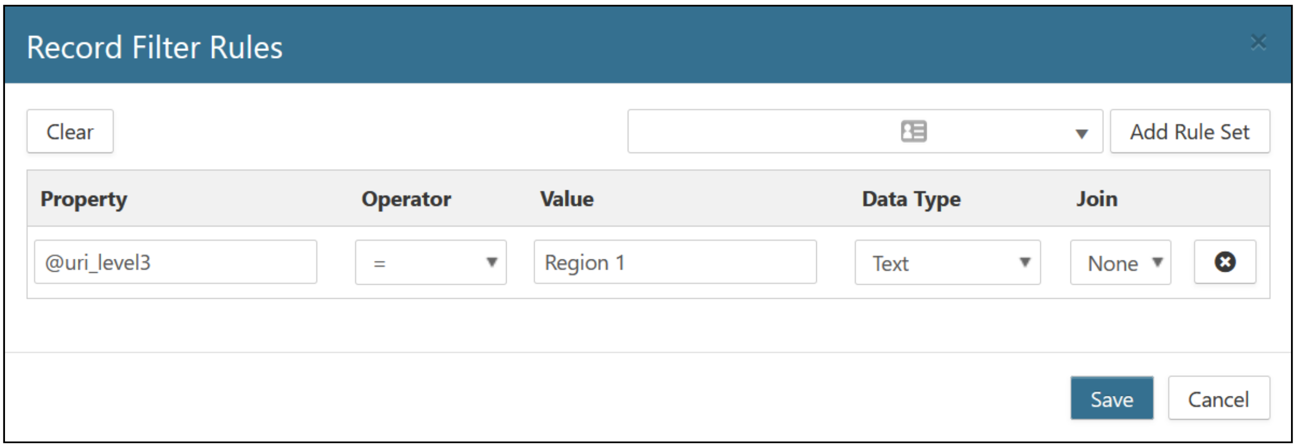
Page 1 of 1 (2 Items)

Set the group membership and rules for Region 1:



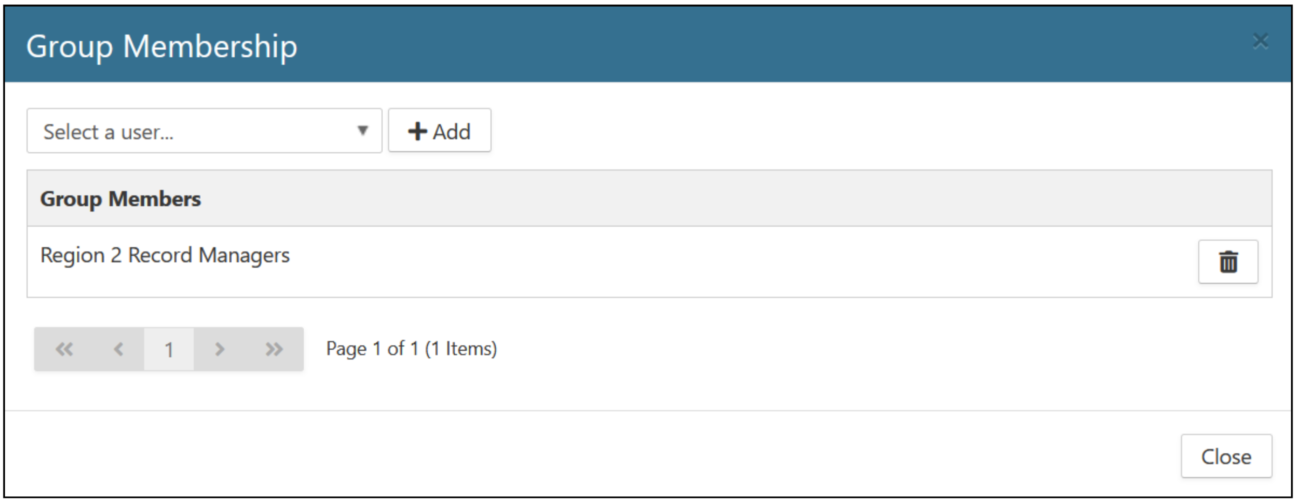
Group Members
Region 1 Record Managers

Page 1 of 1 (1 Items)



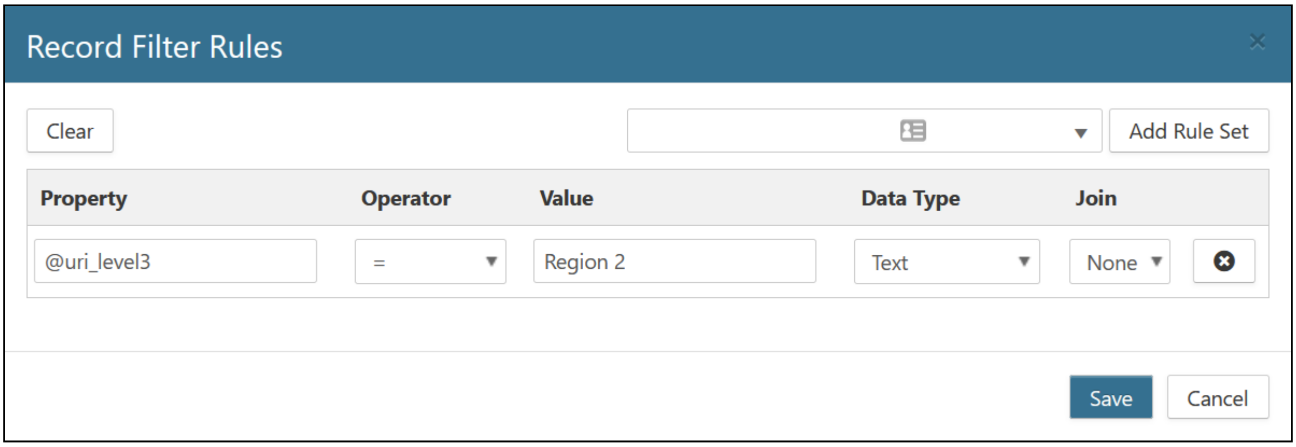
Property	Operator	Value	Data Type	Join
@uri_level3	=	Region 1	Text	None

Set the group membership and rules for Region 2:



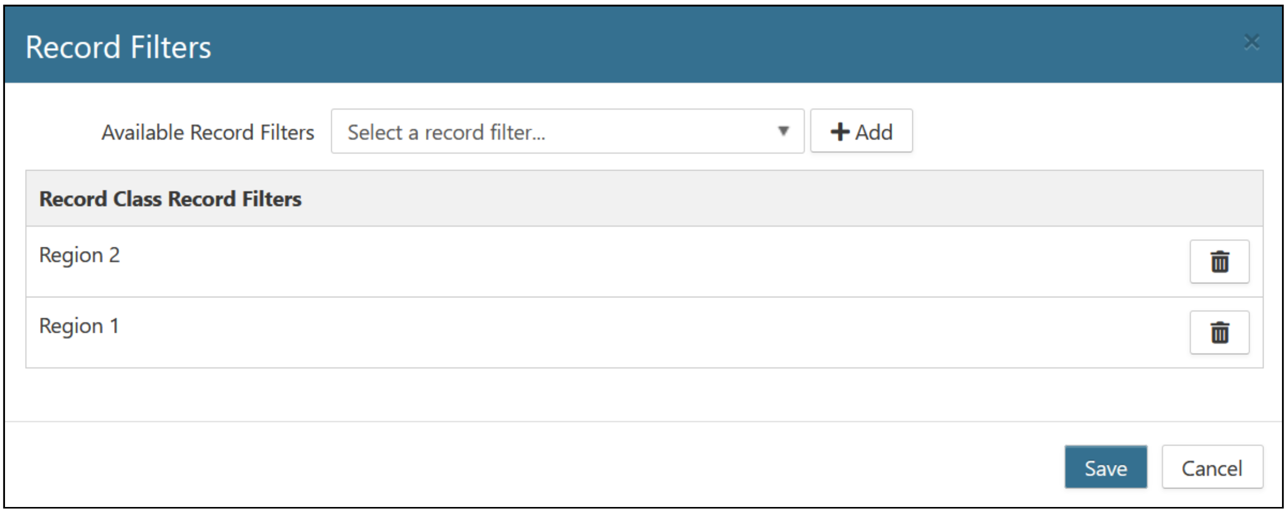
Group Members
Region 2 Record Managers

Page 1 of 1 (1 Items)



Property	Operator	Value	Data Type	Join
@uri_level3	=	Region 2	Text	None

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



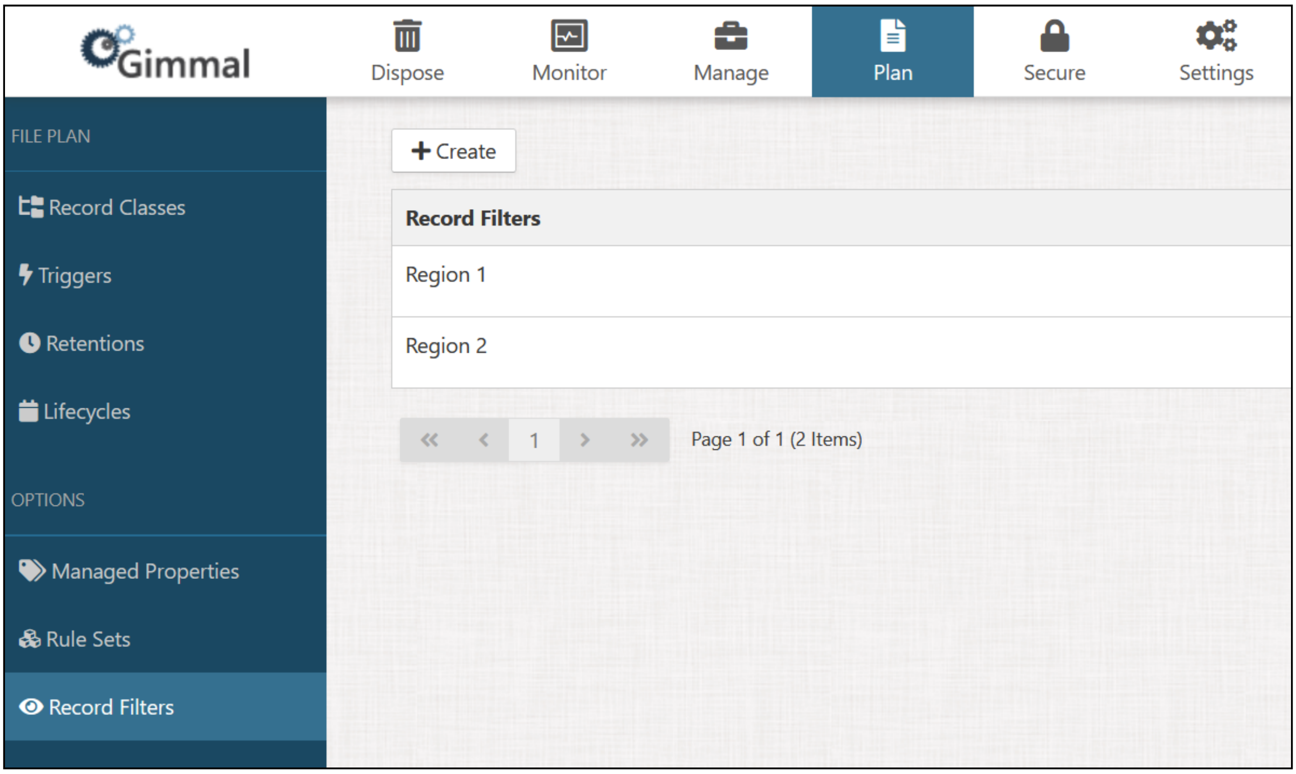
Available Record Filters: Select a record filter...

Record Class Record Filters
Region 2
Region 1

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.

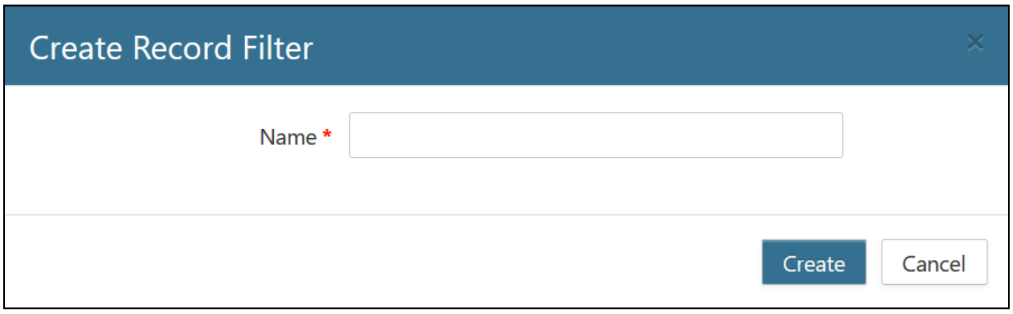
7.14.2 Creating Record Filters

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



Record Filters
Region 1
Region 2

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



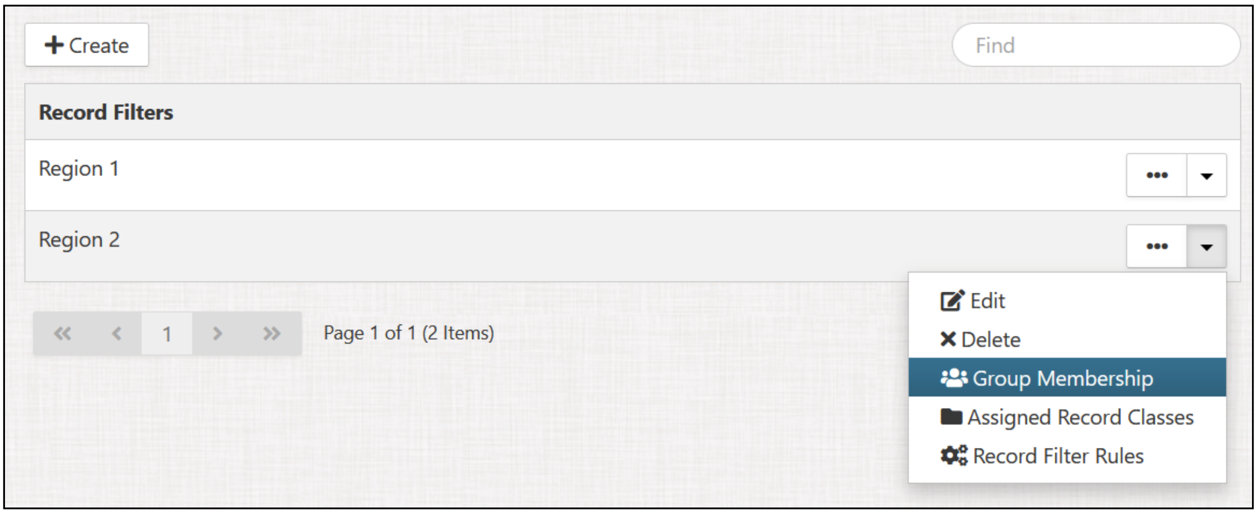
Once a filter is created, the drop-down menu on the right side of each filter allows the following actions:

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

7.14.2.1 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.

