Gimmal

Information Management for Everyone®

Administration Guide

Classified Records

(Feature-Activated)

For SharePoint 2013/2016

Software Version 4.13.1

January 2019

Title: Gimmal Classified Records Admin Guide

If you have questions or comments about this publication, you can email TechnicalPublications@Gimmal.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

Preface

Gimmal delivers market leading content governance and compliant records solutions built on Microsoft® SharePoint®. Gimmal 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.

Gimmal's Compliance Suite combines with SharePoint to give your organization a reliable and centralized repository for collaboration and records management that is compliant with the standards of the Department of Defense (DoD) 5015.2 Records Management Program.

The Classified Records product is a separate, optional solution you install and use with Gimmal Compliance Suite (Cs). Organizations wanting to use this functionality must first install and configure Gimmal Compliance Suite.

Classified records extend the Compliance Suite's RMA Record and all functionality present in the latter is available for Classified Records. Classified Records has extended security controls that can be graded by an authorized user manually or automated by the system.

Gimmal developed Classified Records in accordance with the DoD 5015.2 Chapter 3 - Management of Classified Records and it is certified to this standard http://jitc.fhu.disa.mil/projects/rma/reg.aspx).

Who Should Use This Guide

This guide is intended for beginning and advanced users of the Compliance Suite software. All users must have a basic knowledge of SharePoint 2013/2016 functionality. This manual contains step-by-step instructions for administrating Classified Records as part of Compliance Suite.

Important Notes About Compliance Suite and This Manual

All illustrations are for example purposes and vary depending on how you configure the system during installation.

Introduction

The Gimmal Classified Records application provides enhancements to Gimmal Compliance Suite that enable the management of classified records. These records are compliant with the Department of Defense (DoD) 5015.2 Standard.

The DoD supports both Classified and Standard Baseline Records. In Gimmal Compliance Suite, all records are Standard Baseline Records, while the Gimmal Classified Records product allows for the creation of Classified Records where Compliance Suite manages both record types.

Some of the Gimmal Classified Records' product features include the addition of specific security level functionality and Supplemental Markings as part of the baseline tests.

When creating a Classified Record, a mandatory security classification is required. Your records administrator will create the available security classifications. They are a special type of supplemental marking. Each security classification has a name and a rank value. Security classifications with higher rank values are automatically included into those with lower values. The records administrator will give users and/or groups access to a specific security classification. Classified Records will not grant any access to the item if the users are not part of a security classification applied to a classified record or have access to a lower security classification. The records administrator can give Security Classifications a name and a ranking value to suit an organization's needs. For example, this guide uses "Top Secret", "Secret", "Confidential" and "Unclassified" with ranking values of 3, 2, 1, and 0.

Users that are assigned to a Security Classification of Confidential (rank =1), for example, only have access to classified records whose rank value is equal or lower (Confidential and Unclassified). When creating a classified record, the available security classifications to which the user is a member are displayed in a list when selecting the Initial Classification (an informative label) and the Current Classification (the security classification applied to the classified record). In the previous example, John Smith, who is assigned a security classification of Confidential, will not be allowed to create or interact with any Classified Records that are higher than his level (Secret and Top Secret).

A Security Classification with a higher numeric value is automatically included into the ones with lower ranked numeric values. Users in the "Top Secret" ranking automatically have access to rankings of 2, 1, and 0. Users that are assigned to a Security Classification of Confidential (rank =1) only have access to Classified records whose rank value is equal or lower (Confidential and Unclassified).

The security classifications work in conjunction with supplemental markings and users must belong to the appropriate supplemental markings in addition to having the appropriate security ranking to access a classified record. For example, a user with Top Secret access is not given access to a classified record with supplemental markings assigned to it if this user is not part of all of the supplemental markings.

Setting Up Options

You can set up options in Classified Records, such as managing timeframes, selecting audited columns, and trimming audit logs.

Managing Timeframes Setup

The Timeframes values set the default values for both Default Declassification and the deletion of Working Papers. To change the Timeframe default values, you must have RMA Administrator permissions.

The default values for Timeframes are as follows:

1. *Default Declassification Timeframe* – The default value for this function is 25 years. This value is the basis for the *Declassify On date* property that is used to declare the item as a Classified Record. Declassification occurs as follows by default: Publication Date (this is mandatory and defaults to the current day but can changed – present, past or future) + Default Declassification Timeframe = Declassification date. If you create a record and set the publication date to 1/1/2000 and the default classification is 25 years, then the record is declassified on 1/1/2025. When a classified record is declassified either manually or by the timer job when scheduled, its security classification is lowered to the entry occupying Rank 0 (see Chapter 3) and it can be transferred and purged from the classified system.

2. *Working Papers Deletion Timeframe* – The default value is 180 days and can be changed. If a Working Paper is not made into a classified record before this timeframe, it is deleted.

To change the Timeframe default values, you must have RMA Administrator permissions. Use the following procedure to edit timeframes:

1. Click **Site Actions** -> **Site Settings** -> **Classified Records** -> **Manage Timeframes**.

Figure 1 Manage Timeframes Selection

The Manage Timeframes page displays.

Figure 2 Manage Timeframes

2 Click inside the timeframe fields and enter the desired numbers.

Note

For working papers, Classified Records uses the built-in Expiration policy timer job. If you set the **Working Papers Deletion Timeframe** to a short duration, be sure that the Expiration Timer job is also accordingly set. If you want to apply these timeframes to existing records, click the checkbox next to **Apply declassification timeframe to existing records**.

3 Click **Save**.

Setting Audited Columns

The Classified Records functionality allows you finite control for auditing specific columns. Columns can easily be audited or unaudited by selecting an action button. All audits can be added/removed by a single action.

Note
You do not need to set SharePoint standard auditing events because they will always occur.

Follow these steps enable or disable audited columns:

1 To access the Audited Columns page, select **Site Actions** -> **Site Settings** -> **Classified Records** -> **Audited Columns.**

Figure 3 Audited Columns Selection

The Audited Columns page displays.

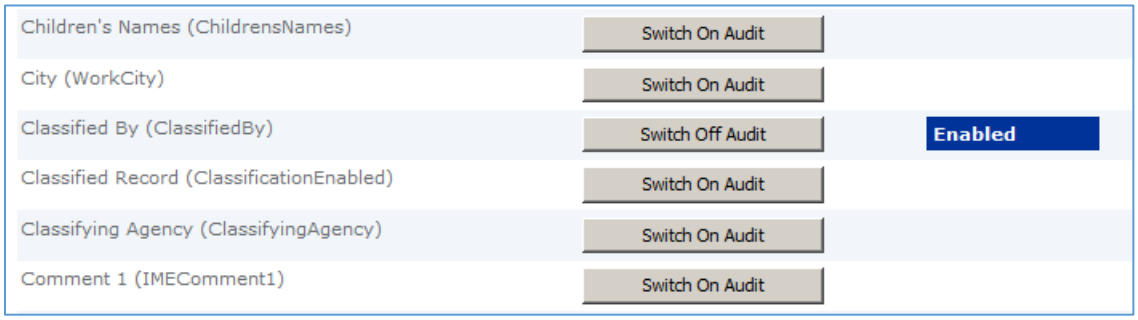


Figure 4 Audited Columns Page

2 Select **Switch On Audit** or **Switch Off Audit** for the desired columns. If you switch on audit, **Enabled** displays next to the column under **Auditing Status**.

