



# Administration Guide

## Compliance Suite File Plan Builder (Feature-Activated)

For SharePoint 2013/2016

Software Version 4.13.1

January 2019

Title: *Compliance Suite File Plan Builder Administration Guide*

© 2019 Gimmel LLC

Gimmel® is a registered trademark of Gimmel Group.

Microsoft® and SharePoint® are registered trademarks of Microsoft.

Gimmel LLC believes the information in this publication is accurate as of its publication date. The information in this publication is provided as is and is subject to change without notice. Gimmel LLC makes no representations or warranties of any kind with respect to the information contained in this publication, and specifically disclaims any implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any Gimmel software described in this publication requires an applicable software license. For the most up-to-date listing of Gimmel product names and information, visit [www.gimmel.com](http://www.gimmel.com). All other trademarks used herein are the property of their respective owners.

If you have questions or comments about this publication, you can email [TechnicalPublications@Gimmel.com](mailto:TechnicalPublications@Gimmel.com). Be sure to identify the guide, version number, section, and page number to which you are referring. Your comments are welcomed and appreciated.

# Contents

- Chapter 1. Introduction ..... 1**
- 1.1 Who Should Use This Guide ..... 1
- 1.2 Important Notes about this Guide ..... 1
  - 1.2.1 File Plan Builder Users ..... 1
- 1.3 Getting Started..... 2
  - 1.3.1 File Plan Builder Records Manager Features..... 2
  - 1.3.2 Compliance Suite File Plan Builder Administrator Features..... 3
  - 1.3.3 Accessing File Plan Builder..... 3
- Chapter 2. Permission Roles..... 5**
- 2.1 Permission Roles List ..... 6
- 2.2 Creating a Permission Role ..... 6
- 2.3 Permission Assignment Configuration ..... 7
- 2.4 Viewing a Permission Role ..... 13
- 2.5 Editing a Permission Role ..... 13
- 2.6 Deleting a Permission Role ..... 14
- 2.7 Permission Roles Permission Assignment..... 15
- Chapter 3. File Plan Structure ..... 16**
- 3.1 Before You Create a File Plan Structure ..... 16
- 3.2 File Plan Nodes List ..... 17
- 3.3 Adding a New File Plan Node ..... 18
- 3.4 Viewing a File Plan Node ..... 27
- 3.5 Editing a File Plan Node ..... 27
- 3.6 Copying a File Plan Node ..... 29
- 3.7 Deleting a File Plan Node ..... 29
- 3.8 Obsoleting a File Plan Node ..... 30
- 3.9 Auditing a File Plan Node ..... 30
- 3.10 File Plan Nodes Permission Assignment ..... 32

<b>Chapter 4. Periods .....</b>	<b>34</b>
4.1 Periods List .....	34
4.2 Adding a New Period .....	35
4.3 Viewing a Period .....	37
4.4 Editing a Period .....	38
4.5 Deleting a Period .....	39
4.6 Periods Permission Assignment.....	39
<b>Chapter 5. Cutoff Events.....</b>	<b>40</b>
5.1 Accessing the Events List .....	41
5.2 Cutoff Events List.....	41
5.3 Adding a New Cutoff Event .....	41
5.4 Viewing a Cutoff Event.....	42
5.5 Editing a Cutoff Event.....	42
5.6 Deleting a Cutoff Event.....	43
5.7 Cutoff Events Permission Assignment.....	44
<b>Chapter 6. Disposition Actions .....</b>	<b>45</b>
6.1 Disposition Actions List .....	46
6.2 Adding a New Disposition Action .....	46
6.3 Viewing a Disposition Action .....	47
6.4 Editing a Disposition Action .....	47
6.5 Deleting a Disposition Action .....	48
6.6 Disposition Actions Permission Assignment.....	49
<b>Chapter 7. Disposition Instructions.....</b>	<b>50</b>
7.1 Disposition Instructions Permission Assignment .....	50
7.2 Disposition Instructions List.....	51
7.3 Creating a Disposition Instruction.....	52
7.3.1 <i>Using Aging Method Cutoff in Disposition Instructions</i> .....	52
7.3.2 <i>Adding a Stage for a Cutoff Disposition Instruction</i> .....	53

7.3.3 Using Alternate Aging Calendar in Disposition Instructions .....	54
7.3.4 Adding a Stage for an Alternate Aging Disposition Instruction .....	55
7.3.5 Using Alternate Aging Enterprise Events in Disposition Instructions.....	58
7.3.6 Adding a Stage for an Enterprise Event Alternate Aging Disposition Instruction.....	60
7.4 Viewing a Disposition Instruction.....	62
7.5 Editing a Disposition Instruction.....	62
7.6 Copying a Disposition Instruction.....	63
7.7 Deleting a Disposition Instruction.....	63
<b>Chapter 8. Legal Authorities .....</b>	<b>64</b>
8.1 Legal Authorities List .....	64
8.2 Creating a New Legal Authority.....	65
8.3 Viewing a Legal Authority.....	66
8.4 Editing a Legal Authority.....	66
8.5 Deleting a Legal Authority.....	67
8.6 Legal Authorities Permission Assignment.....	67
<b>Chapter 9. Legal Requirements.....</b>	<b>69</b>
9.1 Legal Requirements List .....	69
9.2 Creating a New Legal Requirement.....	70
9.3 Viewing a Legal Requirement .....	72
9.4 Editing a Legal Requirement .....	72
9.5 Deleting a Legal Requirement .....	73
9.6 Legal Requirements Permission Assignment.....	74
<b>Chapter 10. Pending Legal Changes.....</b>	<b>75</b>
10.1 Pending Legal Changes Permission Assignment .....	78
<b>Chapter 11. File Plan Report .....</b>	<b>79</b>
11.1 File Plan Report View .....	80
11.1.1 Running a File Plan Report.....	80
11.2 File Plan Report Permission Assignment.....	82

<b>Chapter 12. File Plan Builder Export .....</b>	<b>84</b>
12.1 Exporting Artifacts from File Plan Builder .....	84
<b>Chapter 13. File Plan Builder Import.....</b>	<b>87</b>
13.1 Importing Artifacts.....	87
<b>Chapter 14. Security Groups .....</b>	<b>93</b>
14.1 Security Groups List.....	93
14.2 Creating a New Security Group .....	94
14.3 Viewing a Security Group.....	95
14.4 Editing a Security Group.....	95
14.5 Deleting a Security Group.....	96
14.6 Security Groups Permission Assignment.....	96
<b>Chapter 15. Supplemental Markings.....</b>	<b>97</b>
15.1 Supplemental Markings List.....	98
15.2 Adding a New Supplemental Marking.....	98
15.3 Viewing a Supplemental Marking.....	99
15.4 Editing a Supplemental Marking.....	100
15.5 Deleting a Supplemental Marking.....	101
15.6 Supplemental Markings Permission Assignment.....	101
<b>Chapter 16. Audit Log .....</b>	<b>102</b>
16.1 Audit Context Types and Actions.....	103
16.2 Using the Audit Log.....	104
16.3 Filtering Audit Log Entries.....	105
16.4 Audit Log Permission Assignment.....	106
<b>Chapter 17. File Plan Association .....</b>	<b>107</b>
17.1 File Plan Association Regions .....	107
17.2 Completing a File Plan Association .....	109
17.2.1 File Plan Builder to SharePoint Mapping.....	110

<b>Chapter 18. Association Templates .....</b>	<b>115</b>
18.1 Association Templates Features .....	116
18.2 Association Templates Permission Assignment .....	117
18.3 Configuring File Plan Templates.....	117
18.3.1 <i>Creating a New File Plan Template</i> .....	117
18.3.2 <i>Editing a File Plan Template</i> .....	125
18.3.3 <i>Deleting a File Plan Template</i> .....	126
18.4 Configuring Site Groups .....	126
18.4.1 <i>Creating a New Site Group</i> .....	126
18.4.2 <i>Editing a Site Group</i> .....	129
18.4.3 <i>Deleting a Site from a Site Group</i> .....	130
18.4.4 <i>Deleting a Site Group</i> .....	130
18.5 Committing a Site Group to Create File Plan Associations .....	131
18.6 Instantiating by Group .....	132
18.7 Performing Associations by Query .....	133
<b>Chapter 19. Instantiation Logs.....</b>	<b>137</b>
19.1 Viewing Instantiation Logs.....	137
<b>Chapter 20. Troubleshooting .....</b>	<b>139</b>
20.1 Login Issues .....	139
20.2 Access Denied Error.....	139
<b>Appendix A. Chunking Files for Easier Import .....</b>	<b>141</b>
A.1 Chunking Large Files for Easier Import.....	141
A.1.1 <i>Size of Files</i> .....	141
A.1.2 <i>File Contents</i> .....	141

# 1 Introduction

Gimmel delivers market-leading content governance and compliant records solutions built on Microsoft® SharePoint®. Gimmel solutions drive user adoption and simplify information access by making information lifecycle management of content simple and transparent, ensuring consistent compliance and proactive litigation readiness enterprise-wide while lowering costs.

The Gimmel Compliance Suite application works seamlessly with SharePoint to provide your organization a reliable and centralized repository for collaboration and records management that is compliant with the standards of the Department of Defense (DoD) 5015.2 [Records Management Program](#).

Gimmel Compliance Suite File Plan Builder is a tool to create and manage a file plan that supports your organization's records management policies. A file plan is a classification scheme that describes how records are organized, retrieved, retained, and dispositioned in your organization. The file plan is an essential component of a successful records management program.

## 1.1 Who Should Use This Guide

This guide is intended to be used by beginning and advanced users of the Gimmel Compliance Suite File Plan Builder. All users must have a basic knowledge of SharePoint functionality. This manual contains step-by-step instructions for using File Plan Builder.

## 1.2 Important Notes about this Guide

The following notes explain important information about the use of File Plan Builder and this guide:

- All illustrations are intended as examples and will vary depending on the configuration of your installation.
- This manual is targeted toward the following classifications of users:
  - Records Manager
  - Compliance Suite Administrator

### 1.2.1 File Plan Builder Users

The intended users for File Plan Builder vary by feature and have two roles:

- Record Managers
- Compliance Suite Administrators



## 1.3 Getting Started

To use File Plan Builder features, Gimmel Compliance Suite must be installed in a SharePoint Records Center and the Gimmel Compliance Suite File Plan Builder feature must be active. Also, you must be a member of the File Plan Builder Users SharePoint group.

---

### Note

When using Internet Explorer 11 to access File Plan Builder, the application does not display correctly. The workaround for this is to disable (turn off) the "Display Intranet sites in Compatibility View" option on the **Compatibility View Settings** dialog in Intranet Explorer.

---

### 1.3.1 File Plan Builder Records Manager Features

File Plan Builder Records Manager features include:

- **File Plan Structure:** Manages the file plan structure and nodes.
- **Periods:** Manages cutoff, vital records, and disposition processing periods that are available for assignment to your file plan nodes.
- **Cutoff Events:** Manages cutoff and disposition processing events that are available for assignment to your file plan nodes.
- **Disposition Instructions:** Manages disposition processing instructions that are available for assignment to your file plan nodes. Also allows you to select cutoff or alternate aging for the aging method.
- **Legal Justifications:** Manages the groups with legal authorization to manage the disposition or transfer of records that are available for assignment to your file plan nodes.
- **Legal Requirements:** Manages the code of laws based on your organization's legal jurisdiction that are available for assignment to your Legal Authorities.
- **Pending Legal Changes:** Displays all file plan nodes assigned a Disposition Authority that is based on a Legal Requirement with a Requirement Status set to New, Updated, or Superseded. Supports the management of the Legal Requirement Citation Lifecycle.
- **View Reports:** Views File Plan Reports, which include details for all or selected file plan nodes.
- **Export File Plan:** Provides .xml export of your detailed file plan information.
- **Import File Plan:** Imports .xml files created by the Export File Plan operation.
- **Association Templates:** Enables you to create, edit, or delete templates that associate File Plan Builder nodes in the File Plan Structure to libraries referenced by name, or alternatively to all Compliance Suite-enabled libraries across an organization.

File Plan Builder features listed are described in detail in this administration guide and online in the File Plan Builder application.

### 1.3.2 Compliance Suite File Plan Builder Administrator Features

Administrator features include:

- **Security Groups:** Manages the SharePoint groups and their corresponding Permission Role assignments that enable access to individual features in File Plan Builder.
- **Permission Roles:** Manages the roles that are granted access to individual features in File Plan Builder. Permission Roles are available for assignment to your Security Groups and File Plan Node Security.
- **Disposition Actions:** Manages the technical parameters (actions) that are available for assignment to your disposition instructions.
- **Supplemental Markings:** Manages the security feature that enables site column content to restrict unauthorized users from accessing records. Supplemental Markings are available for assignment to your file plan node.
- **File Plan Association:** Enables a user to map file plan node(s) to one or more Record Libraries across multiple sites and site collections.
- **Audit Log:** Views, exports, and/or removes audit log entries for user actions performed in File Plan Builder.
- **Instantiation Log:** Shows a filtered view of the Gimmel logs so that you can easily see if something went wrong in an instantiation. It also logs start and finish times as two separate entries to show when instantiation finished, and the elapsed time.

### 1.3.3 Accessing File Plan Builder

To access File Plan Builder:

1. Open a **SharePoint Records Center** with Compliance Suite installed. The *Records Center Home Page* opens.
2. There are two ways to access File Plan Builder:
  - In SharePoint, click **File Plan Builder** on the Compliance Suite header ribbon.

- In SharePoint, select **Settings** and then **Site Settings**. In Site Settings, select **File Plan Builder** under the Compliance Suite section.

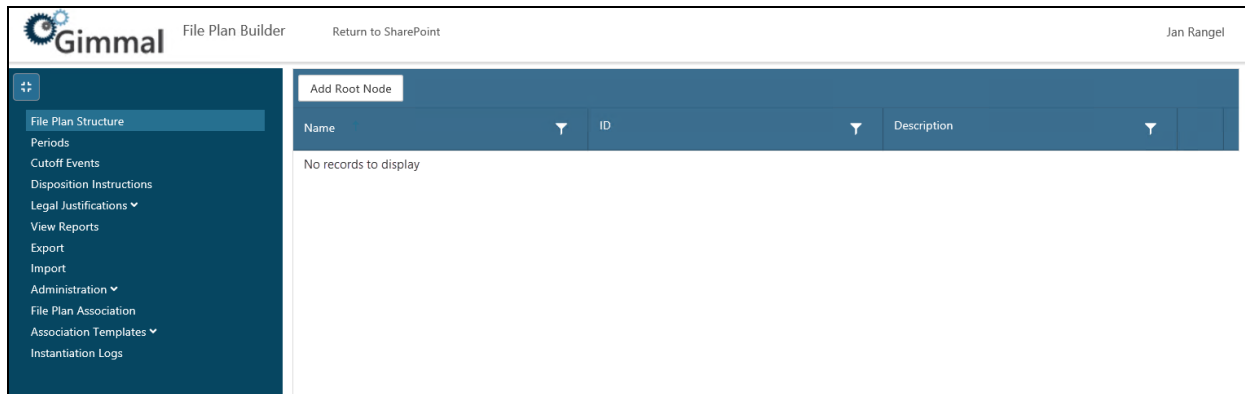


Figure 1-1 File Plan Builder Main Screen

## 2 Permission Roles

Permission Roles features are available in a SharePoint Records Center with Gimmal Compliance Suite enabled. To use the Permission Roles features in File Plan Builder, Gimmal Compliance Suite must be installed and the Gimmal File Plan Builder feature must be active. In addition, you must have the proper Permission Roles assigned; see [2.7 Permission Roles Permission Assignment](#).

Before end users, such as Records Managers, can use File Plan Builder features, the Compliance Suite Administrator must create and assign Permission Roles. Permissions Roles define security access to specific features in File Plan Builder. A Permission Role is a prerequisite step for Security Groups, which grant SharePoint groups access based on the Permission Roles Assignment. In addition, Permission Roles are used to set item-level security on file plan nodes. Permission Roles security can be configured for the following File Plan Builder features:

- Administration
- Disposition Instructions
- Events
- File Plan
- File Plan Association
- Import Export
- Legal Justifications
- Periods
- Reports

Upon installation and feature activation, only the File Plan Builder Administrator(s) is granted permission to create Permission Roles.

**Gimmal Compliance Suite** provides the ability to create, edit, view, or delete Permission Roles.

**Intended User:** Compliance Suite Administrator

To access the **Permission Roles** list:

1. Open **File Plan Builder**.
2. Select **Administration** from the vertical tabs. The Administration context menu opens.
3. Select the **Permission Roles** option. The Permission Roles list opens.

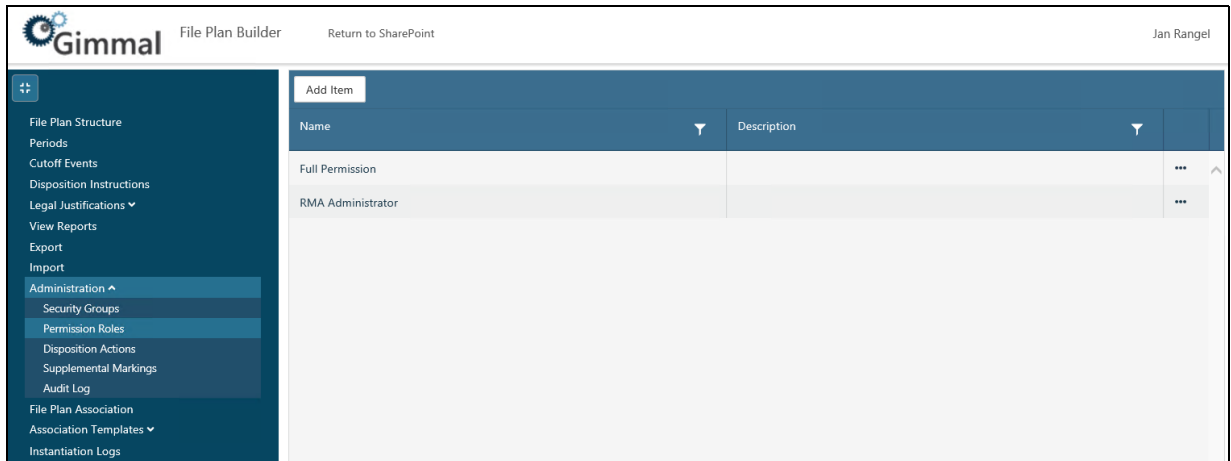


Figure 2-1 Permission Roles List

## 2.1 Permission Roles List

The following table describes the Permission Roles list with a description of each heading.

Table 2-1 Permission Roles List Headings

List View Heading	Description
<b>Name</b>	<p>Unique name that differentiates the Permission Role from other Permission Roles.</p> <p>The <b>Name</b> is used in the <b>Security Groups</b> and <b>File Plan: Security</b> dialog boxes as the selection list for <b>Permission Role Assignments</b>.</p> <p>Example: Records Manager</p>
<b>Description</b>	<p>Descriptive statement used to further differentiate the Permission Role from other Permission Roles.</p>

The **Permission Roles** list uses the standard filter and sort capabilities.

To create, edit, view, and delete permission roles, see the following sections.

## 2.2 Creating a Permission Role

Before a permission role can be used for Security Groups and/or file plan nodes, a Permission Role must be created.

1. From the **Permission Roles** list, click **Add Item** link at the top of the list.

- The Permission Role: Add dialog opens.

The screenshot shows a dialog box titled "Permission Role: Add". It has a close button (X) in the top right corner. The dialog is divided into three sections:

- Name\***: A text input field for the role name.
- Description**: A text input field for the role description.
- Permission Assignments**: This section contains two buttons, "Check All" and "Uncheck All", followed by a list of permission categories, each with a checkbox and a right-pointing triangle:
  - Administration Permissions
  - Cutoff Event Permissions
  - Disposition Instruction Permissions
  - File Plan Association
  - File Plan Permissions
  - Import \ Export Permissions
  - Legal Justification Permissions

At the bottom of the dialog are "OK" and "Cancel" buttons.

Figure 2-2 Creating a Permission Role

- Enter a **Name (Required)**. The **Name** is a unique identifier for the new Permission Role.
- Enter a **Description**. The **Description** is a descriptive statement that defines the purpose of this Permission Role.
- Select the desired **Permission Assignments** to expand it. The **Permission Assignments** define the security configuration for this Permission Role. Users in security groups assigned this Permission Role will have access based on the **Permission Assignments**. These options are described in the following section, [2.3 Permission Assignment Configuration](#).
- Click **OK** to create the new Permission Role. The new role displays in the **Permission Roles** list.
- After you save the new Permission Role,
  - The new Permission Role will appear as a selection in the **Permission Role Assignments** options in the **Security Groups** and **File Plan: Security** dialog boxes.

## 2.3 Permission Assignment Configuration

The **Permission Assignments** field defines the access permission settings for the Permission Role item. The following table describes the Permission Assignments available for each Gimmel File Plan Builder feature. The **Permission Assignments** described in the table below are accessible from the Create, Edit, or View Permission Roles screens. The **Permission Assignments are not**

**cascading**; you must be assigned each Permission Assignment individually. For example, if you are granted *Edit*, you must also be granted *View* to select an item for editing.!

Table 2-2 Gimmel File Plan Builder Feature Permission Assignments

Feature Category	Permission Assignment	Description
<b>Administration Permissions</b>	View Disposition Actions	Provides access to the <b>Disposition Actions</b> tab in the Administration section of File Plan Builder.  Allows a user to read/view an existing disposition action.
<b>Administration Permissions</b>	Add Disposition Actions	Allows a user to create a new disposition action.
<b>Administration Permissions</b>	Edit Disposition Actions	Allows a user to edit a disposition action.
<b>Administration Permissions</b>	Remove Disposition Actions	Allows a user to delete an existing disposition action.
<b>Administration Permissions</b>	View Administration Tab	Provides access to the <b>Administration</b> features in File Plan Builder.  <b>Administration</b> is a vertical tab in File Plan Builder.
<b>Administration Permissions</b>	Add Security Group	Allows a user to create a new Security Group.
<b>Administration Permissions</b>	Edit Security Group	Allows a user to edit an existing Security Group.
<b>Administration Permissions</b>	Remove Security Group.	Allows a user to delete an existing Security Group.
<b>Administration Permissions</b>	View Security Group	Provides access to the <b>Security Groups</b> tab in the Administration section of File Plan Builder.  Allows a user to read/view an existing Security Group.
<b>Administration Permissions</b>	Add Permission Role	Allows a user to create a new Permission Role.
<b>Administration Permissions</b>	Edit Permission Role	Allows a user to edit a Permission Role.
<b>Administration Permissions</b>	Remove Permission Role	Allows a user to delete an existing Permission Role.

Table 2-2 Gimmel File Plan Builder Feature Permission Assignments

Feature Category	Permission Assignment	Description
<b>Administration Permissions</b>	View Permission Role	Provides access to the <b>Permission Roles</b> tab in the Administration section of File Plan Builder.  Allows a user to read/view an existing Permission Role.
<b>Administration Permissions</b>	View Supplemental Markings	Provides access to the <b>Supplemental Markings</b> tab in the Administration section of File Plan Builder.  Allows a user to read/view an existing Supplemental Marking.
<b>Administration Permissions</b>	Add Supplemental Markings	Allows a user to create a new Supplemental Marking.
<b>Administration Permissions</b>	Edit Supplemental Markings	Allows a user to edit an existing Supplemental Marking.
<b>Administration Permissions</b>	Remove Supplemental Markings	Allows a user to remove an existing Supplemental Marking.
<b>Administration Permissions</b>	View Audit Log	Provides access to the <b>Audit Log</b> tab in the Administration section of File Plan Builder.  Allows a user to view existing audit log entries for File Plan Builder.
<b>Administration Permissions</b>	Purge Audit Log	Allows a user to discard the audit log files.
<b>Cutoff Event Permissions</b>	View Cutoff Events	Allows a user to read/view an existing cutoff event type.
<b>Cutoff Event Permissions</b>	Add Cutoff Events	Allows a user to create a new cutoff event type.
<b>Cutoff Event Permissions</b>	Edit Cutoff Events	Allows a user to edit an existing cutoff event type.
<b>Cutoff Event Permissions</b>	Remove Cutoff Events	Allows a user to delete an existing cutoff event type.
<b>Cutoff Event Permissions</b>	View Cutoff Event Tab	Provides access to the <b>Cutoff Events</b> vertical tab in File Plan Builder.



Table 2-2 Gimmel File Plan Builder Feature Permission Assignments

Feature Category	Permission Assignment	Description
<b>Disposition Instruction Permissions</b>	View Disposition Instructions	Allows user to read/view an existing disposition instruction.
<b>Disposition Instruction Permissions</b>	Add Disposition Instructions	Allows a user to create a new disposition instruction.
<b>Disposition Instruction Permissions</b>	Edit Disposition Instructions	Allows a user to edit an existing disposition instruction.
<b>Disposition Instruction Permissions</b>	Remove Disposition Instructions	Allows a user to delete an existing disposition instruction.
<b>Disposition Instruction Permissions</b>	View Disposition Instruction Tab	Provides access to the <b>Disposition Instructions</b> vertical tab in File Plan Builder.
<b>File Plan Association</b>	View File Plan Association Tab	Provides access to the <b>File Plan Association</b> vertical tab in File Plan Builder.
<b>File Plan Association</b>	Instantiate File Plans	Allows a user to schedule the File Plan Instantiation timer job.
<b>File Plan Association</b>	Edit File Plan Associations	Allows a user to edit file plan associations.
<b>File Plan Permissions</b>	Add File Plan Nodes	Allows a user to create a new file plan node.
<b>File Plan Permissions</b>	Remove File Plan Nodes	Allows a user to delete an existing file plan node.
<b>File Plan Permissions</b>	Edit File Plan Nodes	Allows a user to edit an existing file plan node.
<b>File Plan Permissions</b>	Edit File Plan Node Vital Record Information	Allows a user to edit fields on the <b>Vital Records</b> tab for an existing file plan node.
<b>File Plan Permissions</b>	View Content Type Rules	Allows a user to view the content type rules for the existing file plan node.
<b>File Plan Permissions</b>	View File Plan Tab	Provides access to the <b>File Plan</b> vertical tab in File Plan Builder.
<b>File Plan Permissions</b>	View File Plan	Allows a user to read/view an existing file plan node.

Table 2-2 Gimmal File Plan Builder Feature Permission Assignments

Feature Category	Permission Assignment	Description
<b>File Plan Permissions</b>	Edit Supplemental Markings	Allows a user to edit fields on the <b>Supplemental Markings</b> tab for an existing file plan node.
<b>File Plan Permissions</b>	Edit Cutoff Criteria	Allows a user to edit fields on the Cutoff Criteria tab for an existing file plan node.
<b>File Plan Permissions</b>	View Cutoff Workflow	Allows a user to see the <b>Cutoff Workflow</b> field on the <b>Cutoff Criteria</b> tab for file plan nodes.  Hides or displays the <b>Cutoff Workflow</b> field.
<b>File Plan Permissions</b>	Edit SharePoint Security on Record Containers	Allows a user to edit fields on the <b>SharePoint Security on Record Containers</b> tab for an existing file plan node.
<b>File Plan Permissions</b>	View SharePoint Security on Record Containers	Provides access to the <b>SharePoint Security on Record Containers</b> tab for file plan nodes.
<b>Import \ Export Permissions</b>	View Import Tab	Provides access to the <b>Import</b> vertical tab of File Plan Builder.
<b>Import \ Export Permissions</b>	View Export Tab	Provides access to the <b>Export</b> vertical tab of File Plan Builder.
<b>Legal Justification Permissions</b>	View Legal Justifications Tab	Provides access to the <b>Legal Justifications</b> features in File Plan Builder.  <b>Legal Justifications</b> is a vertical tab in File Plan Builder.
<b>Legal Justification Permissions</b>	Add Requirements	Allows a user to create a new Legal Requirement.  This is required to add a new Legal Requirement through the <b>Add</b> link next to a Legal Authority <b>Requirements</b> list.
<b>Legal Justification Permissions</b>	Edit Requirements	Allows a user to edit an existing Legal Requirement.
<b>Legal Justification Permissions</b>	Remove Requirements	Allows a user to delete an existing Legal Requirement.

Table 2-2 Gimmel File Plan Builder Feature Permission Assignments

Feature Category	Permission Assignment	Description
<b>Legal Justification Permissions</b>	View Requirements	Provides access to the <b>Requirements</b> tab in the Legal Justification section of File Plan Builder.  Allows a user to read/view an existing Legal Requirement.
<b>Legal Justification Permissions</b>	View Pending Legal Justification	Provides access to the <b>Pending Legal Changes</b> tab in the Legal Justification section of File Plan Builder.
<b>Legal Justification Permissions</b>	Add Authority	Allows a user to create a new Legal Authority.
<b>Legal Justification Permissions</b>	Edit Authority	Allows a user to edit an existing legal Authority.
<b>Legal Justification Permissions</b>	Remove Authority	Allows a user to delete an existing Legal Authority.
<b>Legal Justification Permissions</b>	View Authority	Provides access to the <b>Authorities</b> tab in the Legal Justifications section of File Plan Builder.  Allows a user to read/view an existing Legal Authority.
<b>Legal Justification Permissions</b>	View Authority Requirements	Allows a user to see the <b>Requirements</b> list for a Legal Authority.  Hides or displays the <b>Requirements</b> list field.
<b>Period Permissions</b>	View Periods	Allows a user to read/view an existing Period.
<b>Period Permissions</b>	Add Periods	Allows a user to create a new Period.
<b>Period Permissions</b>	Edit Periods	Allows a user to edit an existing Period.
<b>Periods</b>	Remove Periods	Allows a user to delete an existing Period.
<b>Period Permissions</b>	View Periods Tab	Provides access to the <b>Periods</b> vertical tab in File Plan Builder.
<b>Report Permissions</b>	View Reports Tab	Provides access to the Report vertical tab of File Plan Builder.

## 2.4 Viewing a Permission Role

To view the details of an existing Permission Role, you must view the Permission Role item.

1. From the **Permission Role** list, select the Permission Role that you want to view. Only one Permission Role can be selected at a time.
2. Click the ellipsis (...) to the right of the permission role name, and then click **View**. The Permission Role: View dialog opens.

Figure 2-3 Viewing a Permission Role

3. View the role details as desired, and then click **Edit** to edit the role, or **Cancel** to close the dialog.

## 2.5 Editing a Permission Role

To change an existing Permission Role, you must edit the Permission Role item.

1. From the **Permission Role** list, select the Permission Role that you want to edit. Only one Permission Role can be selected at a time.
2. Click the ellipsis (...) to the right of the permission role name, and then click **View**. The Permission Role: View dialog opens.

3. Click **Edit** at the bottom of the dialog to make the Permission Role fields editable.

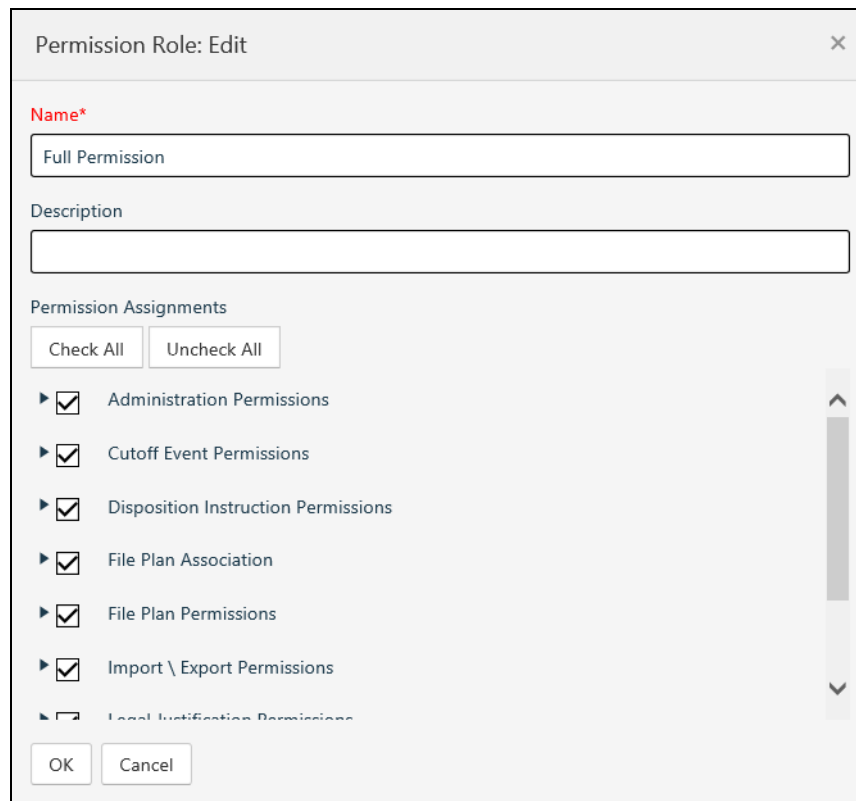


Figure 2-4 Editing a Permission Role

4. Update the information as desired.
5. Click **OK**. The Permission Role is updated and the changes appear in the **Permission Roles** list.
6. After you save the Permission Role changes:
  - Any existing Security Groups or file plan nodes that use this Permission Role will have the updated permissions applied hence forth.
  - The updated Permission Role will appear as a selection in the **Permission Role Assignments** options in the **Security Groups** and **File Plan: Security** dialog boxes.

## 2.6 Deleting a Permission Role

To remove an existing Permission Role from your site, you must delete the Permission Role item.

---

### Note

Please delete with caution and ensure the Permission Role you are removing is not in use.

---

1. From the **Permission Role** list, select the Permission Role that you want to delete. Only one Permission Role can be selected at a time.
2. Click the ellipsis (...) to the right of the permission role name, and then click **Delete**. A message displays asking you to confirm the removal.
  - Click **OK** to delete the Permission Role and remove it from the **Permission Roles** list.
  - If the selected Permission Role is currently used by one or more Security Groups or file plan nodes, the Permission Role will be removed as a selection for the affected items.

## 2.7 Permission Roles Permission Assignment

To access the *Permission Roles* functionality, you must be a member of a Security Group that has an assigned Permission Role that grants permission.

Permission Assignments are not cascading; you must be assigned each Permission Assignment individually. For example, if you are granted *Edit*, you must also be granted *View* to select a Permission Role for editing.

The following table defines the required Permission Assignment needed to access the *Permission Roles* functionality in File Plan Builder.

Table 2-3 *Permission Roles Permission Assignment*

Permission Assignment	Description
View Administration Tab	Provides access to the <b>Administration</b> features in File Plan Builder.  Administration is a vertical tab in File Plan Builder.
View Permission Role	Provides access to the Permission Roles tab in the Administration section of File Plan Builder. Allows a user to read/view an existing Permission Role.
Add Permission Role	allows a user to create a new Permission Role.
Edit Permission Role	Allows a user to edit an existing Permission Role.
Remove Permission Role	Allows a user to delete an existing Permission Role.

## 3 File Plan Structure

File Plan Structure functionality is available in a SharePoint Records Center with Gimmal Compliance Suite enabled. To use the File Plan Structure features in File Plan Builder, Gimmal Compliance Suite must be installed and the Gimmal Compliance Suite File Plan Builder feature must be active. In addition, you must have the proper File Plan Builder Permission Roles assigned.

Gimmal Compliance Suite supports a user-defined File Plan Structure. The File Plan Structure is the framework for your file plan nodes. The file plan nodes are the hierarchical classification scheme for the storage of records based on your organization's records management policies. The file plan nodes are logical SharePoint Record Containers used to organize your organization's records.

The **File Plan Structure** menu in the left pane contains the following options:

- **General:** Standard information such as Name, ID, Description, Disposition Instructions, Disposition Authority, Location, Transfer to NARA, Case-Based Retention, Obsolete, and Notes.
- **Cutoff Criteria:** Information specific to cutoff processing instructions for records in the file plan node. The **Cutoff Criteria** tab and its four options (**Enable Events**, **Enable Periods**, **Enable Relationships**, and **Enable Scripts**) are only available if you select *Cutoff* as the aging method in the Disposition Instructions. Periods or Relationships are not supported in Alternate Aging.
- **Security:** Permission Roles defining groups granted access to the file plan node.
- **Supplemental Markings:** Assignment of Supplemental Markings for the file plan node.
- **Vital Record:** Information specific to vital record review processes for records in the file plan node.
- **SharePoint Security:** Assignment of permission granted to SharePoint users and/or groups when the file plan node is instantiated as a Record Container in SharePoint through File Plan Association.

As part of Gimmal Compliance Suite, the creation of file plan nodes is a prerequisite step for File Plan association and instantiation. The File Plan Instantiation timer job publishes your file plan to your Compliance Suite-activated SharePoint Records Center, making it available to authorized SharePoint users/groups.

### 3.1 Before You Create a File Plan Structure

Before you create your File Plan Structure, the following should be created with Compliance Suite, based on your organization's records management policies:

- **(Required)** Workflows for libraries added
- **(Required)** Disposition Actions
- **(Required)** Disposition Instructions

- **(Required)** Legal Justifications
- **(Optional)** Periods (only available if the **Disposition Aging** method is set to *Cutoff*)
- **(Optional)** Cutoff Events
- **(Optional)** Relationship Types (only available if the **Disposition Aging** method is set to *Cutoff*)
- **(Optional)** Permission Roles
- **(Optional)** Supplemental Markings

Gimmel Compliance Suite provides the ability to create, edit, view, or delete file plan nodes.

**Intended User:** Records Manager

To access the **File Plan Structure** list:

1. Open **File Plan Builder**.
2. Select **File Plan Structure** from the vertical tabs. The File Plan Nodes list displays.