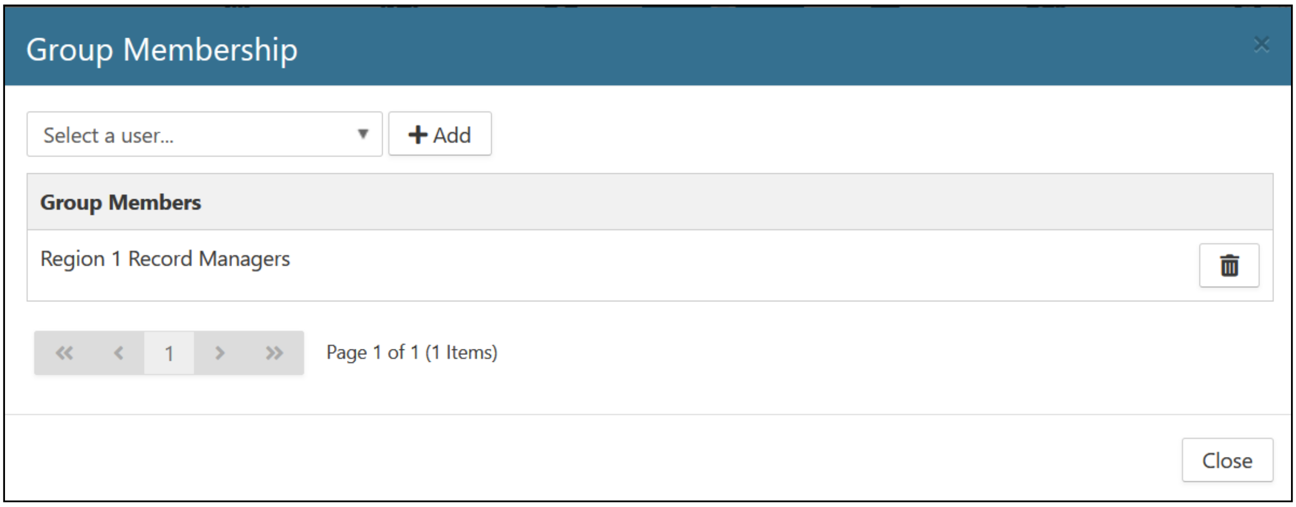
To create Group Memberships, select the drop-down menu for a Record Filter and select Group Membership.



Record Filters
Region 1
Region 2

Page 1 of 1 (2 Items)

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



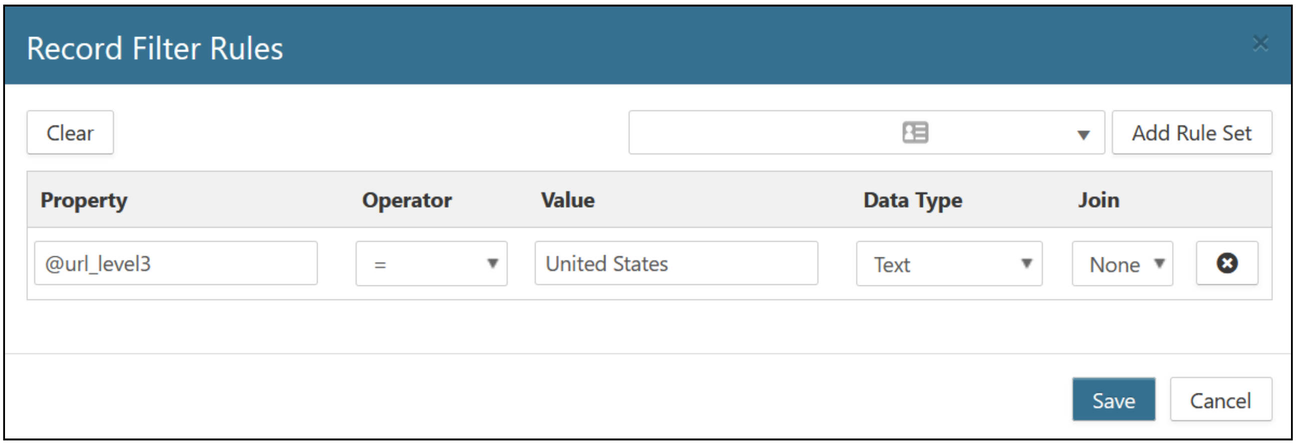
Group Membership

Group Members
Region 1 Record Managers

Page 1 of 1 (1 Items)

7.14.2.2 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:



Record Filter Rules

Property	Operator	Value	Data Type	Join
@url_level3	=	United States	Text	None

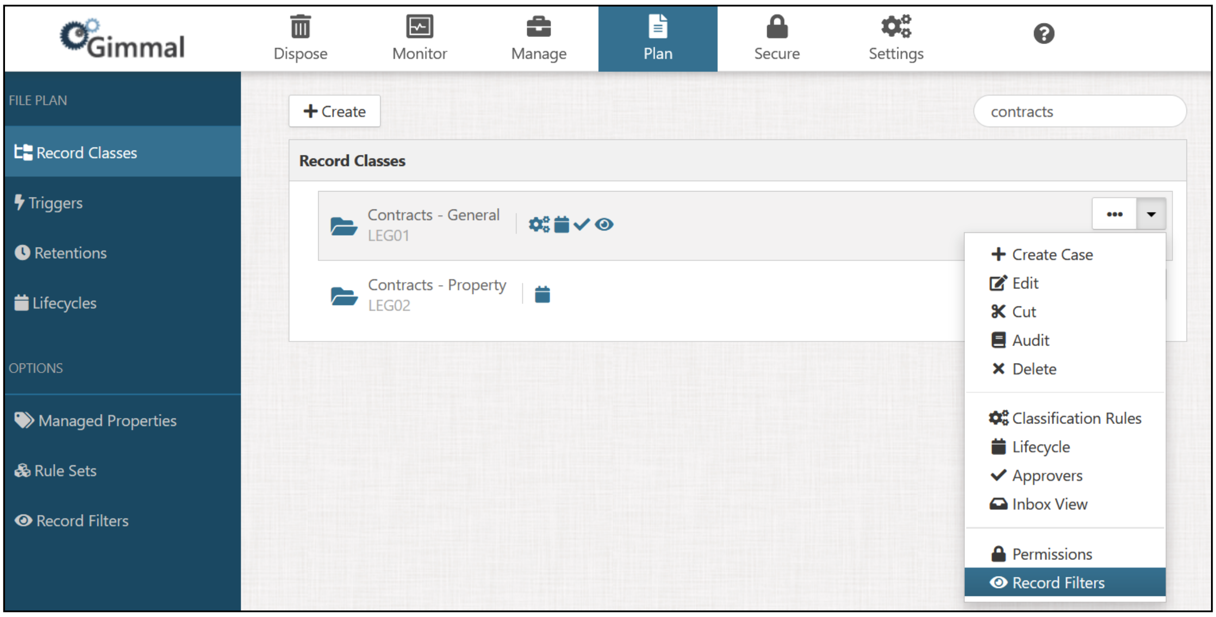
For detailed information on creating rules, see the Rule Builder(see page 148) topic.

7.14.3 Adding Filters to Record Classes

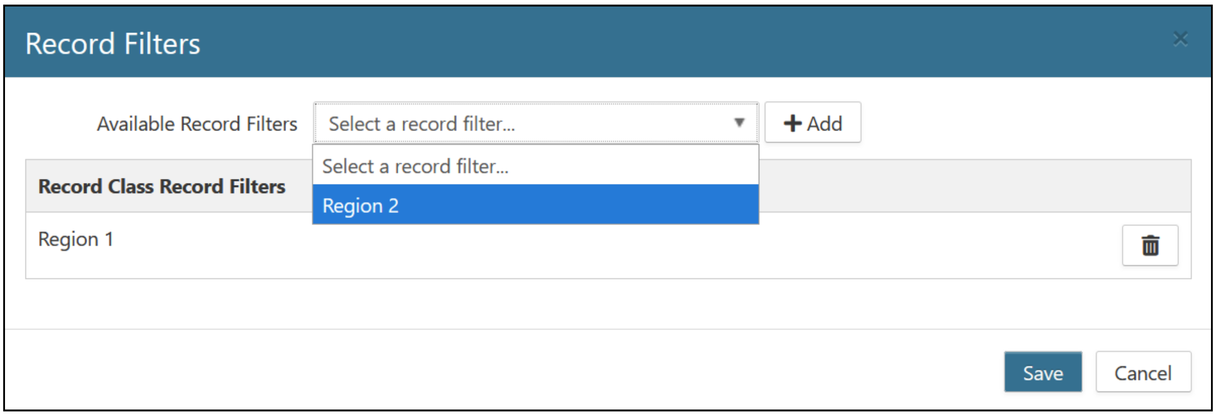
In order for a Record Filter to be applied, it must be added to a Record Class. Each filter will have a set of users/groups that for the specific rules, and any number of Record Filters an be added to a Record Class.

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


Record Filters
Available Record Filters
Select a record filter...
+ Add
Select a record filter...
Region 2
Record Class Record Filters
Region 1
Save
Cancel

4. Click Save

ⓘ 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.

8 Developer Guide

8.1 SDK

Gimmal Records Management has an SDK available at https://github.com/recordlion

8.2 PowerShell CmdLets

8.3 Telerik Reporting Tool

8.4 Power BI

8.5 PowerShell CmdLets

The following topics provide the PowerShell Cmdlets supported by each Records Management component.

8.5.1 Manager Web Cmdlets

8.5.2 File Share Connector Web Cmdlets

8.5.3 File Share Connector Service Cmdlets

8.5.4 Lifecycle Services Cmdlets

8.5.5 SharePoint Connector Cmdlets

8.5.6 SharePoint Online Connector Web Cmdlets

8.5.7 SharePoint Online Connector Service Cmdlets

8.5.8 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).

8.5.8.1 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
-Credentials <pscredential>
-NewCredentials <pscredential>
[-SQLTimeout <int>]
```

8.5.9 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.

8.5.9.1 Cmdlets

Set-FileShareWeb

```
Set-FileShareWeb
-SiteName <lstring>
[-ConnectionString <string>]
[-DataProviderType <string>]
[-JsonProviderFileLocation <string>]
```

8.5.10 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

8.5.10.1 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]
```

8.5.11 Lifecycle Services Cmdlets

Records Management supports the post-installation configuration of Lifeycle 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.

8.5.11.1 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]
```

8.5.12 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
```

8.5.12.1 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]
```

8.5.13 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

8.5.13.1 Set-SPOConnectorWeb

```
Set-SPOConnectorWeb
-SiteName <string>
[-ClientId <string>]
[-ClientSecret <string>]
[-ConnectionString <string>]
```

8.5.14 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.

8.5.14.1 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-SPOListItem