Note
You can also select **Audit All** or **Audit None** at the bottom of the page to set audit status for all columns.

You can display audit events by running a custom audit report from **Site Actions** -> **Site Settings** -> **Audit logs reports** under the **Site Collection Administration** section. Under the **Events** section of the report, select **Custom events** to display the events that are part of classified records.

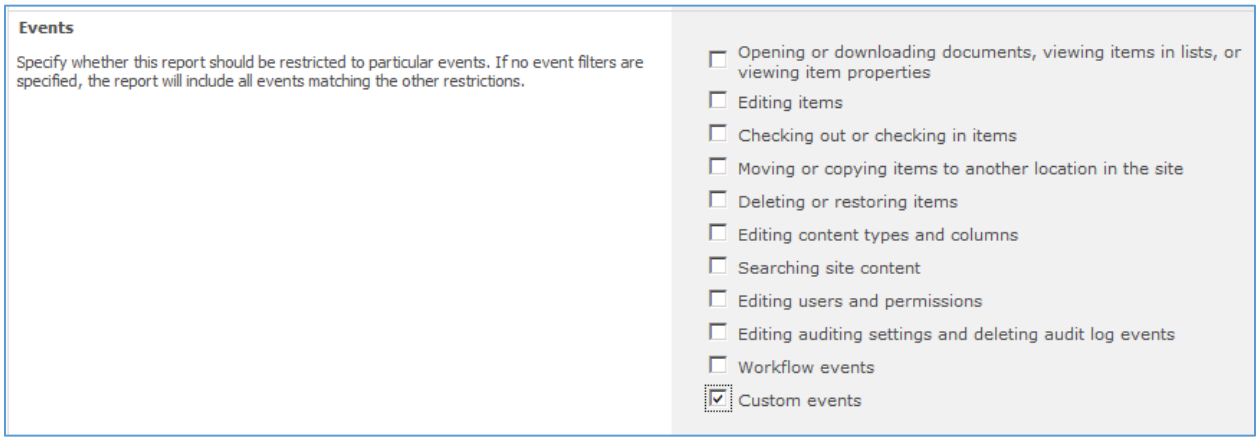


Figure 5 Auditing Events

In the previous example, the **Classified By** column was activated and the resulting report lists the results after creating a Classified Record displaying the before and after values for this column.

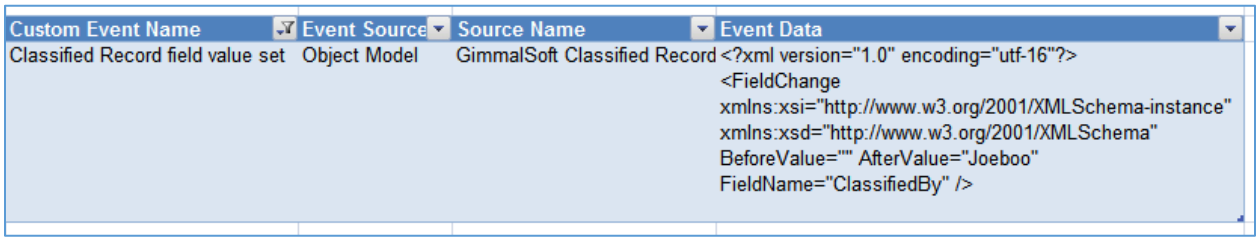


Figure 6 Classified By Before and After Values

Trimming the Audit Log

When you install Classified Records, the Site Collection Audit Settings are modified to automatically trim the audit log and the data is retained for a maximum of 99999 days.

The Trim Audit Log functionality is an alternate way to delete audit entries up to a given date. It allows flexibility so that organizations, if required, can make sure the audit log reports are generated and preserved beforehand. Highly regulated organizations may file the audits reports as permanent records into the system and then trim the audit logs.

Follow these steps to trim the audit log:

3 To access the Trim Audit Log page, select **Site Actions** -> **Site Settings** -> **Classified Records** -> **Trim Audit Log**.

Figure 7 Trim Audit Log Selection

The Trim Audit Logs page displays.

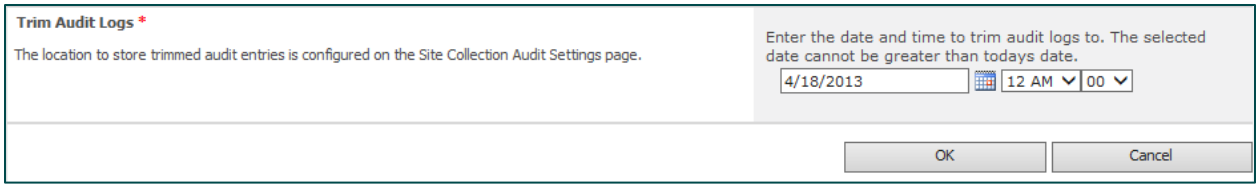


Figure 8 Trim Audit Logs page

4 Enter the date and time to trim audit logs.

5 Click **OK**. Audit entries in SharePoint are deleted up to the date and time that you entered.

Creating the Working Papers Library

Working papers provide a separate non-record area for work in progress on classified information. These are not records, but they contain classified security information. They can optionally be converted into a classified record. They can be considered a precursor to a document that someone is offering that contains classified information. Working papers are retained for a set period of time.

Working papers contain some specific metadata. Documents do not have to be a working paper in order to become a classified record.

Working papers have supplemental markings, which are document markings not necessarily related to classification markings. These markings elaborate on or clarify document handling.

When working records are declared as classified records, the previous values for supplemental markings and security level are stripped.

You must select a document library to use for working papers or create a new document library.

Note
Working Paper content is excluded from Gimmal Access Control functionality.

Creating Working Papers Library

Follow these steps to create the working papers library:

1 In the SharePoint ribbon menu, select **Library Settings**.

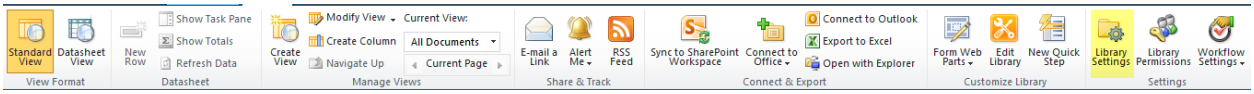


Figure 9 Selecting Library Settings

2 Under **General Settings**, select **Advanced Settings**. The Advanced Settings page displays.

Figure 10 Advanced Settings

3 Ensure Allow management of content types next to Content Types is set to **Yes** and click **OK**.

4 Under **Library Settings** -> **Content Types**, click **Add** from existing site content types. The Select Content Types page displays.