The File Plan Nodes list displays all file plan nodes available in File Plan Builder. This list can be sorted and/or filtered based on **Name**, **ID**, or **Description**. In addition to selecting existing file plan nodes, you can create a new file plan node.

## 3.2 File Plan Nodes List

The following table describes the headings in the **File Plan Nodes** list.

Table 3-1 File Plan Nodes

List View Heading	Description
Name	User-friendly identifier that differentiates the file plan node from other file plan nodes. After the File Plan Instantiation timer job completes, the <b>Name</b> displays in your SharePoint Records Center as the <b>Title</b> of the corresponding Record Container.
ID	Unique identifier that differentiates the file plan node from other file plan nodes at the same level in the File Plan Structure. After the File Plan Instantiation timer job completes, the <b>ID</b> displays in your SharePoint Records Center as the <b>Name</b> and the <b>Specified ID</b> of the corresponding Record Container.
Description	Descriptive statement used to further differentiate the file plan node from other file plan nodes. After the File Plan Instantiation timer job completes, the <b>Description</b> displays in your SharePoint Records Center as the Description of the corresponding Record Container.

The **File Plan Node** list uses the standard filter and sort capabilities.



### 3.3 Adding a New File Plan Node

Before end users can create records based on your organization's records management policies, file plan nodes must be created.

When you first access the Add Root Node dialog, described below, a number of tabs display. Listed below is a description of each tab that is available on the **File Plan Node: Add** dialog:

- **General:** Standard information such as Name, ID, Description, Disposition Instructions, Disposition Authority, Location, Transfer to NARA, Case-Based Retention, Obsolete, and Notes.
- **Cutoff Criteria:** Information specific to cutoff processing instructions for records in the file plan node. The **Cutoff Criteria** tab and its four options (**Enable Cutoff Events**, **Enable Periods**, **Enable Relationships**, and **Enable Scripts**) are only available if you select *Cutoff* as the aging method in the Disposition Instructions. Periods or Relationships are not supported in Alternate Aging.
- **Security:** Permission Roles defining groups granted access to the file plan node.
- **Supplemental Markings:** Assignment of Supplemental Markings for the file plan node.
- **Vital Record:** Information specific to vital record review processes for records in the file plan node.
- **SharePoint Security:** Assignment of permission granted to SharePoint users and/or groups when the file plan node is instantiated as a Record Container in SharePoint through File Plan Association.

To add a new File Plan Node, perform either step 1 or step 2, and then continue with the remaining steps:

1. To add a new root node, from the **File Plan Nodes** list, click **Add Root Node**. The File Plan Node: Add dialog opens.  
OR
2. To add a **Child Node** or **Sibling Node**, click a root node on the File Plan Nodes list, click the ellipsis on the right side, and then select the desired option from the context menu. The File Plan Node: Add dialog opens.

---

#### Note

– If you select **Add Root Node**, the new file plan node is added to the top level of your File Plan Structure.

– If you select **Add Child Node**, the new file plan node is added to the level below the currently selected file plan node.

– If you select **Add Sibling Node**, the new file plan node is added at the same level as the currently selected file plan node.

3. By default, the dialog opens on the **General** tab. Enter the following information:

Figure 3-1 Add File Plan Node General Tab

- a. **(Required)** Enter a **Name** for the new file plan node. After the File Plan Instantiation timer job completes, the **Name** displays in your SharePoint Records Center as the **Title** of the corresponding Record Container.
- b. **(Required)** Enter the **ID**. The **ID** is a unique identifier in the selected level of the File Plan Structure for the new file plan node. After the File Plan Instantiation timer job completes, the **ID** displays in your SharePoint Records Center as the **Name** and **Specified ID** of the corresponding Record Container.
- c. Enter a **Description**. The **Description** is a descriptive statement that defines the purpose of this file plan node. After the File Plan Instantiation timer job completes, the **Description** displays in your SharePoint Records Center as the **Description** of the corresponding Record Container.
- d. **(Required)** Select the **Disposition Instructions**. The **Disposition Instructions** define the disposition processing that will be applied to records in this file plan node. The selection options are based on existing Disposition Instruction items.

- e. **(Required)** Select the **Disposition Authority**. The **Disposition Authority** defines the group with legal authorization to manage the disposition of records in this file plan node. The selection options are based on existing Legal Authority items.
- f. Enter a **Location**. The **Location** should be a descriptive statement that defines the physical location of the *Record Container* that corresponds to this file plan node. This field can be used for Record Container(s) that contain physical records.

For example, 999 Broadway New York; Floor 7; Human Resources File Room, Cabinet 123, Bin 20.

- g. Select **Transfer to NARA**. If this file plan node contains permanent records that are required to be transferred or accessioned to the National Archives and Records Administration (NARA), check this option. Checked indicates **Yes**. Unchecked indicates **Not Applicable (NA)**.
- h. Select **Case-Based Retention**. If this file plan node corresponds to a Record Container that contains Record Items that will be grouped together for records processing such as disposition or holds, select this option. Selected indicates **Yes** and deselected indicates **No**.
- i. Select **Obsolete** if the file node is no longer to be used for future instantiations. You cannot instantiate nodes that are flagged as Obsolete; however, existing nodes that have been previously instantiated will remain. This option is typically not enabled when creating a node unless you want to prevent instantiation of the node.
- j. Enter any **Notes** that you want. The notes are not instantiated and will appear solely in File Plan Builder.

4. Click the **Cutoff Criteria** tab. The tab updates with fields for the file plan node Cutoff Criteria.

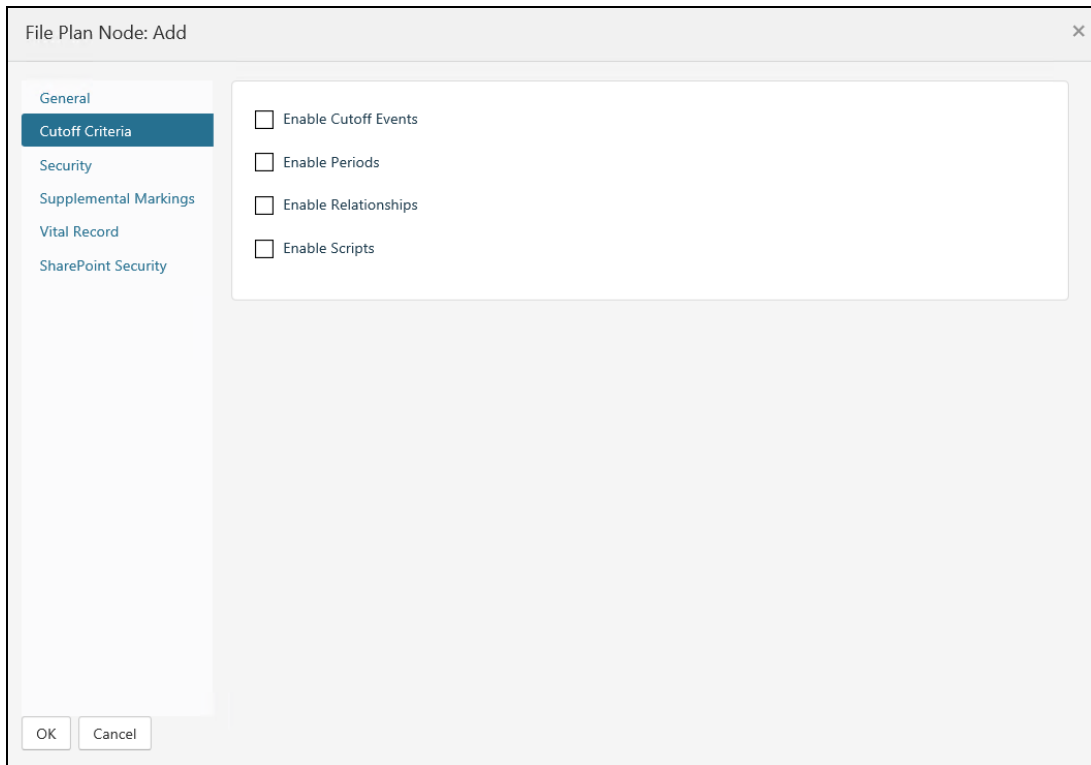


Figure 3-2 File Plan Cutoff Criteria

---

#### Note:

The Cutoff Criteria tab will be disabled if the **Disposition instructions** selected from the **General** tab is set to *Alternate aging*.

---

5. If the new file plan node is **not** a Root Node, radio selection options for **Inherit From Parent** or **Specify Criteria** will display. (If the new file plan node **is** a Root Node, continue with step 6.)
  - If you select **Inherit From Parent**, no fields will be displayed.
  - If you select **Specify Criteria** or the new file plan node is a Root Node, the tab updates with fields for the file plan node **Cutoff Criteria**.
6. Select **Enable Cutoff Events**. If cutoff processing for records in this file plan node is based on one or more event(s), check this option. Checked indicates **Yes**. Unchecked indicates **No**.

If **Enable Events** is checked,

- Select one or more **Cutoff Event(s)**. The selection options are based on existing event items.

- Select an option for **All Cutoff Events Required**. The **All Cutoff Events Required** defines the event(s) occurrence that will trigger cutoff processing. The options are *First Cutoff Event* or *All Cutoff Events*.
- 7. Select the **Enable Periods** checkbox if cutoff processing for records in this file plan node is based on a period. Selected indicates **Yes**. Deselected indicates **No**.
- 8. If **Enable Periods** is selected, select a **Cutoff Period**. You can select an existing period from the list of options or click the **Periods** tab from the vertical tabs on the main navigation pane on the left to create a new period. See [4.2 Adding a New Period](#) for more information.
- 9. Select **Enable Relationships**. If cutoff processing for records in this file plan node is based on a Record Relationship occurrence, check this option. Selected indicates **Yes**. Deselected indicates **No**.

For example, when Employee Manual 1.0 is superseded by Employee Manual 2.0, cutoff processing should be triggered for Employee Manual 1.0.

If **Enable Relationships** is selected, select a **Relationship Role**. The selection options are based on the existing Relationship Types list in your Compliance Suite-enabled SharePoint Records Center.

- 10. Select **Enable Scripts**. **Enable Scripts** allows you to define advanced cutoff criteria that are not based on a combination of one or more events, periods, and/or relationships. For example, a PowerShell script could request information from an external application to determine if the record(s) are eligible for cutoff. Selected indicates **Yes**. Deselected indicates **No**.

If **Enable Scripts** is selected, enter a **Script**.

11. Click the **Security** tab. The tab updates with fields for the file plan node Security.

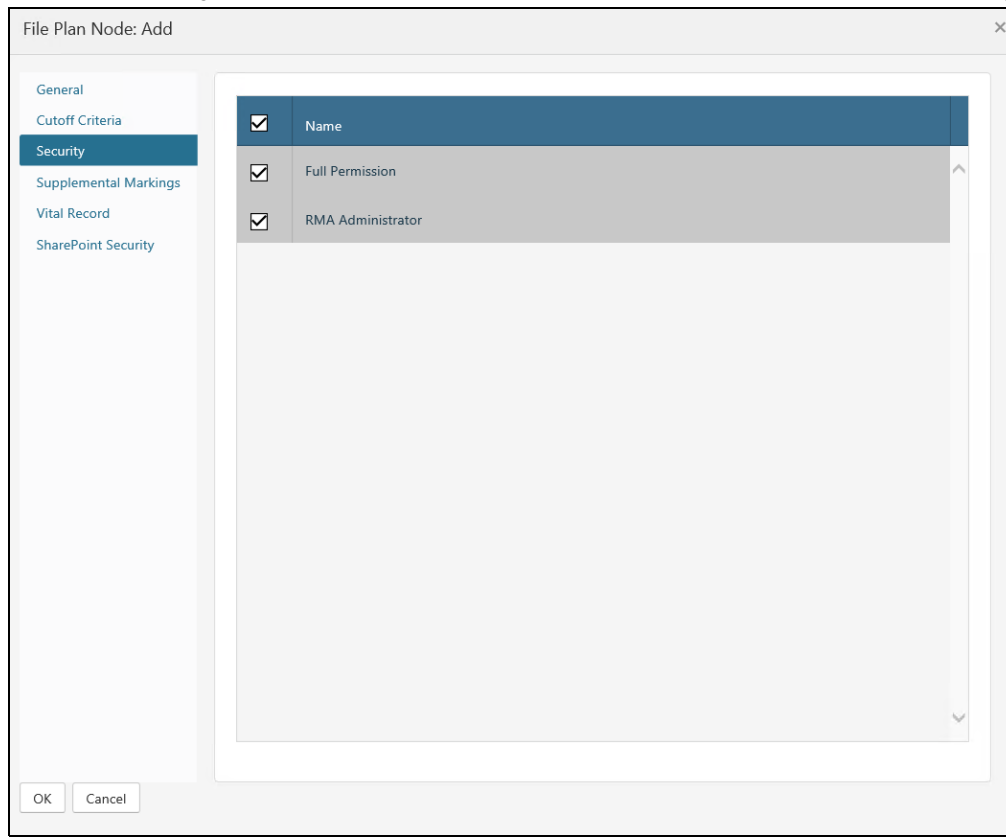


Figure 3-3 File Plan Security

- a. Select one or more **Permission Roles**. The **Permission Roles** grants any *Security Group* that is assigned any of the selected *Permission Roles* access to this file plan node. By default, all *Permission Roles* are granted access.
- b. If this is a sibling or child node, you can select from the following options: **Inherit Permissions** or **Specify Permissions**. Select the option to inherit the permissions from the immediate parent or select **Specify Permissions** to define a unique set for this item.

12. Click the **Supplemental Markings** tab. The item detail section updates with fields for the file plan node Supplemental Markings.

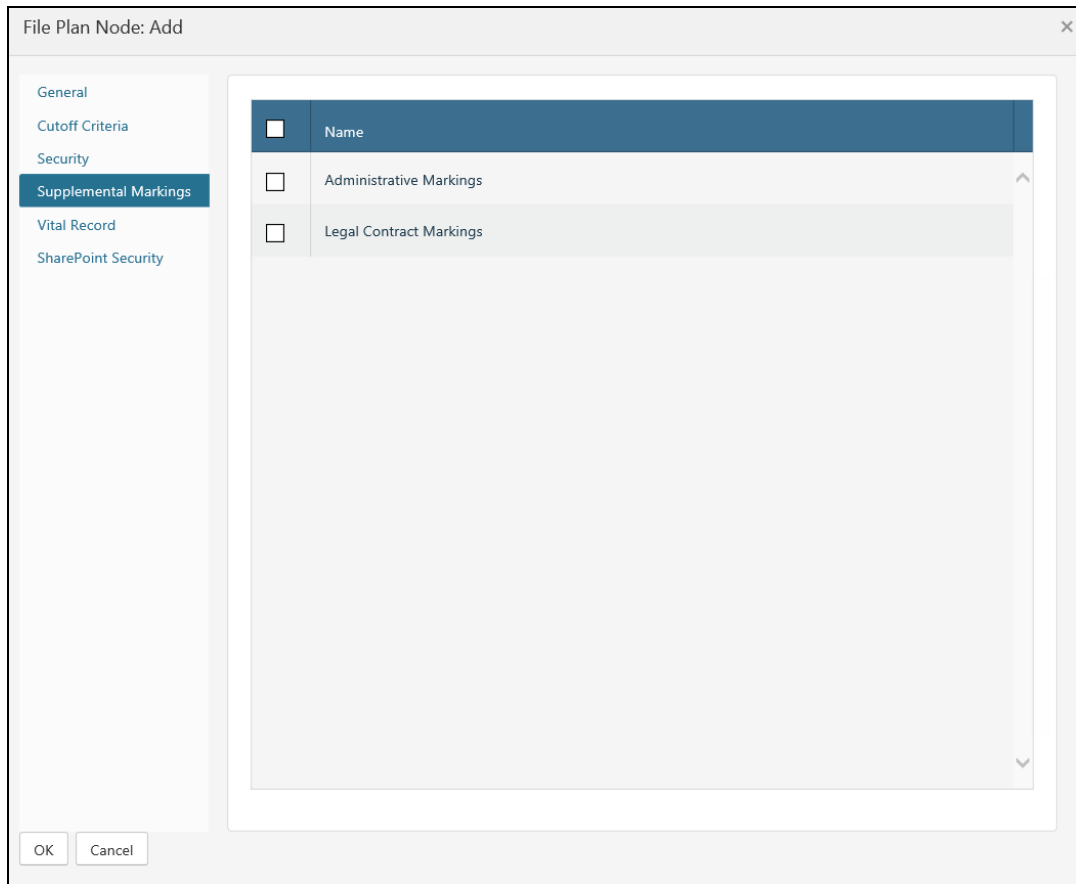


Figure 3-4 Supplemental Markings

- a. Select one or more **Supplemental Markings**. The **Supplemental Markings** restrict access to the *Record Container(s)* and *Record Item(s)* in this file plan node to only authorized users based on the *Access Rules* defined in your Compliance Suite-enabled SharePoint Records Center.
  - b. If this is a sibling or child node, you can select one of the following:
    - o **Inherit Permissions** to inherit the permissions from the immediate parent
    - o **Specify Permissions** to define a unique set of supplemental markings for this item
13. Click the **Vital Record** tab. The tab updates with fields for the file plan node Vital Record.
- a. If this is the root node, the option **Is Vital Record** displays. Select **Is Vital Record** if this file plan node contains vital records that are essential to the functions and protection of rights and interest of your organization. Selected indicates **Yes** and deselected indicates **No**.
 

If you select **Is Vital Record**, the **Review Period**, **Last Review Date**, and **Last Reviewer** fields display.
  - b. If this is a child or sibling node, the following options display:

- **Inherit From Parent:** If you select this option, no fields will be displayed.
- **Specify Criteria:** If you select this option, the tab updates with fields for enabling the Vital Record and the review period. Select the **Is Vital Record** check box to enable the feature.

Figure 3-5 Vital Records File Plan Tab

- (Required)** Select a **Review Period**. You can select an existing period from the list of options or click the **Periods** tab from the vertical tabs on the main navigation pane on the left to create a new period. See [4.2 Adding a New Period](#) for more information.
- (Required)** Enter the **Last Review Date**. The **Last Review Date** is the date records in the file plan node were last reviewed and the date from which the new review date will be calculated. To select a date from a calendar, click to the right of the field.
- (Required)** Enter the **Last Reviewer**. The **Last Reviewer** is the user or group who will be responsible for reviewing records in this file plan node. As soon as you enter four characters in the field, the system displays a picklist that enables you to choose a user or group. Once the user/group is verified, the SharePoint User ID will display.



14. Click the **SharePoint Security** tab. The tab updates with fields for the file plan node SharePoint Security.

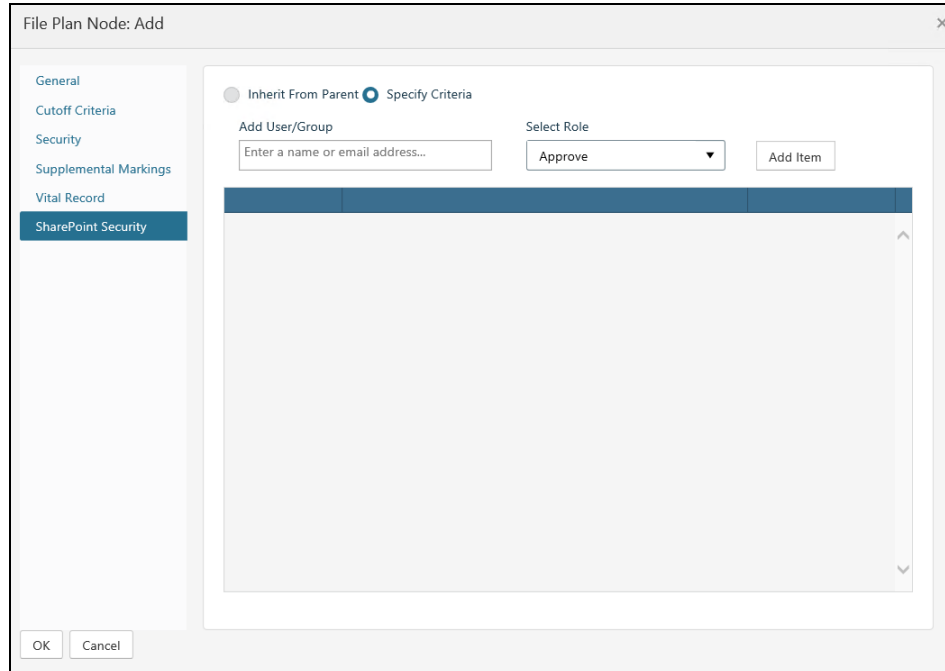


Figure 3-6 SharePoint Security

- a. If this is a child or sibling node, the following options display:
    - **Inherit From Parent:** If you select this, no fields will display.
    - **Specify Criteria:** If you select this, follow the steps in 7(b) to grant a SharePoint user or group permissions.
  - b. If this is the root node or you selected **Specific Permissions** in step 7(a), you can grant a SharePoint user or group permission by following these steps:
    - i. Enter the user or group name in the **Add User/Group** field. The system automatically performs a check as soon as you enter four characters, and provides a picklist to choose from. If the user is verified, the SharePoint User ID will display.
    - ii. Select the SharePoint security role from the Select Role drop-down. The options are based on security level options configured for your SharePoint Records Center. For details on SharePoint security levels, please refer to the SharePoint User Guide.
    - iii. Click **Add Item** to set the new user/group permission on the file plan node.
    - iv. The new user/group permission will be added to the list of user/group permissions at the top of the item detail section.
  - c. To remove a SharePoint user or group permission, click **X** to the right of the SharePoint User/Group name.
15. Click **OK** at the bottom of the File Plan Node: Add dialog. The new file plan node is created and displays in the **File Plan Nodes** list.

## 3.4 Viewing a File Plan Node

To view the details of an existing file plan node, perform the following steps.

1. From the **File Plan Node** list, click the ellipsis (...) to the right of the file plan node you want to view, and select **View**.

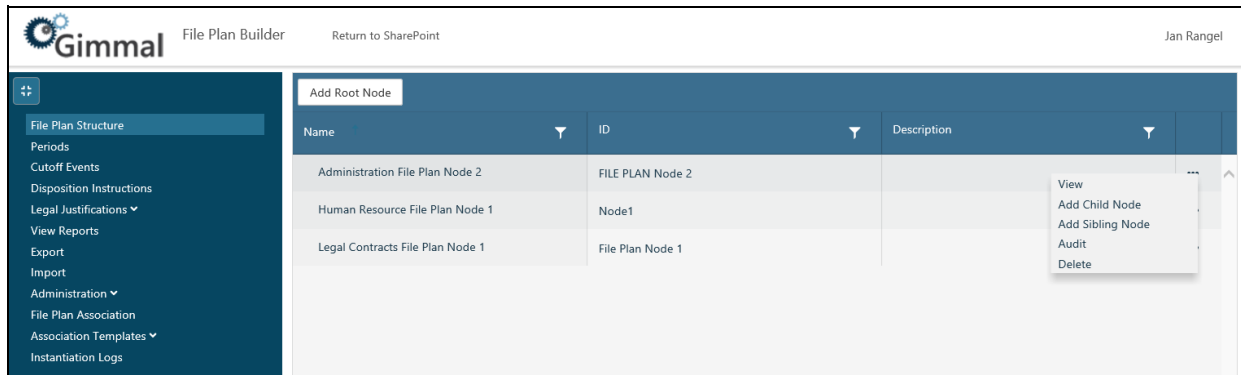


Figure 3-7 Viewing a File Plan Node

The File Plan Node: View dialog opens. The item detail section updates with read-only fields for the selected file plan node.

2. To view the cutoff criteria, select the **Cutoff Criteria** tab. The item detail section updates with read-only fields for the selected file plan node cutoff criteria.
3. To view the security settings, select the **Security** tab. The item detail section updates with read-only fields for the selected file plan node security.
4. To view the supplemental markings settings, select the **Supplemental Markings** tab. The item detail section updates with read-only fields for the selected file plan node supplemental markings.
5. To view the vital record settings, select the **Vital Record** tab. The item detail section updates with read-only fields for the selected file plan node vital record fields.
6. To view the SharePoint security settings, select the **SharePoint Security** tab. The item detail section updates with read-only fields for the selected file plan node SharePoint security.
7. Click **Cancel** to close the dialog.

## 3.5 Editing a File Plan Node

File Plan Builder is the main data repository and will show the changes after the instantiation. To edit an existing file plan node, perform the following steps:

1. From the **File Plan Node** list, click the ellipsis (...) to the right of the file plan node you want to edit, and select **View**.

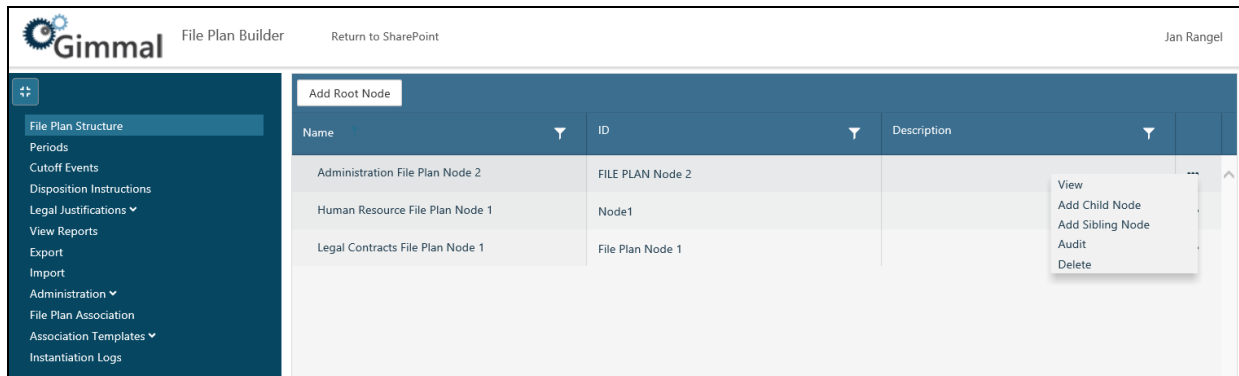


Figure 3-8 Editing a File Plan Node

The File Plan Node: View dialog opens. The item detail section updates with read-only fields for the selected file plan node.

2. Click **Edit** at the bottom of the dialog. The item detail section updates with editable fields for the selected file plan node. By default, the **General** tab displays.
3. Update the information in the **General** tab fields as desired.

---

#### Note:

The **ID** is the value that SharePoint uses and displays. Changing the **Name** does not change what appears in SharePoint.

---

4. (**Required**) The ID must be unique across all file plan nodes in the same level of the File Plan Structure, and cannot be changed.
5. Select the **Cutoff Criteria** tab.
  - If the file plan node is **not** a Root Node, radio selection options for **Inherit From Parent** or **Specify Criteria** display.
  - If you select **Inherit From Parent**, no fields display.
  - If you select **Specify Criteria** or the file plan node is a Root Node, the item detail section updates with editable fields for the selected file plan node Cutoff Criteria.

Update the information in the Cutoff Criteria tab as desired.
6. Select the **Security** tab and update the Permission Roles the information as desired. Permission Roles updates will take affect for all Security Groups that are assigned any of the selected Permission Role(s) from here on.
7. Select the **Supplemental Markings** tab and update the Supplemental Markings information as desired.
8. Select the **Vital Record** tab and update the information as desired.
9. Select the **SharePoint Security** tab and update the information as desired.

10. Click **OK**. The file plan node is updated and the changes appear in the **File Plan Nodes** list.
11. After you save the file plan node changes and the File Plan Instantiation timer job is executed, the following occurs:
  - The updated file plan node will be updated in the corresponding Compliance Suite SharePoint Record Container in your Compliance Suite-enabled SharePoint Records Center.
  - Any existing Record Container(s) and Record Item(s) that are based on this file plan node will have the updated record management information applied hence forth.

### 3.6 Copying a File Plan Node

You can create a copy of a node by performing the following steps;

1. Select a node from the File Plan Node list. At the top of the window, click the **Copy** button to copy the item.
2. Change the properties of the new node as desired, and then save it.

### 3.7 Deleting a File Plan Node

To delete an existing file plan node from your file plan structure, perform the following steps:

1. From the **File Plan Node** list, click the ellipsis (...) to the right of the file plan node you want to remove, and select **Delete**.

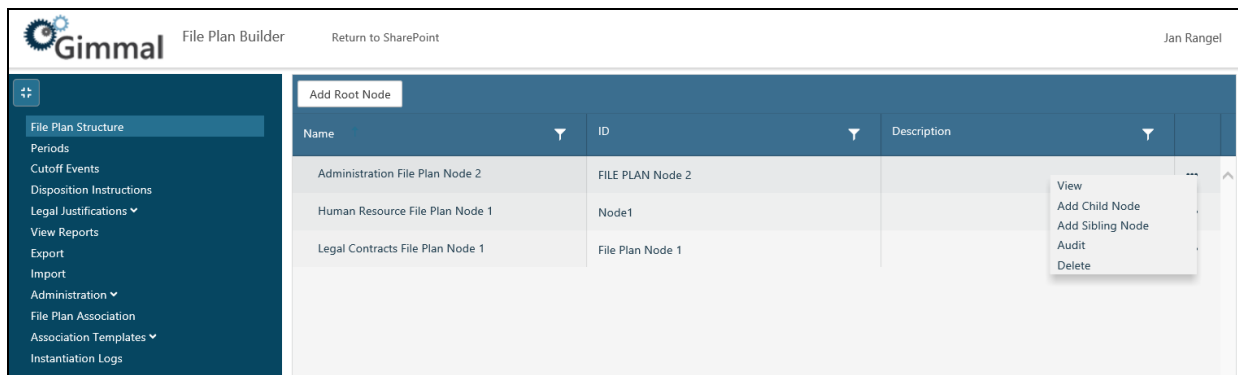


Figure 3-9 Deleting a File Plan Node

A Confirm Removal dialog displays, asking if you are sure you want to delete the item. You are also reminded that any data that is dependent on this node will also be deleted.

2. Click **OK** to delete the file plan node and remove it from the **File Plan Nodes** list.

All child nodes associated with the selected file plan node will be deleted along with the selected file plan node.

## 3.8 Obsoleting a File Plan Node

Any user who has Edit rights on a particular node in File Plan Builder can flag a node as *obsolete*. Obsolete nodes cannot be instantiated or re-instantiated. This feature is useful when an organization wants to either prevent instantiation while building the file plan nodes or when a node has been instantiated and it is no longer required or no further changes are needed. For example, when creating Fiscal year nodes (Ledgers 2014), an organization might want to prevent further instantiation of this node.

- If a root node is made obsolete, all child and sibling nodes under it are also obsolete and the entire grouping is not instantiated or re-instantiated.
- If only a sibling node or a child node is flagged as obsolete, any related subnodes inherit the obsolete flag and are also, along with the original selection, not instantiated. Any other node, however, is instantiated.
- When generating a File Plan Report, any node that is flagged as obsolete appears in the report.
- When exporting the File Plan Structure, the obsolete flag is also exported.
- The obsolete flag can be turned on/off by any user that has edit rights on the particular node in File Plan Builder.

## 3.9 Auditing a File Plan Node

The **Audit** option enables you to view and export the actions performed on a file plan node.

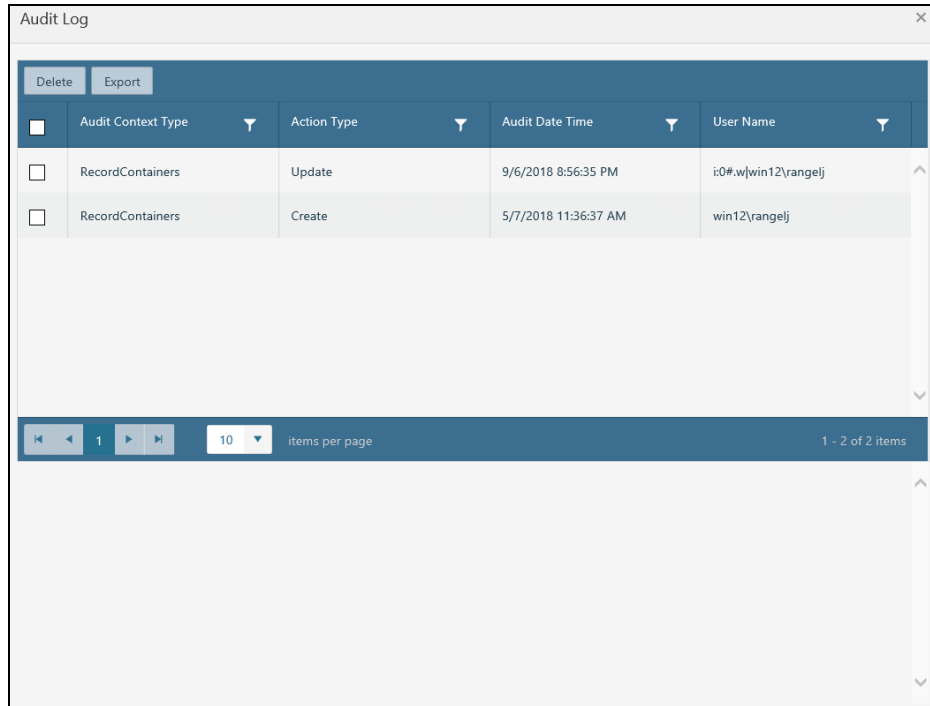
The Audit option is available from the File Plan Nodes list, by clicking the ellipsis to the right of the desired file plan node and selecting **Audit**.

The **Audit** tab is divided into two sections:

1. **Audit Log** list: List of all audit log entries based on the selected audit parameters for the selected file plan node. This list can be filtered by **Audit Context Type**, **Action Type**, **Audit Date Time**, or **User Name**.
2. **Audit Detail**: Audit log details for the selected audit log entry. This table contains the *Before* and *After* values, which can be used to identify exact changes.

To view, delete, or export the audit log entries, perform the following steps:

1. From the **File Plan Node** list, click the ellipsis (...) to the right of the file plan node you want to audit, and select **Audit**. The Audit Log dialog opens.



<input type="checkbox"/>	Audit Context Type	Action Type	Audit Date Time	User Name
<input type="checkbox"/>	RecordContainers	Update	9/6/2018 8:56:35 PM	i:0#.w win12\rangelj
<input type="checkbox"/>	RecordContainers	Create	5/7/2018 11:36:37 AM	win12\rangelj

The screenshot shows a dialog box titled "Audit Log" with a close button (X) in the top right corner. Below the title bar are two buttons: "Delete" and "Export". The main area contains a table with the following columns: "Audit Context Type", "Action Type", "Audit Date Time", and "User Name". There are two rows of data. The first row shows "RecordContainers" with an "Update" action on "9/6/2018 8:56:35 PM" by user "i:0#.w|win12\rangelj". The second row shows "RecordContainers" with a "Create" action on "5/7/2018 11:36:37 AM" by user "win12\rangelj". At the bottom of the table, there is a pagination bar showing "1" of "10" items per page, and "1 - 2 of 2 items".

Figure 3-10 Audit Log Dialog

2. View the **Audit Log** list. The following values are displayed in the **Audit** list.
  - **Audit Context Type:** The only value for a file plan node is *RecordContainers*.
  - **Action Type:** The action performed on the selected file plan node. The options are *Update* or *Create*.
  - **Audit Date Time:** The date and time the audited action was performed.
  - **User Name.** The SharePoint user who performed the audited action.
3. To view the **Audit Details**, click each RecordContainers entry, under the Audit Context Type column, listed in the **Audit Log** list. When selected, the Audit Detail table displays at the bottom of the dialog, and updates with the following values:
  - **Before:** Values for the selected audit log entry before the audited change.
  - **After:** Values for the selected audit log entry after the audited change.

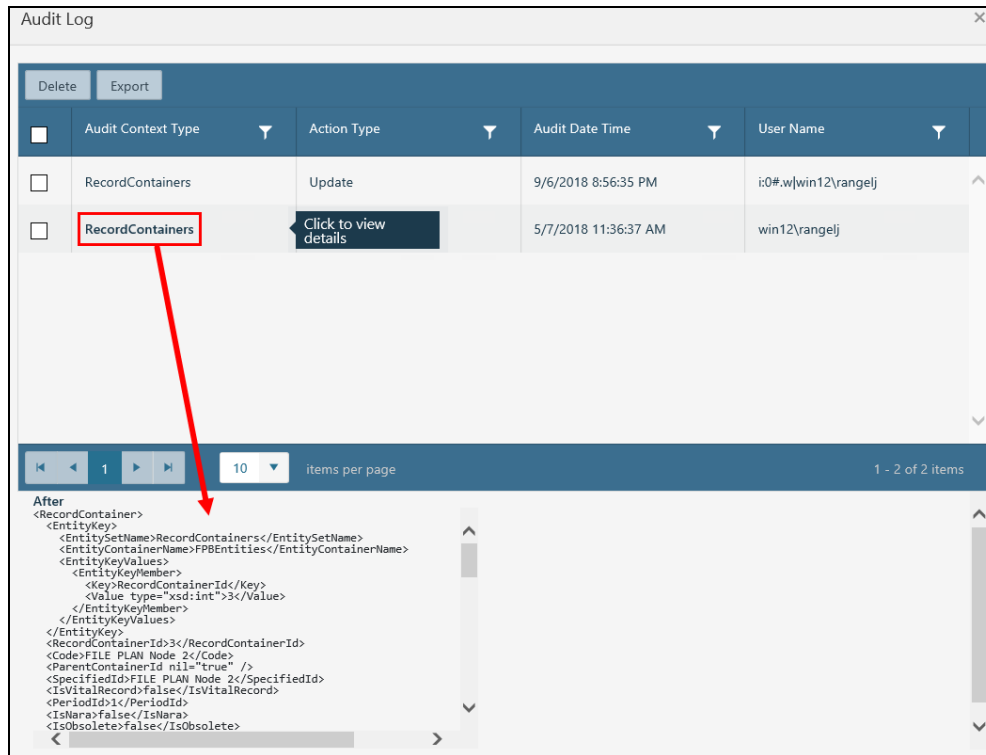


Figure 3-11 Audit Details

4. To remove audit log entries:
  - a. Select one or more audit log entries by checking the box to the left of the **Audit Context Type** column in the **Audit Log** list.
  - b. Click **Delete** above the **Audit Log** list. A confirmation dialog opens, asking you to confirm the deletion.
  - c. Click **OK** and the audit log entry is deleted and removed from the **Audit Log** list.
5. To export audit log entries:
  - a. Select one or more audit log entries by checking the box to the left of the **Audit Context Type** column in the **Audit Log** list.
  - b. Click **Export** above the **Audit Log** list.
  - c. A **File Download** dialog box opens at the bottom of your browser with options for downloading the exported .xml file. Use your standard file browser to save the exported .xml file to your local machine. (The file download dialog may differ, depending on which browser you are using.)