```
Unblock-SPOListItem
-ItemUrl <string>
-SPOnlineCreds <pscredential>
```

8.6 Telerik Reporting Tool

Version: 1.0 and above (Not compatible with the cloud version)

8.6.1 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.

8.6.2 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.

8.6.3 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

8.6.4 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%/gimmal/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 at 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>

8.6.5 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 Gimmal to discuss a Premier Services engagement.

Please submit a Support Ticket[116] requesting this information if desired.

8.6.6 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.

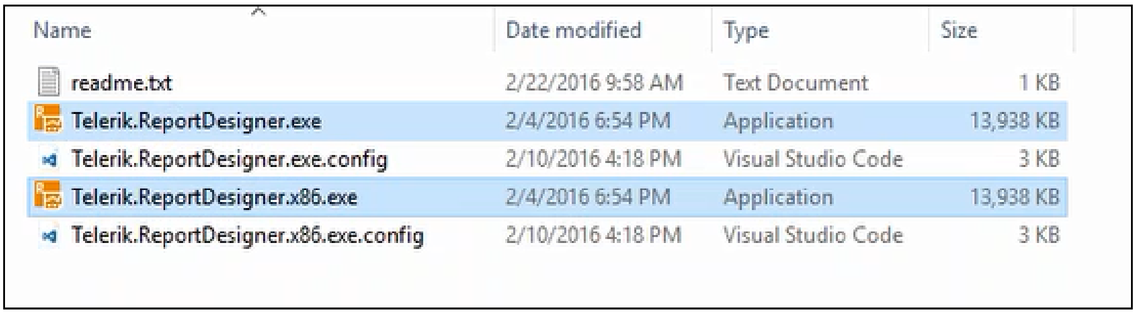
1. Open the Report Designer.
2. Select a Template.
3. Select a Data Source.
4. Build the report.
5. Preview the report.

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.

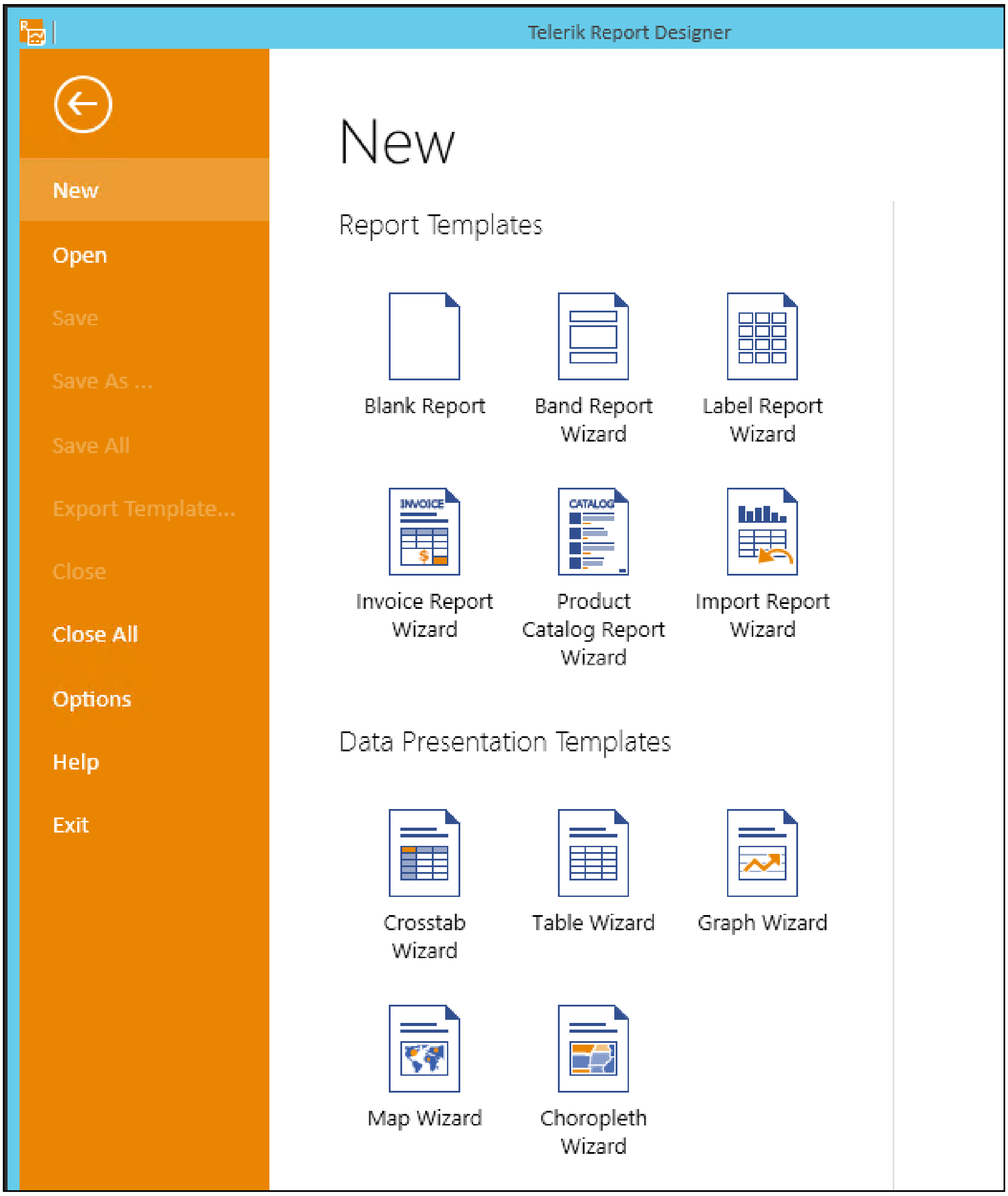
1. Open the Report Designer
   - It is located at: C:\Program Files\Gimmal\Records Management\web\reports
   - There are two EXEs that are included; a 64-bit version and the x86 version. If you are developing these reports from the server, you will use the 64- bit version. If you are going to create 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.

[116] https://support.gimmal.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

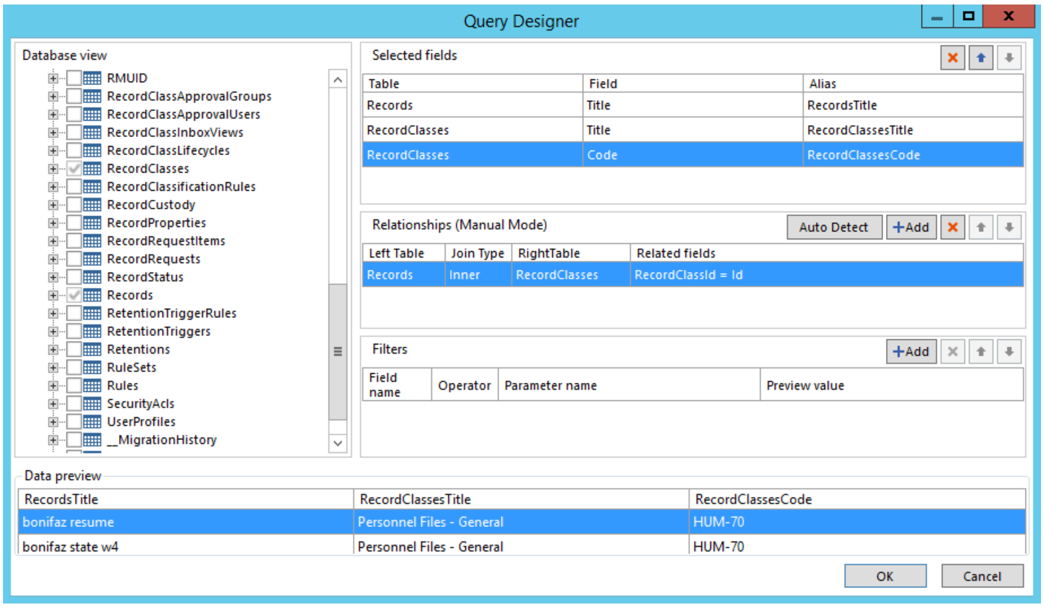
2. Select a Report Template
    - When you open the Report Designer, you can choose to open an existing report or a new report. If you select **New**, you will see a list of Wizards that can be used for creating a report. The wizards will guide you through the process for creating that specific type 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:



Database view

- RMUID
- RecordClassApprovalGroups
- RecordClassApprovalUsers
- RecordClassInboxViews
- RecordClassLifecycles
- RecordClasses
- RecordClassificationRules
- RecordCustody
- RecordProperties
- RecordRequestItems
- RecordRequests
- RecordStatus
- Records
- RetentionTriggerRules
- RetentionTriggers
- Retentions
- RuleSets
- Rules
- SecurityAcls
- UserProfiles
- __MigrationHistory

Selected fields

Table	Field	Alias
Records	Title	RecordsTitle
RecordClasses	Title	RecordClassesTitle
RecordClasses	Code	RecordClassesCode

Relationships (Manual Mode)

Left Table	Join Type	RightTable	Related fields
Records	Inner	RecordClasses	RecordClassId = Id

Filters

Field name	Operator	Parameter name	Preview value

Data preview

RecordsTitle	RecordClassesTitle	RecordClassesCode
bonifaz resume	Personnel Files - General	HUM-70
bonifaz state w4	Personnel Files - General	HUM-70

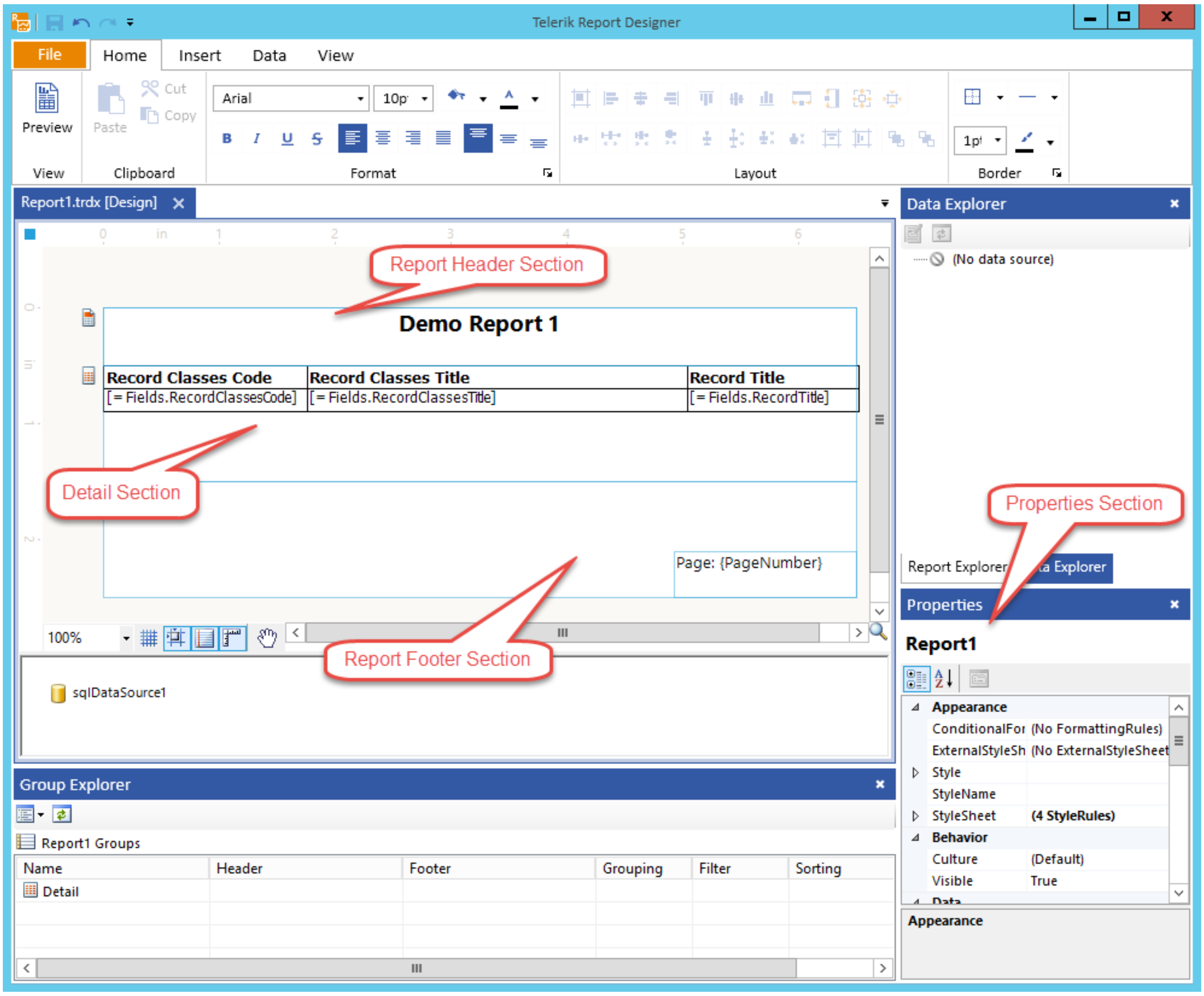
- Validate that the Relationships section contains the correct join for the tables you have selected.
- Enter any Filters that may be needed.
- Select **OK**
- The SQL statement will be displayed in the Select Statement field in the Configure data source commend dialog box. See below for an exampl
- 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.

8.6.7 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.



Report Header Section

Detail Section

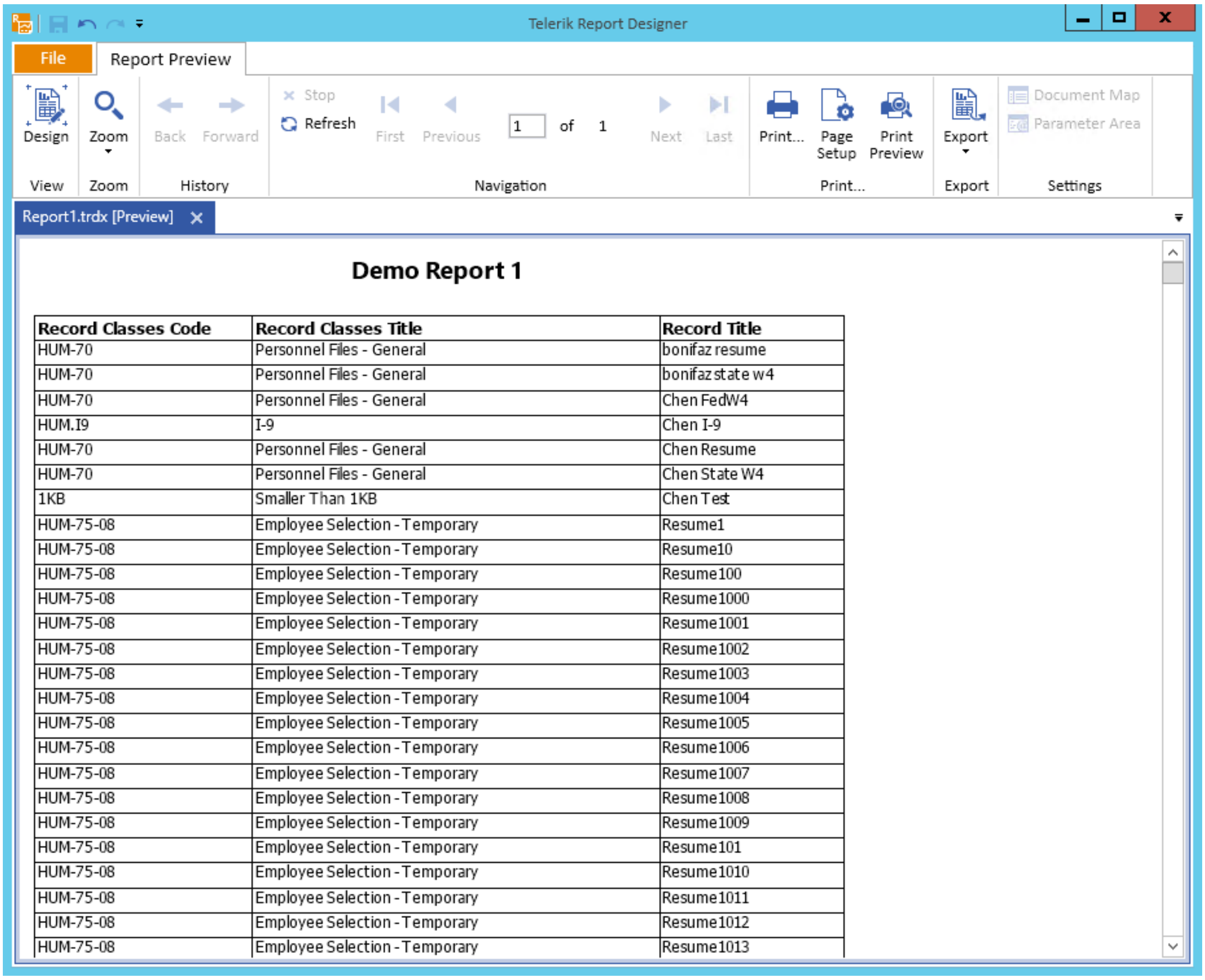
Report Footer Section

Properties Section

Appearance	
ConditionalFor	(No FormattingRules)
ExternalStyleSh	(No ExternalStyleSheet
Style	
StyleName	
StyleSheet	(4 StyleRules)
Behavior	
Culture	(Default)
Visible	True
Data	

Appearance

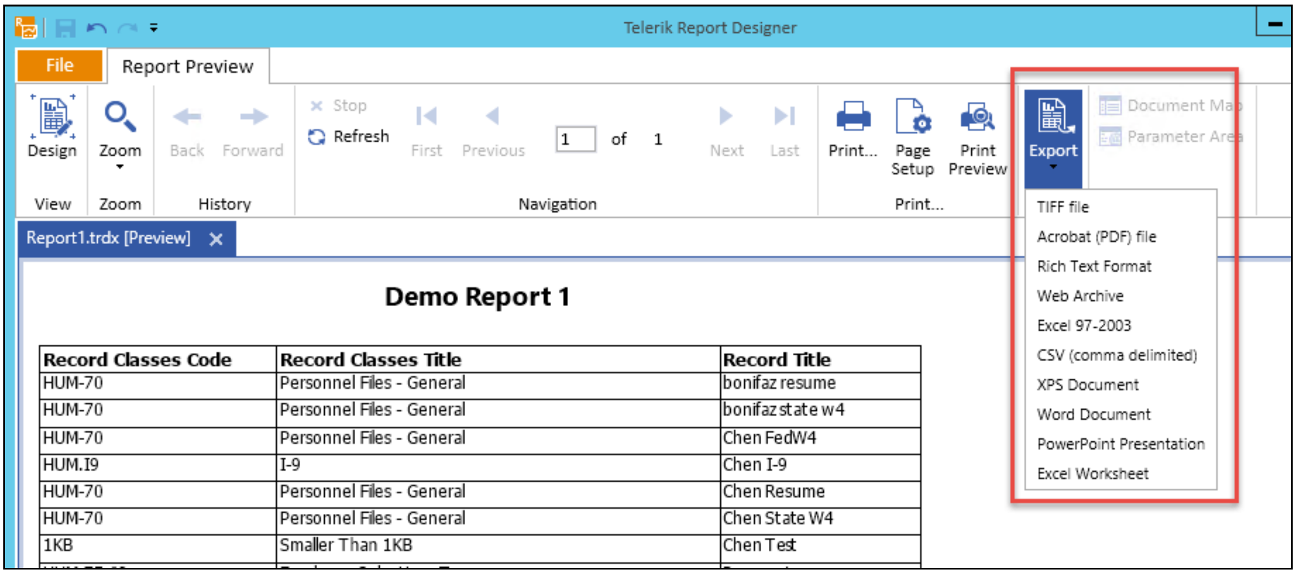
Click **Preview** to go to Report Preview mode and see a preview of your report.



Demo Report 1

Record Classes Code	Record Classes Title	Record Title
HUM-70	Personnel Files - General	bonifaz resume
HUM-70	Personnel Files - General	bonifaz state w4
HUM-70	Personnel Files - General	Chen FedW4
HUM.I9	I-9	Chen I-9
HUM-70	Personnel Files - General	Chen Resume
HUM-70	Personnel Files - General	Chen State W4
1KB	Smaller Than 1KB	Chen Test
HUM-75-08	Employee Selection - Temporary	Resume1
HUM-75-08	Employee Selection - Temporary	Resume10
HUM-75-08	Employee Selection - Temporary	Resume100
HUM-75-08	Employee Selection - Temporary	Resume1000
HUM-75-08	Employee Selection - Temporary	Resume1001
HUM-75-08	Employee Selection - Temporary	Resume1002
HUM-75-08	Employee Selection - Temporary	Resume1003
HUM-75-08	Employee Selection - Temporary	Resume1004
HUM-75-08	Employee Selection - Temporary	Resume1005
HUM-75-08	Employee Selection - Temporary	Resume1006
HUM-75-08	Employee Selection - Temporary	Resume1007
HUM-75-08	Employee Selection - Temporary	Resume1008
HUM-75-08	Employee Selection - Temporary	Resume1009
HUM-75-08	Employee Selection - Temporary	Resume101
HUM-75-08	Employee Selection - Temporary	Resume1010
HUM-75-08	Employee Selection - Temporary	Resume1011
HUM-75-08	Employee Selection - Temporary	Resume1012
HUM-75-08	Employee Selection - Temporary	Resume1013

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.



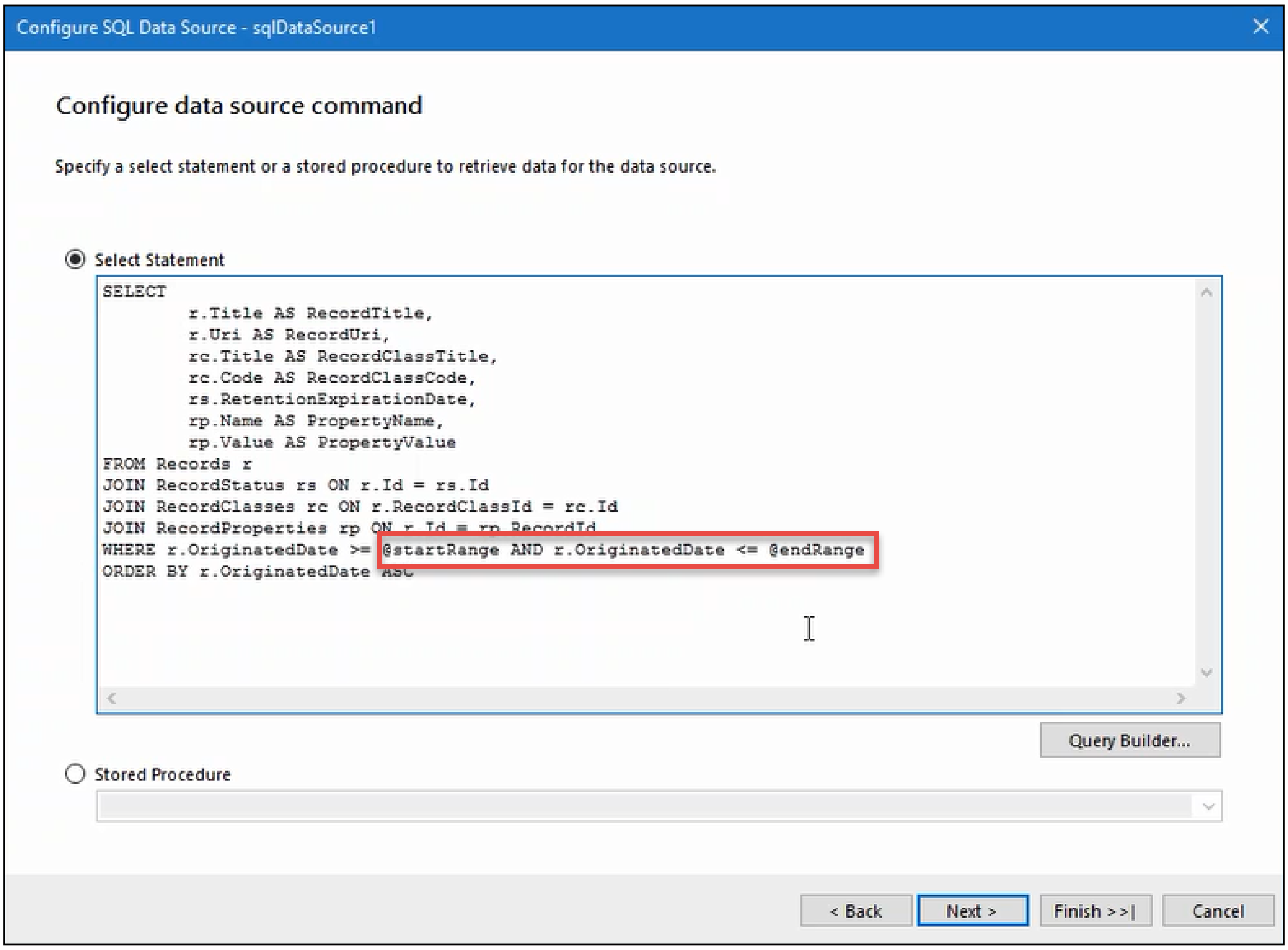
Demo Report 1

Record Classes Code	Record Classes Title	Record Title
HUM-70	Personnel Files - General	bonifaz resume
HUM-70	Personnel Files - General	bonifaz state w4
HUM-70	Personnel Files - General	Chen FedW4
HUM.I9	I-9	Chen I-9
HUM-70	Personnel Files - General	Chen Resume
HUM-70	Personnel Files - General	Chen State W4
1KB	Smaller Than 1KB	Chen Test

8.6.8 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.



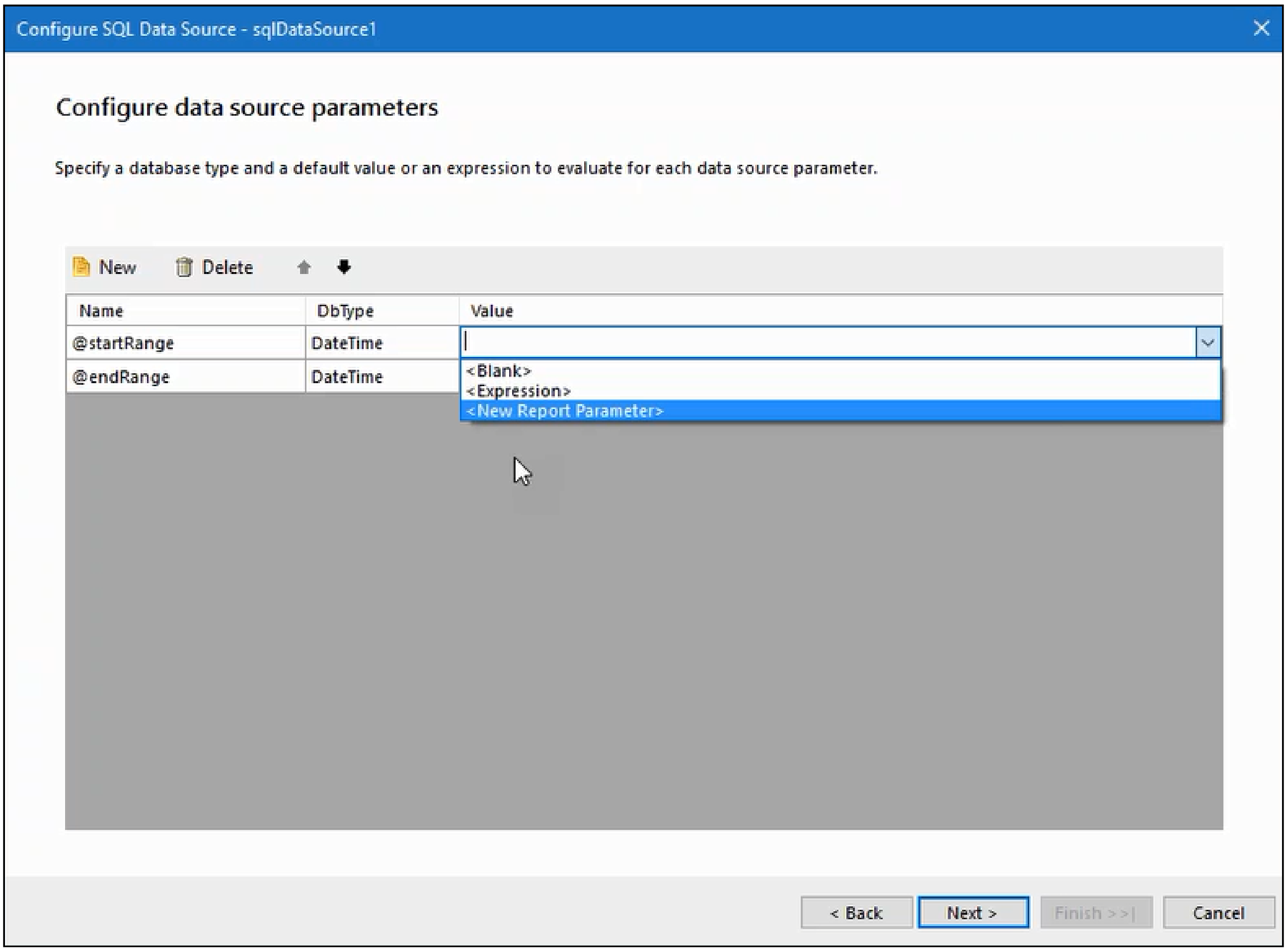
Configure SQL Data Source - sqlDataSource1
Configure data source command

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
```