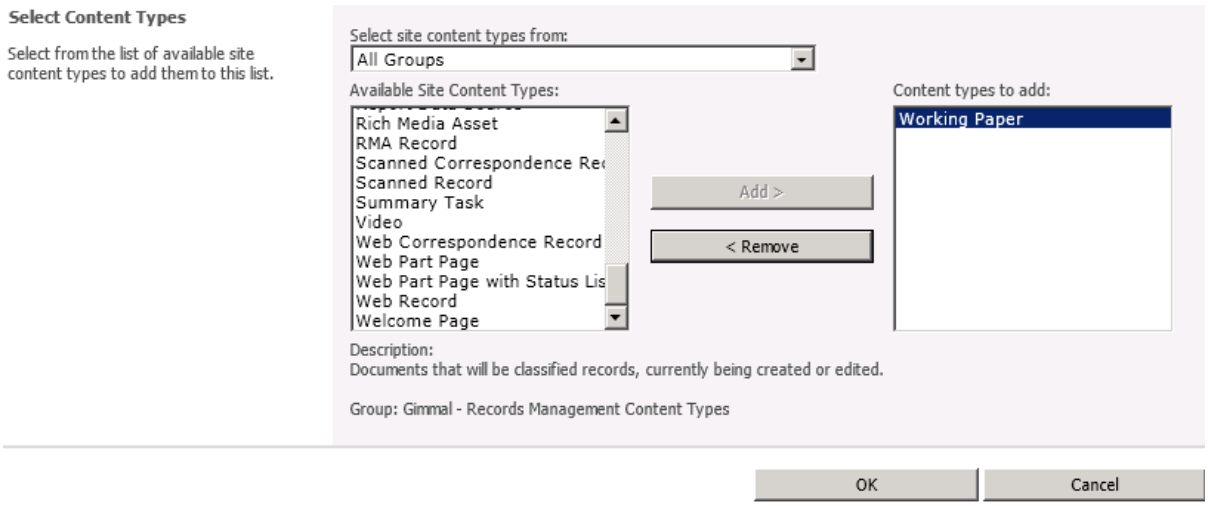


Figure 11 Select Content Types Page

5 Select Working Paper in **Available Site Content Type** and click **Add**.

6 Click **OK**.

Note
You may want to remove the Document content type or set Working Papers as the default content type. In **Library Settings**, click **Change new button order and default content type**. Uncheck **Document** from the list, and/or change the Working Paper **Position from Top** to **1**.

Security Classifications

When declaring a Classified Record or creating a Working Paper, there are two mandatory fields for which end-users must select specific values to determine the Initial and Current Classification state of the record or Working Paper. These values are defined by creating a specific type of Security Classification and enabling these with Access Rules.

Once applied, Security Classifications behave similarly to Access Rules of the Supplemental Markings type with the following exception: A supplemental marking applied to a Record is not hierarchical and access to the record is determined solely by the list of authorized users defined for its Access rule. Security Classifications represent a hierarchy of access where each marking has a specific rank value associated to it and this value is used to automatically grant access to Security Classifications that have a lower rank value. All members of a security classification must also be members of the Site Collection Members group.

Figure 12 shows a representative example of security classifications. Four Security Classifications are created in this example: Top Secret, Secret, Confidential and Unclassified with rank values of 3, 2, 1 and 0. The rank values and the names are created in the following section called Security Classification. The authorized users are associated to the Security Classifications in a second step in the section called Adding Access Rules for Security Classification Entries.

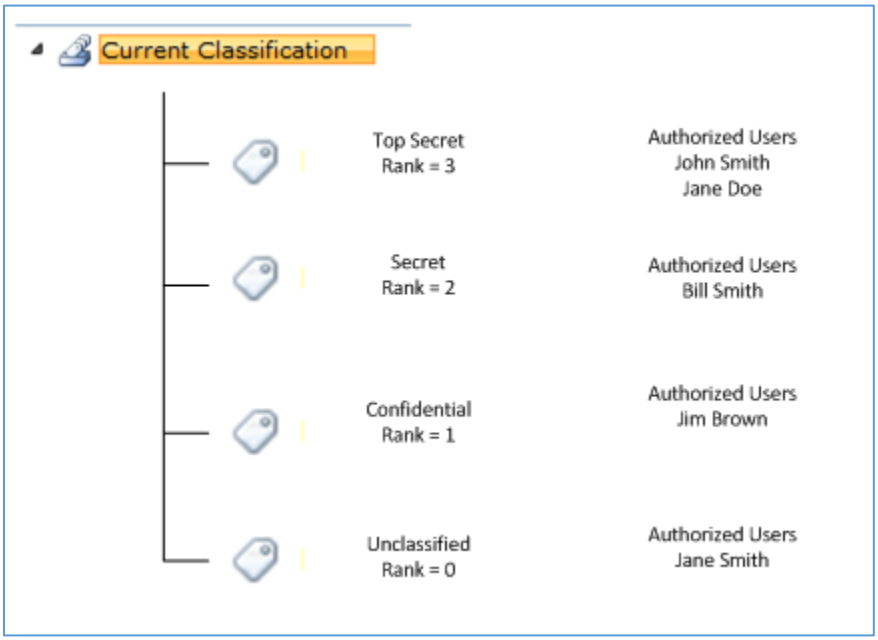


Figure 12 Sample Security Classifications

As a result, John Smith has access to all Classified Records in the system because he is associated to the Security Classification with the highest rank. Bill Smith only has access to Security Classifications in the system whose current classification is of rank 2 and lower, meaning that he has access to Records (or Working Papers) with a Current Classification of Secret, Confidential, and Unclassified.

Bill Smith does not have access to Records that are Top Secret, as the rank value is above his current access.

Creating Security Classifications

The security classifications define the security hierarchy that is imposed on classified records and is also used for working papers. When these security classifications are created, they are automatically added as term store values under the **Site Column** called **Current Classification**.

Creating Security Classifications as an RMA Administrator

Follow these steps to create a Security Classification as an RMA Administrator:

1 From **Site Actions** -> **Site Settings**, select **Security Classifications** under the Classified Records group.

2 Click **Add new item** and enter a **Name** in the Security Classification window.

Note
This name is visible to end-users that have access to this security level and is added as a Term Store entry under the Term Store Set called Current Classification as part of the managed Metadata Service.