### 3.10 File Plan Nodes Permission Assignment

To access the File Plan Nodes functionality, you must be a member of a Security Group that has an assigned Permission Role that grants permission.

Permission Assignments are not cascading; you must be assigned each Permission Assignment individually. For example, if you are assigned *Edit*, you must also be assigned *View* to select a file plan node for editing.

The following table defines the required Permission Assignment needed to access the File Plan Nodes functionality in File Plan Builder. For more information on Permission Roles, [See "Permission Roles" on page 5.](#)

Table 3-2 File Plan Builder Nodes Permission Assignment

Permission Assignment	Description
<b>View File Plan Tab</b>	Provides access to the <b>File Plan</b> vertical tab in File Plan Builder.
<b>View File Plan</b>	Allows a user to read/view an existing file plan node.
<b>Add File Plan Nodes</b>	Allows a user to create a new file plan node.
<b>Edit File Plan Nodes</b>	Allows a user to edit an existing file plan node.
<b>View Cutoff Workflow</b>	Allows a user to see the <b>Cutoff Workflow</b> field on the <b>Cutoff Criteria</b> tab for file plan nodes.  Hides or displays the <b>Cutoff Workflow</b> field.
<b>Edit Cutoff Criteria</b>	Allows a user to edit fields on the <b>Cutoff Criteria</b> tab for an existing file plan node.
<b>Edit Supplemental Markings</b>	Allows a user to edit fields on the <b>Supplemental Markings</b> tab for an existing file plan node.
<b>Edit File Plan Node Vital Record Information</b>	Allows a user to edit fields on the <b>Vital Records</b> tab for an existing file plan node.
<b>View SharePoint Security on Record Containers</b>	Provides access to the <b>SharePoint Security on Record Containers</b> tab for file plan nodes.
<b>Edit SharePoint Security on Record Containers</b>	Allows a user to edit fields on the <b>SharePoint Security on Record Containers</b> tab for an existing file plan node.
<b>Remove File Plan Nodes</b>	Allows a user to delete an existing file plan node.
<b>Add Periods</b>	Allows a user to create a new Period. This is required to add a new Period through the <b>New</b> link next to the <b>Is vital Record: Review Period</b> and <b>Cutoff Criteria: Enable Periods → Cutoff Period</b> menu in the <b>File Plan Structure</b> dialog box. This Permission Assignment is under the <b>Period Permissions</b> category on the Permission Role.



## 4 Periods

Period functionality is available in a SharePoint Records Center with Gimmel Compliance Suite enabled. To use the period features in File Plan Builder, Gimmel Compliance Suite must be installed and the Gimmel Compliance Suite File Plan Builder feature must be active with the Disposition Instruction specifying *Cutoff* as the **Aging Method**. In addition, you must have the proper File Plan Builder Permission Roles assigned; see [4.6 Periods Permission Assignment](#).

Gimmel Compliance Suite supports user-defined *periods*. A period is a unit of time or frequency that defines recurring records management processes and actions. Periods support the management of records based on your organization's record management policies. Features that periods support are:

- Cutoff Processing
- Vital Records Review

Gimmel Compliance Suite provides the ability to create, edit, view, or delete periods. In addition to File Plan Builder: Periods, periods (also known as *period definitions*) can be managed through the **Period Definitions View** list in your SharePoint Records Center.

**Intended User:** Records Manager

To access the **Periods** list:

1. Open **File Plan Builder**.
2. Select **Periods** from the vertical tabs on the left.

### 4.1 Periods List

The following table describes the **Periods** list with a description of each heading.

*Table 4-1 Periods List Headings*

List View Heading	Description
<b>Name</b>	<p>Unique name that differentiates the period from other periods.</p> <p>The <b>Name</b> is used in the File Plan Structure dialog box as the selection list for <b>Is Vital Record: Review Period</b> and <b>Cutoff Criteria: Enable Periods</b> → <b>Cutoff Period</b> menu. The <b>Name</b> is also used on the corresponding <b>Record Container</b> and <b>Record Item</b> dialog boxes in your <b>SharePoint Records Library</b>.</p> <p>Example: Calendar Year</p>
<b>Description</b>	Descriptive statement used to further differentiate the period from other periods.

Table 4-1 Periods List Headings

List View Heading	Description
<b>Start Date</b>	<p>Defines the first calendar date of the first period to be calculated.</p> <p>Example: For a period such as <b>Fiscal Year</b>, the <b>Start Date</b> can be 10/01/2000. On 01/01/2011, we would be in the 10th <b>Fiscal Year</b> period, and on 10/01/2011, the 11th <b>Fiscal Year</b> period would begin.</p>

The **Periods** list uses the standard filter and sort capabilities.

- Select **Add Item** or click any period in the list to view the period detail in the item detail section.

## 4.2 Adding a New Period

Before a period can be used for Vital Records or cutoff processing, you must create a period by performing the following steps:

1. From the **Periods** list, click **Add Item**. The Period: Add dialog opens.

The screenshot shows the Gimmal File Plan Builder interface. On the left is a navigation menu with options like 'File Plan Structure', 'Periods', 'Cutoff Events', etc. The 'Periods' option is selected. In the main area, there is an 'Add Item' button highlighted with a red box. A dialog box titled 'Period: Add' is open, containing the following fields:

- Name\***: A text input field.
- Description**: A text input field.
- Start Date\***: A date picker field.
- Duration\***: A dropdown menu currently set to 'Daily'.
- Every**: A spinner box set to '1' followed by 'days'.
- OK** and **Cancel** buttons at the bottom.

Figure 4-1 Adding a New Period

2. Enter the following information:
  - a. **(Required)** Enter the **Name**. The name is a unique identifier for the new period.
  - b. Enter a **Description**. The **Description** is a descriptive statement that defines the purpose of this period.

- c. **(Required)** Enter the **Start Date**. The **Start Date** defines the first calendar date of the first period to be calculated. To select a date from a calendar, click the Date Selector button in this field.
- d. **(Required)** Select the **Duration**. The **Duration** defines the frequency for processing Record Container(s) or Record Item(s) assigned this Period. The options are **Daily**, **Weekly**, **Monthly**, and **Yearly**.
  - i. If the selected **Period Duration** is **Daily**, the dialog box updates with the following fields:

The screenshot shows a dialog box titled "Duration\*" with a dropdown menu set to "Daily". Below the dropdown is a field labeled "Every" containing the number "1" and a spinner control, followed by the text "days".

Figure 4-2 Daily Period Duration

Enter **Every [number] Days**. Example: **Every 1 days**.

- ii. If the selected **Period Duration** is **Weekly**, the dialog box updates with the following fields:

The screenshot shows a dialog box titled "Duration\*" with a dropdown menu set to "Weekly". Below the dropdown is a field labeled "Every" containing the number "1" and a spinner control, followed by the text "week(s) on". Below this are seven checkboxes for the days of the week: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday. All checkboxes are currently unchecked.

Figure 4-3 Weekly Period Duration

Enter **Every [number] week(s) on [Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday]**. Example: **Every 2 week(s) on Wednesday**.

- iii. If the selected **Period Duration** is **Monthly**, the dialog box updates with the following fields:

The screenshot shows a dialog box titled "Duration\*" with a dropdown menu set to "Monthly". Below the dropdown are two radio buttons. The first radio button is selected and is labeled "Day", followed by a field containing "1" and a spinner control, then the text "of every" and another field containing "1" and a spinner control, followed by the text "Months". The second radio button is labeled "On the [#] [Day] of [Month]" and is currently unselected.

Figure 4-4 Monthly Period Duration

Select one of the following options:

- Enter the **Day** [numerical day of month] **of every** [number] **month(s)**. Example: **Day 30 of every 2 month(s)**.
  - Enter **The** [first, second, third, fourth, or last] [Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday] **of every** [number of months] **month(s)**. Example: **The first Friday of every 3 month(s)**.
3. If the selected **Period Duration** is **Yearly**, the dialog box updates with the following fields:

The screenshot shows a dialog box titled "Duration\*" with a dropdown menu set to "Yearly". Below this, there is a section for "Every" with a spinner box containing the number "1" and the label "Years". There are two radio button options: "On day" (which is selected) and "On the [#] [Day] of [Month]". The "On day" option has a spinner box containing the number "1" and a dropdown menu set to "January".

Figure 4-5 Yearly Period Duration

Select one of the following options:

- Enter **Every** [number] **year(s)**: Example: *Every 2 year(s)*.
  - Enter **On** [date in month] **of** [name of month]. Example: *Every 1 of January*.
  - Enter **On the** [first, second, third, fourth, or last] [Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday] **of** [name of month]. Example: *The first Monday of January*.
4. Click **OK**. The new period is created and appears in the **Periods** list.
5. After you save the new period, the following occurs:
- The new period will appear as a selection in the **Is Vital Record: Review Period** and **Cutoff Criteria: Enable Periods** → **Cutoff Period** menu in the **File Plan Structure** dialog box.
  - After the File Plan Instantiation timer job completes, the new period will display on all relevant SharePoint Record Center dialog boxes.

### 4.3 Viewing a Period

To view the details of an existing period, perform the following step:

- From the **Periods** list, click the ellipsis (...) to the right of the period you want to view, and then click **View** from the drop-down menu. The Period: View dialog opens, showing you the details of that period.

## 4.4 Editing a Period

To edit an existing period, perform the following steps:

1. From the **Periods** list, click the ellipsis (...) to the right of the period you want to edit, and then click **View** from the drop-down menu. The Period: View dialog opens.

Figure 4-6 Editing a Period

2. Click **Edit** at the bottom of the dialog. The dialog updates with editable fields for the selected period, and the title of the dialog title changes from Period: View to Period: Edit.
3. Update the information as desired.
4. Click **OK**. The period is updated and the changes appear in the **Periods** list.

After you save the period changes, the following occurs:

- The updated period will appear as a selection in the **Is Vital Record: Review Period** and **Cutoff Criteria: Enable Periods** → **Cutoff Period** menu in the **File Plan Structure** dialog box.
5. After you save the period changes and the File Plan Instantiation timer job is executed, the following occurs:
    - If the period **Name** was changed, the updated period will appear in your SharePoint Records Center as a **new** Period Definition.
    - The updated period displays on all relevant SharePoint Records Center dialog boxes.
    - Any existing Record Container(s) and Record Item(s) that use this period will have the updates applied hence forth.

## 4.5 Deleting a Period

To delete an existing period from your site, perform the following steps.

---

### Note

You cannot delete a period that is assigned to a file plan node *Cutoff Criteria* or *Vital Record*. If you attempt to do so, the Delete option is grayed out and not available for selection.

---

1. From the **Periods** list, click the ellipsis (...) to the right of the period you want to delete, and then click **Delete** from the drop-down menu. A Confirm Removal dialog opens, asking you confirm the removal.
2. Click **OK** to delete the period and remove it from the **Periods** list.

## 4.6 Periods Permission Assignment

To access the Periods functionality, you must be a member of a Security Group that has an assigned Permission Role that grants permission.

Permission Assignments are not cascading; you must be assigned each Permission Assignment individually. For example, if you are granted *Edit*, you must also be granted *View* to select a period for editing.

The following table defines the required Permission Assignments needed to access the Periods functionality in File Plan Builder. For more information on Permission Roles, [See "Permission Roles" on page 5.](#)

Table 4-2 Periods Permission Assignment

Permission Assignment	Description
<b>View Periods Tab</b>	Provides access to the Periods vertical tab in File Plan Builder.
<b>View Periods</b>	Allows a user to read/view an existing period.
<b>Add Periods</b>	Allows a user to create a new period.
<b>Edit Periods</b>	Allows a user to edit an existing period.
<b>Remove Periods</b>	Allows a user to delete an existing period.

## 5 Cutoff Events

Cutoff Event functionality is available in a SharePoint Records Center with Gimmal Compliance Suite enabled.

To use the Cutoff Event features in File Plan Builder, Gimmal Compliance Suite must be installed and the Gimmal Compliance Suite File Plan Builder feature must be active with the **Disposition Instruction** specifying *Cutoff* as the **Aging Method**. In addition, you must have the proper File Plan Builder: Permission Roles assigned. For File Plan Builder: Permission Roles settings, see [5.7 Cutoff Events Permission Assignment](#).

---

### Note:

This chapter describes Cutoff Events. Information regarding Enterprise Events can be found in the next chapter when the Disposition Instructions specify the aging method as *Alternate Aging*. Enterprise Events allow for selectivity and more control over conditional-based aging than Cutoff Events do and do not require the cutoff process.

---

To instantiate and use the events created in File Plan Builder in your SharePoint Records Center, the **Gimmal Compliance Suite - Event Management Action** must be active.

Gimmal Compliance Suite supports user-defined cutoff events. A cutoff event is a definition of a happening that triggers records management processes and actions for a given record or set of records. An event instance is the actual occurrence of the defined event type. In Gimmal Compliance Suite, events support cutoff processing and Closing of Record Folders based on happenings that will occur at some unspecified/unknown time in the future. A few examples of event types include:

- Employee *John Doe* Termination
- Property *ABC* Sale
- Contract *XYZ* Expiration
- Project *123* Complete

Gimmal Compliance Suite provides the ability to create, edit, view, or delete cutoff events through File Plan Builder: **Cutoff Events**. In addition to **Cutoff Events**, event types can be created and managed through the Gimmal Compliance Suite Event Management: **Manage Events** list in your SharePoint Records Center. However, event types created and managed externally to File Plan Builder will not appear in File Plan Builder: **Cutoff Events**.

**Intended User:** Records Manager

## 5.1 Accessing the Events List

To access the **Cutoff Events** list:

1. Open **File Plan Builder**.
2. Select **Cutoff Events** from the vertical tabs. The Cutoff Events list displays.

## 5.2 Cutoff Events List

The following table describes the **Cutoff Events** list with a description of each heading.

*Table 5-1 Cutoff Events List*

List View Heading	Description
Cutoff Event Name	<p>Unique name that differentiates the cutoff event from other event types.</p> <p>The <b>Cutoff Event Name</b> is used in the <b>File Plan Structure</b> dialog box as the selection list for <b>Cutoff Criteria: Enable Events → Cutoff Event(s)</b>. The <b>Cutoff Event Name</b> is also used on the corresponding <b>Record Container(s)</b> and/or <b>Record Item(s)</b> dialog boxes in your <b>SharePoint Records Library</b>.</p> <p>Example: Project 123 Complete</p>
Description	Descriptive statement used to further differentiate the cutoff event from other event types.

The **Cutoff Events** list uses the standard filter and sort capabilities.

## 5.3 Adding a New Cutoff Event

Before an event can be used for cutoff processing, you must create a cutoff event by performing the following steps:



1. In the **Cutoff Events** list, click **Add Item**. The Cutoff Event: Add dialog opens.

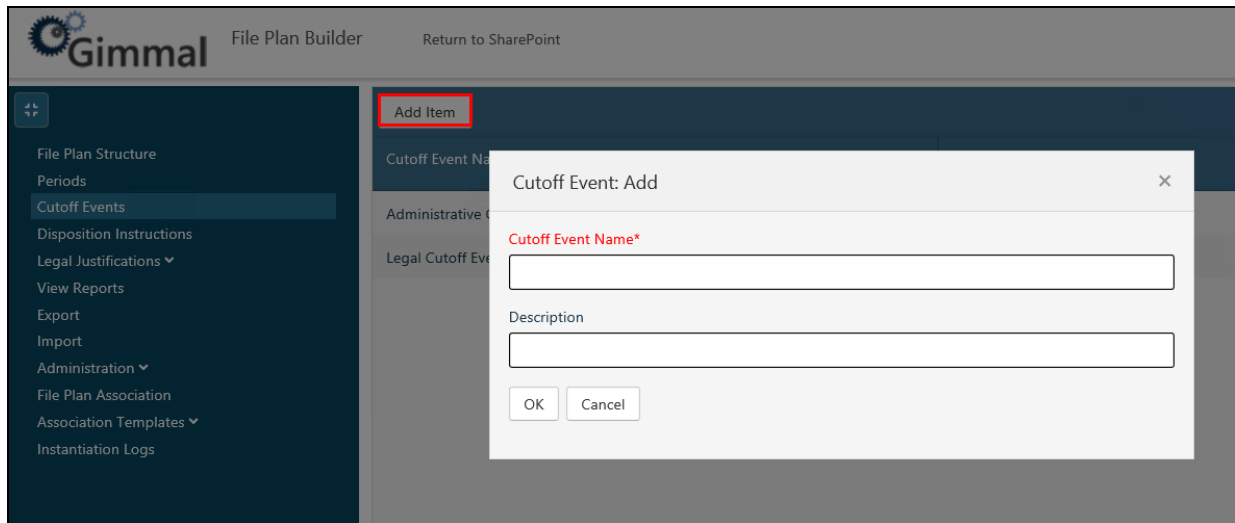


Figure 5-1 Adding a New Cutoff Event

2. Enter the following information:
  - a. **(Required)** Enter the **Cutoff Event Name**. The **Cutoff Event Name** is a unique identifier for the new cutoff event.
  - b. Enter a **Description**. The **Description** is a descriptive statement that defines the purpose of this cutoff event.
  - c. Click **OK**. The new cutoff event is created and displays in the **Cutoff Event** list.
    - After you save the new cutoff event, it will appear as a selection in the **Cutoff Criteria: Enable Events** → **Cutoff Event(s)** on the **File Plan: Cutoff Criteria** tab.
    - After you save the new cutoff event and the File Plan Instantiation timer job is executed, it will appear on all relevant SharePoint Records Center dialog boxes. These dialog boxes include the **Gimmel Compliance Suite Event Management Events** list and the **Cutoff Criteria: Enable Events** field options in the **Record Container and/or Record Item** dialog boxes.

## 5.4 Viewing a Cutoff Event

To view the details of an existing cutoff event, perform the following steps:

- From the **Cutoff Events** list, select the ellipsis (...) to the right of the cutoff event you want to view, and then click **View** from the drop-down menu. The Cutoff Event: View dialog opens, showing you the details of that cutoff event.

## 5.5 Editing a Cutoff Event

To edit an existing cutoff event, perform the following steps:

1. From the **Cutoff Event** list, click the ellipsis (...) to the right of the cutoff event that you want to edit, and then click **View** from the drop-down menu. The Cutoff Event: View dialog opens.

Figure 5-2 Editing a Cutoff Event

2. Click the **Edit** button at the bottom of the dialog. The dialog updates with editable fields for the selected cutoff event, and the title of the dialog title changes from Cutoff Event: View to Cutoff Event: Edit.
3. Update the information as desired.
4. Click **OK** to update the cutoff event and display the changes in the **Cutoff Events** list.
  - After you save the cutoff event change, the updated cutoff event will appear as a selection in the **Cutoff Criteria: Enable Events** → **Cutoff Event(s)** in the **File Plan Structure** dialog box.
  - After you save the cutoff event changes and the File Plan Instantiation timer job is executed, the following occurs:
    - If you changed the cutoff event **Name**, the updated cutoff event will appear in your SharePoint Records Center as a new cutoff event.
    - The updated cutoff event will appear on all relevant SharePoint Records Center dialog boxes. These dialog boxes include the Gimmel Compliance Suite Event Management: **Manage Events** list and the **Cutoff Criteria: Enable Events** field options in the **Record Container** and/or **Record Item** dialog boxes.

## 5.6 Deleting a Cutoff Event

To delete an existing cutoff event from your site, perform the following steps.

---

### Note

You cannot delete a cutoff event that is assigned to a file plan node *Cutoff Criteria*. If you attempt to do so, the **Delete** option is grayed out and not available for selection.

---

1. From the **Cutoff Event** list, select the ellipsis (...) to the right of the cutoff event you want to delete, and then click **Delete** from the drop-down menu. A Confirm Removal dialog opens, asking you confirm the removal.
2. Click **OK** to delete the cutoff event and remove it from the **Cutoff Events** list.

## 5.7 Cutoff Events Permission Assignment

To access the Cutoff Events functionality, you must be a member of a Security Group that has an assigned Permission Role that grants permission.

Permission Assignments are not cascading; you must be assigned each Permission Assignment individually. For example, if you are granted *Edit*, you must also be granted *View* to select a cutoff event for editing.

The following table defines the required Permission Assignment needed to access the Cutoff Events functionality in File Plan Builder. For more information on Permission Roles, [See "Permission Roles" on page 5.](#)

Table 5-2 Cutoff Events Permission Assignment

Permission Assignment	Description
<b>View Event Tab</b>	Provides access to the <b>Cutoff Events</b> vertical tab in File Plan Builder.
<b>View Events</b>	Allows a user to read/view an existing cutoff event.
<b>Add Events</b>	Allows a user to create a new cutoff event.
<b>Edit Events</b>	Allows a user to edit an existing cutoff event.
<b>Remove Events</b>	Allows a user to delete an existing cutoff event.

Cutoff events managed in your SharePoint Records Center Gimmal Compliance Suite Event Management: **Manage Events** list have an additional level of security that can be applied directly to each cutoff event through the **Manage Permissions** dialog box. For more details, see the "Event Management" section of the *Gimmal Compliance Suite User Guide*.

## 6 Disposition Actions

Disposition Actions functionality is available in a SharePoint Records Center with Gimmel Compliance Suite enabled. To use the disposition actions features in File Plan Builder, Gimmel Compliance Suite must be installed and the Gimmel File Plan Builder feature must be active. Workflows are identified by name; therefore, the name of the workflow associated to a library must be the same as the name of the workflow mentioned in the Disposition Action of File Plan Builder. In addition, you must have the proper File Plan Builder: **Permission Roles** assigned. For File Plan Builder: Permission Roles settings, see the [6.6 Disposition Actions Permission Assignment](#)

Gimmel Compliance Suite supports administrator-defined disposition actions. A disposition action defines the technical parameters for records management disposition processes. A disposition action is a prerequisite step for disposition instructions, which are used to define the lifecycle/disposition stages and processes for records based on your organization's record management policies. Workflows are identified by name; therefore, the name of the workflow associated to a library must be the same as the name of the workflow mentioned in the Disposition Action of File Plan Builder. A few examples of disposition actions include:

- Delete
- Delete Previous Version
- Link
- Move
- Record
- Recycle
- Remove Drafts
- Skip
- Workflow Actions

**Gimmel Compliance Suite** provides the ability to create, edit, view, or delete disposition actions.

**Intended User:** Compliance Suite Administrator

To access the **Disposition Actions** list:

1. Open **File Plan Builder**.
2. Select **Administration** from the vertical tabs. The Administration context menu opens
3. Click the **Disposition Actions** option. The Disposition Actions list opens.

## 6.1 Disposition Actions List

The following table describes the **Disposition Actions** list with a description of each heading.

Table 6-1 Disposition Actions List Headings

List View Heading	Description
<b>Name</b>	Unique name that differentiates the disposition action from other disposition actions.  The <b>Name</b> is used in the <b>Disposition Instructions</b> dialog boxes as the selection list for <b>Disposition Action</b> field on the <b>Stages</b> tab.
<b>Description</b>	Descriptive statement used to further differentiate the disposition action from other disposition actions.
<b>Parameter</b>	Technical parameters for the disposition action are shown in the menu, as shown in the illustration later in this chapter.

The **Disposition Actions** list uses the standard filter and sort capabilities.

## 6.2 Adding a New Disposition Action

Before they can be used to support your organization's record management policies, you must create disposition actions by performing the following steps. If you want to add new disposition actions manually, please refer to Microsoft user help for SharePoint.

1. From the **Disposition Actions** list, click **Add Item**. The Disposition Action: Add dialog opens.

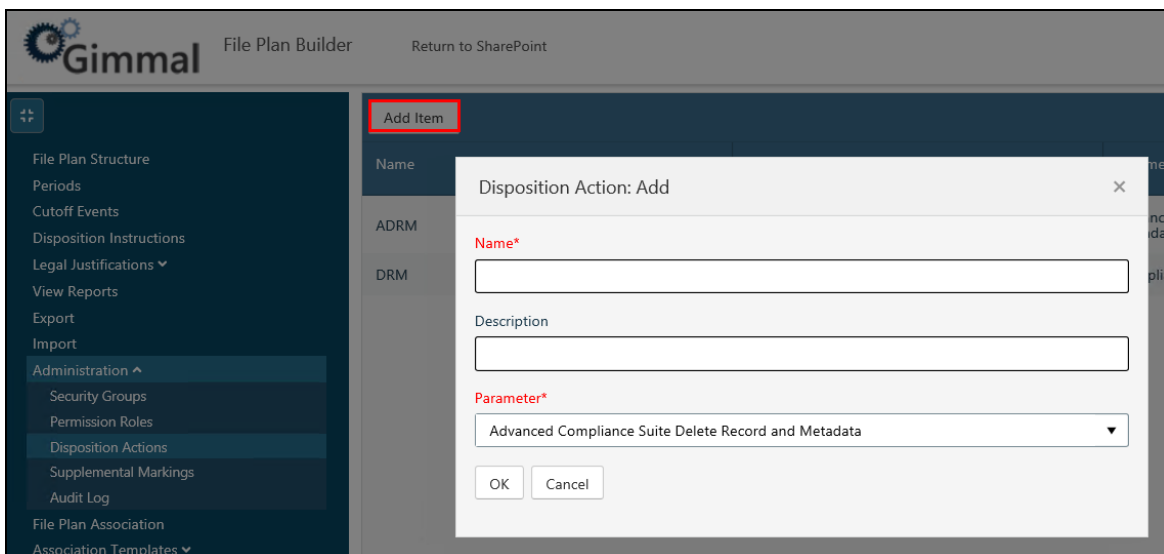


Figure 6-1 Adding a New Disposition Action

2. Enter the following information:
  - a. **(Required)** Enter the **Name**. The **Name** is a unique identifier for the new disposition action. The **Name** is used in the **Disposition Instructions** dialog box as the selection list for **Disposition Action** field on the **Stages** tab.

---

Note:

If you have already added the workflow that will be associated with this Disposition Action to one (or more) libraries, enter the unique name that you entered in the "Enter a unique name for this workflow:" field when adding the workflow to the library. If you have not yet associated the workflow with any libraries, when you do, ensure that you enter this value in the "Enter a unique name for this workflow:" field.

- 
- b. Enter a **Description**. The **Description** is a descriptive statement that defines the purpose of this disposition action.
  - c. **(Required)** Select a Parameter. The Parameter defines what workflow to trigger or action to complete when processing a document. File Plan Builder provides a list of available options to choose from.

---

Note:

If the Parameter selected is a workflow, the specified workflow must exist in the target library where nodes using this action will be deployed to.

- 
3. Click **OK** and the new disposition action is created and now displays in the **Disposition Actions** list.

After you save the new disposition action, it displays as an option in the **Disposition Instructions** dialog box and as the selection list for the **Disposition Action** field on the **Stages** tab.

## 6.3 Viewing a Disposition Action

To view the details of an existing disposition action, perform the following step:

- From the **Disposition Actions** list, select the ellipsis (...) to the right of the disposition action you want to view, and then click **View** from the drop-down menu. The Disposition Action: View dialog opens, showing you the details of that disposition action.

## 6.4 Editing a Disposition Action

To edit an existing disposition action, perform the following steps:

1. From the **Disposition Actions** list, click the ellipsis (...) to the right of the disposition action you want to edit, and then click **View** from the drop-down menu. The Disposition Action: View dialog opens.

Figure 6-2 Editing a Disposition Action

2. Click the **Edit** button at the bottom of the dialog. The dialog updates with editable fields for the selected disposition action, and the title of the dialog title changes from Disposition Action: View to Disposition Action: Edit.
3. Update the information in as desired.
4. Click **OK**. The disposition action is updated and the changes appear in the **Disposition Actions** list.
5. After you save the disposition action, the following occurs:
  - Any existing disposition instructions that use this disposition action will have the updated parameters applied henceforth.
  - The updated disposition action will appear as an option in the **Disposition Instructions** dialog box as the selection list for **Disposition Action** field on the *Stages* tab.

## 6.5 Deleting a Disposition Action

To delete an existing disposition action from your site, perform the following steps.

---

### Note

You cannot delete a disposition action that is assigned to one or more disposition instruction(s). If you attempt to do so, the **Delete** option is grayed out and not available for selection.

---

1. From the **Disposition Actions** list, click the ellipsis (...) to the right of the disposition action you want to delete, and then click **Delete** from the drop-down menu. A Confirm Removal dialog opens, asking you confirm the removal.

2. Click **OK**. The disposition action is deleted and removed from the **Disposition Actions** list.

## 6.6 Disposition Actions Permission Assignment

To access the **Disposition Actions** functionality, you must be a member of a disposition action that has an assigned Permission Role that grants permission.

Permission Assignments are not cascading; you must be assigned each Permission Assignment individually. For example, if you are granted *Edit*, you must also be granted *View* to select a disposition action for editing.

The following table defines the required Permission Assignment needed to access the *Disposition Actions* functionality in File Plan Builder. For more information on Permission Roles, [See "Permission Roles" on page 5.](#)

Table 6-2

Permission Assignment	Description
<b>View Administration Tab</b>	Provides access to the <b>Administration</b> features in File Plan Builder.  <b>Administration</b> is a vertical tab in File Plan Builder.
<b>View Disposition Actions</b>	Provides access to the <b>Disposition Actions</b> tab in the Administration section of File Plan Builder.  Allows a user to read/view an existing disposition action.
<b>Add Disposition Actions</b>	Allows a user to create a new disposition action.
<b>Edit Disposition Actions</b>	Allows a user to edit an existing disposition action.
<b>Remove Disposition Actions</b>	Allows a user to delete an existing disposition action.



## 7 Disposition Instructions

Disposition Instructions functionality is available in a SharePoint Records Center with Gimmel Compliance Suite enabled. To use the disposition instructions features in File Plan Builder, Gimmel Compliance Suite must be installed and the Gimmel Compliance Suite File Plan Builder feature must be active. In addition, you must have the proper File Plan Builder: **Permission Roles** assigned. For File Plan Builder: **Permission Roles** settings, see section ["7.1 Disposition Instructions Permission Assignment"](#).

Gimmel Compliance Suite provides the ability to create, edit, view, or delete disposition instructions. Before the creation of disposition instructions, disposition action(s) must be created by the Compliance Suite Administrator.

Disposition instructions are activities performed on records that fulfill record disposition requirements. They contain commands that define what to do with records at certain points in their lifecycle. The instructions consist of lifecycle stages that define duration specifications (that is, two months) and actions (that is, Delete Record) to be performed when the duration specification is met. There are three types of aging processes for disposition instructions:

- *Cutoff* is a mandatory preapproval process that is necessary for aging to commence and requires Record Manager approval for aging.
- If you select *Alternate Aging*, you can select Calendar or Enterprise Event for Stage Activation. For Alternate Aging, you have the option of having the retention of records based on Calendar-based aging or Enterprise Events, which will activate a disposition instruction. There is no preapproval process for this as there is in Cutoff; therefore, records start aging immediately following the date used for Calendar-based aging or the Enterprise Event. Once the date column specified, such as declared date or fiscal year, contains a date, the expiration date can be calculated. The duration specified in the stage is added to this date to determine the effective expiration date. The disposition action specified in the stage will determine what action to take when the record's expiration date has elapsed.
- *Enterprise Events* (EE) configures information management policies (IMPs) using actions to drive record creation and approval.

**Intended User:** Records Manager

### 7.1 Disposition Instructions Permission Assignment

To access the Disposition Instructions functionality, you must be a member of a Security Group that has an assigned Permission Role that grants permission.

Permission Assignments are not cumulative; you must be assigned each Permission Assignment individually. For example, if you are granted *Edit*, you must also be granted *View* to select a disposition instruction for editing.

The following table defines the required Permission Assignments needed to access the Disposition Instructions functionality in File Plan Builder. For more information on Permission Roles, [See "Permission Roles" on page 5.](#)

Table 7-1 Disposition Instructions Permission Assignment

Permission Assignment	Description
<b>View Disposition Instruction Tab</b>	Provides access to the Disposition Instructions vertical tab in File Plan Builder.
<b>View Disposition Instructions</b>	Allows a user to read/view an existing disposition instruction.
<b>Add Disposition Instructions</b>	Allows a user to create a new disposition instruction.
<b>Edit Disposition Instructions</b>	Allows a user to edit an existing disposition instruction
<b>Remove Disposition Instructions</b>	Allows a user to delete an existing disposition instruction.

To access the **Disposition Instructions** list:

1. Open **File Plan Builder**.
2. Select **Disposition Instructions** from the vertical tabs.

## 7.2 Disposition Instructions List

The following table describes the **Disposition Instructions** list, with a description of each field.

Table 7-2

List View Heading	Description
<b>Name</b>	Unique name that differentiates the disposition instruction from other disposition instructions.  The <b>Name</b> is used in the <b>File Plan: General</b> dialog box as the selection list for <b>Disposition Instructions</b> .
<b>Description</b>	Descriptive statement used to further differentiate the disposition instruction from other disposition instructions.
<b>Aging Method</b>	Lists the Aging Method that was selected for the disposition instruction.
<b>Stage Errors</b>	Descriptive statement about an error received for a stage, due to a change in the aging method of the Disposition Instruction.

## 7.3 Creating a Disposition Instruction

Before end users, such as Records Managers, can create a file plan node, disposition instructions must be created. You can create disposition instructions to use one of two aging methods: *Cutoff* or *Alternate Aging*.

After you create the disposition instruction, you must then define a stage(s) which tells File Plan Builder how to process the instruction (for example, "Delete" or "After X days, move to Folder B"). You can create stages for either the *Cutoff* aging method or *Alternate Aging*.

### 7.3.1 Using Aging Method *Cutoff* in Disposition Instructions

Follow the steps in this section to create a disposition instruction that uses *Cutoff* as the aging method.

1. From the Disposition Instructions list, click **Add Item**. The Disposition Instruction: Add dialog opens.

The screenshot shows the Gimmel File Plan Builder interface. On the left is a navigation menu with options like 'File Plan Structure', 'Periods', 'Cutoff Events', 'Disposition Instructions', 'Legal Justifications', 'View Reports', 'Export', 'Import', 'Administration', 'File Plan Association', 'Association Templates', and 'Instantiation Logs'. The 'Disposition Instructions' menu item is highlighted. In the main area, there is a table with columns for Name, Administrative, Human Resources, Disposition Instructions, and Legal Contracts. An 'Add Item' button is highlighted with a red box. A dialog box titled 'Disposition Instruction: Add' is open, containing the following fields: 'Name\*' (a text input field), 'Description' (a text input field), and 'Aging Method\*' (a dropdown menu with 'Cutoff' selected). At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Figure 7-1 Creating a Disposition Instruction using *Cutoff*

2. Enter the following information:
  - a. **(Required)** Enter the **Name**. The **Name** is a unique identifier for the new disposition instruction.

---

#### Note:

It can be helpful to include the type of aging in the Disposition Instruction name.

---

- b. Enter a **Description**. The **Description** is a descriptive statement that defines the purpose of this disposition instruction.

3. Select *Cutoff* from the **Aging Method** drop-down. See the "Cutoff and Closing Folder Processing" chapter of the *Compliance Suite User Guide* for more details.
4. Click **OK**. The new disposition instruction is created and displays in the **Disposition Instructions** list, or click **Cancel** to close the item detail section without creating a new disposition instruction.
5. After the new disposition instruction is saved, the new disposition instruction displays as an option in the **Disposition Instructions** field in the **File Plan: General** dialog box.

### 7.3.2 Adding a Stage for a *Cutoff* Disposition Instruction

Follow the steps in this section to add a stage for a *Cutoff* disposition instruction.

1. On the Disposition Instructions list, select the disposition instruction you want to add a stage for, ensuring that the Aging Method column reads **Cutoff**.
2. Click the ellipsis (...) to the right, and then click **Stages** from the context menu. The Disposition Stages dialog opens.