Click **Next** and the **Configure data source parameters** window will display.



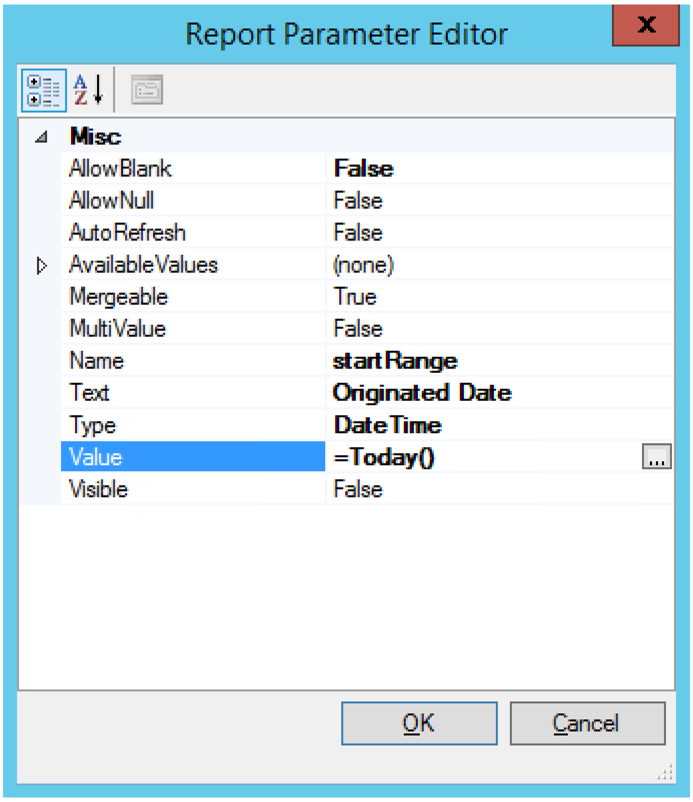
Configure SQL Data Source - sqlDataSource1

Configure data source parameters

Specify a database type and a default value or an expression to evaluate for each data source parameter.