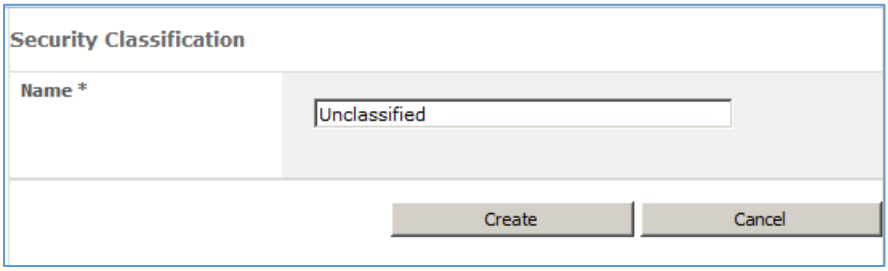


Figure 13 Security Classification Window

The first security classification is assigned a rank value of 0. This represents the lowest security level and is always the value to which declassified records are set. Once the lowest ranked value is set, it cannot be changed.

3 Click **Create** to add the entry to the list.

4 Add successive Security Classifications with increasing rank numbers (higher security) by clicking on the **Add new item** link. A typical example is the following:

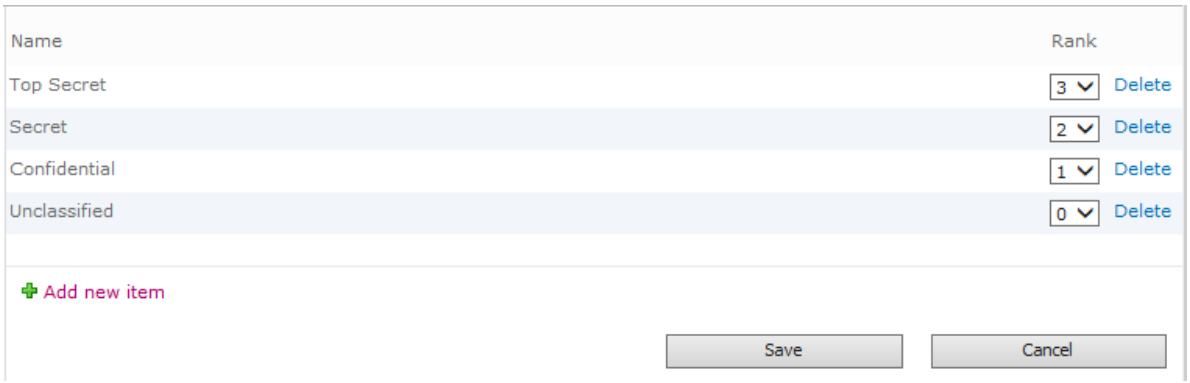


Figure 14 Sample Security Classifications

Note

As long as the list is not saved, you can change the rankings of any item in the list by selecting one of them and clicking their drop-down arrow and selecting a different rank number.

5 Click **Save** to commit the changes and to add the Security Classifications to the Term Store. You are asked to confirm your selection:

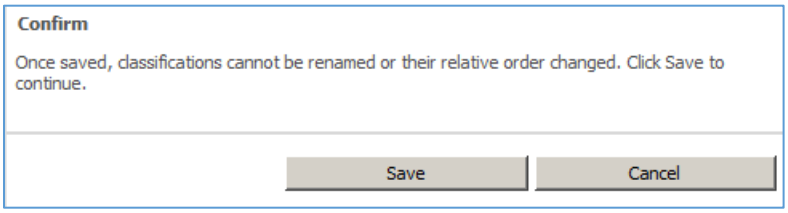


Figure 15 Confirming Security Classifications

Note

Once the list is created and saved, classifications cannot be renamed and their relative order cannot be changed.

Adding a New Security Classification Entry

Once the list of Security Classifications has been established, new levels can be added and inserted in the ranking list.

Follow these steps to create a new security classification entry:

1 From **Site Actions** -> **Site Settings**, select **Security Classifications** under the Classified Records group.

2 Click **Add new item** and enter a **Name** in the Security Classification window that you would like to add. By default, the item is added with the highest ranking at the top of the list.

3 Use the dropdown to adjust rank. The rankings for previous entries are adjusted accordingly.

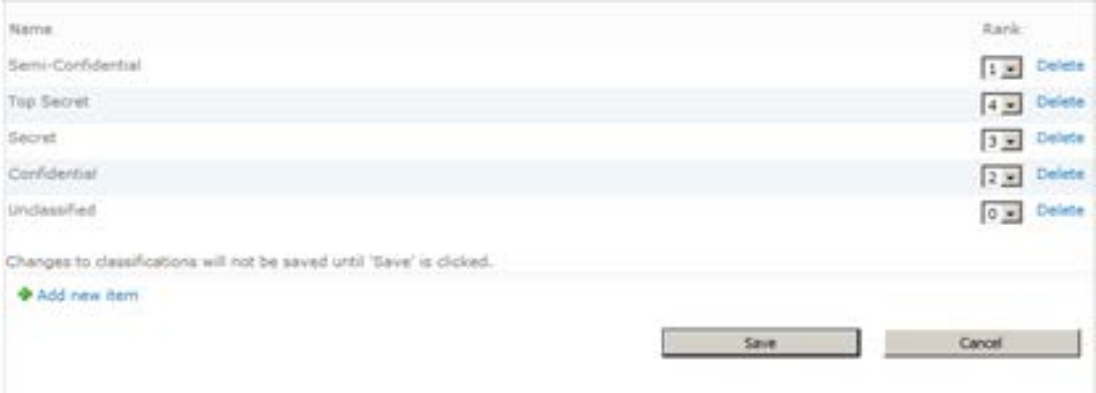


Figure 16 Changing Security Classification Rankings

4 Click **Save** to commit the newly created entry to the list or **Cancel** to revert any changes.

Adding Access Rules for Security Classification Entries

Once the Security Classifications are created and their rank order established, an access rule is required to associate the users and/or groups that will be given access to the entry. Users or Groups that are given access to Security Classifications with a specific rank value will always have access to Security Classifications equal to the rank value and lower. An access rule must be created for each Security Classification.

To create and associate a Security Classification to a group of users, an access rule is created.

1 From the Access Rules list (**Site Actions -> View All Site Content**), there are two ways to initiate the access rule creation process:

2 Click **+Add new item** from the bottom of the list.

3 Select **List Tools -> Items** tab in the Header Ribbon, then select **New Item** -> **Access Rules.**

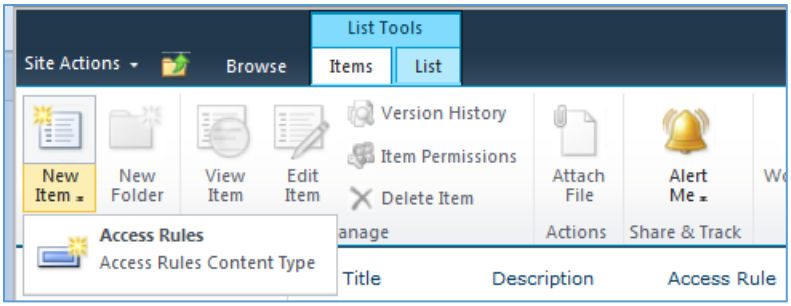


Figure 17 Selecting Access Rules

An **Access Rules - New Item** dialog box opens with fields for creating a new Access Rule.