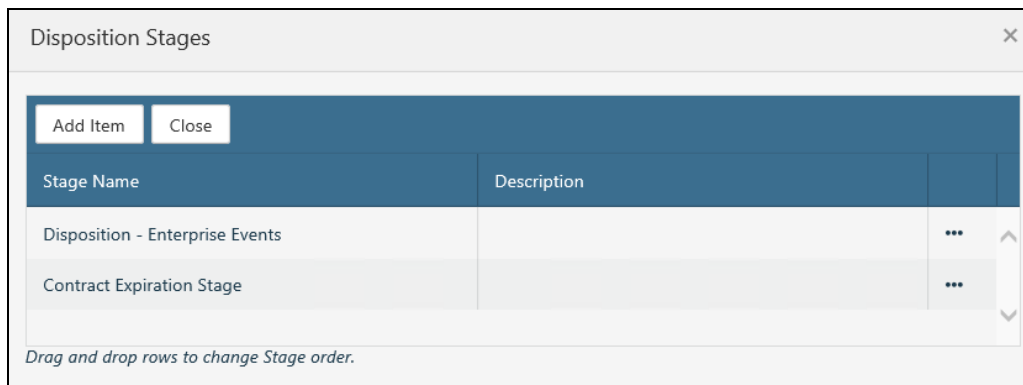


Figure 7-2 Disposition Stages Dialog for *Cutoff* Disposition Instruction

The dialog consists of the following:

- **Add/Save/Close:** The options at the top enable you to add a new stage, save changes made to the Disposition Stages dialog (e.g., after you reorder the stages list, a **Save** button displays at the top), and close the dialog.
  - **Stages** list: The dialog lists stages for this disposition instruction. After you create them, the stages are listed in chronological order, displaying the **Stage Name** and **Description**. This list provides the ability to view, delete, and reorder stages for this disposition instruction.
3. To add a new stage, click **Add Item** at the top of the dialog. The bottom of the dialog expands, and now displays the stage properties.
  4. Enter the following information:
    - a. **(Required)** Enter the **Stage Name**. The **Stage Name** is a unique identifier for the new stage.
    - b. Enter a **Description**. The **Description** is a statement that defines the purpose of this stage.

- c. **(Required)** Select the **Disposition Action**. The **Disposition Action** defines the technical parameters and process to apply to this stage. The selection options are based on existing disposition action items.

---

**Note:**

You must have created at least one Disposition Action for any to be available for selection. Please refer to ["Adding a New Disposition Action"](#) on page 46.

---

- d. **(Required)** Enter the **Duration**. The **Duration** defines the numerical time measurement length of this stage. The **Duration** defaults to 0. The **Duration** is used in combination with the **Units**; for example, **2 months**.
  - e. **(Required)** Select the **Units**. The **Units** define the time measurement unit to apply to this stage. The options are *Days*, *Weeks*, *Months*, *Quarters*, and *Years*. The **Units** defaults to *Days*. The **Units** is used in combination with the **Duration**; for example, **2 months**.
5. Click **OK** to save the stage. The new stage now displays on the Disposition Stages dialog.
  6. Repeat the previous steps to add additional stages to the disposition instruction.
  7. To reorder a stage, select the **Stage** you want to reorder, drag it up or down in the list, and then click **Save** at the top of the dialog.
  8. To view a stage, select the **Stage** you want to view, click the ellipsis (...) to the right of the stage, and then click **View**. The Disposition Stages: View dialog opens, enabling you to see the read-only properties of the stage.
  9. To edit a stage, from the Disposition Stages: View dialog referenced in the previous step, click **Edit** at the bottom of the dialog. The properties become editable.
  10. Make the desired changes to the stage properties, and then click **OK**. The stage updates and redisplay on the Stages list.
  11. To remove a stage, on the Disposition Stages dialog, click the ellipsis (...) to the right of the stage you want to remove, and then click **Delete**. A Confirm Removal message displays, asking if you are sure you want to delete the stage.
    - Click **OK** to remove the stage from the Stages list.
    - Click **Cancel** to return to the Stages list without removing the selected stage.

### 7.3.3 Using Alternate Aging Calendar in Disposition Instructions

Follow the steps in this section to create a disposition instruction that uses *Calendar* as the **Alternate Aging** method.

1. From the Disposition Instructions list, click **Add Item**. The Disposition Instruction: Add dialog opens.

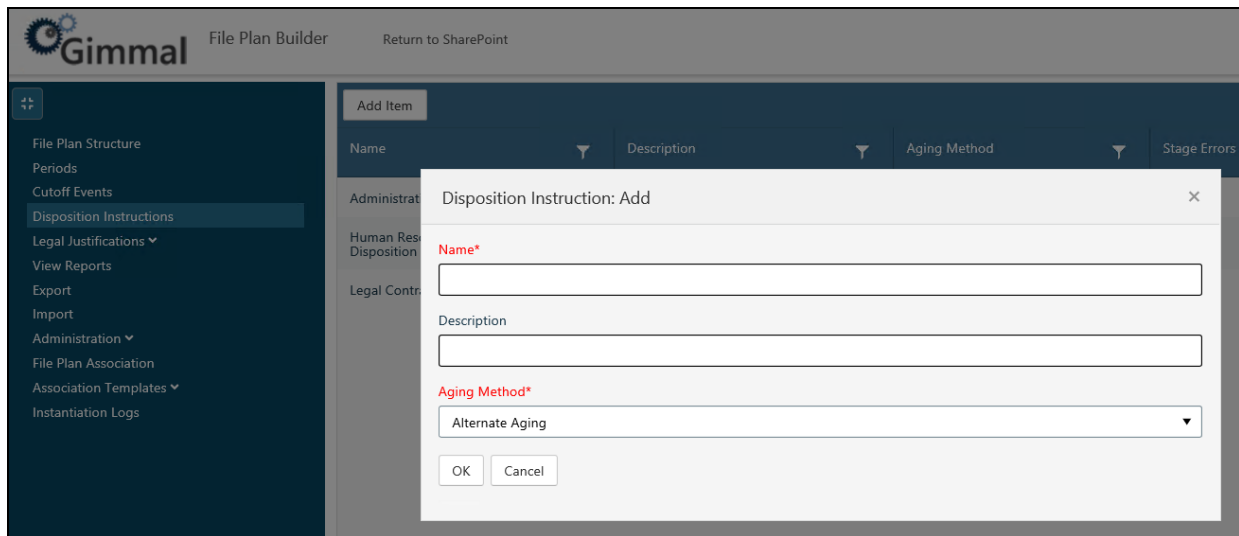


Figure 7-3 Creating a Disposition Instruction using Alternate Aging

2. Enter the following information:
  - a. **(Required)** Enter the **Name**. The **Name** is a unique identifier for the new disposition instruction.

---

#### Note:

It can be helpful to include the type of aging in the Disposition Instruction name.

---

- b. Enter a **Description**. The **Description** is a descriptive statement that defines the purpose of this disposition instruction.
3. Select *Alternate Aging* from the **Aging Method** drop-down.
  4. Click **OK**. The new disposition instruction is created and displays in the **Disposition Instructions** list, or click **Cancel** to close the item detail section without creating a new disposition instruction.
  5. After the new disposition instruction is saved, the new disposition instruction displays as an option in the **Disposition Instructions** field in the **File Plan: General** dialog box.

### 7.3.4 Adding a Stage for an *Alternate Aging* Disposition Instruction

Follow the steps in this section to add a stage for an *Alternate Aging* disposition instruction.

1. On the Disposition Instructions list, select the disposition instruction you want to add a stage for, ensuring that the Aging Method column reads **Alternate Aging**.

2. Click the ellipsis (...) to the right, and then click **Stages** from the context menu. The Disposition Stages dialog opens.

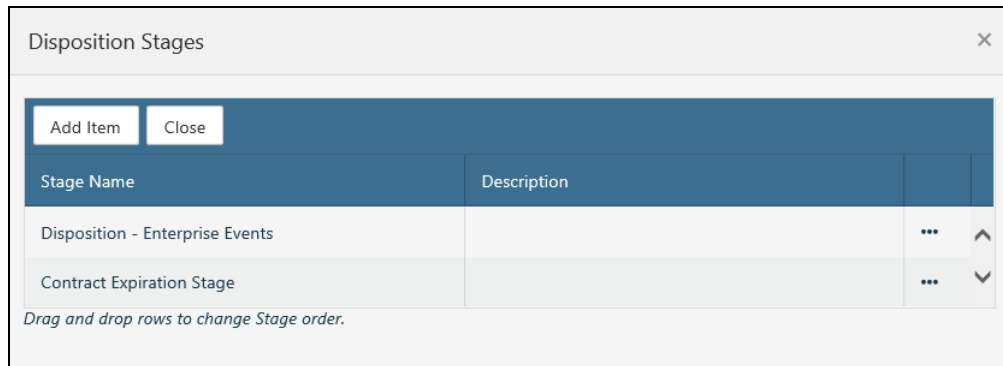


Figure 7-4 Disposition Stages Dialog for Alternate Aging Disposition Instruction

The dialog consists of the following:

- **Add/Save/Close:** The options at the top enable you to add a new stage, save changes made to the Disposition Stages dialog (e.g., if you reorder the stages list, a **Save** button displays at the top), and close the dialog.
  - **Stages** list: The dialog lists stages for this disposition instruction. After you create them, the stages are listed in chronological order, displaying the **Stage Name** and **Description**. This list provides the ability to view, delete, and reorder stages for this disposition instruction.
3. To add a new stage, click **Add Item** at the top of the dialog. The bottom of the dialog expands, and now displays the stage properties.
  4. Enter the following information:
    - a. **(Required)** Enter the **Stage Name**. The **Stage Name** is a unique identifier for the new stage.

---

#### Note:

It can be helpful to include the type of aging in the Disposition Instruction name.

---

- b. Enter a **Description**. The **Description** is a statement that defines the purpose of this stage.
- c. **(Required)** For **Stage Activation Type**, the default is **Calendar**. This cannot be changed.
- d. **(Required)** Select the **Disposition Action**. The **Disposition Action** defines the technical parameters and process to apply to this stage. The selection options are based on existing disposition action items.

---

**Note:**

You must have created at least one Disposition Action for any to be available for selection. Please refer to [“Adding a New Disposition Action” on page 46.](#)

---

- e. **(Required)** Enter the **Duration**. The **Duration** defines the numerical time measurement length of this stage. The **Duration** defaults to 1. The **Duration** is used in combination with the **Units**; for example, **2 months**.
- f. **(Required)** Select the **Units**. The **Units** define the time measurement unit to apply to this stage. The options are *Days, Weeks, Months, Quarters, and Years*. The **Units** defaults to Days. The **Units** is used in combination with the **Duration**; for example, **2 months**.
- g. **(Required)** In the **Date Column Name** field, enter the name of either an existing Date Column as listed in the stage properties of the associated Information Management Policy (IMP) (i.e., Created Declared Record, Modified, etc.), or enter the name of a new Date Column you want to create for that association. The **Date Column Name** applies to all libraries using this disposition instruction.

Existing columns for the **Date Column Name** are searched in the following order:

- i. List Columns (internal name)
- ii. List Columns (display name)
- iii. Site Columns by (internal name)
- iv. Site Columns by (display name)

The screenshot shows a configuration form for a Date Column Name. It includes a text input field for the name, a checkbox for 'Create as list column', and radio buttons for 'Default date value' options: '(None)', 'Today's Date', 'Enter Date' (with a date picker), and 'Calculated Value'. A note below the radio buttons states 'Calculated Value formulas are not validated.' To the right, a tool tip box explains the search order: 'The name of the column that will be used as the date column for the associated Information Management Policy stage. Existing columns will be searched in the following order: List Columns (internal name), List Columns (display name), Site Columns (internal name), Site Columns (display name). If the column is not found, a new column will be created at the site or list level depending on the option selected.'

*Figure 7-5 Date Column Name Tool Tip*

If File Plan Builder cannot find the indicated column under List Columns, but it finds an existing Site Column, it adds the existing Site Column to the list and all content types in the list, along with adding it to the default view. By default, if the column is not found, File Plan Builder creates the column at the site or list level, depending on the option selected, and adds that column to all content types and the default view in the aforementioned list.

- h. If you want to create the **Date Column Name** at the list level instead of the default site level, select the **Create as list column** check box.



- i. Select the **Default date value**, if this is a new column. If an existing column is present, its default date value does not change if you specify it here.
  - **None** (default)
  - **Today's Date**
  - **Enter Date**
  - **Calculated Value**

---

Note:

If you create a new date column, the column is added to content types. You do not see the column until the record has been routed to its final location.

---

5. Click **OK** to save the stage. The new stage now displays on the Disposition Stages dialog.
6. Repeat the previous steps to add additional stages to this disposition instruction.
7. To reorder a stage, select the **Stage** you want to reorder, drag it up or down in the list, and then click **Save** at the top of the dialog.
8. To view a stage, select the **Stage** you want to view, click the ellipsis (...) to the right of the stage, and then click **View**. The Disposition Stages: View dialog opens, enabling you to see the read-only properties of the stage.
9. To edit a stage, from the Disposition Stages: View dialog referenced in the previous step, click **Edit** at the bottom of the dialog. The properties become editable.
10. Make the desired changes to the stage properties, and then click **OK**. The stage updates and redisplay on the Stages list.
11. To remove a stage, on the Disposition Stages dialog, click the ellipsis (...) to the right of the stage you want to remove, and then click **Delete**. A Confirm Removal message displays, asking if you are sure you want to delete the stage.
  - Click **OK** to remove the stage from the Stages list.
  - Click **Cancel** to return to the Stages list without removing the selected stage.

### 7.3.5 Using Alternate Aging *Enterprise Events* in Disposition Instructions

If you want to create a disposition instruction based on an Enterprise Event, Gimmel Enterprise Events must be configured in File Plan Builder.

---

Note:

When using Enterprise Events in File Plan Builder, it is best practice to create all event stages before instantiation.

---

## Configuring File Plan Builder for Enterprise Events

If you do not configure File Plan Builder for Enterprise Events, the **Event** option is not accessible as a **Stage Activation Type** and is disabled.

Follow these steps to configure File Plan Builder for Enterprise Events:

1. Navigate to Central Administration and select **File Plan Builder Settings** under Compliance Suite. The File Plan Builder Settings page displays.
2. Scroll to the bottom of the page to view **Enterprise Events** Settings.

Enterprise Events Location

To enable File Plan Builder to use Enterprise Events, enter the fully qualified hostname and HTTP/SSL port numbers for the server that hosts the Enterprise Events web application.

Hostname  
  
 Example: corp.contoso.com

HTTP Port

SSL Port

Figure 7-6 File Plan Builder Enterprise Events Settings

3. Enter the **Hostname**, **HTTP Port**, and **SSL Port** for the server where Enterprise Events is installed.
4. Click **Save**.

## Using Enterprise Events

Follow the steps in this section to create a disposition instruction that uses *Enterprise Events* as the **Alternate Aging** method.

1. From the Disposition Instructions list, click **Add Item** at the top of the screen. The Disposition Instruction: Add dialog opens.
2. Enter the following information:
  - a. **(Required)** Enter the **Name**. The **Name** is a unique identifier for the new disposition instruction.
  - b. Enter a **Description**. The **Description** is a statement that defines the purpose of this disposition instruction.

3. Select *Alternate Aging* from the **Aging Method** drop-down.

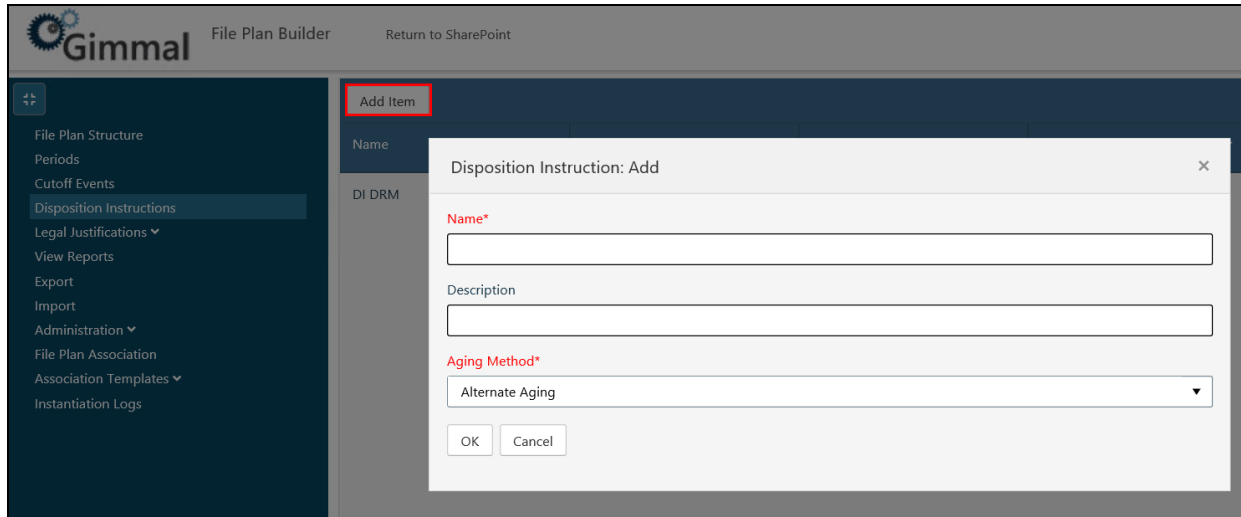


Figure 7-7 Creating a Disposition Instruction Using Alternate Aging

4. Click **OK**. The new disposition instruction is created and displays in the **Disposition Instructions** list, or click **Cancel** to close the item detail section without creating a new disposition instruction.
5. After the new disposition instruction is saved, the new disposition instruction displays as an option in the **Disposition Instructions** field in the **File Plan: General** dialog box.

### 7.3.6 Adding a Stage for an Enterprise Event *Alternate Aging* Disposition Instruction

Follow the steps in this section to add a stage for an Enterprise Events *Alternate Aging* disposition instruction.

1. On the Disposition Instructions list, select the disposition instruction you want to add a stage for, ensuring that the Aging Method column reads **Alternate Aging**.
2. Click the ellipsis (...) to the right, and then click **Stages** from the context menu. The Disposition Stages dialog opens.

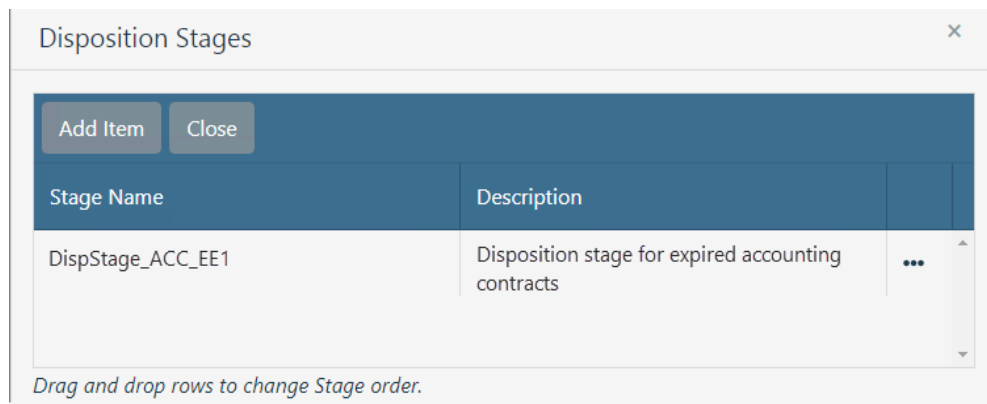


Figure 7-8 Disposition Stages Dialog for Enterprise Events *Alternate Aging* Disposition Instruction

The dialog consists of the following:

- **Add/Save/Close:** The options at the top enable you to add a new stage, save changes made to the Disposition Stages dialog (e.g., if you reorder the stages list, a **Save** button displays at the top), and close the dialog.
  - **Stages** list: The dialog lists stages for this disposition instruction. After you create them, the stages are listed in chronological order, displaying the **Stage Name** and **Description**. This list provides the ability to view, delete, and reorder stages for this disposition instruction.
3. To add a new stage, click **Add Item** at the top of the dialog. The bottom of the dialog expands, and now displays the stage properties.
  4. Enter the following information:
    - a. **(Required)** Enter the **Stage Name**. The **Stage Name** is a unique identifier for the new stage.

---

**Note:**

It can be helpful to include the type of aging in the Disposition Instruction name.

---

- b. Enter a **Description**. The **Description** is a statement that defines the purpose of this stage.
- c. **(Required)** For **Stage Activation Type**, select **Enterprise Events**.
- d. **(Required)** Select the **Disposition Action**. The **Disposition Action** defines the technical parameters and process to apply to this stage. The selection options are based on existing disposition action items.

---

**Note:**

You must have created at least one Disposition Action for any to be available for selection. Please refer to ["Adding a New Disposition Action" on page 46](#).

---

- e. **(Required)** Enter the **Event Stage**.
5. Click **OK** to save the stage. The new stage now displays on the Disposition Stages dialog.
6. Repeat the previous steps to add additional stages to this disposition instruction.
7. To reorder a stage, select the **Stage** you want to reorder, drag it up or down in the list, and then click **Save** at the top of the dialog.
8. To view a stage, select the **Stage** you want to view, click the ellipsis (...) to the right of the stage, and then click **View**. The Disposition Stages: View dialog opens, enabling you to see the read-only properties of the stage.
9. To edit a stage, from the Disposition Stages: View dialog referenced in the previous step, click **Edit** at the bottom of the dialog. The properties become editable.

10. Make the desired changes to the stage properties, and then click **OK**. The stage updates and redisplay on the Stages list.
11. To remove a stage, on the Disposition Stages dialog, click the ellipsis (...) to the right of the stage you want to remove, and then click **Delete**. A Confirm Removal message displays, asking if you are sure you want to delete the stage.
  - Click **OK** to remove the stage from the Stages list.
  - Click **Cancel** to return to the Stages list without removing the selected stage.

## 7.4 Viewing a Disposition Instruction

To view an existing disposition instruction, follow these steps.

1. From the **Disposition Instruction** list, select the disposition instruction you want to edit. Only one disposition instruction can be selected at a time. When a disposition instruction is selected, the item detail section updates with read-only fields for the selected disposition instruction.
2. Click the ellipsis (...) to the right of the instruction, and then select **View**. The Disposition Instruction: View dialog opens, showing you the read-only properties for the selected disposition instruction.

## 7.5 Editing a Disposition Instruction

To change an existing disposition instruction, follow these steps.

1. From the **Disposition Instruction** list, select the disposition instruction you want to edit. Only one disposition instruction can be selected at a time. When a disposition instruction is selected, the item detail section updates with read-only fields for the selected disposition instruction.
2. Click the ellipsis (...) to the right of the instruction, and then select **View**. The Disposition Instruction: View dialog opens, showing you the read-only properties for the selected disposition instruction.
3. Click **Edit** at the bottom of the dialog. The properties now become editable.
4. Update the information for the properties you want to change.
5. Click **OK**. The disposition instruction is updated and the changes appear in the **Disposition Instructions** list.
6. After the disposition instruction change is saved:
  - Any existing file plan nodes that use this disposition instruction will have the updated parameters applied hence forth.
  - The updated disposition instruction will appear as an option in the **Disposition Instructions** field in the **File Plan: General** dialog box.

## 7.6 Copying a Disposition Instruction

You can create a copy of a disposition instruction.

1. Select the disposition instruction you want to copy. A **Copy** button displays at the top of the Disposition Instructions list.
2. Click **Copy**. The Disposition Instruction: Create a Copy dialog opens.
3. Change the parameters of the new disposition instruction as desired. (Note that "- Copy" is appended to the original instruction's name.)
4. Click **OK** to copy the instruction. The new instruction displays in the Disposition Instructions list.

## 7.7 Deleting a Disposition Instruction

To delete an existing disposition instruction, perform the following steps.

---

### Note

You cannot remove a disposition instruction that is assigned to a file plan node; If you attempt to do so, the **Delete** option is grayed out and not available for selection.

---

1. From the **Disposition Instructions** list, select the disposition instruction you want to delete, click the ellipsis (...) to the right, and then click **Delete**. A Confirm Removal dialog opens, asking you to confirm the deletion.
2. Click **OK**. The disposition instruction is deleted and removed from the **Disposition Instructions** list.

---

### Note:

If the selected disposition instruction is currently used by one or more file plan nodes, you will not be able to delete the disposition instruction.

---

## 8 Legal Authorities

Legal Authorities functionality is available in a SharePoint Records Center with Gimmal Compliance Suite enabled. To use the Legal Authorities features in *File Plan Builder*, Gimmal Compliance Suite must be installed and the Gimmal Compliance Suite File Plan Builder feature must be active. In addition, you must have the proper File Plan Builder: Permission Roles assigned. For File Plan Builder: **Permission Roles** settings, see section [8.6 Legal Authorities Permission Assignment](#).

Gimmal Compliance Suite supports user-defined Legal Authorities. Legal Authorities define the group with legal authorization to manage the disposition or transfer of records based on your organization's record management policies. Legal Authorities are a prerequisite step for the creation of file plan nodes, which are the classification scheme for the storage of records based on your organization's records management policies. The Legal Authorities support the legal authorization for the disposition of records based on file plan node assignment.

Before the creation of Legal Authorities, Legal Requirements should be created by the Records Manager.

Gimmal Compliance Suite provides the ability to create, edit, view, or delete Legal Authorities. The terms *Legal Authority*, *Authority*, and *Disposition Authority* are used interchangeably.

**Intended User:** Records Manager

To access the Authorities view:

1. Open File Plan Builder.
2. Select **Legal Justifications** from the vertical tabs. The Legal Justifications context menu opens.
3. Select the **Authorities** option. The Legal Authorities list displays.

### 8.1 Legal Authorities List

The following table describes the **Legal Authorities** list with a description of each heading.

*Table 8-1 Legal Authorities*

List View Heading	Description
<b>Authority Code</b>	<p>Unique identifier that differentiates the Legal Authority from other Legal Authorities.</p> <p>The <b>Authority Code</b> is the name of the group that is granted legal authorization for disposition of records as defined by the selected <b>Requirements</b>.</p> <p>The <b>Authority Code</b> is used in the <b>File Plan: General</b> dialog box as the selection list for <b>Disposition Authority</b>.</p>

Table 8-1 Legal Authorities

List View Heading	Description
<b>Description</b>	<p>Descriptive statement used to further differentiate the Legal Authority from other Legal Authorities.</p> <p>The <b>Description</b> is used in the <b>File Plan: General</b> dialog box as the selection list description for <b>Disposition Authority</b>.</p>

The **Legal Authorities** list uses the standard filter and sort capabilities.

## 8.2 Creating a New Legal Authority

Before end users, such as Records Managers, can create a file plan node, Legal Authorities must be created.

1. From the **Legal Authorities** list, click **Add Item**. The Authority: Add dialog opens.

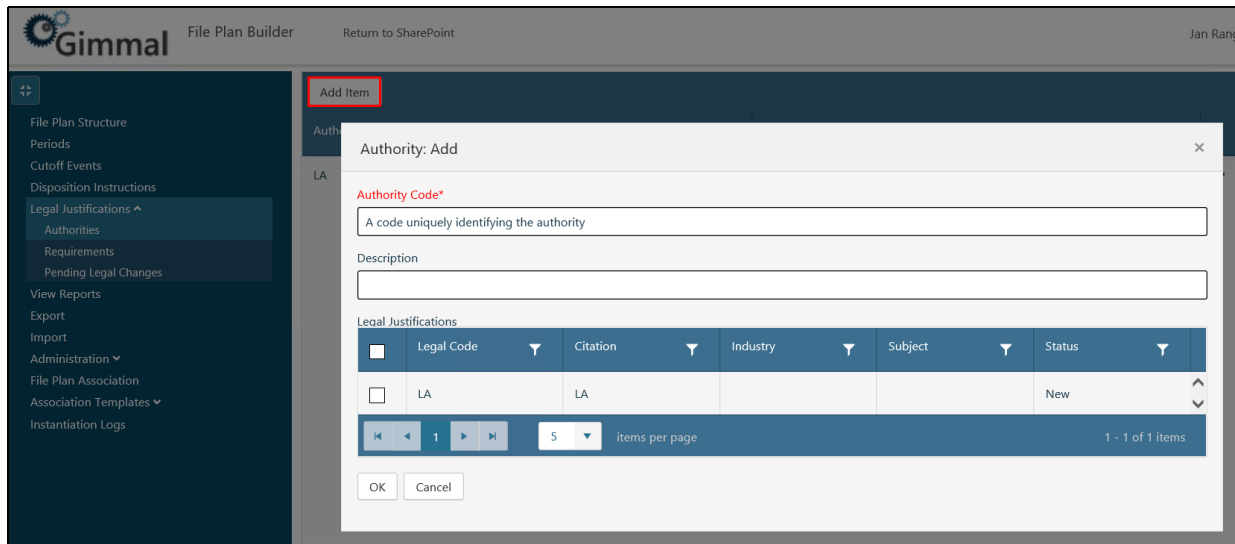


Figure 8-1 Adding a New Legal Authority

2. Enter the following information:
  - a. **(Required)** Enter the **Authority Code**. The **Authority Code** is a unique identifier for the new Legal Authority.
  - b. Enter a **Description**. The **Description** is a descriptive statement that defines the purpose of this Legal Authority.
  - c. Select one or more **Requirements**. The selection options are based on existing Legal Requirement items. The **Requirements** list displays the **Legal Code**, **Citation**, **Industry**, **Subject**, and **Status** for each Legal Requirement item.
    - o To filter the **Requirements** list, select the filter icon (🔍) in the heading for the column you want to filter on, enter your filter parameters, and click **Filter**.



- To add a new Legal Requirement to the list, perform the steps in Chapter 9 [Legal Requirements](#).

3. Click **OK** to save the new Legal Authority and display it in the **Legal Authorities** list.

After you save the new Legal Authority, the Legal Authority displays as an option in the **Disposition Authority** field in the **File Plan: General** dialog box.

## 8.3 Viewing a Legal Authority

To view the details of an existing Legal Authority, you must view the Legal Authority item.

- From the **Legal Authorities** list, click the ellipsis (...) to the right of the authority you want to view, and then click **View** from the drop-down menu. The Authority: View dialog opens, showing you the details of that authority.

## 8.4 Editing a Legal Authority

To change an existing Legal Authority, you must edit the Legal Authority item.

1. From the **Legal Authority** list, click the ellipsis (...) to the right of the authority you want to edit, and then click **View** from the drop-down menu. The Authority: View dialog opens.

Authority: View

Authority Code\*

Administration Legal Authority

Description

Administration Legal Authority

Legal Justifications

	Legal Code	Citation	Industry	Subject	Status
<input type="checkbox"/>	LA	LA			New

1 5 items per page 1 - 1 of 1 items

Edit Cancel

Figure 8-2 Editing a Legal Authority

2. Click the **Edit** at the bottom of the dialog. The dialog updates with editable fields for the selected Legal Authority.
3. Update the information as desired.
4. Click **OK**. The Legal Authority is updated and the changes appear in the **Legal Authorities** list.
5. After you save the Legal Authority, the following occurs:

- Any existing file plan nodes that use this Legal Authority will have the updates applied hence forth.
- The updated Legal Authority will appear as an option in the **Disposition Authority** field in the **File Plan: General** dialog box.
- If any file plan node has a **Disposition Authority** set to the updated Legal Authority, the Legal Authority change will appear in the **Pending Legal Changes** tab along with the affected file plan node.

## 8.5 Deleting a Legal Authority

To delete an existing Legal Authority from your site, perform the following steps.

---

### Note

You cannot remove a Legal Authority that is assigned to a file plan node. If you attempt to do so, the Delete option is grayed out and not available for selection.

---

1. From the **Legal Authorities** list, click the ellipsis (...) to the right of the authority you want to delete, and then click **Delete** from the drop-down menu. A Confirm Removal dialog opens, asking you confirm the removal.
2. Click **OK**, and the Legal Authority is deleted and removed from the **Legal Authorities** list.

## 8.6 Legal Authorities Permission Assignment

To access the Legal Authorities functionality, you must be a member of a Security Group that has an assigned Permission Role that grants permission.

Permission Assignments are not cascading; you must be assigned each Permission Assignment individually. For example, if you are granted *Edit*, you must also be granted *View* to select a Legal Authority for editing.

The following table defines the required Permission Assignment needed to access the *Legal Authorities* functionality in File Plan Builder. For more information on Permission Roles, [See "Permission Roles" on page 5.](#)

Table 8-2 Legal Authorities Permission Assignment

Permission Assignment	Description
<b>View Legal Justifications Tab</b>	Provides access to the <b>Legal Justification</b> features in File Plan Builder.  <b>Legal Justifications</b> is a vertical tab in File Plan Builder.

Table 8-2 Legal Authorities Permission Assignment

Permission Assignment	Description
<b>View Authority</b>	Provides access to the <b>Authorities</b> tab in the Legal Justification section of File Plan Builder.  Allows a user to read/view an existing Legal Authority.
<b>Add Authority</b>	Allows a user to create a new Legal Authority.
<b>Edit Authority</b>	Allows a user to edit an existing Legal Authority.
<b>Remove Authority</b>	Allows a user to delete an existing Legal Authority.
<b>View Authority Requirements</b>	Allows a user to see the <b>Requirements</b> list for a Legal Authority.  Hides or displays the <b>Requirements</b> list field.
<b>Add Requirements</b>	Allows a user to create a new Legal Requirement.  This is required to add a new Legal Requirement through the <b>Add</b> link next to the <b>Requirements</b> list.

## 9 Legal Requirements

Legal Requirements functionality is available in a SharePoint Records Center with Gimmal Compliance Suite enabled. To use the Legal Requirements features in File Plan Builder, Gimmal Compliance Suite must be installed and the Gimmal Compliance Suite File Plan Builder feature must be active. In addition, you must have the proper File Plan Builder: Permission Roles assigned. For File Plan Builder: Permission Roles settings, see [9.6 Legal Requirements Permission Assignment](#).

Gimmal Compliance Suite supports user-defined Legal Requirements. Legal Requirements define the code of laws based on legal jurisdiction required to support your organization's records management policies. Legal Requirements are used to support the legal authorization for the disposition of records based on the assigned Legal Authority.

Gimmal Compliance Suite provides the ability to create, edit, view, or delete Legal Requirements. The terms *Legal Requirement*, *Requirement*, *Citation*, and *Legal Justification* are used interchangeably.

**Intended User:** Records Manager

To access the *Legal Requirements* list:

1. Open File Plan Builder.
2. Select **Legal Justifications** from the vertical tabs. The Legal Justifications context menu opens.
3. Select the **Requirements** option. The Legal Requirements list displays.

### 9.1 Legal Requirements List

The following table describes the **Legal Requirements** list with a description of each heading.

Table 9-1 *Legal Requirements List*

List View Heading	Description
<b>Legal Code</b>	<p>Unique identifier based on the code of laws for your organization's legal jurisdiction.</p> <p>The <b>Legal Code</b> is used in the <b>Authorities</b> dialog box in the selection list for <b>Requirements</b>.</p>
<b>Citation</b>	<p>Unique reference to the authoritative legal source/documentation based on the code of laws for your organization's legal jurisdiction.</p> <p>The <b>Citation</b> is used in the <b>Authorities</b> dialog box in the selection list for <b>Requirements</b>.</p>

Table 9-1 Legal Requirements List

List View Heading	Description
<b>Industry</b>	Business categorization for the Legal Requirement. Legal Requirements are often based on industry or business specific legal regulations.  Example: Finance
<b>Subject</b>	Categorization used to further classify the Legal Requirement. in an Industry Legal Requirements are often categorized by topics for ease of use and improved searching.  Example: Mergers and Acquisitions
<b>Status</b>	State in the Citation Lifecycle for the Legal Requirement.  The <b>Status</b> identifies if the Legal Requirement is <i>New, Updated, Active, Superseded, or Inactive</i> .  The <b>Status</b> is used in the <b>Authorities</b> dialog box in the selection list for <b>Requirements</b> .

The **Legal Requirements** list uses the standard filter and sort capabilities.

## 9.2 Creating a New Legal Requirement

Legal Requirements are not required for any of the other File Plan Builder features, but it is recommended for Legal Authorities. Before a Legal Requirement can be assigned to a Legal Authority, a Legal Requirement must be created.

1. From the **Legal Requirements** list, click **Add Item**. The Requirements: Add dialog opens.

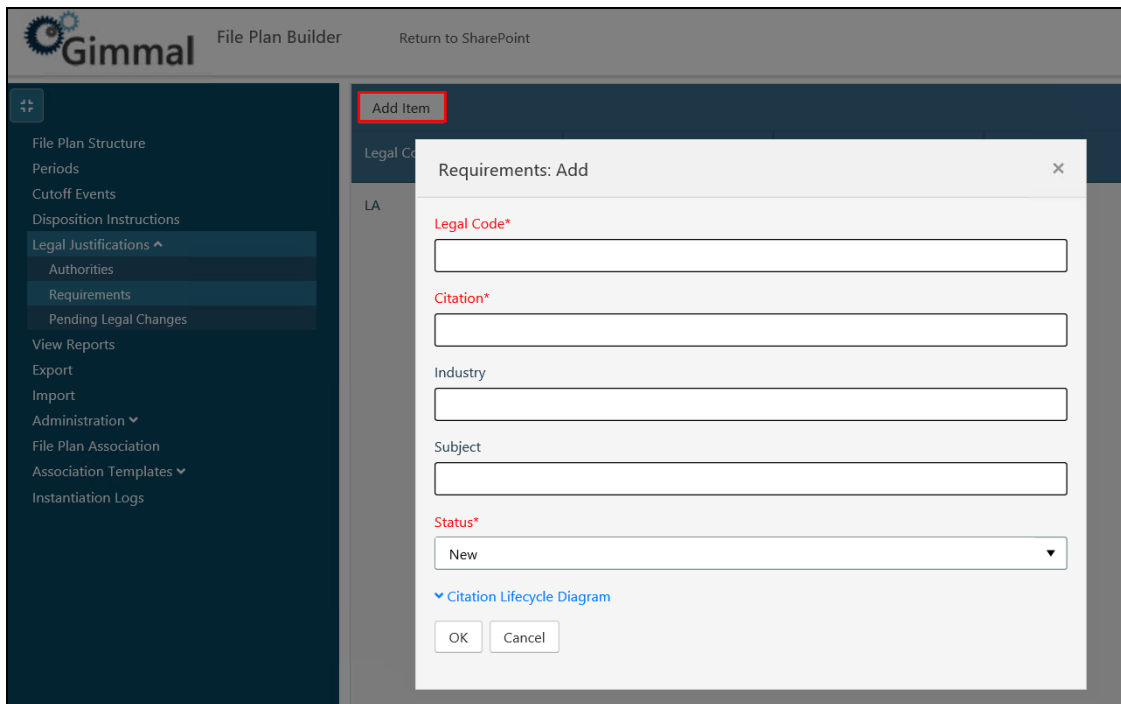


Figure 9-1 Adding a New Legal Requirement

2. Enter the following information:
  - a. **(Required)** Enter the **Legal Code**. The **Legal Code** is a unique identifier based on the code of laws for your organization's legal jurisdiction.
  - b. **(Required)** Enter the **Citation**. The **Citation** is a unique reference to the authoritative legal source/documentation based on the code of laws for your organization's legal jurisdiction.
  - c. Enter an **Industry**. The **Industry** is a business categorization used to classify the Legal Requirement. Legal Requirements are often based on industry or business specific legal regulations; for example, *Finance*.
  - d. Enter a **Subject**. The **Subject** is a categorization used to classify the Legal Requirement. In an Industry, Legal Requirements are often categorized by topics for ease of use and improved searching; for example, *Mergers and Acquisitions*.
  - e. **(Required)** Select a **Requirement Status**. The **Requirement Status** is the current state in the Citation Lifecycle for the Legal Requirement. The options are *New*, *Updated*, *Active*, *Superseded*, and *Inactive*. The **Requirement Status** defaults to *New*.
    - *New*: The Legal Requirement is new and is not currently being used by any Legal Authorities.
    - *Updated*: An existing Legal Requirement that has been changed. Items set to this value will be added to *Pending Legal Changes* upon save.
    - *Active*: The Legal Requirement is current. Only active Legal Requirements should be used by Legal Authorities.