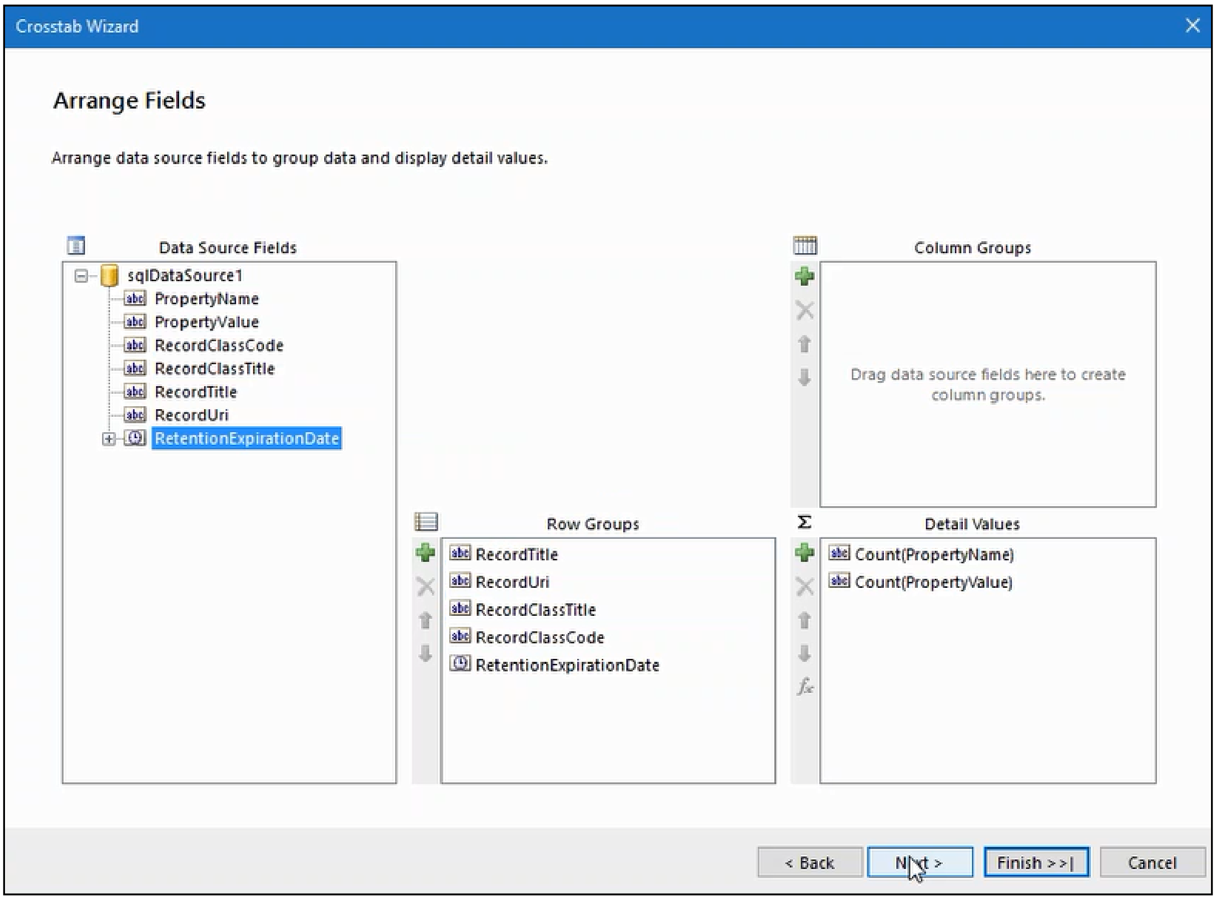
Name	DbType	Value
@startRange	DateTime	
@endRange	DateTime	

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.



Misc	
AllowBlank	**False**
AllowNull	False
AutoRefresh	False
AvailableValues	(none)
Mergeable	True
MultiValue	False
Name	**startRange**
Text	**Originated Date**
Type	**DateTime**
Value	**=Today()**
Visible	False

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 elipses 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**



Row Groups:
RecordTitle
RecordUri
RecordClassTitle
RecordClassCode
RetentionExpirationDate

Detail Values:
Count(PropertyName)
Count(PropertyValue)

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**.

8.7 Power BI

It is recommended that only those experienced with Power BI connect to the OData API for Gimmal Records with Power BI Desktop.

8.7.1 Connect to the OData API

8.7.2 Power BI Template

8.7.3 Connect to the OData API

ⓘ The steps in this article can be skipped by downloading the Power BI template from the Gimmal Records download site. If you don't have access to this site, please contact Gimmal Support.

The Gimmal Records OData API allows you to access reporting data in your Gimmal Records cloud tenant from reporting tools such as Excel, Tableau, and Power BI. This article walks you through connecting to the API with Power BI Desktop.

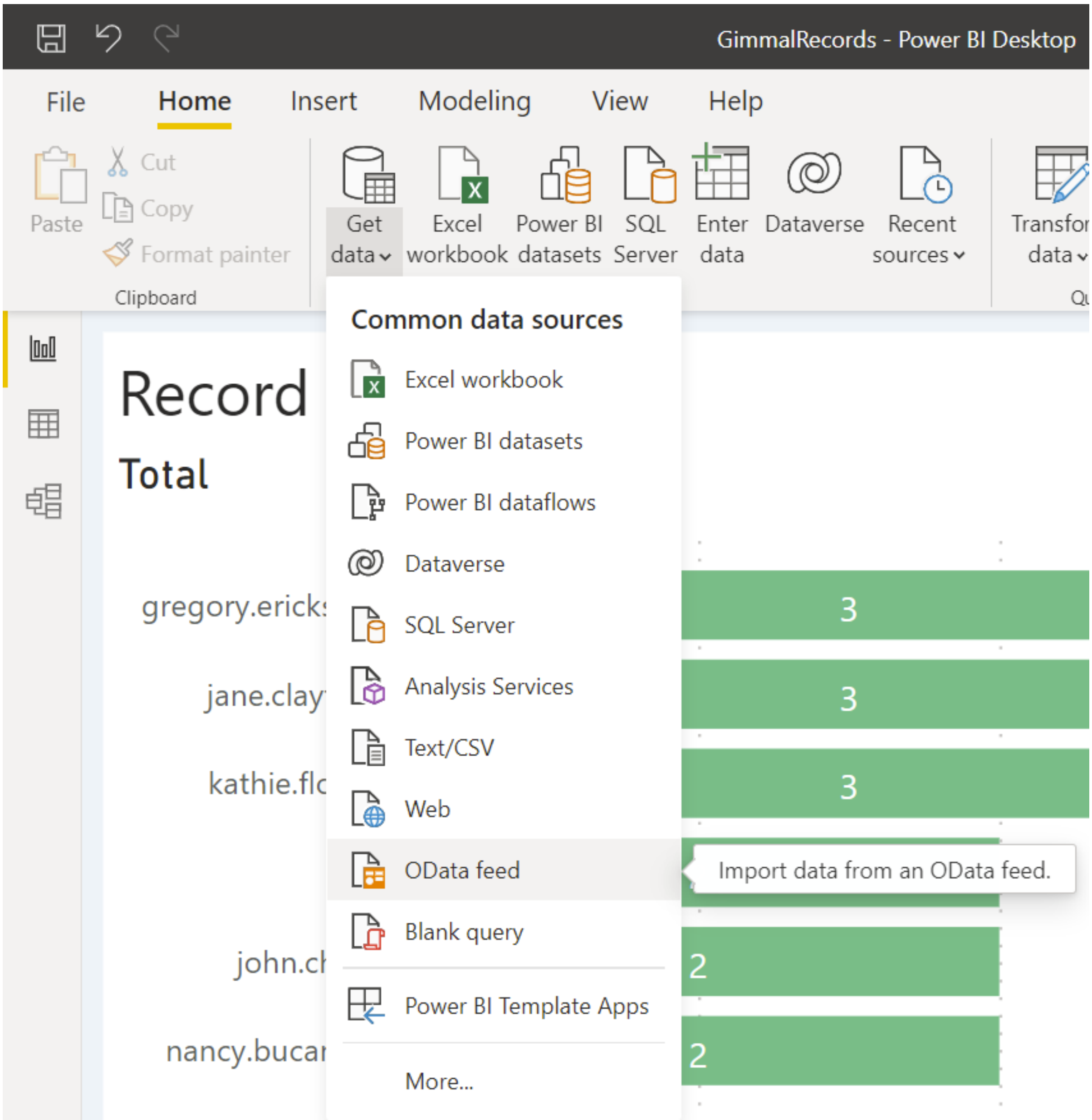
⚠ Currently reporting data is only available for production tenants, and is not available on test tenants.

8.7.3.1 Prerequisites

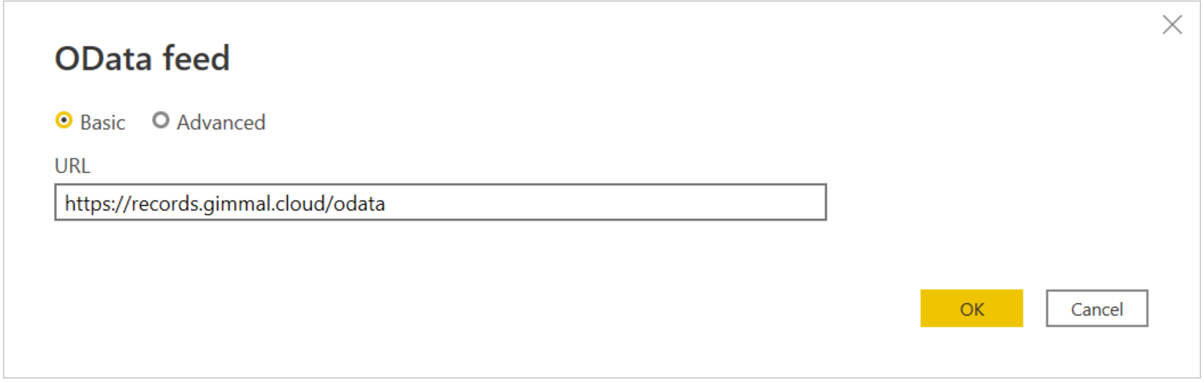
- Access to the Gimmal Records cloud service.
- The user name and password to a Service Account in the Gimmal Records cloud service.
- Advanced knowledge of Power BI Desktop.

8.7.3.2 Loading Data into Power BI

1. From the Home ribbon select Get Data | OData feed.



2. The OData feed window appears.



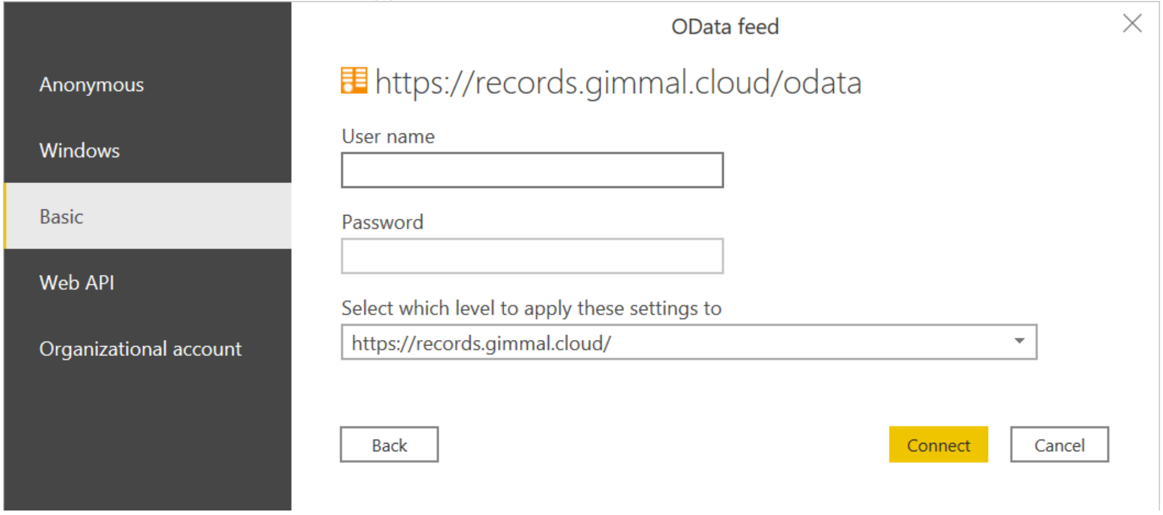
OData feed

● Basic ○ Advanced

URL

https://records.gimmal.cloud/odata

3. Enter the Uri for the Gimmal Records base OData endpoint (**https://records.gimmal.cloud/odata**) and click OK.
4. The authentication window will appear.



OData feed

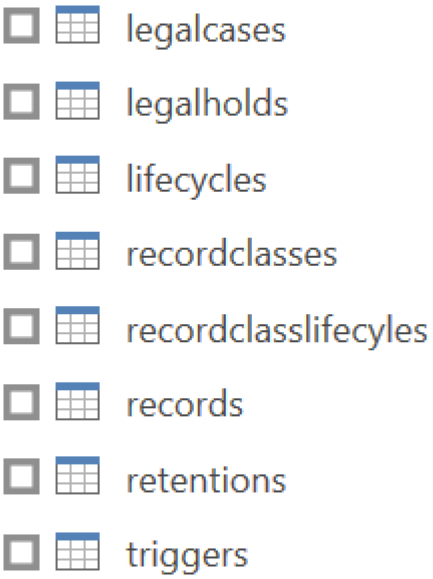
https://records.gimmal.cloud/odata

User name

Password

Select which level to apply these settings to: https://records.gimmal.cloud/

5. Select **Basic** authentication and enter the user name and password for a service account.
6. Ensure **https://records.gimmal.cloud/odata** is selected (rather than https://records.gimmal.cloud/) and click **Connect**.
7. The Navigator windows will appear.



□ legalcases

□ legalholds

□ lifecycles

□ recordclasses

□ recordclasslifecyles

□ records

□ retentions

□ triggers

8. Select the tables needed and click Load. If this is your first time connecting, it may be best to load all tables to get an understanding of the data.