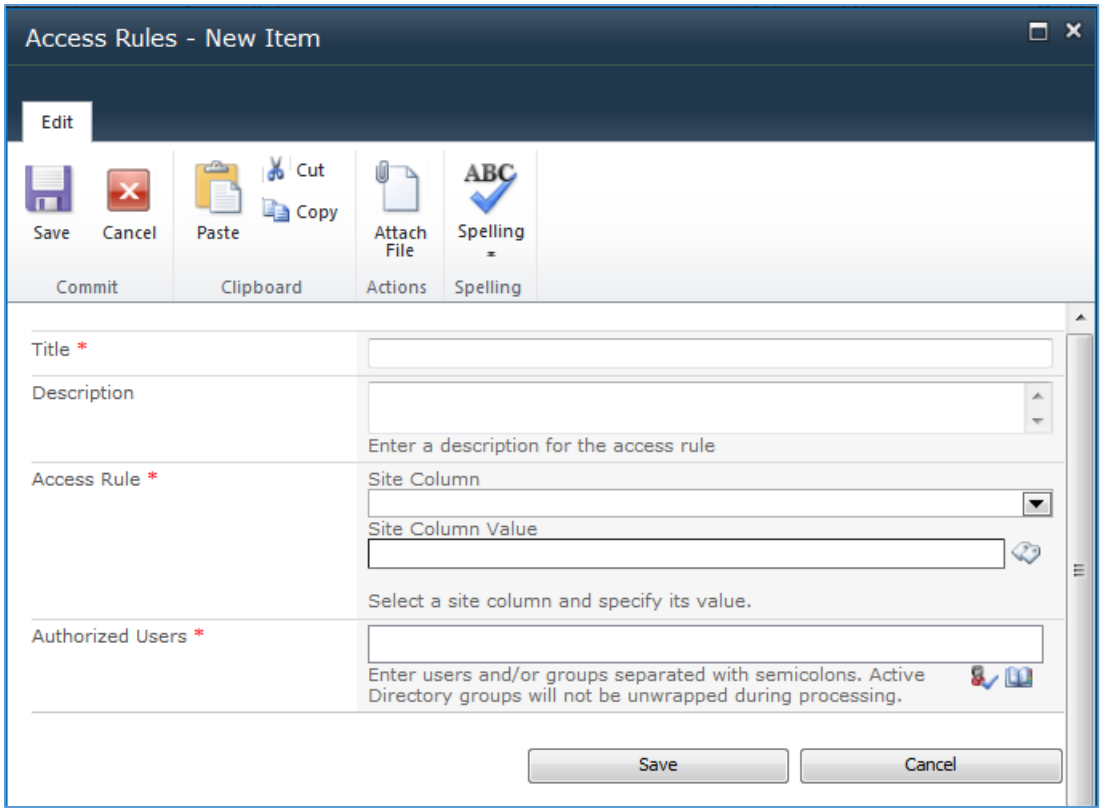


Figure 18 Access Rules Dialog Box

4 In **Title**, enter a descriptive identifier for the new Access Rule. (Required)

5 Enter a descriptive statement that defines the purpose of this Access Rule in **Description**.

6 Select **Access Rule: Site Column**. **Site Column** defines the SharePoint site column used to restrict records access based on this Access Rule. The selection list is populated with all SharePoint site columns that are of the type Supplemental Marking or Current Classification.

7 Select the Current Classification as the Site Column. (Required)

8 Select the **Access Rule: Site Column Value** from the displayed list. Click **Select ->->** to add the term and then click **OK**. The selected term is set in the **Access Rule: Site Column Value** field.

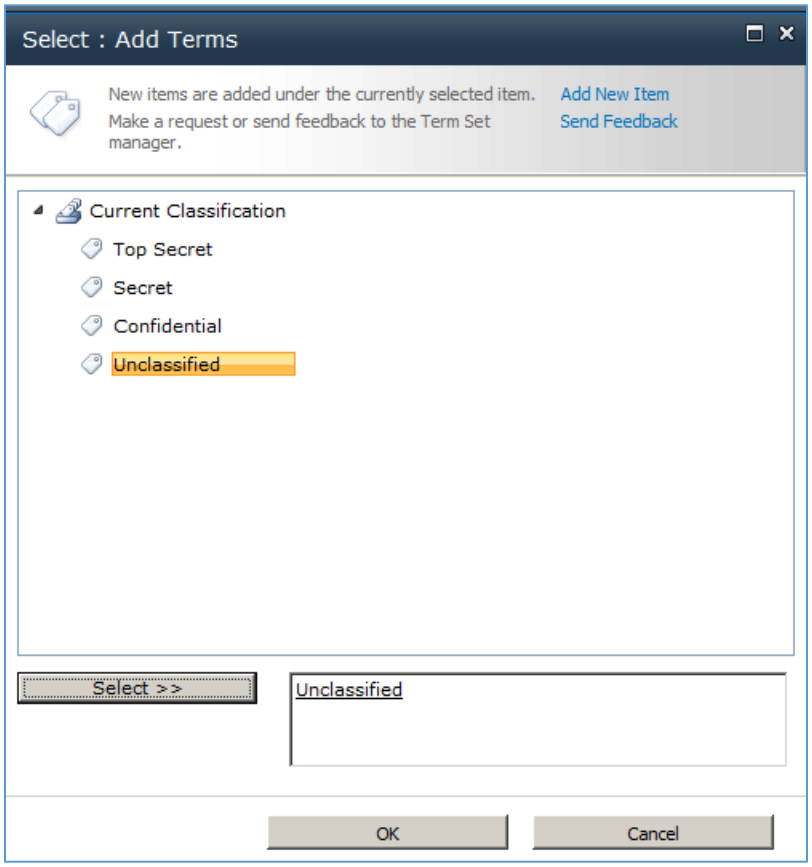


Figure 19 Add Terms

The site column value must be unique across all Access Rules of all types (Supplemental Markings and Current Classification). This value defines the Managed Metadata term that restricts Classified Records access for the selected Access Rule: Site Column. (Required)

Note

If the selection list is blank or an entry that you expect is not present, then the previous section (Creating Security Classifications) must be performed first. That section ensures that the Security Classifications are properly created as terms under the appropriate term set. These terms are not to be created from the term store itself or from the Select: Add Terms window (Add New item), as this will not create the term entries appropriately.