- *Superseded*: The Legal Requirement has been replaced by another Legal Requirement. Hence forth, this Legal Requirement should not be used by Legal Authorities.
  - *Inactive*: The Legal Requirement should not be used. It is no longer current or valid.
- f. To view the **Citation Lifecycle Diagram**, click the drop-down arrow next to the **Citation Lifecycle Diagram** label.
3. Click **OK**. The new Legal Requirement is created and displays in the **Legal Requirements** list.
  4. After you save the new Legal Requirement,
    - The new Requirement will appear as an option in the **Legal Requirements** table at the bottom of the Authorities dialog boxes.

### 9.3 Viewing a Legal Requirement

To view the details of an existing Legal Requirement, perform the following step.

- From the **Legal Requirements** list, click the ellipsis (...) to the right of the requirement you want to view, and then click **View** from the drop-down menu. The Requirements: View dialog opens, showing you the details of that requirement.

### 9.4 Editing a Legal Requirement

To change an existing Legal Requirement, you must edit the Legal Requirement item.

1. From the **Legal Requirements** list, click the ellipsis (...) to the right of the requirement you want to edit, and then click **View** from the drop-down menu. The Requirements: View dialog opens.

Figure 9-2 Editing a Legal Requirement

2. Click the **Edit** at the bottom of the dialog. The dialog updates with editable fields for the selected Legal Requirement.
3. Update the information as desired.
4. Click **OK**. The Legal Requirement is updated and the changes appear in the **Legal Requirements** list.
5. After you save the Legal Requirement changes, the following occurs:
  - Any existing Legal Authority that uses this Legal Requirement will have the updates applied as well.
  - The updated Legal Requirement will appear as an option in the Legal Requirements table at the bottom of the Authorities dialog boxes.
  - If any file plan node has an assigned **Disposition Authority** that is based on the updated Legal Requirement, the Legal Requirement change will appear in the Pending Legal Changes tab along with the affected file plan node.

## 9.5 Deleting a Legal Requirement

To remove an existing Legal Requirement from File Plan Builder, perform the following steps.



---

## Note

You cannot remove a Legal Requirement that is assigned to a File Plan Node or if it is currently used by one or more Legal Authorities. If you attempt to do so, the Delete option is grayed out and not available for selection.

---

1. From the **Legal Requirements** list, click the ellipsis (...) to the right of the requirement you want to delete, and then click **Delete** from the drop-down menu. A Confirm Removal dialog opens, asking you confirm the removal.
2. Click **OK** and the requirement is deleted and removed from the **Legal Requirements** list.

## 9.6 Legal Requirements Permission Assignment

To access the Legal Requirements functionality, you must be a member of a Security Group that has an assigned Permission Role that grants permission.

Permission Assignments are not cascading; you must be assigned each Permission Assignment individually. For example, if you are granted *Edit*, you must also be granted *View* to select a Legal Requirement for editing.

The following table defines the required Permission Assignment needed to access the *Legal Requirements* functionality in File Plan Builder. For more information on Permission Roles, [See "Permission Roles" on page 5.](#)

Table 9-2 Legal Requirements Permission Assignment

Permission Assignment	Description
<b>View Legal Justifications Tab</b>	Provide access to the <b>Legal Justifications</b> features in File Plan Builder.  <b>Legal Justifications</b> is a vertical tab in File Plan Builder.
<b>View Requirements</b>	Provides access to the <b>Requirements</b> tab in the Legal Justifications section of File Plan Builder.  Allows a user to read/view an existing Legal Requirement.
<b>Add Requirements</b>	Allows a user to create a new Legal Requirement.
<b>Edit Requirements</b>	Allows a user to edit an existing Legal Requirement.
<b>Remove Requirements</b>	Allows a user to delete an existing Legal Requirement.

## 10 Pending Legal Changes

Pending Legal Changes functionality is available in a SharePoint Records Center with Gimmal Compliance Suite enabled. To use the Legal Requirements features in File Plan Builder, Gimmal Compliance Suite must be installed and the Gimmal Compliance Suite File Plan Builder feature must be active. In addition, you must have the proper File Plan Builder: Permission Roles assigned. For File Plan Builder: Permission Roles settings, see the Pending Legal Changes Permission Assignment help section.

Pending Legal Changes supports the Legal Requirements *Citation Lifecycle* through the identification and promotion of Legal Requirement **Requirement Status** based on Citation Lifecycle states. When a Legal Requirement **Requirement Status** is *New, Updated, or Superseded* for any Legal Requirement assigned to a Legal Authority that is the **Disposition Authority** for a file plan node(s), the Legal Requirement goes into a *Pending* status. The *Pending Legal Changes* tab displays all file plan nodes that have Legal Requirements in this *Pending Status*.

The **Pending Legal Changes** tab provides a view into all file plan nodes affected by the Legal Requirement change. From the **Pending Legal Changes** tab, a user can:

- View affected file plan nodes
- View affected Legal Authorities
- Promote Legal Requirement to next Lifecycle State

**Intended User:** Records Manager

To access the **Pending Legal Changes** view:

1. Open File Plan Builder.
2. Select **Legal Justifications** from the vertical tabs. The Legal Justifications context menu opens.

3. Select the **Pending Legal Changes** option. The Pending Legal Changes list displays.

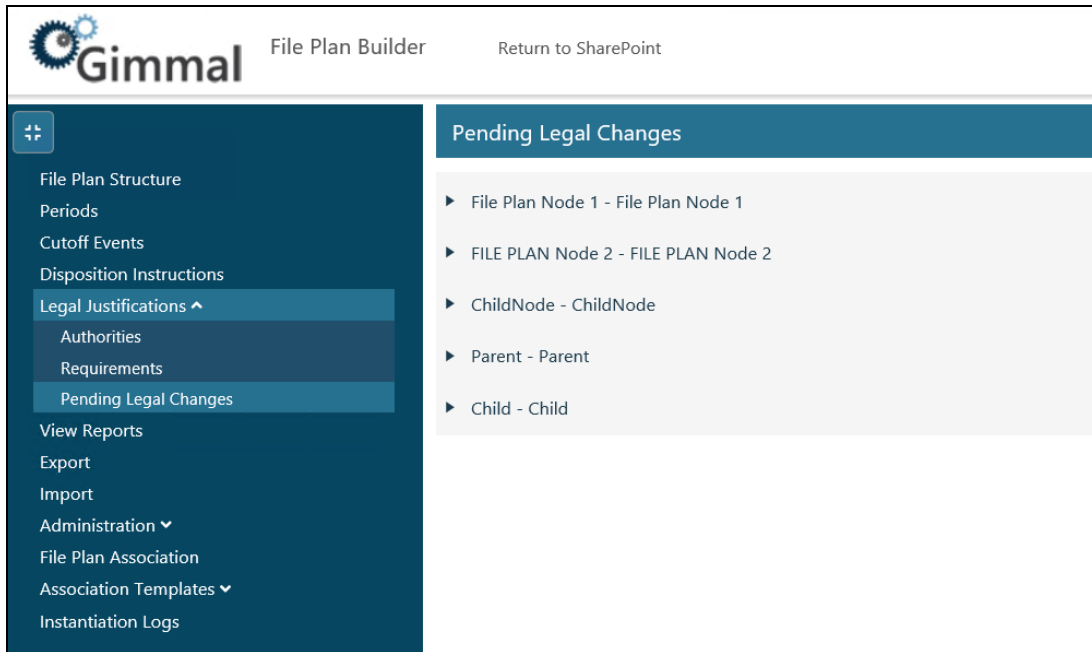


Figure 10-1 Pending Legal Changes List

The **Pending Legal Changes** list is grouped first by file plan node(s), then by Legal Authority based on assigned Legal Requirement **Requirement Status** values (*New, Updated, Superseded*) that affects the displayed file plan node(s).

The Legal Requirement that has triggered the Pending Legal Change is displayed under the affected Legal Authority(ies).

To view and promote Pending Legal Changes, perform the following steps:

1. On the Pending Legal Changes list, click ▶ to the left of a file plan node to display the **Disposition Authority** that contains a Legal Requirement that triggered the Pending Legal Change.

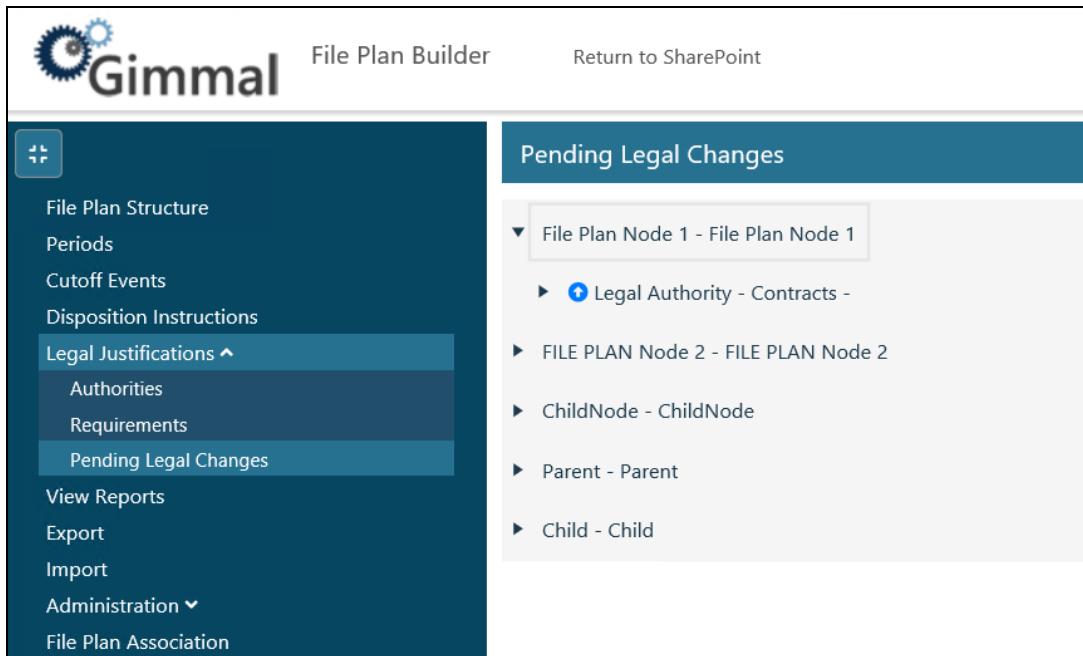


Figure 10-2 Disposition Authority

2. Click ▶ to the left of the Legal Authority to display the Legal Requirements that triggered the Pending Legal Change.

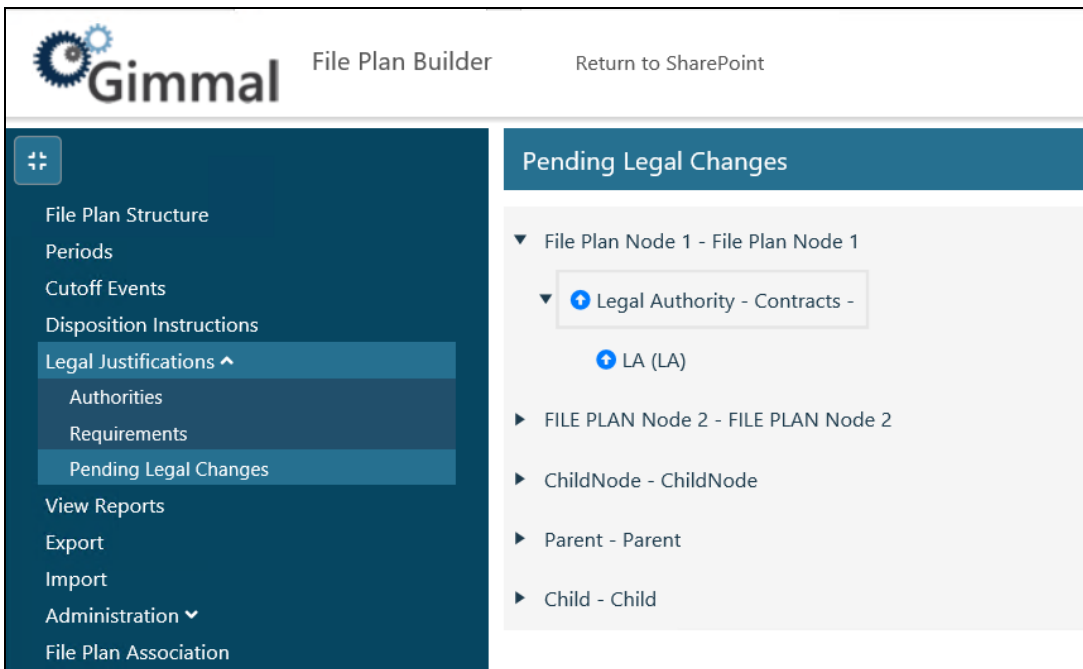




Figure 10-3 Legal Requirements Causing Change

- To promote all Legal Requirements grouped in a specific Legal Authority to the next Citation Lifecycle state, click the blue up arrow icon  to the left of the Legal Authority.

The affected Legal Requirement(s) **Requirement Status** will be updated based on the **Citation Lifecycle**:

- *New* promotes to *Active*.
  - *Updated* promotes to *Active*.
  - *Superseded* promotes to *Inactive*.
- To promote a single Legal Requirement to the next *Citation Lifecycle* state, click the up arrow icon  to the left of the Legal Requirement.
    - *New* promotes to *Active*
    - *Updated* promotes to *Active*
    - *Superseded* promotes to *Inactive*
  - After you promote a Legal Requirement, the corresponding Legal Authority and file plan node will be removed from the *Pending Legal Changes* view.

## 10.1 Pending Legal Changes Permission Assignment

To access the Pending Legal Changes functionality, you must be a member of a Security Group that has an assigned Permission Role that grants permission.

Permission Assignments are not cascading; you must be assigned each Permission Assignment individually. For example, if you are granted *View Pending Legal Justification* you must also be granted *View Legal Justifications* to have access to the Legal Justifications vertical tab in File Plan Builder.

The following table defines the required Permission Assignment needed to access the Pending Legal Changes functionality in File Plan Builder. For more information on Permission Roles, [See "Permission Roles" on page 5.](#)

Table 10-1 Pending Legal Changes Permission Assignment

Permission Assignment	
<b>View Legal Justifications Tab</b>	Provides access to the <b>Legal Justifications</b> features in File Plan Builder.  <b>Legal Justifications</b> is a vertical tab in File Plan Builder.
<b>View Pending Legal Justification</b>	Provides access to the <b>Pending Legal Changes</b> tab in the Legal Justifications section of File Plan Builder.

## 11 File Plan Report

File Plan Report functionality is available in a SharePoint Records Center with Gimmal Compliance Suite enabled. To use the File Plan Report feature in *File Plan Builder*, Gimmal Compliance Suite must be installed and the *Gimmal Compliance Suite File Plan Builder* feature must be active. In addition, you must have the proper *File Plan Builder: Permission Roles* assigned. For *File Plan Builder: Permission Roles* settings, see the *File Plan Report Permission Assignment* help section.

File Plan Report allows reporting on a single or all file plan nodes. The report contains the following file plan node information:

- **General Information:** Name, ID, Description, Disposition Instructions with link to report details for the disposition instruction, Location, Transfer to NARA, Is Vital Record, and Vital Record Review Period.
- **Roles with Security Access:** List of assigned Permission Roles.
- **Cutoff Criteria:** Cutoff Workflow, Enable Events, Cutoff Events, Enable Periods, Cutoff Period, Enable Relationships, Relationship Role, Enable Scripts, and Scripts.
- **Disposition Instructions:** Name, Description, and Disposition Stages. For each disposition stage, the following information is displayed:
  - Name
  - Description
  - Disposition Action: Link to report details for the disposition action.
  - Authority
  - Duration
- **Disposition Authorities:** Name, Description, and Requirements. For each requirement, the following information is displayed:
  - Legal Code
  - Citation
  - Status
- **Disposition Actions:** Name, Description, and Parameter

**Intended User:** Records Manager

To access the File Plan Report function:

1. Open **File Plan Builder**.
2. Select **View Reports** from the vertical tabs.

---

### Note:

File plan instantiations are included in the report.

---

## 11.1 File Plan Report View

The File Plan Report view displays a hierarchical view of the file plan nodes. This is the same view that is displayed on the *File Plan* tab. The following table describes the *File Plan Report View* with a description of each heading.

Table 11-1 File Plan Report View

List View Heading	Description
<b>Name</b>	User friendly identifier that differentiates the file plan node from other file plan nodes.
<b>ID</b>	Unique identifier that differentiates the file plan node from other file plan nodes at the same level in the File Plan Structure.
<b>Description</b>	Descriptive statement used to further differentiate the file plan node from other file plan nodes.

The File Plan Report view uses the standard filter and sort capabilities.

### 11.1.1 Running a File Plan Report

To run a File Plan Report, perform the following steps from the View Reports page:

1. To report on one file plan node and its children, select the file plan node. Only one file plan node can be selected at a time. To select a child node, click the button to the left of the file plan node **Name** to view the child node(s).

When a file plan node is selected, the **Report Selected Node** button becomes active.

Click the **Report Selected Node** button. The File Plan Report opens in a new window.

2. To report on all file plan node(s), click the **Report All Nodes** button. The File Plan Report opens in a new window.
3. The File Plan Report is broken into four sections:

- *File Plan Node (Record Category)*

**User Documentation Record Category 1 - hlpdoc0001**

**General Information**

Name: User Documentation Record Category 1  
ID: hlpdoc0001  
Description: Sample file plan node/record container for user documentation.  
Disposition Instructions: [User Documentation: Destroy after 10 years](#)  
Location:  
Transfer to NARA: No  
Is Vital Record: No  
Review Period:

**Organization-Defined Fields**

User Documentation Text Field 1: [Help](#)  
User Documentation Selection List Field 1:

**Roles with security access**

**Full Permissions**  
**Limited Access Permissions Test**

**Cutoff Criteria**

Cutoff Workflow:  
Enable Events: True  
Cutoff Events:  
Enable Periods: True  
Cutoff Period: Monthly  
Enable Relationships: True  
Relationship Role: Has versions(Hierarchical)  
Enable Scripts: True  
Scripts:

Figure 11-1 File Plan Node (Record Category) Section

- *Disposition Instructions*

**User Documentation: Destroy after 10 years**

Name: User Documentation: Destroy after 10 years  
Description: Sample disposition instructions for documentation.

**Disposition Stages:**

Name: User Documentation Stage 1  
Description: Sample disposition staget for documentation  
Disposition Action: [User Documentation Destroy all previous versions](#)  
Authority:  
Duration: 1 Days

**Disposition Stages:**

Name: User Documentation Stage 2  
Description: Sample disposition staget for documentation  
Disposition Action: [User Documentation Destroy all previous versions](#)  
Authority:  
Duration: 1 Days

**Disposition Stages:**

Name: User Documentation Stage 3  
Description: Sample disposition staget for documentation  
Disposition Action: [User Documentation Destroy all previous versions](#)  
Authority:  
Duration: 1 Days

Figure 11-2 File Disposition Instructions Section



- *Disposition Authorities*

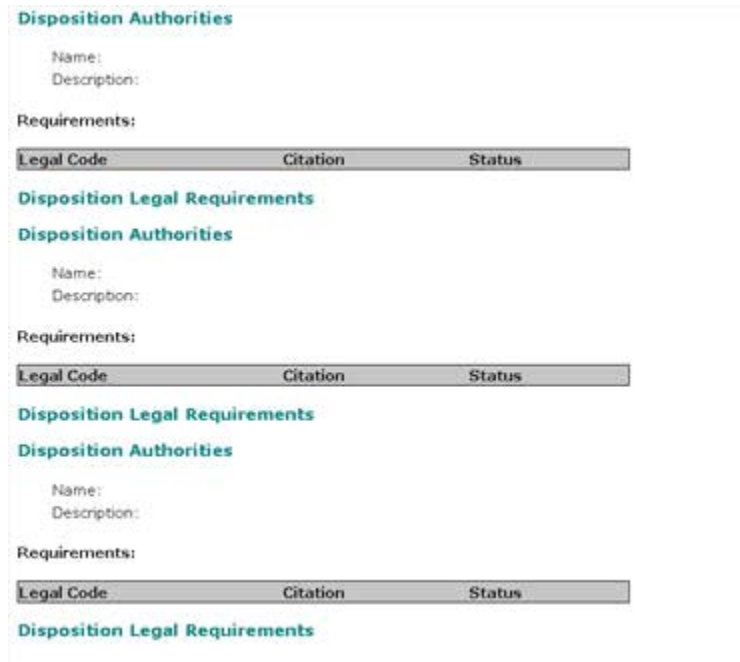


Figure 11-3 Disposition Authorities Section

- *Disposition Actions*

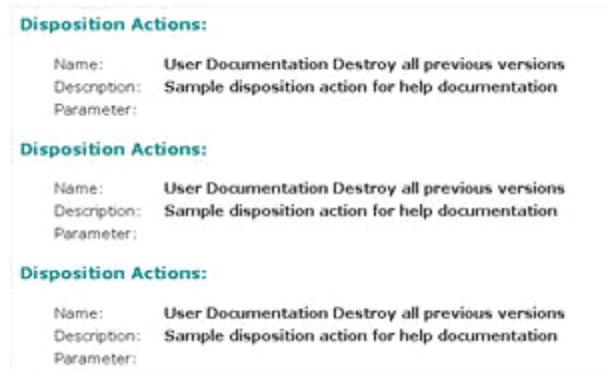


Figure 11-4 Disposition Actions Section

## 11.2 File Plan Report Permission Assignment

To access the File Plan Report, you must be a member of a Security Group that has an assigned Permission Role that grants permission.

27 March 2019

The following table defines the required Permission Assignment needed to access the File Plan Report in File Plan Builder.

*Table 11-2 File Plan Report Permission Assignment*

Permission Assignment	Description
<b>View Reports Tab</b>	Provides access to the <b>Report</b> vertical tab of File Plan Builder.

## 12 File Plan Builder Export

File Plan Builder's Export functionality is available in a SharePoint Records Center with Gimmal Compliance Suite enabled. To use the Export File Plan function, Gimmal Compliance Suite must be installed and the Gimmal Compliance Suite File Plan Builder feature must be active.

Export allows you to copy artifacts from File Plan Builder into another instance of File Plan Builder running in a different farm, enabling migration of data artifacts in File Plan Builder from a QA/DEV environment to a production environment. You can also use the Export as a backup of File Plan Builder or more commonly, use it to make bulk changes to existing artifacts in File Plan Builder.

To access the Export File Plan functionality, you must be a member of a Security Group that has an assigned Permission Role that allows access. If you previously had access to Export, that permission is maintained in a Compliance Suite upgrade. See the "Permission Roles" chapter later in this guide for assigning permission roles.

If you experience any errors accessing the Export feature, refer to ["Troubleshooting" on page 139](#).

**Intended User:** Records Manager/File Plan Builder Administrator

### 12.1 Exporting Artifacts from File Plan Builder

**Export File Plan** allows you to selectively export File Plan Builder artifacts information to an .xml file. The exported .xml file contains the following File Plan Builder feature items:

- File Plan Artifacts
  - File Plan Structure
  - Periods
  - Cutoff Events
  - Disposition Instructions
- Legal Justifications
  - Authorities
  - Requirements
- Administration Settings
  - Security Groups
  - Permission Roles
  - Disposition Actions
  - Supplemental Markings

To export a file plan to an .xml file, perform the following steps:

1. Launch **File Plan Builder** and select **Export** from the vertical tabs. The **Export** page displays.

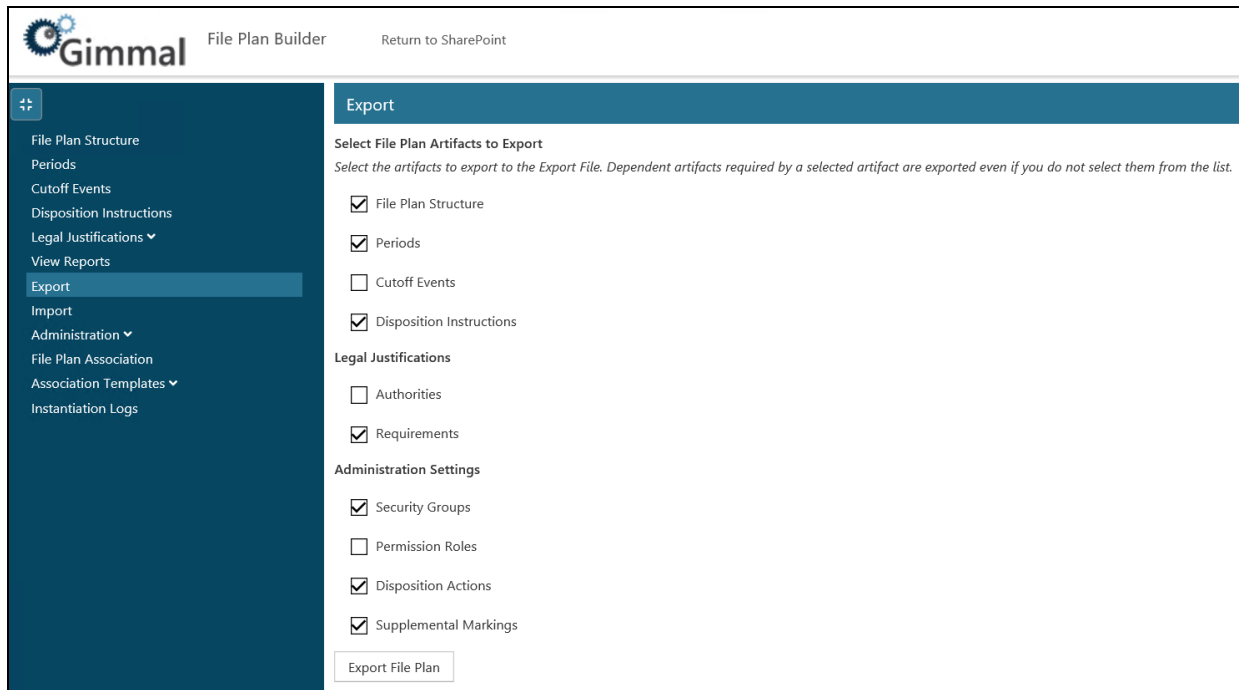


Figure 12-1 Export File Plan Page

2. Select the check boxes for the **File Plan Artifacts** that you want to export in this file plan. By default, all are checked. If you select an artifact with dependent items, those artifacts are exported, even if you do not select them from the list. For example, selecting **File Plan Nodes** adds the Disposition Instructions, Disposition Authority, and any other references for all of the nodes present in the exported file.

---

**Note:**

You must select at least one artifact to export.

---

3. Select **Export File Plan** at the bottom of the screen. When the export is complete, a *File Plan Exported Successfully* message displays and the browser prompts you to open or save the file.
4. Save the file to a location that is accessible by the host machine doing the import process.



## 13 File Plan Builder Import

File Plan Builder Import functionality is available in a SharePoint Records Center with Gimmal Compliance Suite enabled. To use the Import File Plan features in *File Plan Builder*, Gimmal Compliance Suite must be installed and the *Gimmal Compliance Suite File Plan Builder* feature must be active.

File Plan Builder Import is a multi-step process where the export file is read and compared to the existing entries in File Plan Builder. You can rename an item, skip an item that has an identical name, or overwrite an item with the new information from the selection screen. If you choose to rename an item, a newly-created artifact is generated in File Plan Builder. When overwriting an item, the old entry and any association references are kept when you are overwriting an existing file plan node.

You can use an File Plan Builder Export file to selectively import artifacts into the File Plan Builder Import utility. From the Import interface, you can select which artifacts you want to import. Importing an artifact, such as a File Plan Node that references other artifacts, will automatically import the references.

You can also modify the file plan before import to use only the artifacts you desire.

To access the Import File Plan functionality, you must be a member of a Security Group that has an assigned Permission Role that allows access and you must set view access in Administration Settings. See [2 Permission Roles](#) for assigning permission roles.

Import files must be valid .xml files created by the Export File Plan process (see [12 File Plan Builder Export](#)). You can import files that were exported in versions after Compliance Suite 4.0.0. If you make modifications to an exported .xml file and want to import it, you must be sure that the syntax for the schema is correct. You must also be logged in as a system account to import files that were exported from another environment.

---

### Note:

See [Appendix A Chunking Files for Easier Import](#) for more detail on how edit an exported file.

---

**Intended User:** Records Manager

### 13.1 Importing Artifacts

The Import feature of File Plan Builder allows importing .xml files that were generated by the Export process. To access the Import File Plan function:

1. Open **File Plan Builder** and select **Import** from the vertical tabs. The **Import File Plan** page displays.

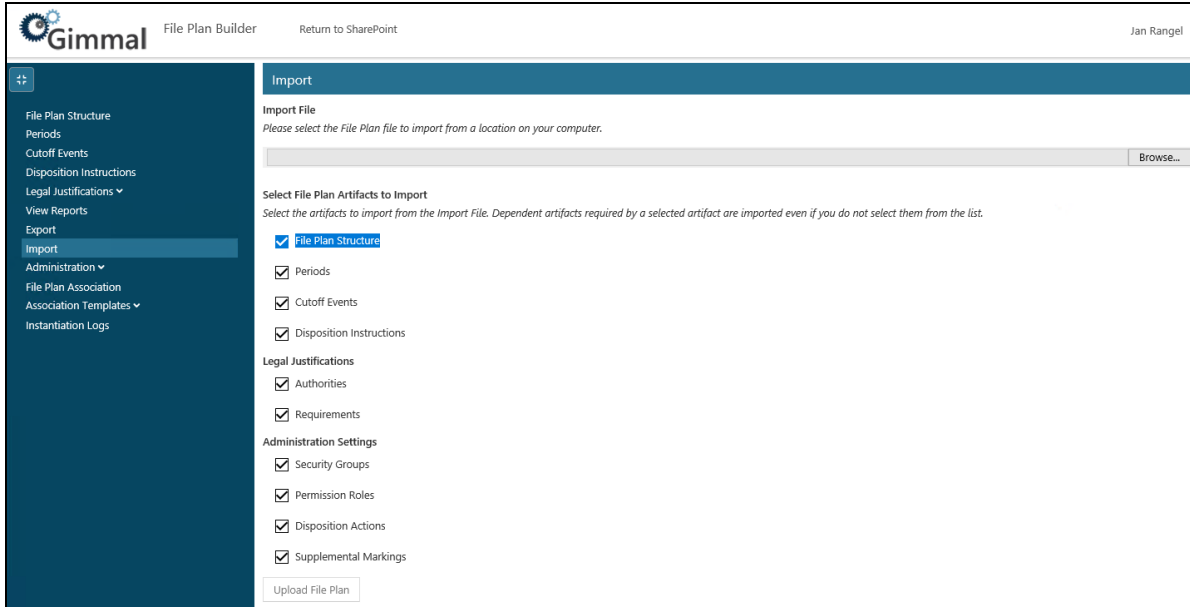


Figure 13-1 Import File Plan Page

2. Click **Browse** to locate the file that you want to import, and then click **Open**. The file path and name display in the Browse field.

---

#### Note:

You must browse for a file to enable the **Upload File Plan** button located at the bottom of the page.

---

3. Select the File Plan Artifacts you want to import in this file plan. If you select an artifact with dependent items, those artifacts are imported, even if you do not select them from the list. The options include:
  - File Plan Structure (Nodes)
  - Periods
  - Cutoff Events
  - Disposition Instructions
  - Legal Justifications
    - Authorities
    - Requirements
  - Administration Settings
    - Security Groups
    - Permission Roles

- Disposition Actions
- Supplemental Markings

---

**Note:**

You must select at least one artifact to import to enable the **Upload File Plan** button.

---

4. Click **Upload File Plan**. The system processes the request.
5. The **Import - Principal Mappings** dialog displays if you are uploading a file with users/roles. If you are not uploading a file with users/roles, go to the next step.

During the upload, File Plan Builder locates any usernames associated with the imported file and tries to match them in SharePoint. The user mappings come from two places:

- Security groups under the **Administration Settings > Permissions**
- Under each node in the File Plan Structure under the SharePoint Security tab

If a username is validated, a green check mark displays beside it. If it is not validated, a red **X** displays beside it and you can use **People Picker** to map a new one. This verification works in a cross-domain environment.

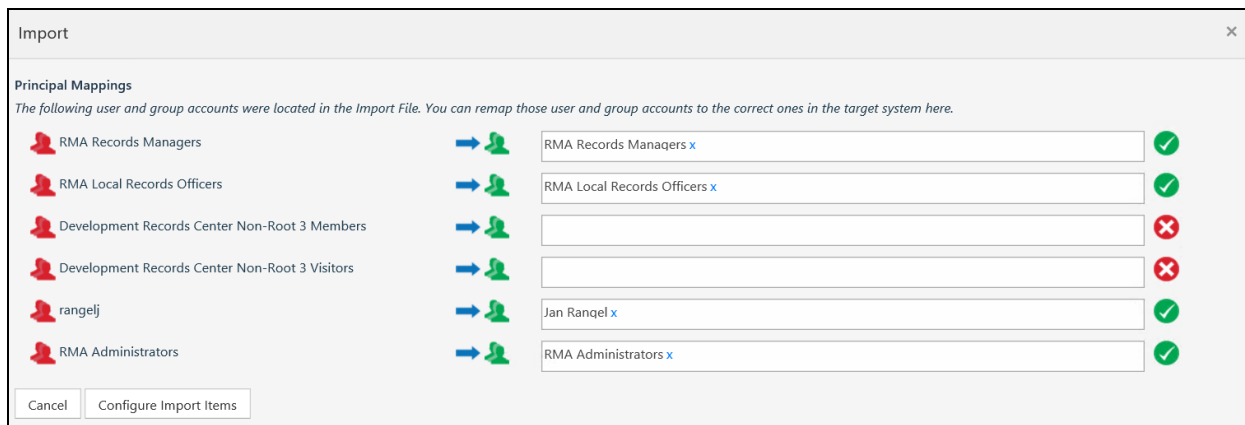


Figure 13-2 Principal Mappings Dialog

If File Plan Builder cannot validate the usernames, you must map the usernames found with valid SharePoint users.

- a. Enter a valid SharePoint username in the box with the red **X**.
  - b. Click **Validate Users**.
6. Click **Configure Import Items** at the bottom of the Principal Mappings dialog. The Import - Select Individual Artifacts to Import dialog opens.



- Each tab of this page displays the data to import (as specified from the **Import** screen). The tabs that display can also be the result of an artifact with a dependency.