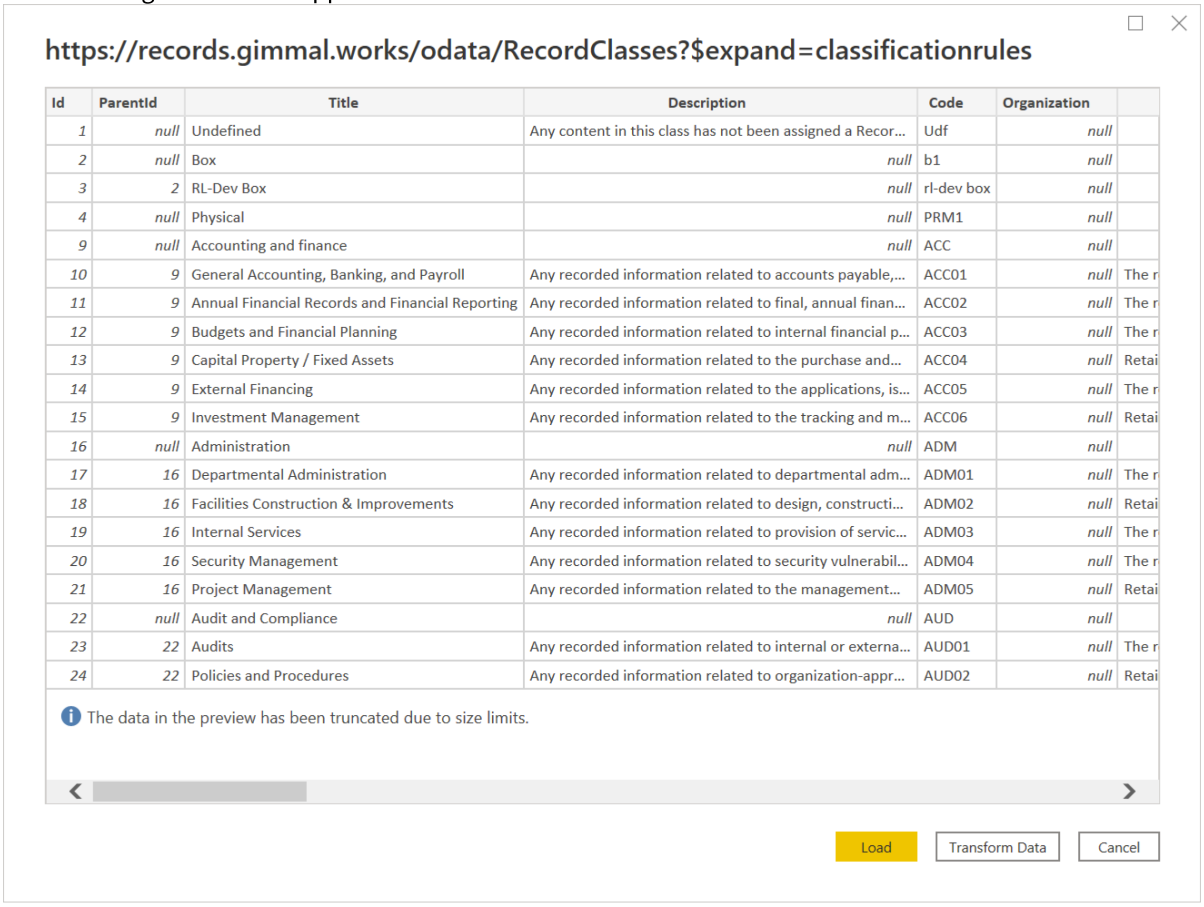
8.7.3.3 Loading related tables

The default OData API will give you basic information in Gimmal Records, however, there are also some related tables you may want to connect to. Use any of the following URLs to connect to the related data. *ODataAPI* is most likely **https://records.gimmal.cloud/odata.**

URL	Description
ODataAPI/RecordClasses?$expand=classificationrules	Record Class classification rules
ODataAPI/lifecycles?$expand=phases	Lifecycle phases
ODataAPI/legalcases?$expand=holdrules	Legal hold rules
ODataAPI/triggers?$expand=triggerrules	Trigger rules

Follow these steps to load a related table in Power BI Desktop:

1. From the Home ribbon select Get Data | OData feed (just like step one above.)
2. Enter the URL of the related table you need from the table above (*ODataAPI* is the base URL for the OData API) and click **OK**.
3. If you are asked for authentication, see step 4 above.
4. The following window will appear:

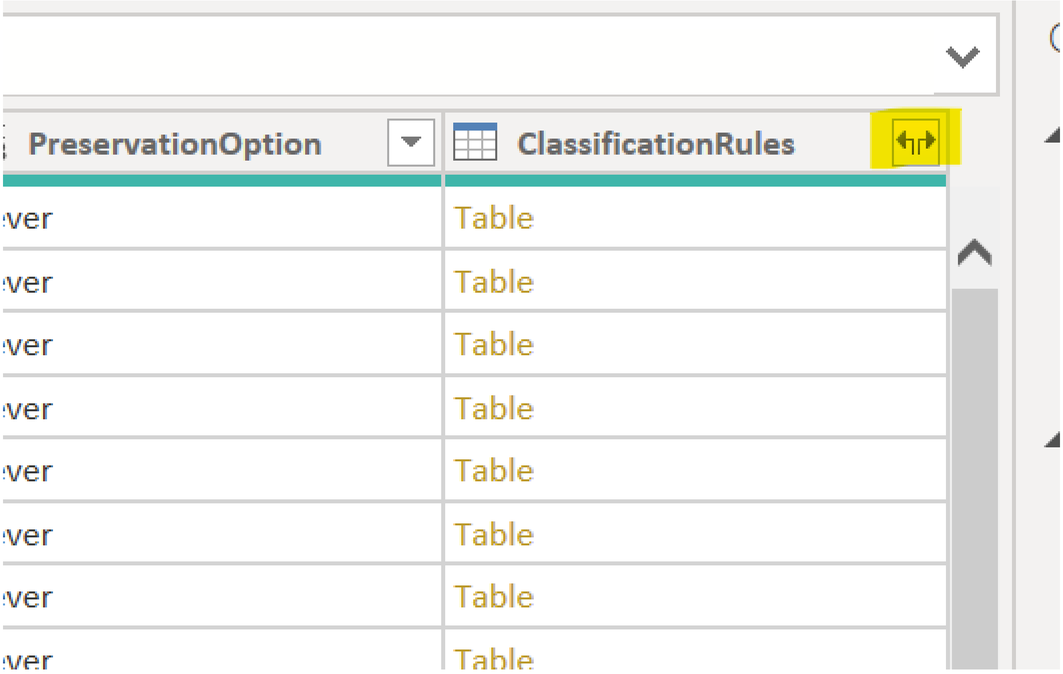


https://records.gimmal.works/odata/RecordClasses?$expand=classificationrules

Id	ParentId	Title	Description	Code	Organization	
1	null	Undefined	Any content in this class has not been assigned a Recor...	Udf	null	
2	null	Box	null	b1	null	
3	2	RL-Dev Box	null	rl-dev box	null	
4	null	Physical	null	PRM1	null	
9	null	Accounting and finance	null	ACC	null	
10	9	General Accounting, Banking, and Payroll	Any recorded information related to accounts payable,...	ACC01	null	The r
11	9	Annual Financial Records and Financial Reporting	Any recorded information related to final, annual finan...	ACC02	null	The r
12	9	Budgets and Financial Planning	Any recorded information related to internal financial p...	ACC03	null	The r
13	9	Capital Property / Fixed Assets	Any recorded information related to the purchase and...	ACC04	null	Retai
14	9	External Financing	Any recorded information related to the applications, is...	ACC05	null	The r
15	9	Investment Management	Any recorded information related to the tracking and m...	ACC06	null	Retai
16	null	Administration	null	ADM	null	
17	16	Departmental Administration	Any recorded information related to departmental adm...	ADM01	null	The r
18	16	Facilities Construction & Improvements	Any recorded information related to design, constructi...	ADM02	null	Retai
19	16	Internal Services	Any recorded information related to provision of servic...	ADM03	null	The r
20	16	Security Management	Any recorded information related to security vulnerabil...	ADM04	null	The r
21	16	Project Management	Any recorded information related to the management...	ADM05	null	Retai
22	null	Audit and Compliance	null	AUD	null	
23	22	Audits	Any recorded information related to internal or externa...	AUD01	null	The r
24	22	Policies and Procedures	Any recorded information related to organization-appr...	AUD02	null	Retai

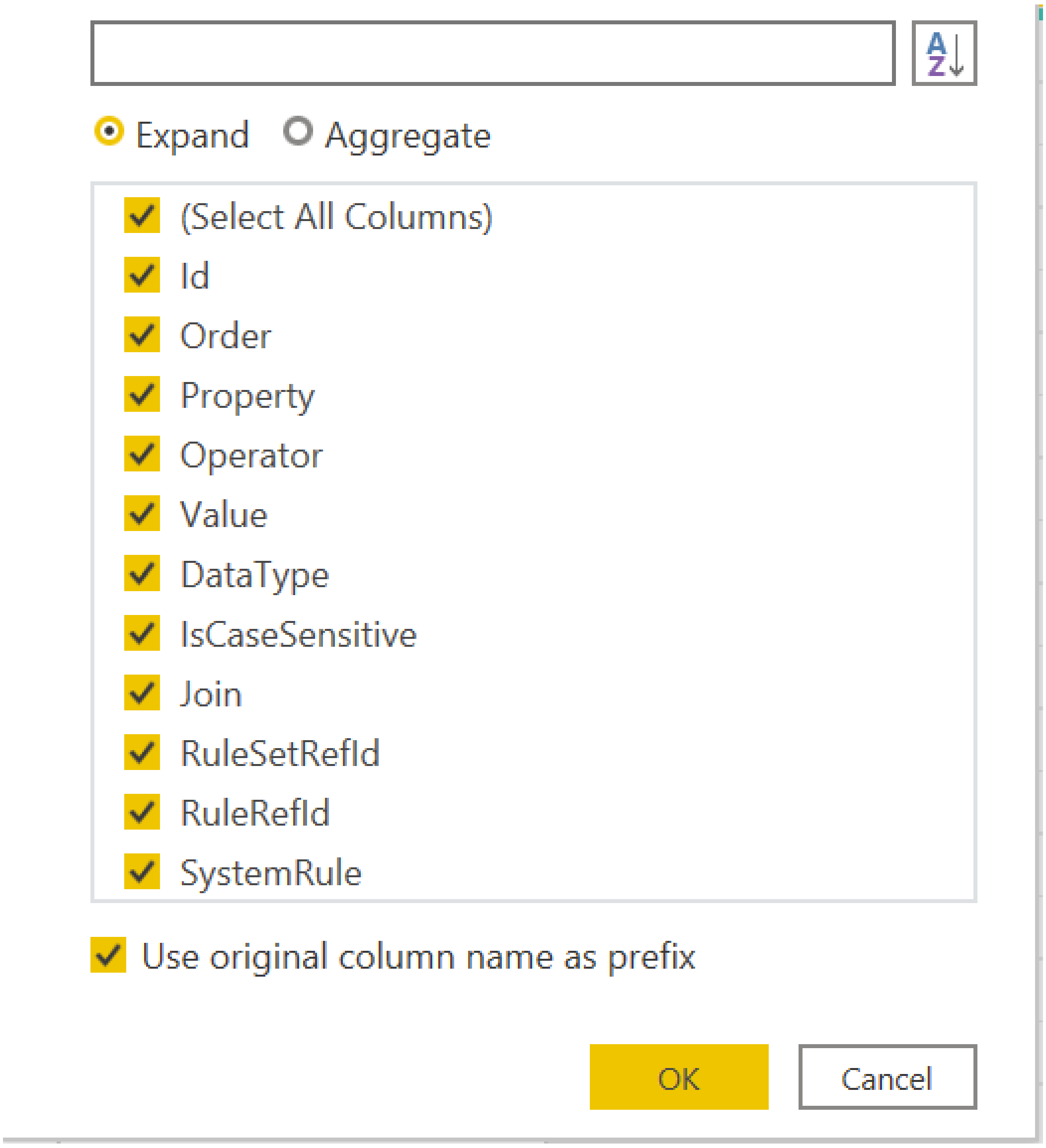
The data in the preview has been truncated due to size limits.

5. Select **Transform Data**.
6. The Power Query Editor will open. For any related table, you will need to expand the column listed in the URL, in this case, **ClassificationRules**.



PreservationOption	ClassificationRules
ver	Table
ver	Table
ver	Table
ver	Table
ver	Table
ver	Table
ver	Table
ver	Table

7. Click the highlighted button to expand the column. The following window will appear:



● Expand ○ Aggregate

☑ (Select All Columns)

☑ Id

☑ Order

☑ Property

☑ Operator

☑ Value

☑ DataType

☑ IsCaseSensitive

☑ Join

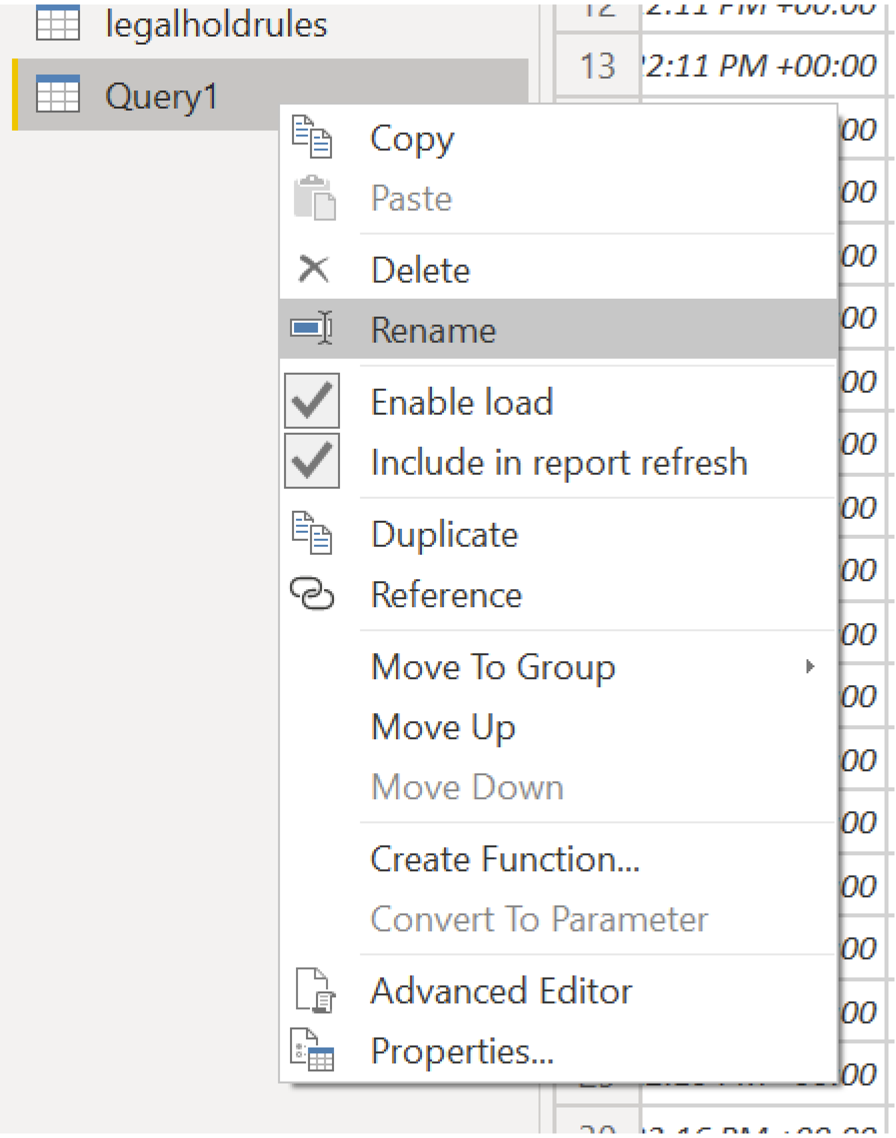
☑ RuleSetRefId

☑ RuleRefId

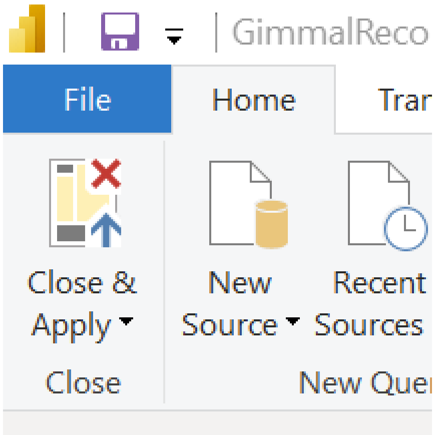
☑ SystemRule

☑ Use original column name as prefix

8. Unselect any columns you do not want to expand, however, if this is your first time using this data, it may be best to select them all. Click **OK**.
9. We recommend you rename the table (likely Query1) to something more user-friendly, such as **classificationrules**.