9 Enter the **Authorized Users** by using a semicolon separated list or standard SharePoint address book lookup. The Authorized Users identify users that have access to view Classified

Records and Working Papers that have metadata content equal to or less than the Access Rule: Site Column and Access Rule: Site Column Value combination as described previously. (Required)

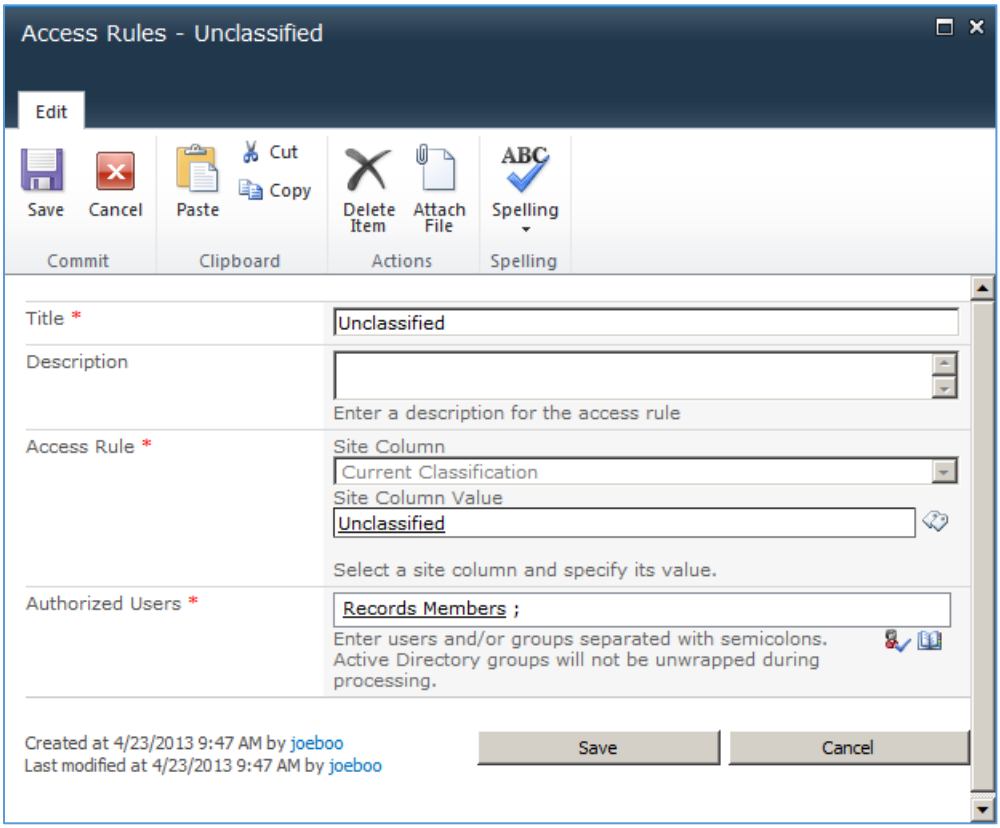


Figure 20 Entering Authorized Users

10 Click **Save**. The new Access Rule is created and appears in the Access Rules View list. Click **Cancel** to return to the Access Rules View list without creating a new Access Rule.

Note
You must ensure that an access rule is not in use prior to deleting it.

Title	Description	Access Rule	Authorized Users
Unclassified	Unclassified Security Classification	Current Classification=Unclassified	Records Members
Top Secret	Top Secret Security Classification	Current Classification=Top Secret	RMA Administrators
Secret	Secret Security Classification	Current Classification=Secret	Jane Doe
Confidential	Confidential Security Classification	Current Classification=Confidential	John Smith

Figure 21 Access Rules for Current Classification

Field Level Access

These settings apply to all classified records with the exception of Working Papers.

Configuring Column Access Control

The fields shown in Figure 22 are automatically added to the GimmalSoft Column Access control content classification at the root web. The RMA Security Officers Group is added as a metadata Editor and can add other groups or users as your organization needs. Once a Classified Record is saved in the system, only members of this group can edit these fields.

Edit	Field Name	Metadata Editors	Metadata Security List Exceptions
	CurrentClassification	RMA Security Officers	Drop Off Library
	DeclassifyOnTrigger	RMA Security Officers	Drop Off Library
	DeclassifyOnDate	RMA Security Officers	Drop Off Library
	DeclassifyOnEvent	RMA Security Officers	Drop Off Library
	DeclassifyOnExemptionCategory	RMA Security Officers	Drop Off Library
	DowngradeOnTrigger	RMA Security Officers	Drop Off Library
	DowngradeOnDate	RMA Security Officers	Drop Off Library
	DowngradeOnEvent	RMA Security Officers	Drop Off Library
	DowngradeInstructions	RMA Security Officers	Drop Off Library
	ReasonsForUpgrade	RMA Security Officers	Drop Off Library
	ReasonsForClassification	RMA Security Officers	Drop Off Library
	TargetDowngradeClassification	RMA Security Officers	Drop Off Library
	ReviewedOn	RMA Security Officers	Drop Off Library
	ReviewedBy	RMA Security Officers	Drop Off Library
	ClassificationEnabled	RMA Security Officers	Drop Off Library
	ClassifyingAgency	RMA Security Officers	Drop Off Library
	DerivedFromType	RMA Security Officers	Drop Off Library
	DerivedFromSources	RMA Security Officers	Drop Off Library

Figure 22 Field Level Access

Follow these steps to manually configure additional field level access, if required by your organization. The existing entries can also be edited if necessary.

1 Click **Lists** and select GimmalSoft Column Access Control. The New Item window displays.

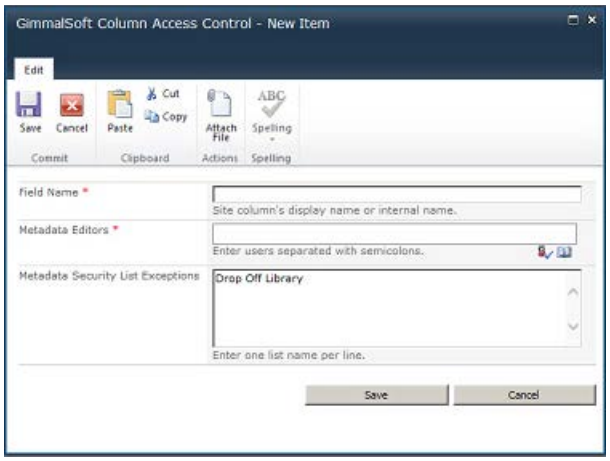


Figure 23 New Column Access Control Item

2 Add the desired **Field Name** (exactly as displayed in Figure 22), the allowed Metadata Editors, and the Metadata Security List Exceptions.

3 Click **Save**.

4 Repeat steps 2 and 3 for each desired field. These fields are applied to the record properties in this library.

Configuring Field Level Access at the Site Level

Field level access is automatically configured at the root level upon installation, but you must configure it at the site level. Once you manually configure field level access at the site level, it is shared between sites.

Follow these steps to manually configure field level access at the site level:

1 Click **Libraries** on the left navigation pane. The Document Libraries display.

2 Click **Create** at the top of the page. The types of libraries display.

3 Select the type of library you want to create and click **More Options** in the right navigation pane. The Create form displays.