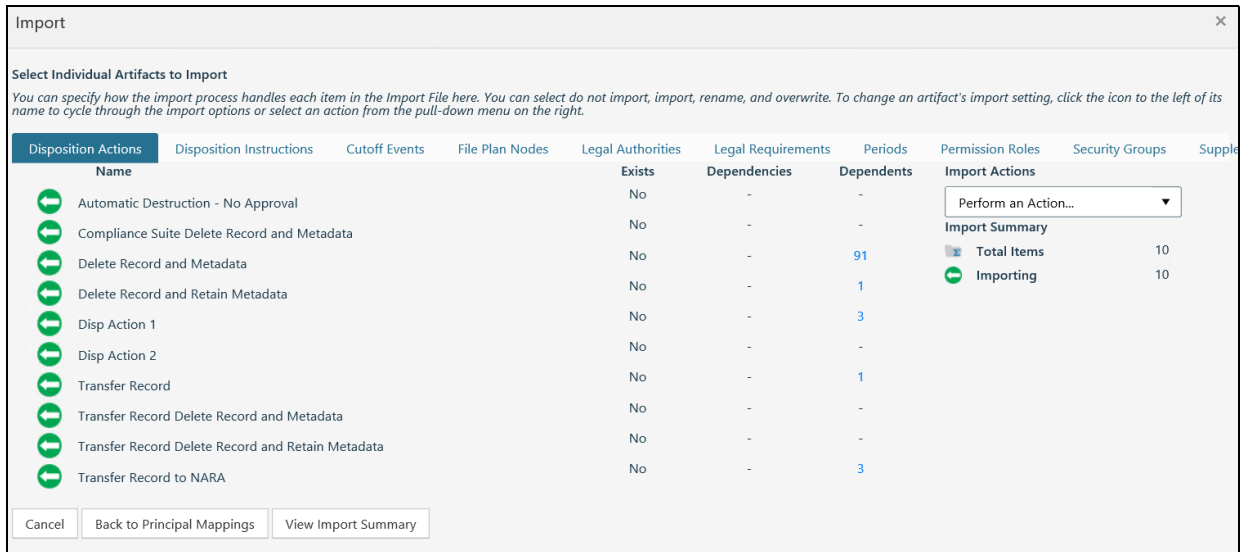
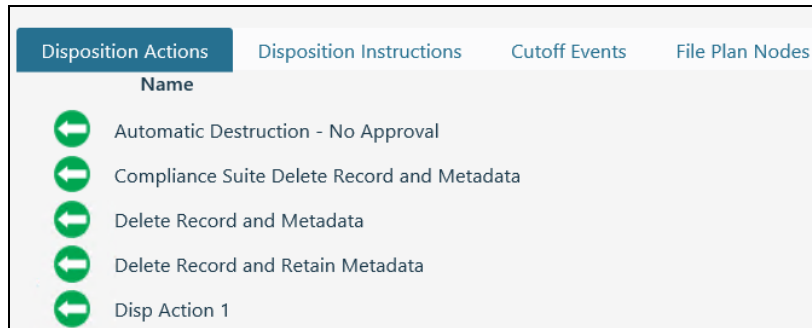




Figure 13-3 Select Individual Artifacts to Import Dialog

- Specify how the import process handles each artifact by selecting one of three options available for each item in each tab.
  - If an item does not exist, the default behavior is to import the item, indicated by the green arrow pointing to the left.



- If an item with the same name exists, the default behavior is to not import the item, indicated by a red slash through the left arrow.



- For every item with a red slash through the left arrow, you can click the icon to cycle through the choices, or alternatively, use the menu under **Import Actions**, on the right, to select one of the following actions:
  - i. Rename the item, indicated by the blue icon (  ).
  - ii. Overwrite the item, indicated by a red exclamation point  .

**Note:**

The menu lets you select all items in the list to rename, allowing you to perform actions in bulk.

9. Review each tab to specify how artifacts are imported.
10. Once you are satisfied with your choices, click **View Import Summary**. A summary page displays the items and how they will be imported. Any warning messages will display at the bottom of the dialog.

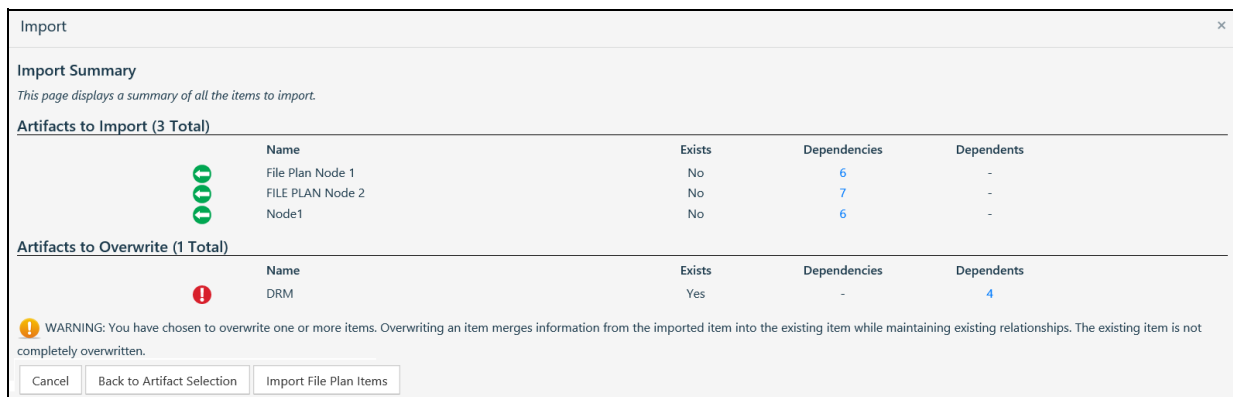


Figure 13-4 Import Summary Page

11. If you want to make further changes, click **Back to Artifact Selection**.

If you are satisfied with the import, click **Import File Plan Items**. The **Import Results** screen displays.

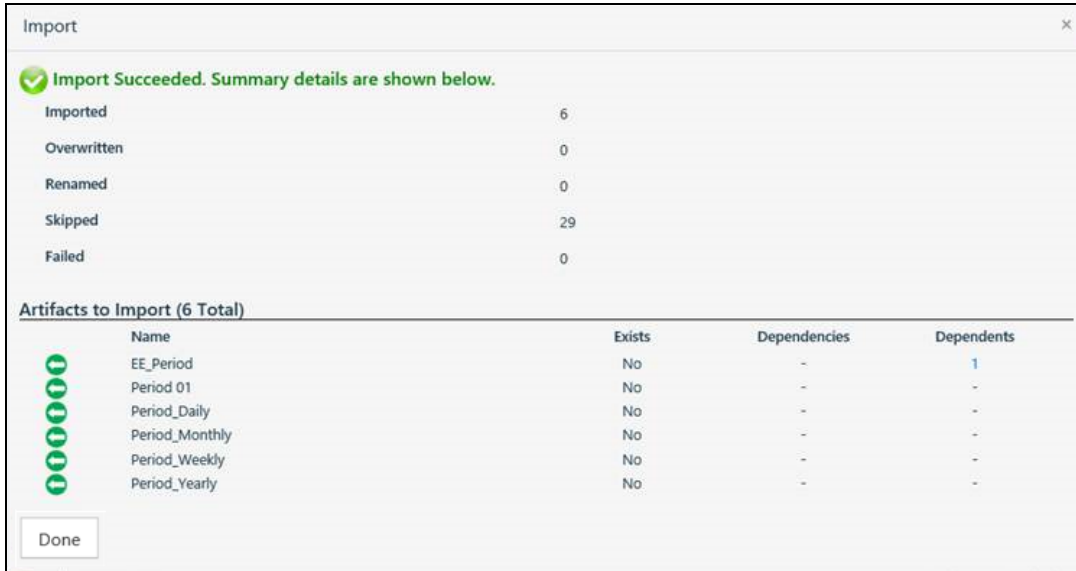


Figure 13-5 Import Succeeded Page

12. Click **Done** to return to the **Import File Plan** page.

---

**Note:**

If you have problems importing a file, see [A.1 Chunking Large Files for Easier Import](#) for information on how edit an exported file to make it easier to import.

---

## 14 Security Groups

Security Groups functionality is available in a SharePoint Records Center with Gimmal Compliance Suite enabled. To use the Security Groups features in File Plan Builder, Gimmal Compliance Suite must be installed and the Gimmal File Plan Builder feature must be active. In addition, you must have the proper File Plan Builder: **Permission Roles** assigned. For File Plan Builder: **Permission Roles** settings, see [14.6 Security Groups Permission Assignment](#).

Before end users such as Records Managers can use File Plan Builder features, the Compliance Suite Administrator must create Security Groups and assign each Security Group one or more Permission Roles. A Security Group builds upon the Permission Roles and grants a SharePoint group access to specific functionality in File Plan Builder.

Before the creation of Security Groups, the corresponding SharePoint groups must exist.

Gimmal Compliance Suite provides the ability to create, edit, view, or delete Security Groups.

**Intended User:** Compliance Suite Administrator

To access the **Security Groups** list:

1. Open **File Plan Builder**.
2. Select **Administration** from the vertical tabs. The Administration context menu opens.
3. Select the **Security Groups** option. The Security Groups list displays.

### 14.1 Security Groups List

The following table describes the **Security Groups** list with a description of each heading.

*Table 14-1 Security Groups*

List View Heading	Description
<b>Name</b>	<p>Unique name that differentiates the Security Group from other Security Groups. The <b>Name</b> connects the Security Group with its corresponding SharePoint group.</p> <p>The <b>Name</b> must be the same as its corresponding SharePoint group.</p> <p>Example: RMA Records Managers</p>

The **Security Groups** list uses the standard filter and sort capabilities.

## 14.2 Creating a New Security Group

Before end users, such as Records Managers, can access features in File Plan Builder, Security Groups must be created.

1. From the **Security Groups** list, click **Add Item** at the top of the list. The Security Group: Add dialog opens.

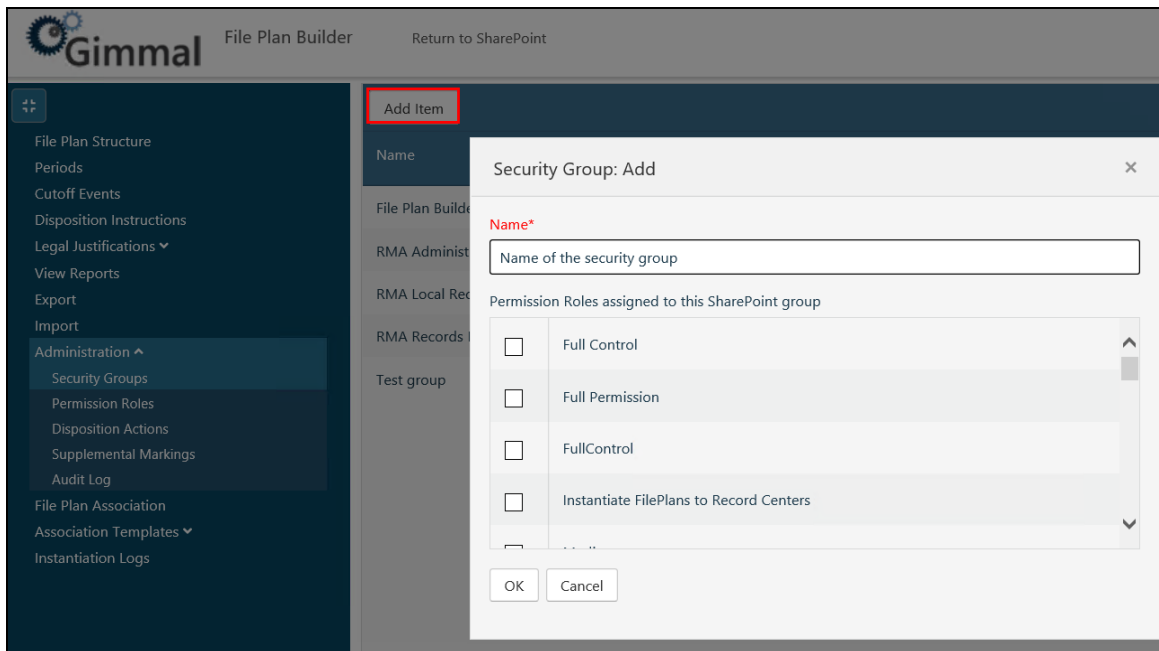


Figure 14-1 Creating a New Security Group

2. Enter the following information:
  - **(Required)** Enter the **Name**. The **Name** is a unique identifier for the new Security Group. The **Name** must match the name of its corresponding SharePoint group name.

---

### Note:

The name of the Security Group must exist in the site collection to which File Plan Builder Settings in Central Administration is pointing.

---

3. Select the **Permission Role Assignments**. The **Permission Role Assignments** define File Plan Builder permission configuration for this Security Group. Users that are members of this Security Group will have access based on the selected **Permission Role Assignments**. The selection options are based on existing Permission Role items.
4. Click **OK**. The new Security Group is created and displays in the **Security Groups** list.

After you save the new Security Group, users who are members of the new Security Group are granted access to the features as defined in the selected **Permission Role Assignments**.

## 14.3 Viewing a Security Group

To view the details of an existing period, perform the following step:

- From the **Security Groups** list, click the ellipsis (...) to the right of the security group you want to view, and then click **View** from the drop-down menu. The Security Group: View dialog opens, showing you the details of that group.

## 14.4 Editing a Security Group

To change an existing Security Group, perform the following steps.

1. From the **Security Groups** list, click the ellipsis (...) to the right of the security group you want to edit, and then click **View** from the drop-down menu. The Security Group: View dialog opens.

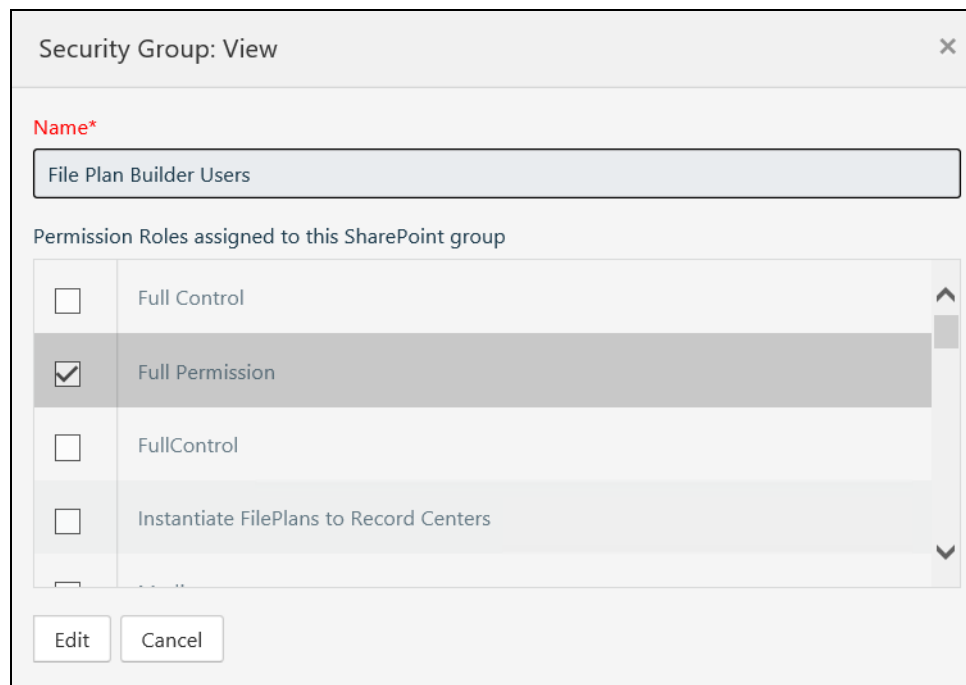


Figure 14-2 Editing a Security Group

2. Click the **Edit** at the bottom of the dialog. The dialog updates with editable fields for the selected period, and the title of the dialog title changes from Security Group: View to Security Group: Edit.
3. Update the information as desired.
4. Click **Save Changes**, and the Security Group is updated and the changes appear in the **Security Groups** list.

After you save the Security Group changes, users that are members of this Security Group will have the updated permissions applied as well.

## 14.5 Deleting a Security Group

To delete an existing Security Group from your site, perform the following steps.

1. From the **Security Groups** list, click the ellipsis (...) to the right of the security group you want to delete, and then click **Delete** from the drop-down menu. A Confirm Removal dialog opens, asking you confirm the removal.
2. Click **OK** to delete the Security Group and remove it from the **Security Groups** list. Users that are members of the deleted Security Group will have their access removed from this point going forward.

## 14.6 Security Groups Permission Assignment

To access the Security Groups functionality, you must be a member of a Security Group that has an assigned Permission Role that grants permission.

Permission Assignments are not cascading; you must be assigned each Permission Assignment individually. For example, if you are granted *Edit*, you must also be granted *View* to select a Security Group for editing.

The following table defines the required Permission Assignment needed to access the *Security Groups* functionality in File Plan Builder. For more information on Permission Roles, [See "Permission Roles" on page 5.](#)

Table 14-2 Security Groups Permission Assignment

Permission Assignment	Description
<b>View Administration Tab</b>	Provides access to the <b>Administration</b> features in File Plan Builder.  <b>Administration Settings</b> is a vertical tab in File Plan Builder.
<b>View Security Group</b>	Provides access to the Security Groups tab in the Administration section of File Plan Builder.  Allows a user to read/view an existing Security Group.
<b>Add Security Group</b>	Allows a user to create a new Security Group.
<b>Edit Security Group</b>	Allows a user to edit an existing Security Group.
<b>Remove Security Group</b>	Allows a user to delete an existing Security Group.

## 15 Supplemental Markings

Supplemental Markings functionality is available in a SharePoint Records Center with Gimmel Compliance Suite enabled. To use the Supplemental Markings features in File Plan Builder, Gimmel Compliance Suite must be installed and the Gimmel File Plan Builder feature must be active. In addition, you must have the proper File Plan Builder: **Permission Roles** assigned. For File Plan Builder: **Permission Roles** settings, see [15.6 Supplemental Markings Permission Assignment](#).

Gimmel Compliance Suite supports administrator-defined Supplemental Markings. Supplemental Markings are security features that enable site column content to restrict unauthorized users from accessing records. When Supplemental Markings are assigned to a file plan node, the Supplemental Marking(s) restricts record access to only authorized users based on the file plan node's **Supplemental Markings** site column value(s), even if the unauthorized user had access to the specific record under normal circumstances.

**Gimmel Compliance Suite** provides the ability to create, edit, view, or delete Supplemental Markings.

**Prerequisite:** Before a Supplemental Marking can be used, follow these steps:

1. Navigate to the **Access Rules** list and create the Supplemental Marking.
2. After a Supplemental Marking is created in the **Access Rules** list, if you create a Supplemental Marking in File Plan Builder with the same name, File Plan Builder will associate it with the Records Category.

**Intended User:** Compliance Suite Administrator

To access the **Supplemental Markings** list:

1. Open **File Plan Builder**.
2. Select **Administration** from the vertical tabs. The Administration context menu opens.
3. Select the **Supplemental Markings** option. The Supplemental Markings list displays.



## 15.1 Supplemental Markings List

The following table describes the **Supplemental Markings** list with a description of each heading.

*Table 15-1 Supplemental Markings List Headings*

List View Heading	Description
Name	<p>Unique name that differentiates the Supplemental Marking from other Supplemental Markings.</p> <p>The <b>Name</b> is used for the selection options on the <b>File Plan: Supplemental Markings</b> tab.</p> <p>After the <b>File Plan Instantiation timer job</b> is executed, the <b>Name</b> will appear in your SharePoint Records Center <b>Access Rules</b> dialog box as a selection option for the <b>Supplemental Markings Site Column Value</b>.</p>
Description	<p>Descriptive statement used to further differentiate the Supplemental Marking from other Supplemental Markings.</p> <p>The <b>Description</b> is displayed with the <b>Name</b> on the <b>File Plan: Supplemental Markings</b> tab.</p>

The **Supplemental Markings** list uses the standard filter and sort capabilities.

## 15.2 Adding a New Supplemental Marking

Before Supplemental Markings can be applied to file plan nodes, Supplemental Markings must be created by performing the following steps.

1. From the **Supplemental Markings** list, click **Add Item**. The Supplemental Markings: Add dialog opens.

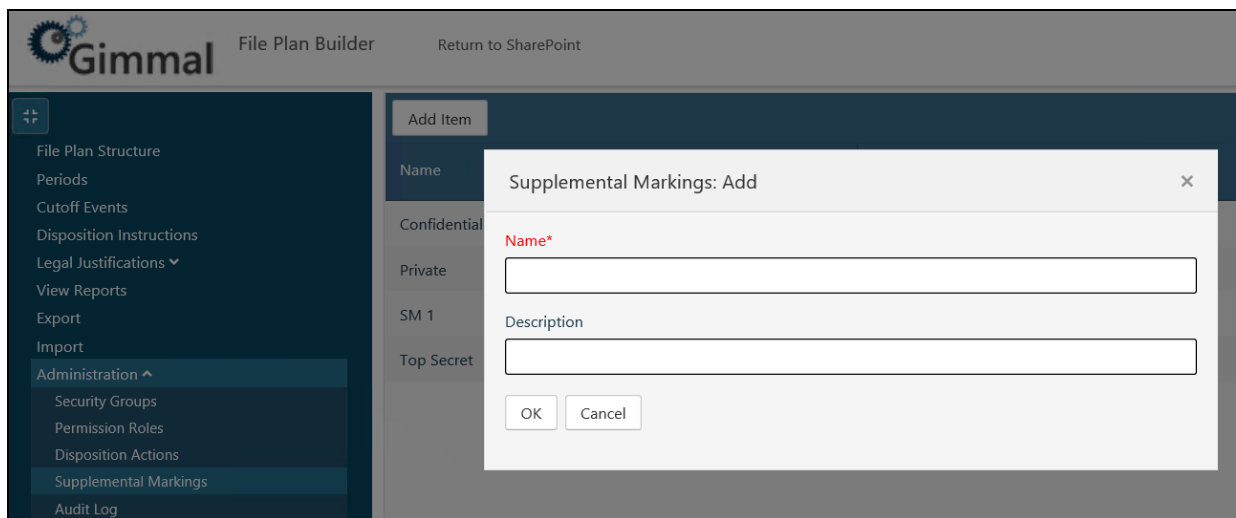


Figure 15-1 Creating a Supplemental Marking

2. Enter the following information:
  - a. **(Required)** Enter the **Name**. The **Name** is a unique identifier for the new Supplemental Marking. The **Name** is used for the selection options on the **File Plan: Supplemental Markings** tab.
  - b. Enter a **Description**. The **Description** is a descriptive statement that defines the purpose of this Supplemental Marking. The **Description** is displayed with the Name in the **File Plan: Supplemental Markings** tab.
3. Click **OK**. The new Supplemental Marking is created and appears in the **Supplemental Markings** list.
4. After you save the new Supplemental Marking, the following occurs:
  - The new Supplemental Marking displays as an option on the **File Plan: Supplemental Markings** tab.
5. After you save the new Supplemental Marking and the File Plan Instantiation timer job is executed, the following occurs:
  - The new Supplemental Marking displays in your SharePoint Records Center Access Rules dialog box as a **Site Column Value** selection option for Supplemental Markings.

## 15.3 Viewing a Supplemental Marking

To view the details of an existing Supplemental Marking, perform the following step:

- From the **Supplemental Markings** list, click the ellipsis (...) to the right of the Supplemental Marking you want to view, and then click **View** from the drop-down menu. The Supplemental Markings: View dialog opens, showing you the details of that Supplemental Marking.

## 15.4 Editing a Supplemental Marking

To change an existing Supplemental Marking, follow these steps.

1. From the **Supplemental Markings** list, click the ellipsis (...) to the right of the Supplemental Marking you want to edit, and then click **View** from the drop-down menu. The Supplemental Markings: View dialog opens.

Figure 15-2 Editing a Supplemental Marking

2. Click **Edit** at the bottom of the dialog. The dialog updates with editable fields for the selected Supplemental Marking, and the title of the dialog changes from Supplemental Markings: View to Supplemental Markings: Edit.
3. Update the information as desired.
4. Click **OK**. The Supplemental Marking is updated and the changes appear in the **Supplemental Markings** list.
5. After you save the Supplemental Marking change, the following occurs:
  - The updated Supplemental Marking will appear as an option on the **File Plan: Supplemental Markings** tab.
  - Any existing file plan node(s) that use this Supplemental Marking will have the update applied hence forth.
6. After you save the Supplemental Marking change and the File Plan Instantiation timer job is executed, the following occurs:
  - The updated Supplemental Marking will appear in your SharePoint Records Center **Access Rules** dialog box as a **Site Column Value** selection option for Supplemental Markings.
  - If the **Name** was changed, the updated Supplemental Marking will appear as a new entry in SharePoint Records Center.

## 15.5 Deleting a Supplemental Marking

To delete an existing Supplemental Marking, follow these steps.

---

### Note

You cannot delete a Supplemental Marking if it is currently assigned to one or more file plan nodes. If you attempt to do so, the Delete option is grayed out and not available for selection

---

1. From the **Supplemental Markings** list, click the ellipsis (...) to the right of the Supplemental Marking you want to delete, and then click **Delete** from the drop-down menu. A Confirm Removal dialog opens, asking you confirm the removal.
2. Click **OK** and the Supplemental Marking is deleted and removed from the **Supplemental Markings** list. The Supplemental Marking will be removed as a selection option for **File Plan: Supplemental Markings** tab.

## 15.6 Supplemental Markings Permission Assignment

To access the Supplemental Markings functionality, you must be a member of a Security Group that has an assigned Permission Role that grants permission.

Permission Assignments are not cascading; you must be assigned each Permission Assignment individually. For example, if you are granted *Edit*, you must also be granted *View* to select a Supplemental Marking for editing.

The following table defines the required Permission Assignment needed to access the Supplemental Markings functionality in File Plan Builder. For more information on Permission Roles, [See "Permission Roles" on page 5.](#)

Table 15-2 Supplemental Markings Permission Assignment

Permission Assignment	Description
View Administration Tab	Provides access to the <b>Administration</b> features in File Plan Builder.  <b>Administration Settings</b> is a vertical tab in File Plan Builder.
View Supplemental Markings	Provides access to the <b>Supplemental Markings</b> tab in
Add Supplemental Markings	Allows a user to read/view an existing Supplemental Marking.
Edit Supplemental Markings	Allows a user to edit an existing Supplemental Marking.
Remove Supplemental Markings	Allows a user to delete an existing Supplemental Marking.

## 16 Audit Log

File Plan Builder Audit Log functionality is available in a SharePoint Records Center with Gimmel Compliance Suite enabled. To use the Audit Log features in *File Plan Builder*, Gimmel Compliance Suite must be installed and the Gimmel File Plan Builder feature must be active. In addition, you must have the proper File Plan Builder: **Permission Roles** assigned. For File Plan Builder: **Permission Roles** settings, see [16.4 Audit Log Permission Assignment](#).

The **Audit Log** tab provides the ability to view and export user actions performed in File Plan Builder. In addition, it supports deletion of audit log entries.

**Intended User:** Compliance Suite Administrator

To access the **Audit Log** view:

1. Open **File Plan Builder**.
2. Select **Administration** from the vertical tabs.
3. Select **Audit Log**. The Audit Log page displays.

The screenshot displays the Gimmel File Plan Builder interface. On the left is a navigation pane with 'Administration' selected and 'Audit Log' highlighted. The main area shows a table of audit log entries. The table has columns for 'Audit Context Type', 'Action Type', 'Audit Date Time', and 'User Name'. One entry for 'RecordContainers' is highlighted with a red box. Below the table, there is a pagination bar showing '11 - 20 of 720 Items' and a dropdown for 'items per page' set to '10'. Below the pagination bar, there is an 'After' section with XML data for the selected entry.

Audit Context Type	Action Type	Audit Date Time	User Name
Import-Started		9/10/2018 7:51:43 PM	WIN12\sp-neo
Export		9/10/2018 7:50:07 PM	WIN12\sp-neo
Import-Successful		9/10/2018 7:47:29 PM	WIN12\sp-neo
CutoffCriteria	Create	9/10/2018 7:47:29 PM	WIN12\sp-neo
RecordContainers	Create	9/10/2018 7:47:29 PM	WIN12\sp-neo
CutoffCriteria	Create	9/10/2018 7:47:29 PM	WIN12\sp-neo
RecordContainers	Create	9/10/2018 7:47:29 PM	WIN12\sp-neo

```

After
<RecordContainer>
  <AuditUserName>WIN12\sp-neo</AuditUserName>
  <RecordContainerId>102</RecordContainerId>
  <Code>Container1</Code>
  <ParentContainerId>97</ParentContainerId>
  <SpecifiedId>Container1</SpecifiedId>
  <IsVitalRecord>false</IsVitalRecord>
  <PeriodId nil="true" />
  <IsHara>false</IsHara>
  <IsCaseBasedRetention>false</IsCaseBasedRetention>
  <IsObsolete>false</IsObsolete>
  <DispositionInstructionId>7</DispositionInstructionId>
  <AuthorityId>4</AuthorityId>
  <InheritCutoffFromParent>false</InheritCutoffFromParent>
  <VitalLastReviewedDate nil="true" />
  <ImportSourceID></ImportSourceID>

```

Figure 16-1 Audit Log Page

The Audit Log page consists of the following elements:

1. **Audit Log** list: At the top of the page is a list of all Audit log entries based on the selected **Audit Parameters**. Use the filters in the column headers to filter on **Audit Context Type**, **Action Type**, **Audit Date Time**, or **User Name**.

2. **Audit Log Detail:** At the bottom of the page is the Audit log details section for the selected Audit log entry. This section contains the *Before* and *After* values that can be used to identify exact changes.

## 16.1 Audit Context Types and Actions

Audit Log entries are supported for create, update, and delete File Plan Builder actions. The **Audit Context Type** that correlates to a File Plan Builder feature determines the available audited action(s) as described in the table below.

The following table describes the Audit Context Types/Item Types/File Plan Builder Features and their corresponding actions that are available in the Audit Log.

Table 16-1 Audit Context Types

Audit Context Types	Description
<b>Authorities</b>	Actions for items on the <b>Authorities</b> tab in the <b>Legal Justifications</b> vertical tab. <i>Create</i> , <i>Update</i> , and <i>Delete</i> actions are audited for this type.
<b>AuthorityLegalJustifications</b>	Actions for Legal Requirement item assignment in the <b>Requirement</b> list field for a Legal Authority. <i>Create</i> and <i>Delete</i> actions are audited for this type.
<b>CutoffCriteria</b>	Actions for fields on the <b>Cutoff Criteria</b> tab in an existing file plan node. Only <i>Update</i> action is audited for this type.
<b>DispositionActions</b>	Actions for items on the <b>Disposition Actions</b> tab in the Administration vertical tab. <i>Create</i> , <i>Update</i> , and <i>Delete</i> actions are audited for this type.
<b>DispositionInstructionEvents</b>	Not Applicable
<b>DispositionInstructions</b>	Actions for items on the <b>Disposition Instructions</b> vertical tab. <i>Create</i> , <i>Update</i> , and <i>Delete</i> actions are audited for this type.
<b>DispositionPhases</b>	Actions for information on the <b>Stages</b> tab in an existing disposition instructions. <i>Create</i> , <i>Update</i> , and <i>Delete</i> actions are audited for this type.
<b>Events</b>	Actions for items on the <b>Events</b> vertical tab. <i>Create</i> , <i>Update</i> , and <i>Delete</i> actions are audited for this type.
<b>LegalJustifications</b>	Actions for items on the <b>Requirements</b> tab in the <b>Legal Justifications</b> vertical tab. <i>Create</i> , <i>Update</i> , and <i>Delete</i> actions are audited for this type.
<b>Parties</b>	Actions for items on the <b>Security Groups</b> tab in the <b>Administration</b> vertical tab. <i>Create</i> , <i>Update</i> , and <i>Delete</i> actions are audited for this type.

Table 16-1 Audit Context Types

Audit Context Types	Description
<b>PartyPermissionRoleAssignments</b>	Actions for Permission Role item assignment in the <b>Permission Role Assignments</b> field for an existing Security Group. <i>Create</i> and <i>Delete</i> actions are audited for this type.
<b>Periods</b>	Actions for items on the <b>Periods</b> vertical tab. <i>Create</i> , <i>Update</i> , and <i>Delete</i> actions are audited for this type.
<b>PermissionRoleAssignments</b>	Actions for <b>Permission Assignments</b> field for a Permission Role. <i>Create</i> and <i>Delete</i> actions are audited for this type.
<b>PermissionRoles</b>	Actions for items on the <b>Permission Roles</b> tab in the <b>Administration</b> vertical tab. <i>Create</i> , <i>Update</i> , and <i>Delete</i> actions are audited for this type.
<b>RecordContainer</b>	Not Applicable
<b>RecordContainers</b>	Actions for items on the <b>File Plan</b> vertical tab. <i>Update</i> and <i>Delete</i> actions are audited for this type.
<b>RecordContainerSPPermissions</b>	Actions for information on the <b>SharePoint Security</b> tab in an existing file plan node. <i>Create</i> , <i>Update</i> , and <i>Delete</i> actions are audited for this type.

## 16.2 Using the Audit Log

To view, delete, or export the Audit Log entries, perform the following steps:


1. Open **File Plan Builder**.
2. Select **Administration** from the vertical tabs, and then select **Audit Log**. The Audit Log page displays.
3. View the **Audit Log** list. The following columns display for the list:
  - **Audit Context Type:** Item type for this audit log entry.
  - **Action Type:** The action performed on the selected item type.
  - **Audit Date Time:** The date and time the audited action was performed.
  - **User Name:** The SharePoint user who performed the audited action.
4. To view the Audit Log detail, select one audit log entry by mousing over the Audit Context Type name in the left column. (The following tooltip displays: "Click to view details.") You can only view one audit log entry at a time. When you select an entry, the Audit log details section displays at the bottom of the page with the following values:
  - **Before:** Values for the selected audit log entry before the audited change. **Before** information displays for the *Update* and *Delete* actions.
  - **After:** Values for the selected audit log entry after the audited change. **After** information displays for *Create* and *Update* actions.

5. To remove audit log entries, perform the following steps:
  - a. Select one or more audit log entries by checking the check box(es) to the left of the Audit Context Type column in the **Audit Log** list. The **Delete** button located above the Audit Log list becomes enabled.
  - b. Click **Delete**. A Confirm Removal dialog opens asking, *Are you sure you want to delete the selected audit entries?*
  - c. Click **OK**. The audit log entry(ies) is deleted and removed from the **Audit Log** list
6. To export audit log entries, perform the following steps:
  - a. Select one or more audit log entries by checking the check box(es) to the left of the Audit Context Type column in the **Audit Log** list. The **Export** button located above the Audit Log list becomes enabled.
  - b. A **File Download** dialog box opens, with options for downloading the exported .xml file. Use your standard file browser to save the exported .xml file to your local machine. (Download options may vary, depending on which browser you are using.)

## 16.3 Filtering Audit Log Entries

File Plan Builder enables you to filter the display of log entries by using the filters available in each column header (**Audit Context Type**, **Action Type**, **Audit Date Time**, and **User Name**).

To filter your log entries, perform the following steps:

1. On the Audit Log list, click the filter icon (  ) for the column(s) you want to filter on. The filter criteria box opens.






		Delete	Export				
<input type="checkbox"/>	Audit Context Type		Action Type		Audit Date Time		User Name
<input type="checkbox"/>	DispositionActions	Show items with value that: <input type="text" value="Is equal to"/>  <input type="text" value="--Select Value--"/>  <input type="button" value="Filter"/> <input type="button" value="Clear"/>			9/10/2018 7:51:43 PM		WIN12\sp-neo
<input type="checkbox"/>	DispositionActions				9/10/2018 7:51:43 PM		WIN12\sp-neo
<input type="checkbox"/>	DispositionActions				9/10/2018 7:51:43 PM		WIN12\sp-neo
<input type="checkbox"/>	Import-Started				9/10/2018 7:51:43 PM		WIN12\sp-neo
<input type="checkbox"/>	Export				9/10/2018 7:50:07 PM		WIN12\sp-neo
<input type="checkbox"/>	Import-Successful				9/10/2018 7:47:29 PM		WIN12\sp-neo

Figure 16-2 Filtering Options on Audit Log List

2. Select/enter the desired filter criteria and click **Filter**. The following occurs:



- Log entries that meet your criteria now display in the Audit Logs list. (Log entries not meeting the filter criteria are hidden from view until the filter is removed.)
  - The Filter icon(s) for the heading or headings you filtered on are highlighted in orange, indicating that the filter is active.
3. To remove the filter, click the orange filter icon for the desired heading. The filter criteria box opens.
  4. Click **Clear**. The Audit Log list refreshes, and now shows the log entries that were previously filtered.

## 16.4 Audit Log Permission Assignment

To access the Audit Log functionality, you must be a member of a Security Group that has an assigned Permission Role that grants permission.

Permission Assignments are not cascading; you must be assigned each Permission Assignment individually. For example, if you are granted *View Audit Log*, you must also be granted *View Administration Tab* to have access to the Administration vertical tab.

The following table defines the required Permission Assignment needed to access the *Administration: Audit Log* functionality in File Plan Builder.

Table 16-2 Administration: Audit Log Permission Assignment

Permission Assignment	Description
<b>View Administration Tab</b>	Provides access to the <b>Administration</b> features in File Plan Builder.  <b>Administration Settings</b> is a vertical tab in File Plan Builder.
<b>View Audit Log</b>	Provides access to the Audit Log tab in the Administration section of File Plan Builder.  Allows a user to view existing audit log entries for File Plan Builder.

## 17 File Plan Association

File Plan Association functionality is available in a SharePoint Records Center with Gimmal Compliance Suite enabled. To use the File Plan Association features Gimmal Compliance Suite must be active. In addition, you must have the proper File Plan Builder: **Permission Roles** assigned. For File Plan Builder: **Permission Roles** settings, see ["Permission Roles" on page 5](#).

The File Plan Association tab enables a user to map file plan node(s) to one or more Record Libraries across multiple sites and site collections. After the mapping is complete, the user can then start the File Plan Instantiation timer job, which instantiates File Plan Builder file plan node(s) and their corresponding features into the mapped SharePoint Record Center(s). This instantiation process enables records to be classified and processed according to your organization's records management policies.

Before mapping your file plan node(s), the following must be completed:

1. File plan node(s) and supporting items must be created using File Plan Builder.
2. SharePoint Record Library(ies) must be created.

**Intended User:** Records Manager; Compliance Suite Administrator

File Plan Association maps and instantiates the following File Plan Builder features:

- File Plan Nodes
- Periods
- Events
- Supplemental Markings

File Plan Builder features listed above are described in detail in the relevant help sections in this guide and online in your SharePoint Records Center and File Plan Builder help.