10. Click **Close and Apply** from the Home Ribbon in the Power Query Editor.

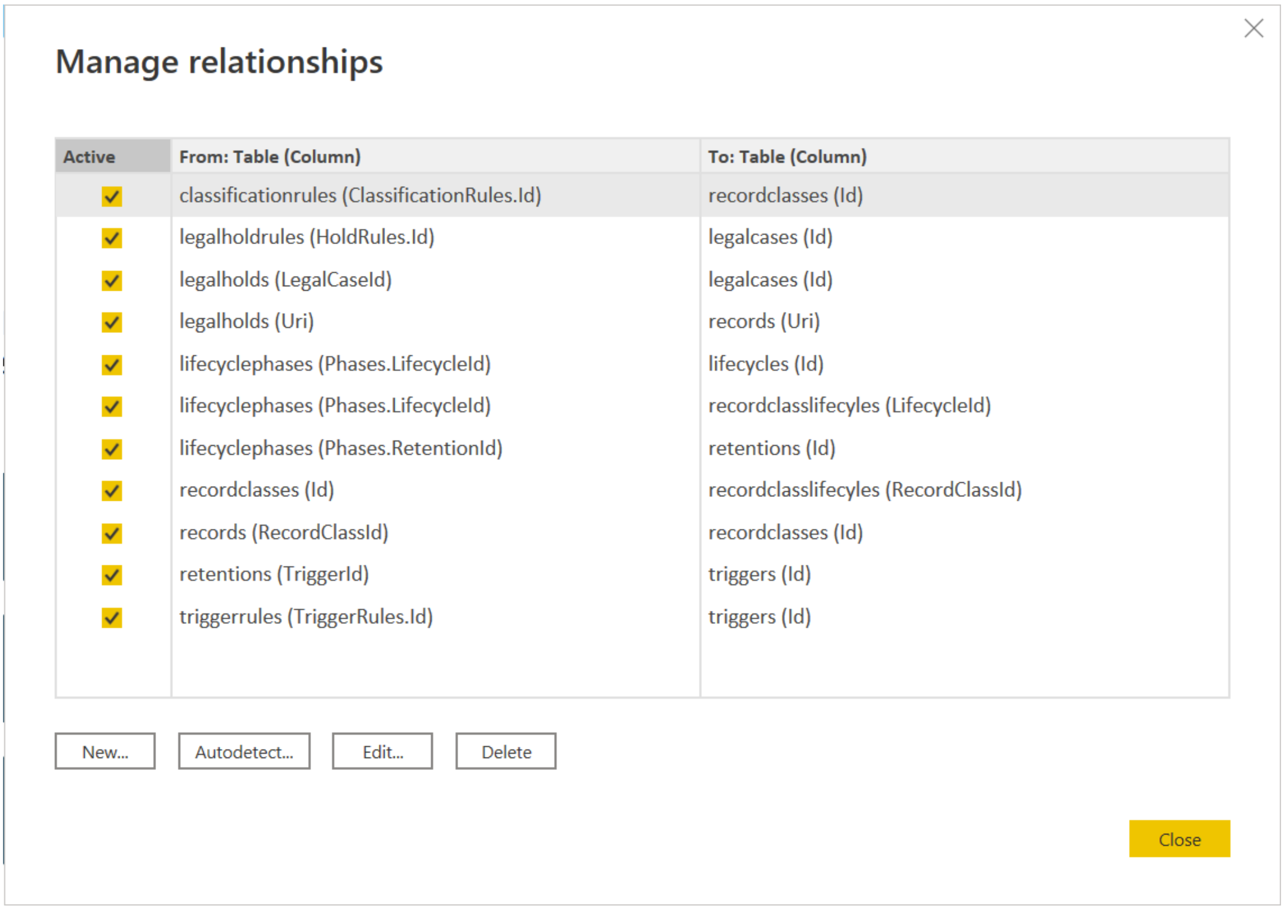


11. Your new table will be loaded into Power BI Desktop.

12. Repeat these steps for the other tables as necessary.

8.7.3.4 Managing Relationships

When loading the tables, Power BI Desktop will attempt to automatically create relationships. Unfortunately, it will most likely do this incorrectly for Gimmal Records. You will likely have to remove, modify, and create relationships manually. The correct relationships for all tables, including related tables should look similar to the following:



Manage relationships

Active	From: Table (Column)	To: Table (Column)
☑	classificationrules (ClassificationRules.Id)	recordclasses (Id)
☑	legalholdrules (HoldRules.Id)	legalcases (Id)
☑	legalholds (LegalCaseId)	legalcases (Id)
☑	legalholds (Uri)	records (Uri)
☑	lifecyclephases (Phases.LifecycleId)	lifecycles (Id)
☑	lifecyclephases (Phases.LifecycleId)	recordclasslifecyles (LifecycleId)
☑	lifecyclephases (Phases.RetentionId)	retentions (Id)
☑	recordclasses (Id)	recordclasslifecyles (RecordClassId)
☑	records (RecordClassId)	recordclasses (Id)
☑	retentions (TriggerId)	triggers (Id)
☑	triggerrules (TriggerRules.Id)	triggers (Id)

8.7.4 Power BI Template

A Power BI template is provided to simplify the process of connecting to and using the OData API. The template can be downloaded from the Gimmal Software Downloads site. If you need access to this site please contact Gimmal Support.

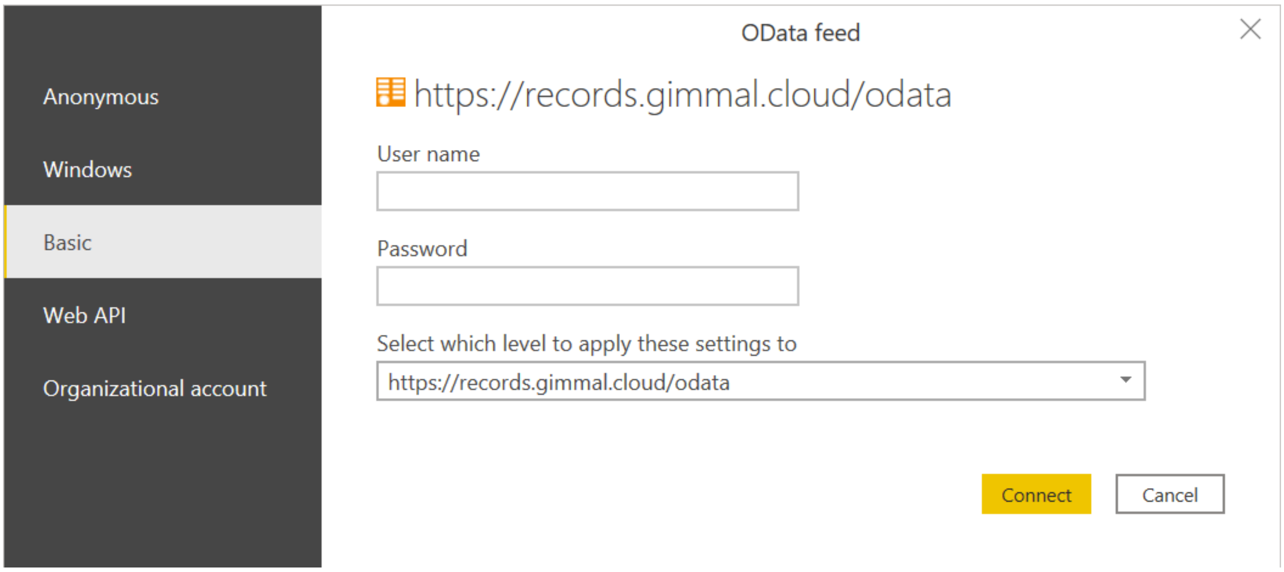
This template will automatically connect to primary data as well as the related tables.

8.7.4.1 Prerequisites

- Access to the Gimmal Records cloud service.
- The user name and password to a Service Account in the Gimmal Records cloud service.
- Gimmal Records Power BI template.
- Knowledge of Power BI Desktop.

8.7.4.2 Opening the Power BI template

Once downloaded, open the template in Power BI Desktop. You will be prompted with the following window to authenticate:



OData feed

https://records.gimmal.cloud/odata

User name

Password

Select which level to apply these settings to: https://records.gimmal.cloud/odata

Enter the user name and password of the Gimmal Records Service account.

Select **https://records.gimmal.cloud/odata** from the drop-down and click **Connect**.

You may be asked for the credentials more than once. If so just repeat the steps above.

8.7.4.3 Relationships

Relationships have been pre-created to show the proper relationships between tables.

8.7.4.4 Report Pages

The Power BI template provides four pages, each described in this section.

Dashboard

The Dashboard shows several high-level visuals focused on the current state of records in the system. This dashboard uses the following tables:

- records
- legalholds

Additional columns were created in Power Query to aid in creating visuals:

ExpiredDays	How many days have expired since retention has expired on a record, or blank if retention has not expired
FileName	Parsed from **PropertyBag**, it contains the name of file

FileSize	Parsed from **PropertyBag**, it contains the size, in bytes, of the file
Repository	Parsed from **PropertyBag**, it contains the repository a record exists in

Measures were created to help show some quick visual of records in the system:

DeclaredRecords	Uses **IsRecord** to count the number of declared records in the system
SumManagedFileSize	Uses **FileSize** and **RecordClassTitle** to sum the size of records that are classified to a Record Class
SumUnmanagedFileSize	Uses **FileSize** and **RecordClassTitle** to sum the size of records that are not classified to a Record Class

Records

The Records page displays a table of records meeting the criteria of the dropdowns in the header. By default, only manually classified records are displayed, however, you can also choose Obsolete, Superseded, Permanent, and Vital records.

> ⚠ This table could grow very large depending on the values selected. Be cautious of your selections.

Trigger Impact

The Trigger Impact page displays several tables. Moving from left to right, you can select elements of the File Plan and see which records are impacted. By default, the table will now show any records as that list could be extremely large.

An additional Measure was created (TriggerRetentionLifecycle) to prevent records from showing in the table until a File Plan element was selected.

File Plan Exceptions

The File Plan Exceptions page displays several lists showing potential exceptions in the File Plan.

- Record Classes without Classification Rules
- Record Classes without Lifecycles
- Triggers without Retentions
- Retentions without Lifecycles

9 Release Notes

9.1 December 2021 Sprint 66

9.2 November 2021 Sprint 64

9.3 July 2021 Sprint 57

9.4 June 2021 Sprint 54

9.5 February 2021

9.6 (5.21) Release Notes

9.7 (5.20) Release Notes

9.8 December 2021 Sprint 66

9.8.1 Release Date

December 3, 2021 (Sprint 66) Release

9.8.2 New Features

9.8.2.1 Record Overview

The Record Overview interface is a new landing page for a Record that displays the record details and encapsulates access to all records management functions.

The Record Overview Details tab provides detailed information pertaining to an individual record. From this screen you can see what Record Class a record has been assigned, where the record is in its Lifecycle, its Declaration status, its Legal Hold status, and if Preservation is enabled for that record. Users can copy and paste the link to this page for other users to reference.

This new User Interface has been provided to work with the new Manage Record functionality that will be forthcoming in Gimmal's new Microsoft 365 SharePoint Connector.

Formal introduction of this feature set will be covered in an upcoming blog post introducing the Microsoft M365 SharePoint Connector.

9.8.2.2 Preservation Copies

There is a new user interface setting to enable Preservation Copies on a Record Class in Gimmal Records to allow preservation of content to an Azure Blob Storage location. In this version - Preservation Copies will only function for SharePoint Online content for customers using Gimmal Records in the Cloud with Gimmal's new Microsoft 365 SharePoint Connector. Formal introduction of this feature set will be covered in an upcoming blog post introducing the Microsoft M365 SharePoint Connector.

9.8.3 Deprecated Features

None.

9.8.4 Resolved Issues

The following issues have been resolved in this release.

ID	Component	Description	Ticket #
65701	SharePoint Online Connector	The SharePoint Online feature In-place Records Management is now enabled by SharePoint Online Connector Service and will remain enabled on newly registered sites.	00011726
66122	SharePoint Online Connector	Added general optimizations for larger VMs in the cloud.	
64205	SharePoint Online Connector	Retention job will process an inactive site.	
63030	SharePoint Online Connector	Added general optimization: Incremental Classification processing.	
63139	SharePoint Online Connector	Record properties don't update in Core after moving a folder (> 1,000 files) from one site to a different site.	

9.9 November 2021 Sprint 64

9.9.1 Release Date

November 5, 2021 (Sprint 64) Release

9.9.2 New Features

This version is comprised entirely of minor bug fixes and improvements.

There are no new features to report in this release.

9.9.3 Deprecated Features

None.

9.9.4 Resolved Issues

The following issues have been resolved in this release.

ID	Component	Description	Ticket #
64103	Core	Fixed an issue where Destruction Certificate is incorrect if using multiple approval groups on a Record Class.	00011667
64205	SharePoint Online Connector	Added general optimization: Retention job and inactive sites.	
64220	SharePoint Online Connector	Added general optimization: Configurable timeout for RM Client used for sending a batch.	
63937	Core	User interface fix: Title field extends outside of Records Class Records dialog.	
61507	Core	User interface fix: Clicking the ellipsis in Inbox as a User causes error message.	
63534	SharePoint Online Connector	Added general optimization: Folder query LVT optimization.	
63953	SharePoint Online Connector	Resolved, unhandled exception while fetching pending action items while performing retention.	00011680
62869	Physical Records Management	Fixed PRM bug where menu options are missing from Container Dropdown.	