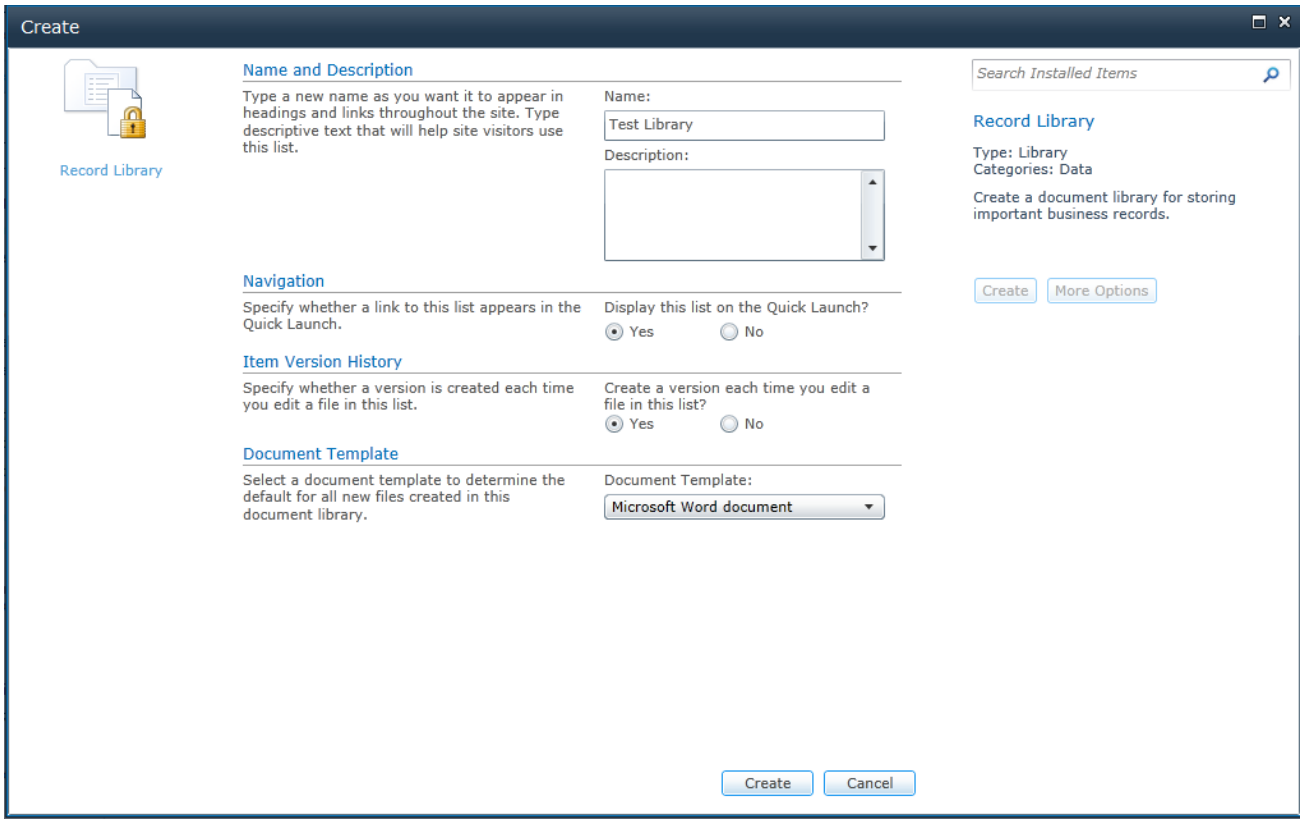


Figure 24 Creating a Library

4 Enter the **Name** and **Description** and select if you want this library to display in Quick Launch, if you want versioning, and the template you want to use.

5 Click **Create**. The blank library displays.

6 Click **Lists** and select GimmalSoft Column Access Control. The New Item window displays.

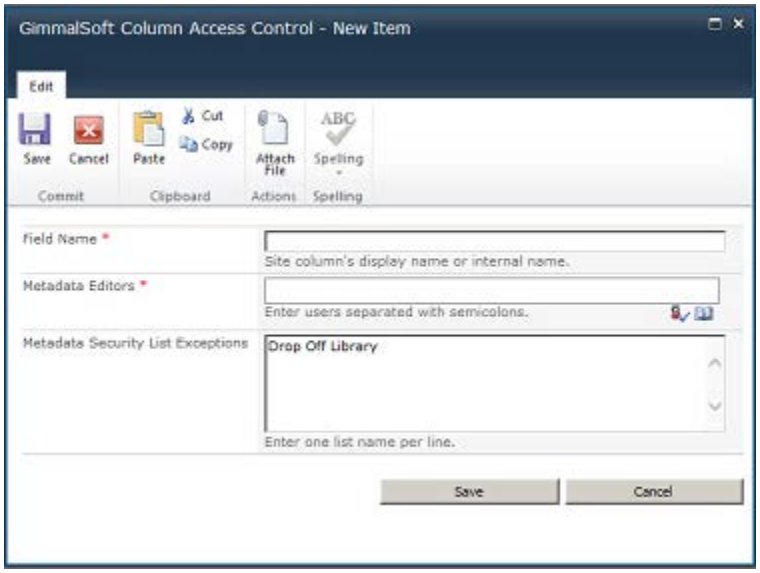


Figure 25 New Column Access Control Item

7 Add the desired **Field Name**, the allowed **Metadata Editors**, and the **Metadata Security List Exceptions**.

8 Click **Save**.

9 Repeat step 7 and 8 for each desired field.

10 These fields are applied to the record properties in this library.

Classification Guides

Note
Users should see the entire classification guide, but can only select the topics that correspond to their assigned Security Classification.

Creating, Editing, and Deleting Classification Guides

To access the Classification Guides page to create, edit, or delete entries, select **Site Actions** -> **Site Settings** -> **Classified Records** -> **Classification Guides**. You can also access the page by selecting **Classification Guides** under the Classified Records Quick Launch region.

Figure 26 Classification Guides Selection

Creating Classification Guides

Once you identify a classification guide, you must create it in Classified Records.