To access File Plan Association:

1. Open **File Plan Builder**.
2. Select **File Plan Association** from the vertical tabs.

The **File Plan Association** view is split into the following three sections:

- **Site Hierarchy Tree**
- **File Plan Nodes** list
- **Associated Record Libraries** list

### 17.1 File Plan Association Regions

The following three figures illustrate the regions of the File Plan Association view.

The *Site Hierarchy Tree* gives a hierarchical view of the SharePoint farm. It will display any site collections, sites, Record Libraries, and Record Containers to which your current site collection has proper access.

**Note:**

User must have at least contribute permissions on a library for the hierarchy to display it.

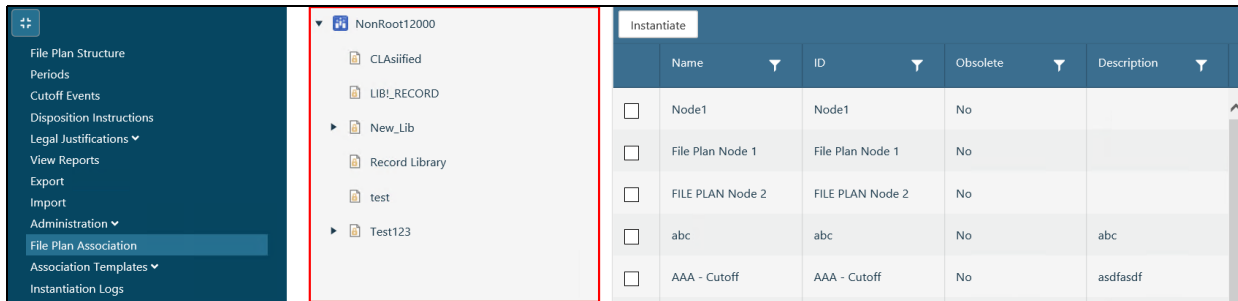


Figure 17-1 File Plan Association Regions - Site Hierarchy Tree

The **File Plan Node** list will display all top-level node(s) in your file plan structure.

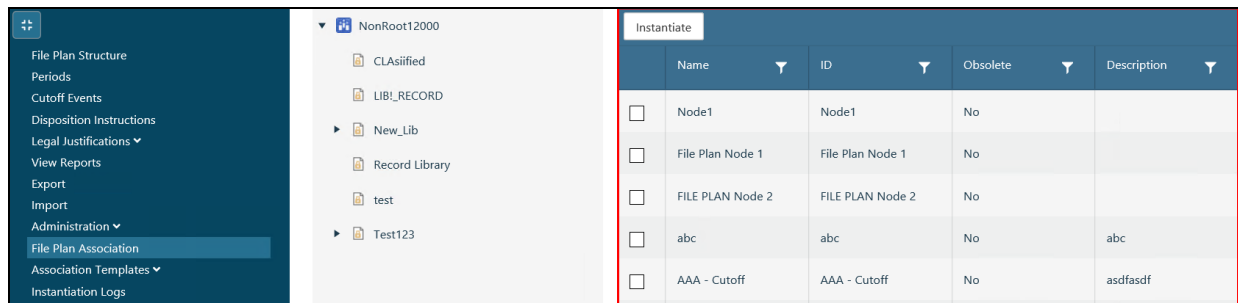


Figure 17-2 Top Level Nodes

The **Associated Record Libraries** list displays any currently associated/mapped Record Libraries to the selected file plan node.

Name	ID	Obsolete	Description
<input type="checkbox"/> Node1	Node1	No	
<input type="checkbox"/> File Plan Node 1	File Plan Node 1	No	
<input type="checkbox"/> FILE PLAN Node 2	FILE PLAN Node 2	No	
<input type="checkbox"/> abc	abc	No	abc
<input type="checkbox"/> AAA - Cutoff	AAA - Cutoff	No	asdfasdf

Title	Path
FPB_26July	NonRoot544/FPB_26July
FPB_Insta	NonRoot544/FPB_Insta
FPB_Library	NonRoot544/FPB_Library

Figure 17-3 Associated Record Libraries

## 17.2 Completing a File Plan Association

The following scenario describes the actions you will take to complete a File Plan Association:

1. Open the *File Plan Association* tab. The Site Hierarchy Tree loads all accessible site collections, sites, record libraries, and record containers. The **File Plan Nodes** list displays all top-level nodes.
2. Select a record library from the *Site Hierarchy Tree*. Check the boxes next to the top-level nodes you want to instantiate into that record library (the mapping portion), then click **Save**. Repeat this step for the other Record Libraries.

---

### Note:

If you select anything in the tree other than a Record Library, you cannot place checks in the **File Plan Node** list.

---

3. You can select a top-level node in the **File Plan Node** list at any point. The **Associated Record Libraries** list will display any Record Libraries that are currently associated (mapped) to the selected file plan node; this is purely for informational purposes.
4. When you complete setting up the Record Library-to-File Plan(s) mapping, and you are ready to instantiate your file plan node(s) into SharePoint, click the **Instantiate** button. This action schedules the *File Plan Instantiation timer job*, which completes synchronizes:

27 March 2019

- a. Periods
- b. Supplemental Markings
- c. Events
- d. File Plans (Record Containers)

### **17.2.1 File Plan Builder to SharePoint Mapping**

When the *File Plan Instantiation timer job* is executed, the selected *File Plan Builder* file plan node(s) and their corresponding supporting items are created or updated in your SharePoint Records Center. The following table describes the mapping of *File Plan Builder* items to *SharePoint Records Center* items.

Table 17-1 File Plan Builder to SharePoint Records Center Mappings

File Plan Builder Feature	SharePoint Content Type	Instantiation Details
<b>File Plan Node</b>	Record Container	<p>Each top-level file plan node and its child node(s) are instantiated in the mapped Record Library. The top-level file plan node is instantiated as a Record Container at the top-level of the mapped Record Library. The child node(s) are instantiated as Record Container(s) in the top-level file plan node's corresponding Record Container.</p> <p>All values set on the selected file plan node in File Plan Builder are instantiated as the set value in the corresponding site column on the Record Container. In addition, the values are instantiated as supporting SharePoint content types, where applicable. For example, a period is set as the <b>Cutoff Review Period</b> and a new <b>Period Definition</b> item is created.</p> <p>The Record Container's <b>ID</b> is used to map a file plan node to its corresponding Record Container.</p> <p><b>Create:</b> If the Record Container does not exist, a new Record Container is created.</p> <p><b>Update:</b> The Record Container's <b>ID</b> cannot be changed. Therefore, the existing Record Container is updated.</p> <p><b>Delete:</b> No action is taken.</p>

Table 17-1 File Plan Builder to SharePoint Records Center Mappings

File Plan Builder Feature	SharePoint Content Type	Instantiation Details
<b>Period</b>	Period Definition	<p>All periods assigned to a selected file plan node are instantiated as a Period Definition item and will appear in the <b>Period Definitions</b> list.</p> <p>The period definition's <b>Period Name</b> is used to map a File Plan Builder period to its corresponding period definition.</p> <p><b>Create:</b> If the period definition does not exist, a new period definition is created.</p> <p><b>Update:</b> If the period definition's Period Name is changed, a new period definition is created. For all other changes, the existing period definition is updated.</p> <p><b>Delete:</b> No action is taken.</p>
<b>Event</b>	Event Management Service item	<p>All Events assigned to a selected file plan node are instantiated as an event in the Gimmel Compliance Suite Event Management Service and will be displayed in the <b>Gimmel Compliance Suite Event Management</b> list.</p> <p>The event's <b>Name</b> is used to map a File Plan Builder event to its corresponding <b>Gimmel Compliance Suite Event Management</b> item.</p> <p><b>Create:</b> If the event does not exist, a new event is created.</p> <p><b>Update:</b> If the event's Name is changed, a new Event is created. For all other changes, the matching event is updated.</p> <p><b>Delete:</b> No action is taken.</p>

Table 17-1 File Plan Builder to SharePoint Records Center Mappings

File Plan Builder Feature	SharePoint Content Type	Instantiation Details
<b>Disposition Instruction</b>	Information Management Policy (IMP)	<p>All disposition instructions assigned to a selected file plan node are instantiated as an Information Management Policy (IMP) and display in the Information Management Policy Settings of each Record Library.</p> <p>The IMP's <b>Name</b> is used to map a File Plan Builder disposition instruction to its corresponding IMP.</p> <p><b>Create:</b> If the IMP does not exist, a new IMP is created.</p> <p><b>Update:</b> If the Disposition Instruction's <b>Name</b> is changed, the assigned <b>Disposition Instruction Name</b> of any corresponding <b>Record Container(s)</b> updates.</p>
<b>Disposition Instruction: Stage(s)</b>	Expiration Policy	<p>All disposition instruction stages assigned to a selected file plan node are instantiated as an Expiration Policy.</p> <p><b>Create:</b> If the Expiration Policy does not exist, a new Expiration Policy is created.</p> <p><b>Update:</b> If the Expiration Policy's is changed, a new Expiration Policy is created overriding previous Expiration Policy created manually or through File Plan Builder.</p> <p><b>Delete:</b> The Expiration Policy is removed.</p>



Table 17-1 File Plan Builder to SharePoint Records Center Mappings

File Plan Builder Feature	SharePoint Content Type	Instantiation Details
<b>Administration: Disposition Action</b>	Policy Action	<p>All disposition actions assigned to a disposition instruction stage that is assigned to a selected file plan node must match an existing SharePoint Policy Action.</p> <p>The disposition action is instantiated as a part of the <b>Disposition Instruction: Stage(s)</b> described above. The <b>Disposition Instruction: Stage</b> comprises both an Expiration Policy and Policy Action.</p>
<b>Administration: Supplemental Marking</b>	Supplemental Marking Managed Metadata Terms	<p>All Supplemental Markings assigned to a selected file plan node are instantiated as an item in the Supplemental Markings Managed Metadata Terms and will appear as an option in the Access Rules Supplemental Markings <b>Site Column Value</b>.</p> <p>The Supplemental Markings Managed Metadata Term's <b>Name</b> is used to map a File Plan Builder Supplemental Markings to its corresponding term.</p> <p><b>Create:</b> If the term does not exist, a new term is created.</p> <p><b>Update:</b> A new term is created.</p> <p><b>Delete:</b> No action is taken.</p>

## 18 Association Templates

Association Templates functionality is available in a SharePoint Records Center with Gimmel Compliance Suite enabled. To use the Association Templates features in File Plan Builder, Gimmel Compliance Suite must be installed and the Gimmel Compliance Suite File Plan Builder feature must be active. In addition, you must have the proper File Plan Builder: **Permission Roles** assigned. For File Plan Builder: **Permission Roles** settings, see [“Association Templates Permission Assignment” on page 117](#).

The Association Templates feature is an alternate mechanism for performing file plan associations and instantiations. It provides a means for associating a selected root node or nodes with numerous libraries across your SharePoint architecture. This “bulk” instantiation process provides a more flexible and convenient way to associate and instantiate several File Plan Builder nodes across multiple Records Center libraries versus using the original File Plan Builder instantiation process.

For example, let’s say that you have a common library across different locales in your organization called Accounting and Finance. Each locale has a root node where financial records are managed. If you want to create the “Tax” node across all locales, the Association Templates feature enables you to configure a file plan template that associates the “Tax” node to all occurrences of that Accounting and Finance library across any number of site collections. You can perform this process if you want the same disposition rules to be applied across a number of libraries on more than one site.

The process is illustrated in the following diagram:

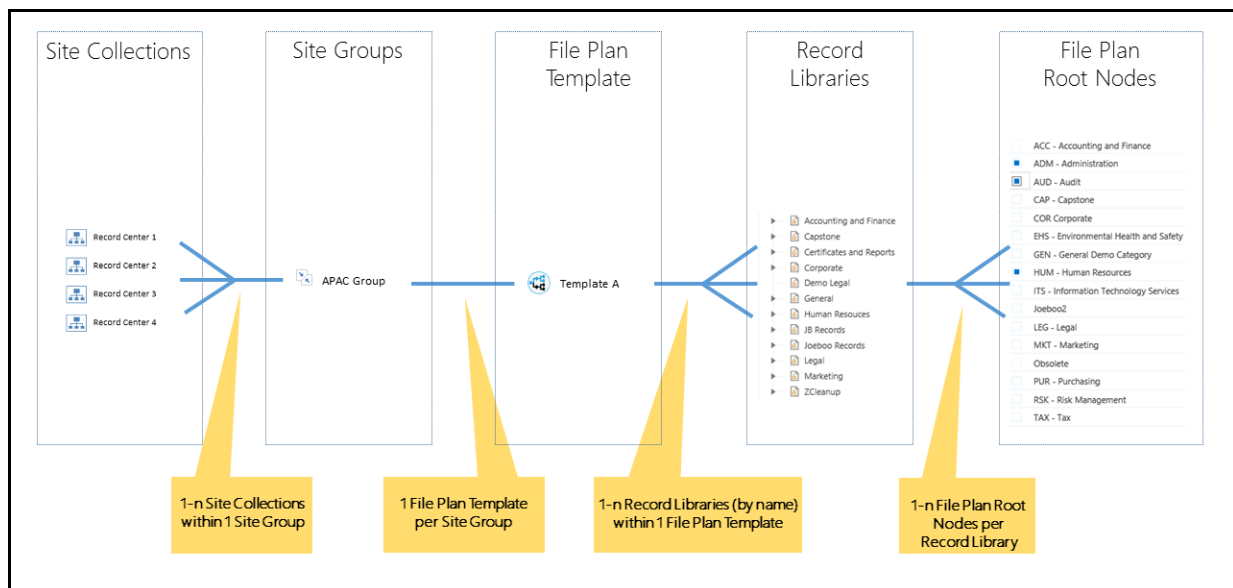


Figure 18-1 File Plan Template Association Process

**Intended User:** Compliance Suite Administrator

To access the **Association Templates** options, follow these steps:

1. Open **File Plan Builder**.
2. Click **Association Templates** in the vertical menu. The Association Templates context menu opens.
3. Select the **File Plan Templates** option. The File Plan Templates list displays

---

**Note:**

Do not try to use a saved URL to access the **Association Templates** view; you must access it from the File Plan Builder menu.

---

## 18.1 Association Templates Features

The following table describes the features available from the **Association Templates** context menu.

*Table 18-1 Association Templates Features*

List View Heading	Description
<b>File Plan Templates</b>	<p>Enables you to create, edit, or delete templates that associate File Plan Builder nodes in the File Plan Structure to libraries referenced by name, or alternatively to all Compliance Suite-enabled libraries across an organization.</p> <p>This template stores information about libraries (by name) or, alternatively, All Record Libraries, and specifies which nodes to associate to them. The Site Groups option directs File Plan Builder where to associate and instantiate them.</p>
<b>Site Groups</b>	Enables you to create, edit, or delete site groups to define which sites a specific File Plan Template will apply to.
<b>Commit Template</b>	Associates a Site Group to Compliance Suite-enabled Records libraries. It will not instantiate the file plan nodes, but it will associate those nodes to the file plans for any sites associated with the selected Site Group.
<b>Instantiate by Group</b>	Runs the File Plan Builder instantiation job for the sites in the selected Site Group.
<b>Associations by Query</b>	Enables you to perform manual associations and instantiations using a more robust system that specializes in searches across large organizations/SharePoint implementations.

---

**Note:**

If you experience any issues with your pages loading correctly in the Internet Explorer browser, ensure that your File Plan Builder site has been added to the Trusted Sites list in Internet Explorer.

---

## 18.2 Association Templates Permission Assignment

To access the **Association Templates** functionality, you must be a member of a Security Group that has an assigned Permission Role that grants permission.

The following table defines the required Permission Assignment needed to access the Association Templates functionality in File Plan Builder. For more information, [See "Permission Roles Permission Assignment" on page 15.](#)

*Table 18-2 Association Templates Permission Assignment*

Permission Assignment	Description
<b>View File Plan Association Tab</b>	Provides access to the Association Templates vertical tab in File Plan Builder.

## 18.3 Configuring File Plan Templates

A file plan template defines a collection of libraries by name, as well as nodes that are associated to each library. It enables you to create, edit, or delete templates that associate File Plan Builder nodes (located in the File Plan Structure) to libraries referenced by name, or to all Compliance Suite-enabled libraries across an organization. For information on creating, editing, and deleting file plan templates, see the following sections.

### 18.3.1 Creating a New File Plan Template

To create a new file plan template, you must perform the following high-level tasks:

- Add a name and description to the new file plan template.
- Add one or more record library names to the template.
- Associate file plan nodes to the record libraries.

Each task is described in detail below.

#### Adding a Name and Description to a New File Plan Template

To add a name and description to a new file plan template, follow these steps:

1. From the Association Templates context menu, click **File Plan Templates**. The File Plan Templates page opens.

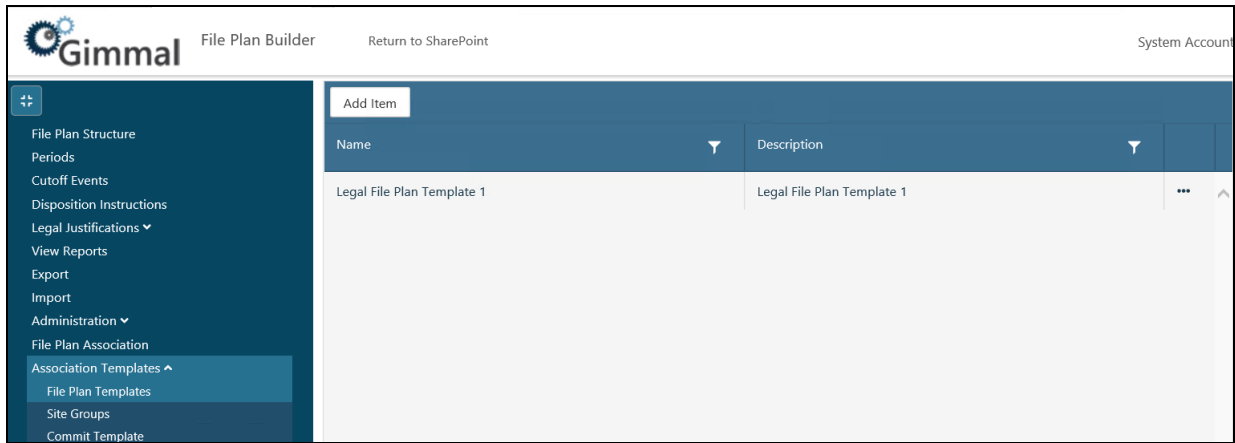


Figure 18-2 File Plan Templates Page

2. Click **Add Item** to create a new template. The Template: Add dialog opens.

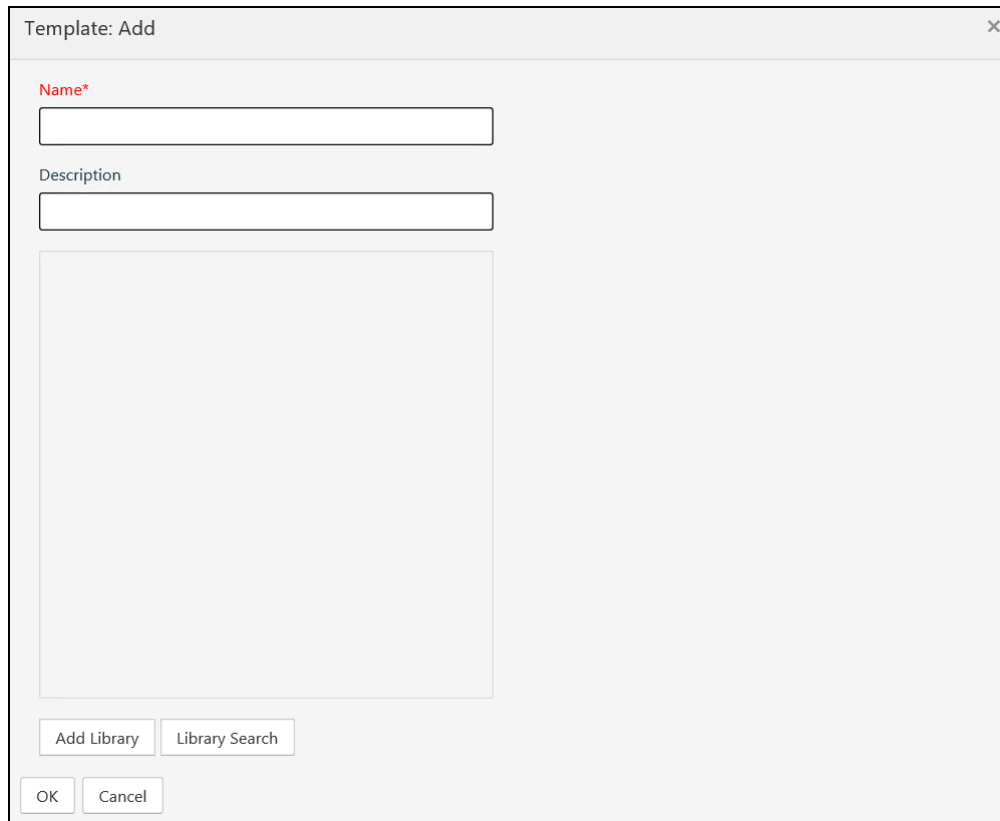


Figure 18-3 Add Template Dialog

3. In the Template: Add dialog, enter a **Name** (required) and a **Description** for the new template. The template name must be unique.
4. Continue with the next section.

## Adding a Record Library Name to the File Plan Template

Next, you must add a record library name(s) to the file plan template. You can add the library name using one of two methods, by typing it in or by searching for it. See the following sub-sections for the scenario that applies to you:

- [Adding a Library Name to a File Plan Template by Typing the Name](#)
- [Adding a Library Name to a File Plan Template by Performing a Query](#)

---

### Note:

When you add libraries to a file plan template, they are stored by name only. File Plan Builder does not create libraries for you. During the commit template and subsequent instantiation by group phases (described below), File Plan builder will parse all sites for the library or libraries by name for a match, and create the specified nodes.

For the instantiation process to take place successfully, a library(ies) must already exist, and must be in a site that has a Record Center where Compliance Suite is installed and configured. You can add one library name or multiple names, and every library name can have unique nodes associated to it.

---

### ***Adding a Library Name to a File Plan Template by Typing the Name***

If you know the record library name that you want to add to the file plan template, perform the following steps:

1. Click **Add Library** at the bottom of the Template: Add dialog. The Add Libraries panel displays on the right side of the dialog.

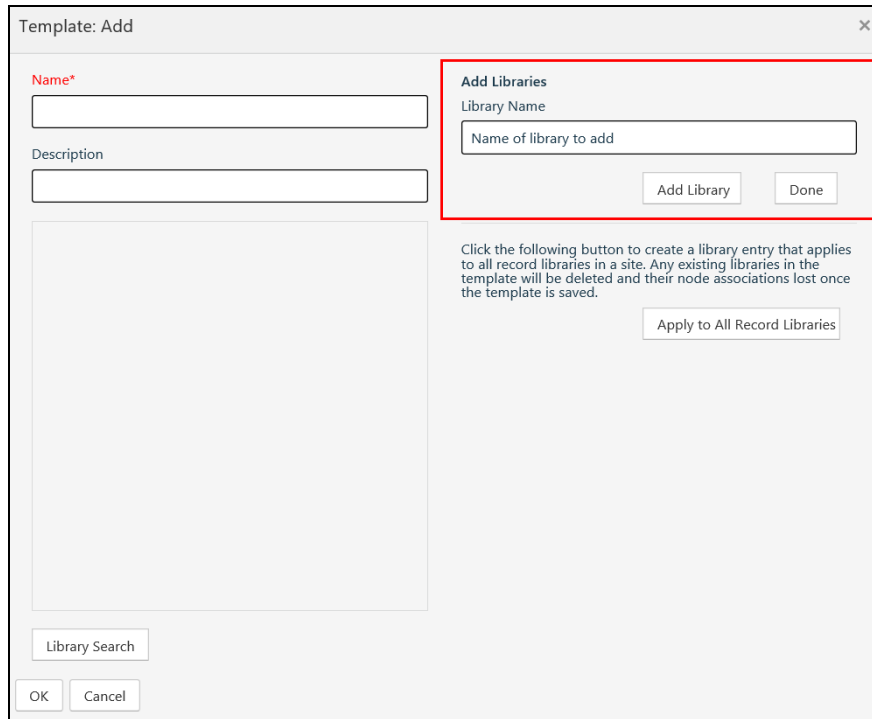


Figure 18-4 Adding a Library by Name

2. Enter the name of a library that you want to add to the template in the **Library Name** field. This field is not case-sensitive.
3. Click **Add Library**. The library name displays in the dialog, under the Description field on the left side.
4. Repeat these steps to add as many library names as desired.

---

#### Note:

You can click the **Apply to All Record Libraries** option at the bottom of the panel to add a common node to all Compliance Suite-enabled record libraries. Any libraries that are already in the template will be removed and the entry **[All Record Libraries]** will display in the Template: Add dialog under the Description field. Any nodes that are associated to the **[All Record Libraries]** entry will be created for every Compliance Suite enabled record library when this file plan template is added to a Site group that is subsequently committed and instantiated.

---

5. Click **Done** to close the Add Libraries panel.
6. Click **OK** to save the new file plan template. At this point you have not associated any root nodes to the library, so the File Plan Template is incomplete.
7. Continue with the remaining steps in this chapter.

## Adding a Library Name to a File Plan Template by Performing a Query

If you want to query for a library name, perform the following steps:

1. Click **Library Search** at the bottom of the Template: Add dialog. The Search for Libraries panel displays on the right side of the dialog.

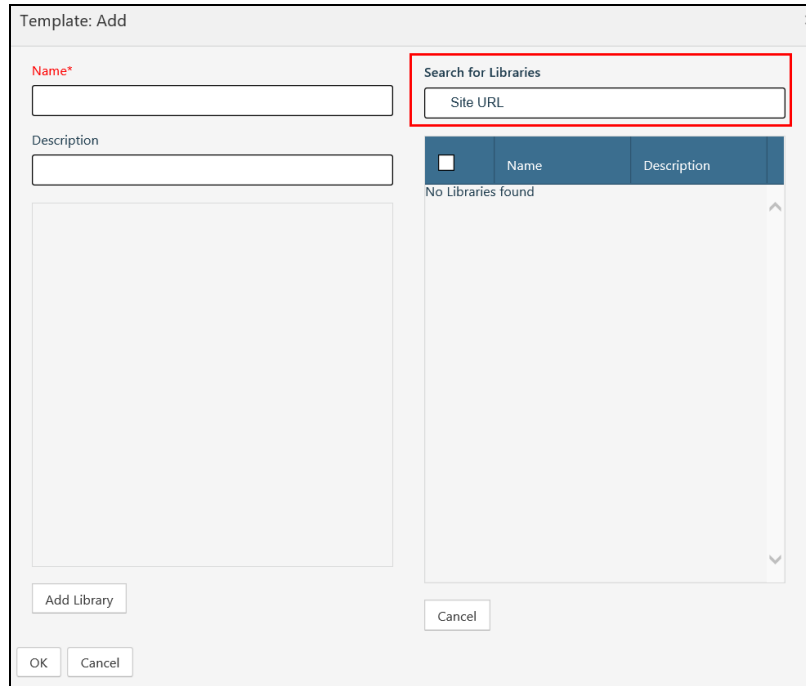


Figure 18-5 Add Libraries to Template by Searching

2. Type a *complete* site URL in the **Site URL** field on the dialog. A partial URL will not work.
3. Press **Enter**. The system will return all of the record libraries that exist in the site URL that you entered in the previous step, and display them in a list in the Template: Add dialog.

---

### Important!

The list of libraries that are returned from the library search are **not** security trimmed.

---

---

### Note:

If a library has already been added to the file plan template, it will no longer be available in the list of libraries to select.

---

4. Select the check box for the library(ies) that you want to add to the file plan template, and then click **Add libraries**.



5. To add all of the listed libraries to the file plan template, click **Add all libraries** (located under the site URL field).
6. Click **Save** to save the new file plan template. At this point you have not associated any root nodes to the library, so the File Plan Template is incomplete.
7. Continue with the remaining steps in this chapter.

---

**Note:**

A File Plan Template stores only the name of the library; not the URL.

---

### *Deleting a Library Name from a Template*

To delete a library name from a file plan template, follow these steps.

1. Open **File Plan Builder**.
2. Click **Association Templates** in the vertical menu, and then click **File Plan Templates**.
3. On the File Plan Templates page, locate the template you want to delete library names from, and click the ellipsis (...) to the right of the template name. A context menu displays.
4. Click **View** from the context menu. The Template: View dialog opens, showing read-only fields for that template.
5. Click **Edit** at the bottom of the dialog to enable the fields. The dialog name changes to Template: Edit. You are now in edit mode.

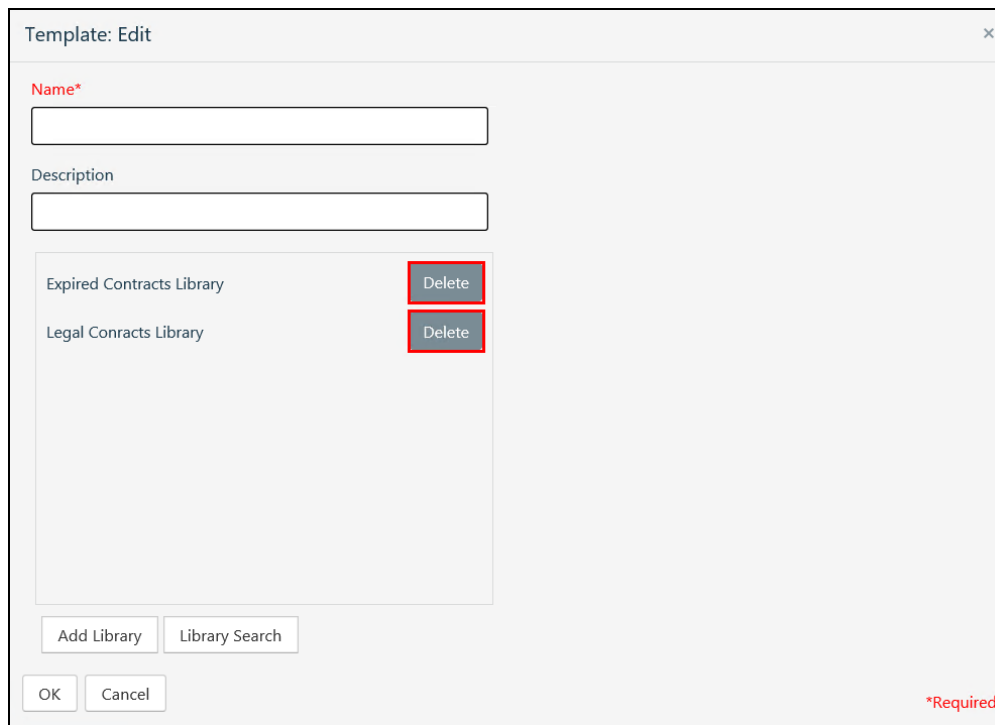


Figure 18-6 Deleting a Library Name

6. Click **Delete** to the right of the library name that you want to delete. A confirmation dialog displays.
7. Click **OK** to delete the library name and close the dialog.
8. Click **OK** on the Template dialog to save your changes to the file plan template.

## Associating File Plan Nodes to the Record Library

Next, you must designate which root nodes will be associated with a particular library. To do this, you must first display the available root nodes in your system, and then you must select the node(s) you want to associate with a specific library name.

To display the available root nodes in your File Plan Builder system and associate them to a selected record library name that is listed, perform the following steps:

---

### Note:

The root nodes that you will associate with a library name are those nodes that currently exist in the File Plan Structure tab of File Plan Builder.

---

1. On the Template dialog, in Edit mode, select the library name that you want to associate root nodes to. (If you opted to create a library entry that applies to all record libraries, then you will only have one entry listed - [**All Record Libraries**]. Click on this to associate nodes.)

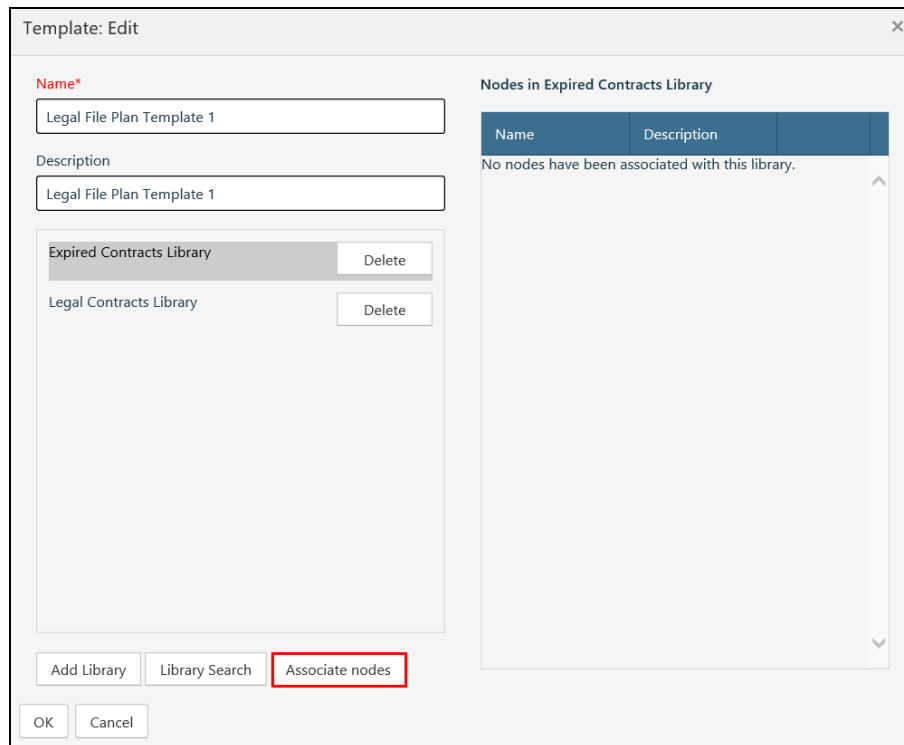


Figure 18-7 Selecting a Library to Associate Root Nodes To

2. Click **Associate nodes**. The **Add Root FPB Nodes to Library** panel displays on the right side of the editor, displaying a list of all the available root nodes. This root node list will display for any library by name or the **[All Record Libraries]** entry.

The screenshot shows a 'Template: Edit' dialog box. On the left, there are fields for 'Name\*' (Legal File Plan Template 1) and 'Description' (Legal File Plan Template 1). Below these are two library entries: 'Expired Contracts Library' and 'Legal Contracts Library', each with a 'Delete' button. At the bottom left are 'Add Library' and 'Library Search' buttons. On the right, the 'Add Root FPB Nodes to Library' panel is active. It features a 'Filter Nodes' search field and a table of root nodes. The table has columns for a checkbox, 'Name', and 'Description'. The nodes listed are: ADM - Administration (Administration Records), AUD - Audit (Audit Records), BBB - Cutoff, CAP - Capstone (Capstone Email Records), CCC - Cutoff, COR Corporate (Corporate Records), EHS - Environmental Health and Safety (Environmental Health and Safety Records), and GEN - General (Used for testing). A 'Cancel' button is located below the table.

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	ADM - Administration	Administration Records
<input type="checkbox"/>	AUD - Audit	Audit Records
<input type="checkbox"/>	BBB - Cutoff	
<input type="checkbox"/>	CAP - Capstone	Capstone Email Records
<input type="checkbox"/>	CCC - Cutoff	
<input type="checkbox"/>	COR Corporate	Corporate Records
<input type="checkbox"/>	EHS - Environmental Health and Safety	Environmental Health and Safety Records
<input type="checkbox"/>	GEN - General	Used for testing

Figure 18-8 Viewing Available Root Nodes

You are now ready to associate these root nodes with your record library(ies).

---

**Note:**

When associating a root node to a record library, you must select each individual library, one by one, and add the root nodes.

---

3. There are several methods you can use to associate your root nodes to a selected library:
  - Click the check box next to the desired node(s), and then click **Add Nodes**. (The **Add Nodes** button displays below the list on the right when one or more root nodes are selected.)
  - Click the check box in the heading, to the left of the Name column, to associate every root node.
  - In the **Filter Nodes** field at the top, you can filter the nodes based on name or description by typing the first few letters of the node name/description. When you get your desired results, perform either of the steps above to associate your nodes.

Note the following filtering tips:

- Filtering is not case-sensitive.
  - Filtering will execute on partial words. For example, if you type **B**, all the nodes with **B** anywhere in their names will only display.
  - Filtering does not support multiple keywords. For example, if you filter on “financial ledgers”, the system will only return items with the exact phrase “financial ledgers” in them, and in that order. It will not return items containing only “financial” or “ledgers”.
  - If you click the **X** in the Filter Nodes field, it will clear any entry and return all nodes.
4. To **disassociate** a root node from a library, perform these steps:
    - a. Select the library in the Template dialog. The list of associated root nodes displays to the right.
    - b. Click **Delete** beside each node that you want to disassociate from that library. It will be removed from the list immediately with no confirmation message.
  5. Repeat Steps 1 through 3 for each library that you want to add root nodes to.
  6. When you are satisfied with the root nodes that you have associated to your record libraries, click **OK** on the Template dialog to save your changes to the file plan template.

### 18.3.2 Editing a File Plan Template

To edit an existing file plan template, perform the following steps.