ID	Component	Description	Ticket #
61159	SharePoint Online Connector	Fixed bug where @folder token was not properly listing nested folders in SharePoint Online.	
62800	Physical Records Management	Fixed ambiguous reference to security object. Build error corrected. No functional change.	
63154	SharePoint Online Connector	Added logging to tenant controller and job control creation.	
62369	SharePoint Online Connector	Fixed issue with SPO Site Registration via API.	00011287

9.9.5 Known Issues

The following issues are known to exist at this time.

ID	Component	Description	Workaround
65433	Core	Manage Record log in "refused to connect" from Chrome browser.	This issue does not currently occur in Firefox or Microsoft Edge. If using Chrome, workaround is to log into Gimmal Records first and then navigating to the Manage Records button.
65408	Core	User can remove their own access which prevents them from logging in.	Gimmal Records users should use care to accidentally revoke their own access. Workaround would have a System Administrator restore the Users access.

9.10 July 2021 Sprint 57

9.10.1 July 2021 Cloud Release

9.10.1.1 Release Date

July 23, 2021 (Sprint 57) Release

9.10.1.2 New Features

This version is comprised entirely of minor bug fixes and improvements.

There are no new features to report in this release.

9.10.1.3 Deprecated Features

None

9.10.1.4 Resolved Issues

The following issues have been resolved in this release.

ID	Component	Description	Ticket #
60629	SharePoint Online Connector	Display full error message when logging updateexception from recordization api. Improved logging in App Insights.	N/A.
60628	SharePoint Online Connector	Remove obsolete code to update changeitemobjecttype. Removed code in the SPOC incremental crawl job to set the filesystemobjecttype of changeitems before reconciliation. This code was necessary when folder changes were treated as list changes, but that is no longer the case.	N/A.
60587	Core	Remove code to update RSA password encryption to AES. This code is no longer necessary.	N/A.
60773	SharePoint Online Connector	Manage Record Dialog won't load properly with '+' character in URI. Fixes issue where manage record dialog does not load in SharePoint Online when a record URI contains '+'.	00011025
60692	Core	Fixed an issue where Case Files were not selectable when creating an Event Occurrence target.	
60632	SharePoint Online Connector	Ensure users can always save a valid connection in SPOC web connection.	

ID	Component	Description	Ticket #
60630	SharePoint Online Connector	Set AES KeyValue for new tenants when password is saved.	
61021	Core	Improved logging in App Insights.	

9.10.1.5 Known Issues

The following issues are known to exist at this time.

ID	Component	Description	Workaround
59841	SharePoint Online Connector	Wrong error message displayed for Password. Incorrect SharePoint Online Password when deploying SharePoint Online Connector App Package results in "The App Catalog URL is invalid" message.	Ensure correct password is specified.
59540	Core	Inbox-Error with "Submit Approvals" button if filter on "Record Class" column for a Record Class that contains #. If a user filters their Dispose Inbox on a record class title that contains a # "Submit Approvals" does not work properly. Approvals on these records work when no filter is applied.	Ensure your record class does not use # in the title.
61099	SharePoint Online Connector	Plus sign missing in multiple property values @sp.folderurl @uri @uri_level_x. @sp.folderurl @uri @uri_level_x tokens do not contain the '+' sign when '+' sign is used in those parts of the URI in SharePoint Online.	None required.
61159	SharePoint Online Connector	Incorrect @folder token value when a file is in a folder that is not in the root directory of a document library. @folder token will display the incorrect value when the file is contained within a folder that is not in the root directory of a document library in SharePoint Online.	None available.

ID	Component	Description	Workaround
61238	Core	Case files don't leave Inbox if use "Approve & Submit" menu (Record Manager). In certain cases, where no approvers are set for a Case-Based Record Class, Record Managers can see Case Files ready for approval in the Inbox. However, using the inbox drop-down menu item for "Approve & Submit" does not work.	Add the Record Manager(s) as an approver to the Case-Based Record Class.

9.11 June 2021 Sprint 54

9.11.1 June 2021 Cloud Release

9.11.1.1 Release Date

June 18, 2021 (Sprint 54) Release

9.11.1.2 New Features

Gimmal E-mail Service

For Gimmal Cloud customers who wish to receive email notifications, this Email Service is a new option that allows a customer to bypass use of their own email delivery service settings to instead utilize Gimmal's built-in email service.

When enabled this email service will be used for communications sent by Gimmal Records for our Cloud customers.

Please ensure that if your organization has any email security settings for spam or junk notifications that you need to whitelist "no-reply@gimmal.com[117]".

9.11.1.3 Performance

SharePoint Online Connector Optimizations

A number of performance optimizations have been implemented in the SharePoint Online Connector. These optimizations will enhance and address performance around incremental classification. In addition, an automatic retry to Activate sites that have gone Inactive due to previous error has been added.

Monitor Tab

Today the Monitor Tab in Gimmal Records provides a summary of Records by Repository and summary of Top Record Classes in use (also known as dashboard of KPIs).

[117] mailto:no-reply@gimmal.com

Prior to this release the information on the Monitor Tab / dashboard was updated automatically whenever the page was accessed causing performance issues reported by customers. New for this release the Monitor Tab page is now cached and updated once every 24 hours. If a user wishes to locate a new Record they can continue to locate the Record in real-time from the Manage Tab.

9.11.1.4 Resolved Issues

The following issues have been resolved in this release.

ID	Component	Description	Ticket #
59381	SharePoint Online Connector	Fixed issues with folder restores not being processed and item modifications not being processed if the items were indirectly deleted.	

9.11.1.5 Known Issues

The following issues are known to exist at this time.

ID	Component	Description	Workaround
59021	Core	When a record class has closed all records in that record class are re-assigned to another record class.	None.
59540	Core	If a user filters their Dispose Inbox on a record class title that contains a # "Submit Approvals" does not work properly.	Ensure your record class does not use # in the title.
59841	Core	Incorrect SharePoint Online Password when deploying SharePoint Online Connector App Package results in "The App Catalog URL is invalid" message.	None required.
59825	Core	Record class originated date time may be off when user changes their preference for Time Zone in "My Preferences" other than UTC may result in times not matching the current user's time.	Ensure current user time preference is set to UTC.
59812	Core	If an automatic record declaration occurs on a record after it has already been declared a record (manual declaration) the Audit trail has repeating entries for "Skipped Declare Record Action".	None required.

9.12 February 2021

9.12.1 Release Date

February 28, 2021

9.12.2 User interface updates

- Sign out moved to drop down under signed-in user
- Main menu icons have changed
- Inbox item on the main menu has been replaced with Dispose
- Disposition inbox has been moved to a navigation menu under Dispose
- Expired Records has been added as a navigation menu under Dispose
- Rejected Records has been added as a navigation menu under Dispose
- Physical Confirmation has been added as a navigation menu under Dispose
- Exceptions has been added as a navigation menu under Dispose
- Destruction Certificates has been moved from Monitor to Dispose
- Archive has been renamed Disposed Records and moved to Dispose
- The ability to Filter on columns has been added to the Inbox
- The ability to Sort on Record Class and Expiration Date has been added to the Inbox
- The ability to add and remove columns has been added to the Inbox
- The ability to rearrange columns has been added to the Inbox
- The ability to save and reopen views has been added to the Inbox
- The ability to take action on items in bulk has been added to the Inbox
- The ability to add items to a legal hold has been added to the Inbox
- The ability to reclassify records has been added to the Inbox
- Checking an item no longer directly approves it in the Inbox, and now requires a second mouse click
- Dismiss has been renamed to Pause throughout the application
- The Pause (previously Dismiss) duration when creating/editing a Lifecycle is no longer visible until the Require Approval box is checked

9.12.3 New features

9.12.3.1 Global Record Manager Role

This new role replaces the previous Records Manager role and gives access to records regardless of the Record Filters. Upon upgrade, all users with Record Manager roles will be converted to Global Record Manager. The Record Manager role going forward will be subject to Record Filters.

9.12.3.2 Records 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 a 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.

Learn more about Record Filters.(see page 415)

9.12.3.3 Inbox

The disposition inbox has been relocated to a navigation menu under the Dispose on the main menu. The inbox no longer allows users with the Record Manager role to see items in the inbox that have an approval group they are not a member of.

9.12.3.4 Expired Records

The Expired Records area shows all records that have expired or are nearing expiration.

9.12.3.5 Rejected Records

A new feature to reject records during disposition has been created. When a record is rejected, it will move to an area that can be accessed via the Rejected Records navigation under Dispose. These records cannot be approved for disposition until they are reinstated.

Learn more about Rejected Records.(see page 133)

9.12.3.6 Physical Confirmation

Physical records that have been approved for disposition will show up under Physical Confirmation and await to be completed. The purpose of this area is to verify that the records have been destroyed since that action cannot be taken automatically. These verifications previously were displayed in the Inbox.

9.12.3.7 Exceptions

The Exceptions area shows exceptions that may have happened during the disposition process, such as not being able to remove content from a repository during the Dispose and Delete action. These actions previously were displayed in the Inbox.

9.12.3.8 Custom Inbox Columns

Previously custom columns could only be added to the Inbox globally. These can now be added per user under Settings → My Preferences. Custom columns can then be added and removed from a view in any of the disposition areas.

9.12.4 Performance

Many performance improvements have been made to the cloud service to improve most aspects of the system. The most noticeable improvements will be when using the Inbox with large amounts of expired records.

9.12.5 Upgrading

9.12.5.1 Connectors

When using the Gimmal cloud it is recommended to upgrade the connectors as soon as possible after the service has been updated. If you are reading this before the service has been upgraded, please wait until the Gimmal cloud service is updated before upgrading your connectors.

The connectors are no longer part of the core installer, and each has a separate ISO to download and install.

9.12.6 Deprecated features

- Internet Explorer is no longer supported
- SharePoint 2010 is no longer supported
- The File Share Connector is not supported with this release. It has been replaced with the Universal File Share Connector.

9.12.7 Resolved issues

The following issues have been resolved in this release.

ID	Component	Description	Ticket #
38032	SharePoint Online Connector	Destruction Certificate and Archive records not created for SharePoint records	20123

9.12.8 Known issues

The following issues are known to exist at this time.

ID	Component	Description	Workaround
52054	Core	When a record is ready for manual transfer in Physical Confirmation, if the user clicks the Complete button at the top of the screen, the user is not given the option to enter an updated URL.	Use the drop-down menu next to each record in the Physical Confirmation view and click Complete.
51914	Core	Case base record classes with Record Declaration set to Never still allow users to choose the Declare Record option for records.	Do not declare the individual records of a case, declare the case itself.

ID	Component	Description	Workaround
51885	Core	When creating a Legal Hold and no legal cases are available if a user clicks Confirm an error is presented in the web browser's developer console.	No workaround is necessary.
51790	Core	Assigned Record Filters for a user do not show assignments via Group Membership in the Secure page.	View the individual user accounts to see assigned Record Filters.
51613	Documentum Connector	The rest connector does not use paging for the incremental job. Page size is sent as a param, but it is not used. This can cause out of memory errors when there are many changes returned from the changelog query.	A full crawl does use paging and will resolve the problem.
51558	Box Connector	When completing the Records Management Configuration for the Box Connector, clicking Save more than once can result in multiple configuration entries in the Box Connector database.	Leave the page and coming back will load the form with saved data, and the page will update the existing entry as expected.
51694	SharePoint Server Connector	In rare occurrences, a new record that falls under an existing legal hold might not get locked.	Run Force Processing of All Items resolves the issue.
51338	Core	In rare occurrences, deleting a record class generates an error in the web browser's developer console.	No workaround is necessary, record class is still deleted.
49042	Reports	Bar Graph data in the Approaching Phase Expiration report can take up multiple pages when there are many items in the report.	None.

9.13 (5.21) Release Notes

9.13.1 Bug Fixes

- Gimmal Records - Failed actions now reliably appear on the Exceptions Page.
- Gimmal Records - Users with single quotes can be searched on the Users page.
- Gimmal Records - Users can no longer classify a Record into a Closed Case File.

- Gimmal Records - Action items are now removed for any records when removing their Lifecycle from a Record Class.
- Gimmal Records - Removed unnecessary modal when deleting a Record Class.
- Gimmal Records - Rejected Inbox items remain rejected if lifecycle changes on Record Class.
- Gimmal Records - When a rule set is changed, Permission Group Rules are changed correctly.
- Gimmal Records - When Inbox Items are submitted for approval, physical records are not submitted as well for approval.
- Gimmal Records SDK - GetRecordsForRecordClass returns all Record Classes.
- Gimmal Records - Only System Admins and the master 'Administrator' account can now create or edit Record Filters
- Gimmal Records - Bulk Manual Classifications are not logged with Audit Entries.
- Gimmal Records - Various guards against SQL Injection added

9.13.2 SharePoint Online Connector

- Ability to explicitly specify whether a SharePoint Library should be crawled or ignored
- Ability to configure the number of workers and the batch sizes for retention jobs.

9.13.3 Known Issues

- For the ability to explicitly specify whether a SharePoint Library should be crawled or ignored
    - “Remove Records” Post Action Override doesn't trigger for Libraries with spaces in them.
    - The validation message displays "Local" instead of the SharePoint domain name in the single-tenant context.
    - Create override dialog sometimes freezes on the initial load.

9.13.4 Upgrading

The installer for all components can be found on the Gimmal software download site[118].

9.13.4.1 Core Service

The core service can only be upgraded from version 5.1. Any previously supported version can be upgraded to 5.1.

It is recommended to stop all connectors before upgrading the core service.

9.13.5 End of support update

See Gimmal end of life notifications[119]

[118] https://gimmal1.sharepoint.com/sites/EXT-download/SitePages/Home.aspx
[119] https://gimmal1.sharepoint.com/sites/EXT-Software/SitePages/Upcoming-End-of-Life-Notification.aspx

9.14 (5.20) Release Notes

9.14.1 Documentum Connector

- Implemented clickable DRL Links.
- Implemented URI Levels for Documents via Webtop.

9.14.2 SharePoint Online Connector

- Retry count increments correctly.
- Refactored retry logic.
- Added ELMAH logs for cloud customers.
- Corrected error while getting file during retention.
- Retention jobs now will not stop as a result of an exception raised.
- Removed error when changing pages and searching for a user on the Permissions dialog for a Record Class.
- Fixed updates for expired change tokens.