1. Open **File Plan Builder**.
2. Click **Association Templates** in the vertical menu, and then click **File Plan Templates**.
3. On the File Plan Templates page, locate the template you want to edit, and click the ellipsis (...) to the right of the template name. A context menu displays.
4. Click **View** from the context menu. The Template: View dialog opens, showing read-only fields for that template.
5. Click **Edit** at the bottom of the dialog to enable the fields. The dialog name changes to Template: Edit. You are now in edit mode.
6. Revise the template settings as necessary. (The **Name** must still be unique.)
7. Click **OK** to save your changes.

---

#### Note:

You can rename a file plan template if it has already been associated to a site group (described below). File Plan Builder associations are assigned an internal ID number that will remain the same, regardless of name changes.

---

### 18.3.3 Deleting a File Plan Template

To delete an existing file plan template, perform the following steps.

1. Open **File Plan Builder**.
2. Click **Association Templates** in the vertical menu, and then click **File Plan Templates**.
3. On the File Plan Templates page, locate the template you want to edit, and click the ellipsis (...) to the right of the template name. A context menu displays.
4. Click **Delete** from the context menu. A Confirm Removal dialog opens.
5. Click **OK** to delete the template and close the confirmation box.

## 18.4 Configuring Site Groups

Site groups define which site(s)/site collection(s) a specific file plan template will apply to.

For example, consider a file plan template that defines *Marketing Contracts* as the record library name with root nodes *2016* and *2017* configured for it, and this template is associated to a site group that has two entries: `http://yourdomain.com/` and `http://yourdomain2.com/`. When this template is associated and instantiated, File Plan Builder searches for all libraries matching *Marketing Contracts* in these two sites and creates the nodes (Record Categories) *2016* and *2017* for each Records Center site that is enabled with Compliance Suite.

This section describes how to create, edit, or delete site groups.

---

#### Note:

If you select a site that Compliance Suite is not installed on, no libraries on that site will be associated with the template.

---

### 18.4.1 Creating a New Site Group

To create a new site group, you must perform the following high-level tasks:

- Add a name, description, and template to a new site group.
- Add specific, or all, sites to a site group.

Each task is described in detail below.

1. From the Association Templates context menu, click **Site Groups**. The Site Groups page opens.

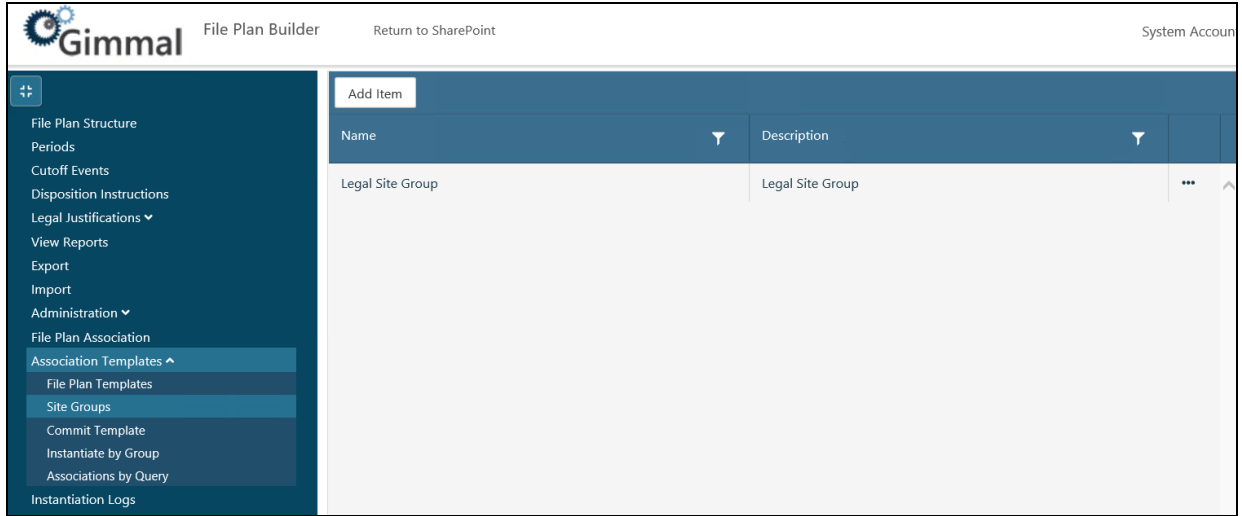


Figure 18-9 Site Groups Page

2. Click **Add Item**. The Site Group: Add dialog opens.

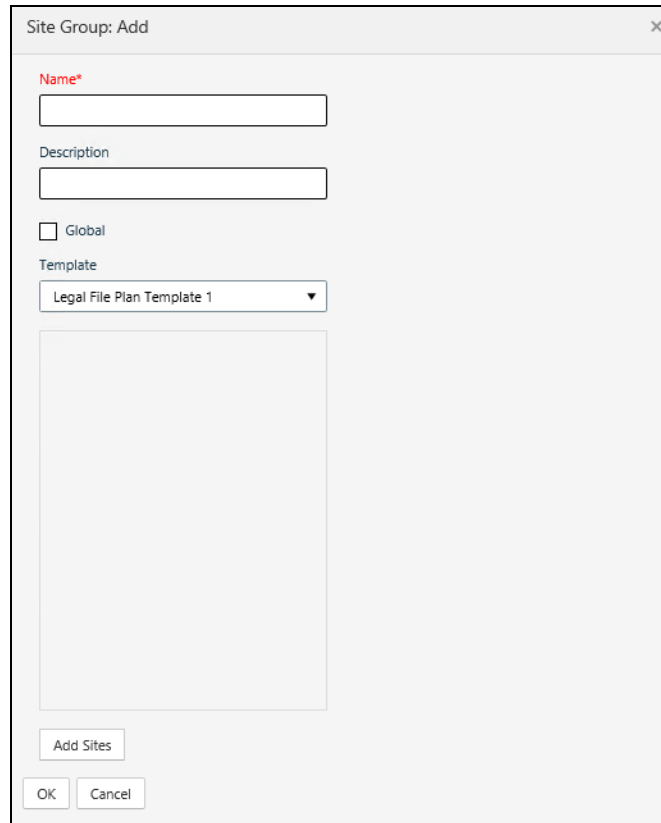


Figure 18-10 Site Group: Add Dialog

3. In the Site Group dialog, enter a **Name** (required) and a **Description** for the new site group. The site group name must be unique.
4. Select a file plan template from the **Template** drop-down list to apply the template to all the sites in this site group (described in the next section).

5. Next, you must add specific sites to your site group.
6. Click **Add sites** at the bottom of the Site Group Editor. The Search for Sites panel displays on the right side of the editor.

Figure 18-11 Searching for Sites to Add to Site Group

7. To search for sites, type a search term in the search field.

Note the following search tips:

- The only sites that are returned are those with a Records Center configured. File Plan Builder does not check whether this is a Records Center with Compliance Suite configured - only that it's a Records Center.
- You can search against the URL, Title, and Description.
- The search is not case-sensitive.
- Partial matches work.

8. Press **Enter** to execute the search.

---

### Important!

The list of sites that are returned from the search are **not** security trimmed.

The sites that are returned may not have Gimmel Compliance Suite installed on them. This is verified during the association and instantiation process.

---

9. For any sites that are returned, select the check box(es) for individual site(s) or select the "Add All" check box in the header to the left of the Name column.
10. Click **Add sites** at the bottom to add the selected site(s) to the site group.
11. Repeat Steps 6 to 10 as needed to add any additional sites to the site group.
12. Click **OK** to save your changes to the site group.

## Adding All Sites to the Site Group

If you want your new site group to include all the sites in the farm, follow these steps.

1. In the Site Group dialog, select the **Global** check box.

The screenshot shows the 'Site Group: Add' dialog box. It has a title bar with a close button. On the left side, there are four input fields: 'Name\*' (containing 'Legal Department Site Group'), 'Description' (containing 'Site group for company legal department'), 'Global' (checkbox, highlighted with a red box), and 'Template' (dropdown menu showing 'Legal File Plan Template 1'). On the right side, there is a 'Search for Sites' section with a 'Find a site' input field and a table with columns 'Name', 'Desc...', and 'URL'. The table is currently empty with the text 'No Sites found' below it. At the bottom of the dialog, there are 'OK' and 'Cancel' buttons.

Figure 18-12 Site Group Editor - Global Option

2. Ensure that a template has been selected from the Template drop-down list.
3. Click **OK** to save this group and close the Site Group dialog.

## 18.4.2 Editing a Site Group

To edit an existing site group, follow these steps.



1. On the Site Groups page, locate the site group you want to edit, and click the ellipsis (...) to the right of the site group name. A context menu displays.

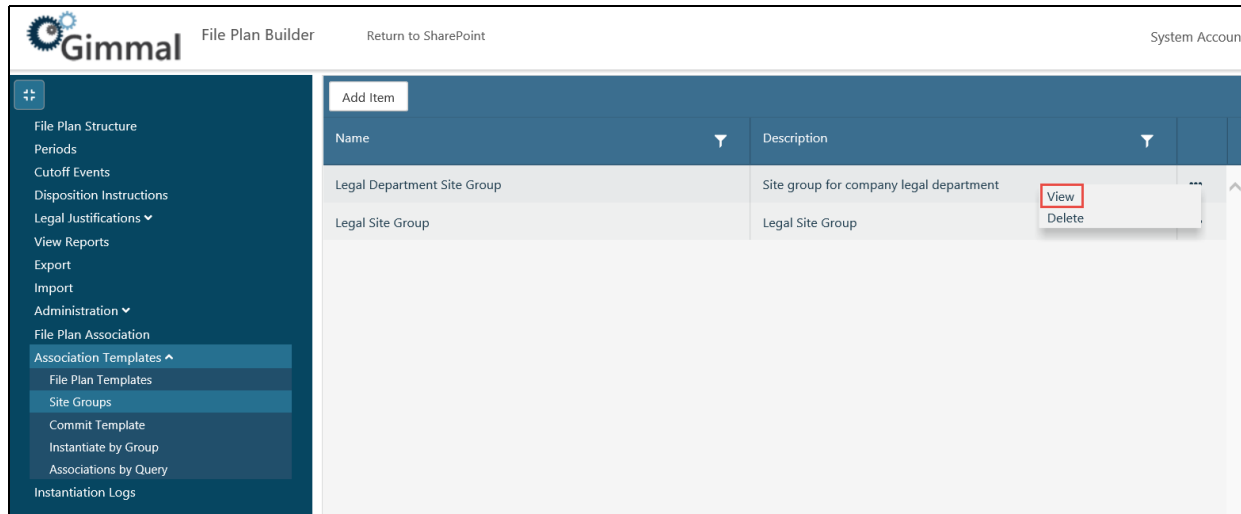


Figure 18-13 Editing a Site Group

2. Click **View** from the context menu. The Site Group: View dialog opens, showing read-only fields for that site group.
3. Click **Edit** at the bottom of the dialog to enable the fields. The dialog name changes to Site Group: Edit. You are now in edit mode.
4. Revise the site group **Name, Description, Template, or Sites** as necessary. The **Name** must still be unique.
5. Click **OK** to save your changes.

### 18.4.3 Deleting a Site from a Site Group

To delete a site from a site group, follow these steps.

1. Navigate to the Site Group: Edit dialog for the site group that you want to delete a site from.
2. Click the **Delete** button beside the site that you want to delete, It is deleted immediately with no confirmation message.
3. Click **OK** to save your changes.

### 18.4.4 Deleting a Site Group

To delete an existing site group, follow these steps.

1. Open **File Plan Builder**.
2. Click **Association Templates** in the vertical menu, and then click **Site Groups**.
3. On the Site Groups page, locate the site group you want to remove, and click the ellipsis (...) to the right of the template name. A context menu displays.

4. Click **Delete** from the context menu. A Confirm Removal dialog opens.
5. Click **OK** to delete the site group and close the confirmation box.

## 18.5 Committing a Site Group to Create File Plan Associations

The **Commit Template** tab enables you to map root node(s) to one or more record libraries (as defined in the file plan template) across multiple sites and site collections as defined in the Site Groups. It does not instantiate the file plan nodes. The Commit Template feature takes a site group and creates file plan associations. This is no different than saving an association (as described above in Chapter 17.)

---

### Note:

Associations are only committed for Records Center sites that have Compliance Suite installed.

---

1. From the Association Templates context menu, click **Commit Template**. The Commit Template by Group page opens.

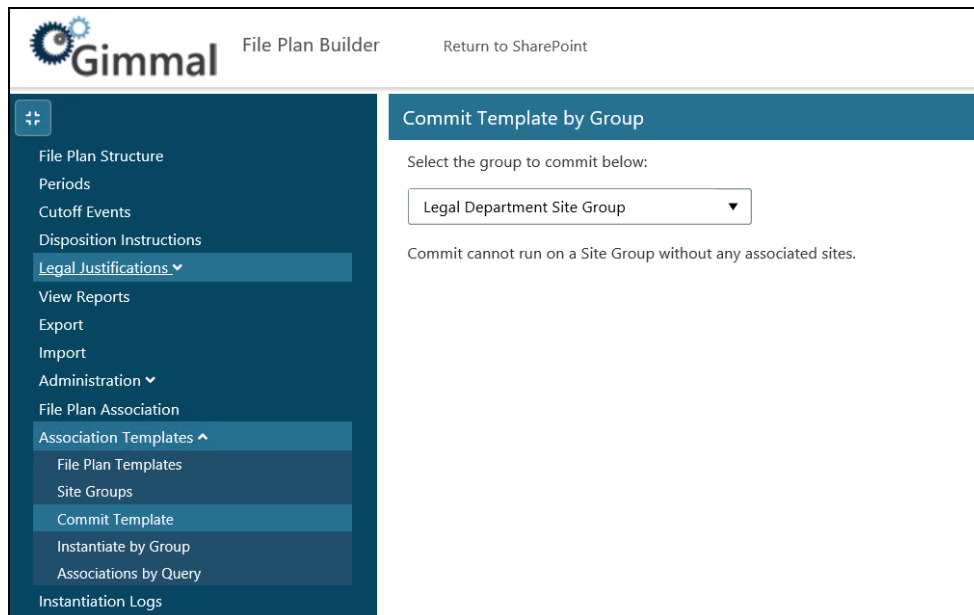


Figure 18-14 Commit Template by Group Page

2. Select the site group that you want to use to create an association.

---

Note:

If the group you choose has no site(s) and/or no file plan template associated with it, the **Commit** button does not display. A group without sites or a template cannot be committed.

---

3. Click **Commit**.

The GimmelSoft Compliance Suite Template Association Timer Job begins in the background. Navigate to **Central Administration**, and go to **Monitoring > Check Job Status** to see the status of the job.

---

Note:

**Instantiate** and **Commit** jobs cannot run at the same time.

---

## 18.6 Instantiating by Group

*Instantiation* applies the file plan template root node/library mappings to matching Compliance Suite record libraries in the locations specified by the Site Group. The result is that Compliance Suite Record Categories (the nodes selected in the libraries) will be created in all sites that match the library names for the sites defined in the instantiated site group.

---

Note:

You must **Commit** before **Instantiating**, otherwise the File Plan Builder system will not process the instantiation request.

**Instantiate** and **Commit** jobs cannot run at the same time.

---

To instantiate a template, perform the following steps:

1. From the Association Templates context menu, click **Instantiate by Group**. The Run File Plan Instantiation by Group page opens.

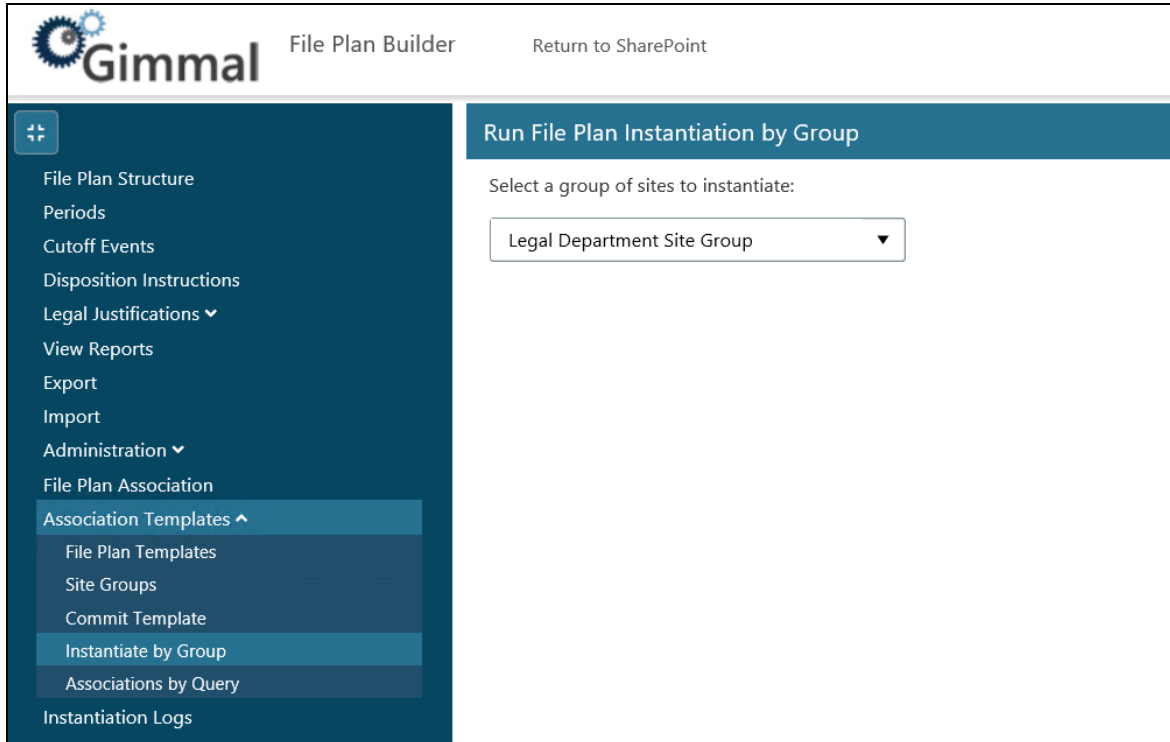


Figure 18-15 Instantiating by Group Dialog

2. Select the site group that you want to instantiate.
3. Click **Instantiate**.

The GimmelSoft Compliance Suite FPI Timer Job begins in the background. Navigate to **Central Administration**, and go to **Monitoring > Check Job Status** to see the status of the job.

## 18.7 Performing Associations by Query

The **Associations by Query** feature enables you to perform manual associations and instantiations similar to the File Plan Builder [File Plan Association](#) feature, with several notable exceptions:

- The Associations by Query feature specializes in performing robust searches across organizations with large SharePoint implementations. Gimmel recommends that you use this feature if you have numerous libraries that you want to perform associations and instantiations for.
- The list of sites that are returned from the search are not security trimmed.
- To initiate an association and instantiation using Associations by Query, you must enter a search term to search for a site that contains your Compliance Suite record libraries.

- File Plan Builder does not filter search results on Record Centers with Compliance Suite-installed-only Records Centers due to performance reasons. You can select a node and add it to a library. This library will come from a Records Center, but it may not be a Records Center with Compliance Suite. When you instantiate, the logs will say the following: *http://gsdemo/sites/ootbrc is not a Record Center or does not have Gimmel Compliance Suite installed.*

To use the Associations by Query feature, perform the following steps:

1. On the Association Templates interface, click **Associations by Query**. The Associations by Query page opens, displaying a search box on the left and all of the File Plan Builder nodes on the right.

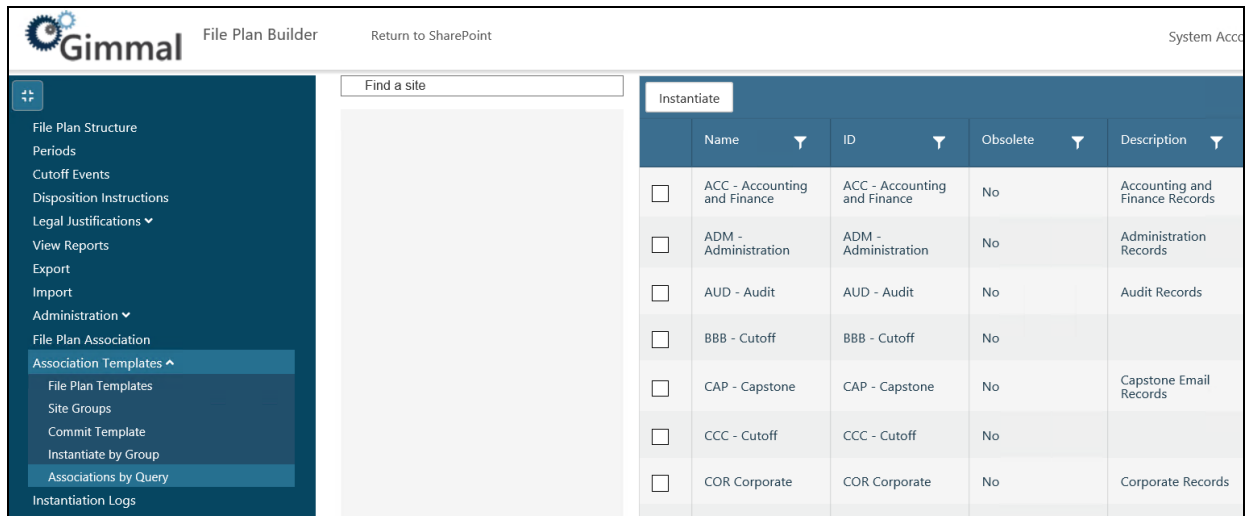


Figure 18-16 Associations by Query Page

2. In the **Find a Site** field, type a search term to search for a site(s) where you want to perform the association and instantiation. You can search against a site name, a site description, and a site URL. Your search results will display in a list under the search field.
3. In the search results list, click and expand a site to see the libraries that are already associated with the site. Click and expand a library to see the current instantiated root node folders in the panel on the right.

Instantiate				
	Name	ID	Obsolete	Description
<input type="checkbox"/>	ACC - Accounting and Finance	ACC - Accounting and Finance	No	Accounting and Finance Records
<input type="checkbox"/>	ADM - Administration	ADM - Administration	No	Administration Records
<input type="checkbox"/>	AUD - Audit	AUD - Audit	No	Audit Records
<input type="checkbox"/>	BBB - Cutoff	BBB - Cutoff	No	
<input type="checkbox"/>	CAP - Capstone	CAP - Capstone	No	Capstone Email Records
<input type="checkbox"/>	CCC - Cutoff	CCC - Cutoff	No	
<input type="checkbox"/>	COR Corporate	COR Corporate	No	Corporate Records
<input type="checkbox"/>	EHS - Environmental Health and Safety	EHS - Environmental Health and Safety	No	Environmental Health and Safety Records

Figure 18-17 Expanded Sites/Libraries List

---

#### Note:

If the **Obsolete** column in the node list is "Yes" for a specific node, this means you can't associate that node to any libraries; the node checkbox will be disabled. To remove a root node or to make a node obsolete, see the [File Plan Structure](#) tab of File Plan Builder.

---

- To associate a node(s) with a library, select a library from the search results list, and in the node list on the right, check the boxes for the root nodes you want to associate, and then click **Save Changes**. Repeat this step for **each** library that you want to associate a node(s) with.
- 

#### Note:

Gimmel recommends that you click **Save Changes** each time you select a library and associate a node, as you move down your libraries list. If you select a library and associate a node, and then select another library without clicking **Save Changes**, your initial selections will be cleared.

---

- When you are done associating your libraries and nodes, click **Instantiate**. After a moment, a message displays at the top of the page that says "Successfully started the Instantiation timer job", indicating that the process has begun.

---

Note:

If you associate libraries and nodes, and then you click the **Instantiate** button without clicking **Save Changes** first, a confirmation dialog displays, asking you if you want to save the association changes before instantiating. Click **OK** to save your changes and begin the instantiation process. Click **Cancel** to close the dialog and return to the libraries/nodes list page.

---

## 19 Instantiation Logs

Instantiation Logs show a filtered view of the Gimmel logs so that you can easily see if something went wrong in an instantiation. They also log start and finish times as two separate entries to show when instantiation finished and the elapsed time. With these logs, you do not have to search through the main Gimmel log and can quickly see instantiations.

The log displays messages that are specific to a particular instantiation. They are grouped by date, display start/finish, and any error messages that occurred with that instantiation.

**Intended User:** Compliance Suite Administrator

### 19.1 Viewing Instantiation Logs

After instantiating a file plan template, you can view the Instantiation Log to be sure the process completed with no serious errors.

To access the Instantiation Logs:

1. Open **File Plan Builder**.
2. Select **Instantiation Logs** from the vertical tabs.
3. Select the log for the instantiation you want to review.

Instantiation Logs							
Log Filtering							
Select the severity levels to show.							
Severity Level							
<input checked="" type="checkbox"/> Trace <input checked="" type="checkbox"/> Message <input checked="" type="checkbox"/> Warning <input checked="" type="checkbox"/> Exception <input checked="" type="checkbox"/> Critical Exception							
All <span>▼</span>							
Date	Category	Message	Severity	User	Location	Machine	
Date: 9/10/2018 1:41:02 PM							
9/10/2018 1:41:03 PM	GimmelSoft.ComplianceSuite.FilePlanBuilder.SharePoint	Template Association Finished. Total Time: 00:00:01.8528976	Trace			VM-Ch10_Pending_Legal_Ch...	
9/10/2018 1:41:02 PM	GimmelSoft.ComplianceSuite.FilePlanBuilder.SharePoint	Template Association Started	Trace			VM-NEO2	Details
Date: 9/10/2018 1:24:01 PM							
9/10/2018 1:24:07 PM	GimmelSoft.ComplianceSuite.FilePlanBuilder.SharePoint	File Plan Instantiation Finished. Total Time: 00:00:05.9495375	Trace			VM-NEO2	Details
9/10/2018 1:24:01 PM	GimmelSoft.ComplianceSuite.FilePlanBuilder.SharePoint	File Plan Instantiation Started	Trace			VM-NEO2	Details
Date: 9/10/2018 1:22:01 PM							
9/10/2018 1:22:02 PM	GimmelSoft.ComplianceSuite.FilePlanBuilder.SharePoint	Template Association Finished. Total Time: 00:00:01.2001218	Trace			VM-NEO2	Details
9/10/2018 1:22:01 PM	GimmelSoft.ComplianceSuite.FilePlanBuilder.SharePoint	Template Association Started	Trace			VM-NEO2	Details

Figure 19-1 Sample Instantiation Logs



---

Note

You can select a specific instance to look at by clicking the "All" drop-down list. This list contains all time stamps of instantiation jobs that have been run.

---

## 20 Troubleshooting

Use this section to troubleshoot issues with File Plan Builder.

### 20.1 Login Issues

If any user or AD group cannot access File Plan Builder even if they are members of the correct groups, be sure the name of the site collection where the groups exist is exactly the same name that Central Administration uses to point to File Plan Builder.

### 20.2 Access Denied Error

In certain environments, the configured File Plan Builder Administrator may experience a "401" (access denied) error when the Administrator has not been given access through the File Plan Builder security configuration. This issue requires manual configuration to correct.

Perform the following steps to address this issue:

1. Open File Plan Builder.
2. Click **Export** in the left navigation pane.
3. Make note of the 'Logon User' value in the error page that displays, as shown below.

**HTTP Error 401.0 - Unauthorized**  
You do not have permission to view this directory or page.

**Most likely causes:**

- The authenticated user does not have access to a resource needed to process the request.

**Things you can try:**

- Create a tracing rule to track failed requests for this HTTP status code. For more information about creating a tracing rule for failed requests, click [here](#).

**Detailed Error Information:**

<b>Module</b>	global.asax	<b>Requested URL</b>	http://dev.devdomain.gimmal.com:4545/Pages/Export.html?currentUser=YQD3ADsA3AApAHIA2gCnAEQAFwA%2BAPcA9gDbALUANAC%2FALKAJAAeAIEA7gAdICkA4gA1AOQAgQA6ANsAPgDNAA%3D%3D&culture=en&css=http%3a%2f%2fdev.devdomain.gimmal.com%3a333%2f/sites%2f/ga%2f_layouts%2f15%2fdefaultcss.ashx?_=635300821920000000
<b>Notification Handler</b>	AuthenticateRequest	<b>Physical Path</b>	C:\Program Files (x86)\Gimmal Compliance Suite\Installer\Pages\Export.html
<b>Handler</b>	StaticFile	<b>Logon Method</b>	Federation
<b>Error Code</b>	0x00000000	<b>Logon User</b>	0#.w devdomain\sharepoint

Figure 20-1 File Plan Builder 401 Error

4. In Windows Explorer, navigate to the install directory of the File Plan Builder Web Service. By default this location is C:\Program Files (x86)\Gimmal Compliance Suite\Installer on the Central Administration Web Front End.
5. Open web.config. Locate the <appSettings> section.
6. In the key="\_FilePlanBuilderAdmin" node, edit the value. Add a comma after the existing value, then the logon user value from step 3 above. In our example, the value will be changed from "DEVDOMAIN\sharepoint" to "DEVDOMAIN\sharepoint,0#.w|devdomain\sharepoint".

```

</system.webserver>
<system.serviceModel>
  <serviceHostingEnvironment aspNetCompatibilityEnabled="true" />
  <domainServices>
    <endpoints>
      <add name="soap" type="Microsoft.ServiceModel.DomainServices.Hosting.SoapXmlEndpointFactory, Microsoft.
    </endpoints>
  </domainServices>
  <services>
    <service name="GimmelSoft.ComplianceSuite.FilePlanBuilder.Web.FpbWebService" />
  </services>
</system.serviceModel>
<connectionStrings>
  <add connectionString="metadata=res://*/Models.FilePlanBuilder.csdl|res://*/Models.FilePlanBuilder.ssdl|res
</connectionStrings>
<appSettings>
  <add key="__FilePlanBuilderAdmin" value="DEVDOMAIN\sharepoint,0#.w|devdomain\sharepoint" />
  <add key="SharePointSiteUrl" value="http://dev.devdomain.gimmel.com:3333/sites/recordcenter" />
</appSettings>
</configuration>

```

Figure 20-2 Edit the FilePlanBuilderAdmin Node

7. Save the web.config.

---

### Important!

Gimmel recommends that you save a copy of the web.config file. If it is ever necessary to modify File Plan Builder Settings in Central Administration, the manually added Administrator value will be overwritten.

---

## Appendix A Chunking Files for Easier Import

File Plan Builder (FPB) Import functionality is available in a SharePoint Records Center with Gimmal Compliance Suite enabled. To use the Import File Plan features in *File Plan Builder*, Gimmal Compliance Suite must be installed and the *Gimmal Compliance Suite File Plan Builder* feature must be active.

If a file is too big to upload or will not process, then it must be broken up. A number of issues can affect the file size limitations that determine if a file is *too big*: IIS, .NET, and SharePoint all have their own configurable file size limits, and the size limit is defined by the smallest size allowed by any of the three. For example, if IIS allows a 1GB file, SharePoint allows a 2GB file, but .NET only allows a 2MB file, then you cannot upload a file larger than 2MB.

A recommendation is to try uploading a particular file, and if it consistently fails, then you might need to break the file up.

If you still have the option to export the original data, you can export it in multiple smaller files. Please see [Exporting Artifacts from File Plan Builder](#) for more information.

If you have a large file to import and no options to export the data in smaller files, you can chunk a large file into smaller files for easier import.

### A.1 Chunking Large Files for Easier Import

Since the File Plan Builder Import function is additive, you can safely divide a large file into smaller files that can be imported into File Plan Builder faster and more reliably than one large file.

---

#### Note:

You must have knowledge of .XML (eXtensible Markup Language) to perform this task.

---

#### A.1.1 Size of Files

You might need to go through some “trial and error” to find the ideal size of the .XML files to import into your system; each system is unique. The basic rule is that the smaller the file is, the faster the import will be and the less stress will be put upon the browser and system.

#### A.1.2 File Contents

All import .XML files have required elements. The File Plan Builder import function will not allow you to proceed with an import without all expected and required elements in each .XML file.

Here is a sample of the contents of an .XML file:

```

<filePlan version="2.0" language="en-US">
  <info username="i:0#.w|domain\user" exportDate="2017-01-01T00:00:00Z" siteCollection="Records Center" />
  <events />
  <filePlanNodes />
  <dispositionActions />
  <dispositionInstructions />
  <legalAuthorities />
  <legalJustifications />
  <periods />
  <permissionRoles />
  <securityGroups />
  <supplementalMarkings />
</filePlan>

```

Expand the appropriate elements with the actual data, depending on your specific file's contents. For example, the following .XML code shows how to import a root node and a child node. Notice that all other nodes (events, disposition actions, disposition instructions, etc.) are still here and populated.

```

<filePlan version="2.0" language="en-US">
  <info username="i:0#.w|domain\user" exportDate="2017-04-01T00:00:00Z" siteCollection="Records Center" />
  <filePlanNodes>
    <filePlanNode code="Node A" description="Legal" inheritCutoffFromParent="false" isCaseBasedRetention="false" isNara="false" isObsolete="false" isVitalRecord="false" specifiedId="Node A" inheritVitalRecordFromParent="false" inheritSecurityFromParent="false" inheritPermissions="false" inheritDispositionInstruction="false" inheritSupplementalMarkingFromParent="false" dispositionInstructionName="No Disposition" authorityName="TBD">
      <cutoffCriteria allEventsRequired="false" enableEvents="false" enablePeriods="false" enableRelationships="false" enableScripts="false">
        <cutoffEvents />
      </cutoffCriteria>
      <permissionRoleAssociations>
        <permissionRoleAssociation name="All-Read" />
        <permissionRoleAssociation name="Full Control" />
      </permissionRoleAssociations>
    </filePlanNode>
  </filePlanNodes>
</filePlan>

```

```

    <permissionRoleAssociation name="SystemAdmin" />
  </permissionRoleAssociations>
  <associations />
  <sharePointPermissions>
    <permission roleKey="Read" principalName="Local Security Team" displayName="
Local Security Team" />
  </sharePointPermissions>
  <supplementalMarkingAssociations />
  <children>
    <filePlanNode code="Node A-
A" description="Legal" inheritCutoffFromParent="false" isCaseBasedRetention="false"
isNara="false" isObsolete="false" isVitalRecord="false" specifiedId="Node A-
A" inheritVitalRecordFromParent="false" inheritSecurityFromParent="false" inheritPer
missions="false" inheritDispositionInstruction="false" inheritSupplementalMarkingFrom
Parent="false" parentContainerKey="Node A" dispositionInstructionName="Legal TAX+10"
authorityName="RRS">
      <cutoffCriteria allEventsRequired="false" enableEvents="false" enablePerio
ds="false" enableRelationships="false" enableScripts="false">
        <cutoffEvents />
      </cutoffCriteria>
      <permissionRoleAssociations>
        <permissionRoleAssociation name="All-Read" />
        <permissionRoleAssociation name="Full Control" />
        <permissionRoleAssociation name="SystemAdmin" />
      </permissionRoleAssociations>
      <associations />
      <sharePointPermissions>
        <permission roleKey="Contribute" principalName="Corporate Security Team"
displayName="Corporate Security Team" />
      </sharePointPermissions>
      <supplementalMarkingAssociations />
      <children />
    </filePlanNode>
  </children>

```

```

    </filePlanNode>
  </filePlanNodes>
  <dispositionActions>
    <dispositionAction name="Legal Disposition" description="Disposition workflow for all Legal records" parameter="&lt;action type='workflow' id='c97658a5-d635-4fb1-8896-3d73d7f19305'" />
  </dispositionActions>
  <dispositionInstructions>
    <dispositionInstruction name="Legal TAX+10" description="Legal Disposition" agingMethod="Alternate">
      <phases>
        <dispositionPhase stageActivation="Calendar" name="Dispose" description="Legal Disposition" dispositionActionName="Legal Disposition" duration="10" durationUnit="Years" sequence="0">
          <calendarAging columnName="Tax Year" createAsListColumn="true" defaultDateType="None" />
        </dispositionPhase>
      </phases>
    </dispositionInstruction>
    <dispositionInstruction name="No Disposition" description="No disposition performed due to no records stored at this level" agingMethod="Cutoff">
      <phases />
    </dispositionInstruction>
  </dispositionInstructions>
  <events />
  <legalAuthorities>
    <legalAuthority authorityCode="RRS" description="Record Retention Schedule">
      <justifications>
        <legalJustification legalCode="RRS" />
      </justifications>
    </legalAuthority>
    <legalAuthority authorityCode="TBD" description="TBD">
      <justifications />
    </legalAuthority>
  </legalAuthorities>

```

```

    </legalAuthority>
</legalAuthorities>
<legalJustifications>
    <legalJustification legalCode="RRS" citation="RRS" status="Active" />
</legalJustifications>
<periods>
    <period name="Daily Cutoff Processing" startDate="2015-03-
24T00:00:00" duration="FREQ=DAILY;INTERVAL=1" />
</periods>
<permissionRoles>
    <permissionRole name="All-Read" />
    <permissionRole name="Full Control" />
    <permissionRole name="SystemAdmin" />
</permissionRoles>
<securityGroups>
    <securityGroup name="File Plan Builder Users" type="SharePoint Group">
        <permissionRoleAssociations>
            <permissionRoleAssociation name="Full Control" />
            <permissionRoleAssociation name="SystemAdmin" />
        </permissionRoleAssociations>
    </securityGroup>
    <securityGroup name="RMA Records Managers" type="SharePoint Group">
        <permissionRoleAssociations>
            <permissionRoleAssociation name="SystemAdmin" />
            <permissionRoleAssociation name="Full Control" />
        </permissionRoleAssociations>
    </securityGroup>
</securityGroups>
<supplementalMarkings />
</filePlan>

```



27 March 2019

After you have completed breaking a large file into smaller chunks, you can follow the procedures in [Importing Artifacts](#) to import the small files.