Follow these steps to create a classification guide:

1 Log into Classified Records and select **Classification Guides**. The Classification Guides page displays.

2 Click **Add new Classification Guide**. The New Classification Guides page displays.

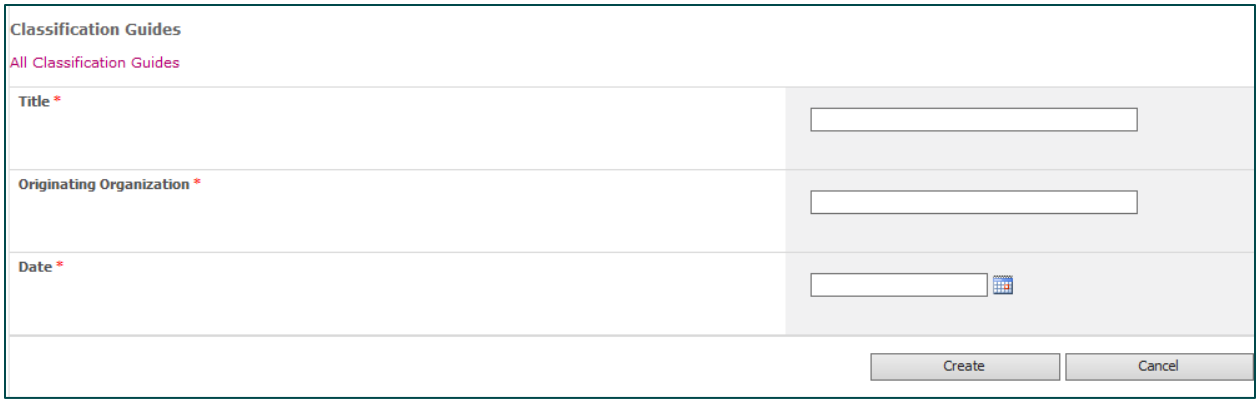


Figure 27 New Classification Guides Page

3 Enter the **Title**, **Originating Organization** from where the guide came, and the **Date** the guide was published.

4 Click **Create**. The Classification Guides page displays the guide you just created.

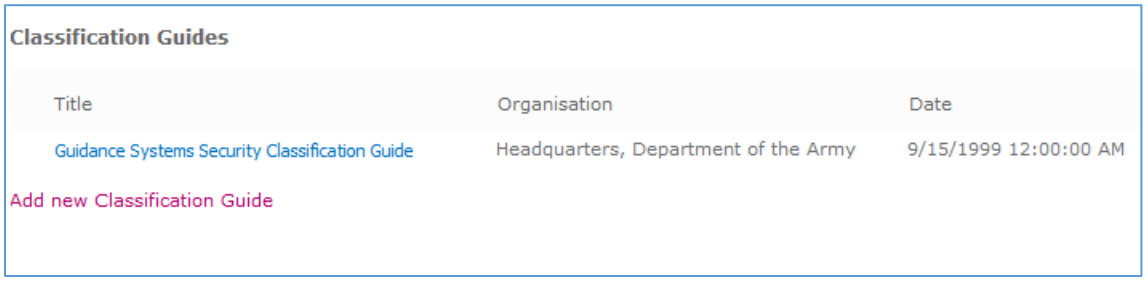


Figure 28 Created Classification Guide

Editing Classification Guides

You can edit the Title, Originating Organization, or Date for a Classification Guide currently in Classified Records.

Follow these steps to update a classification guide:

1 Log into Classified Records and select **Classification Guides**. The Classification Guides page displays.

2 Select **Edit** from the dropdown menu next to the entry that you want to update.

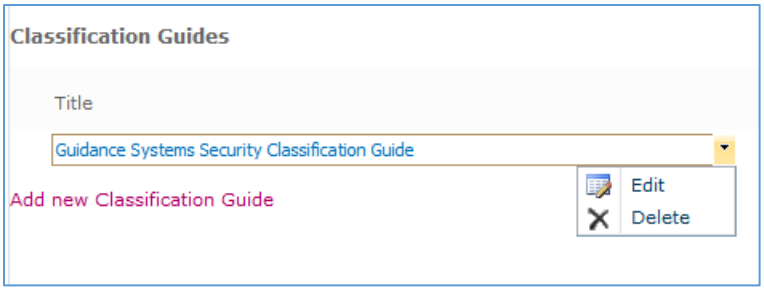


Figure 29 Editing a Classification Guide

The Classification Guides page displays with the selected guide's information.

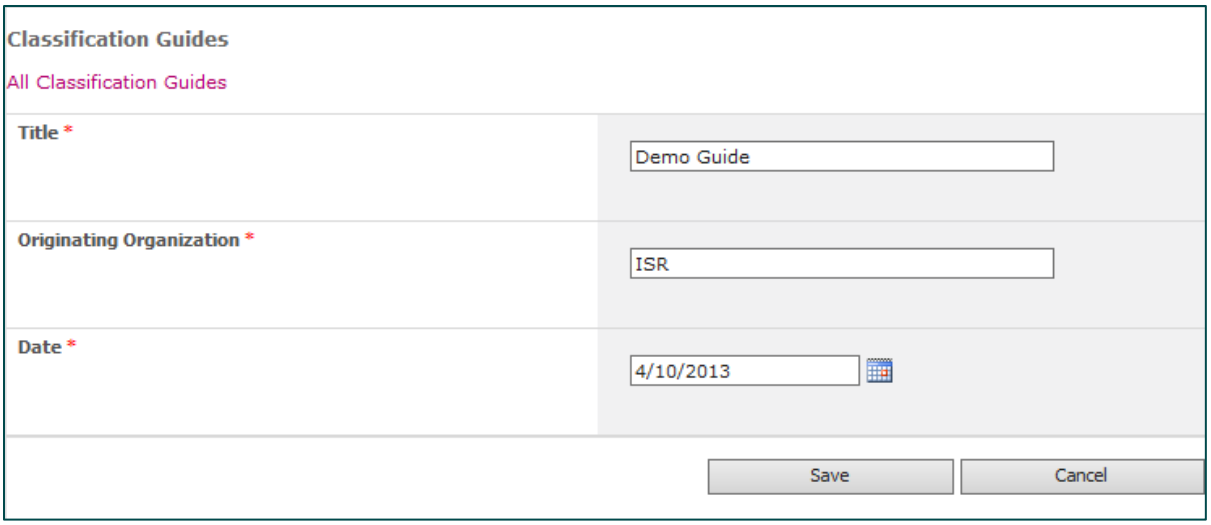


Figure 30 Editing a Classification Guide

3 Enter a new Title, Originating Organization, or Date.

4 Click **Save**. The Classification Guides page displays the updated guide information.

Deleting Classification Guides

You can delete a classification guide at any time.

Follow these steps to delete a classified guide:

1 Log into Classified Records and select **Classification Guides**. The Classification Guides page displays.

2 Next to the guide entry that you want to delete, select **Delete** from the dropdown menu.

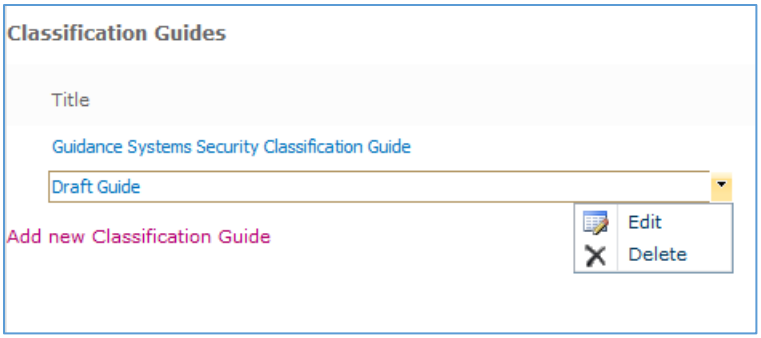


Figure 31 Deleting a Classification Guide

A confirmation page displays.

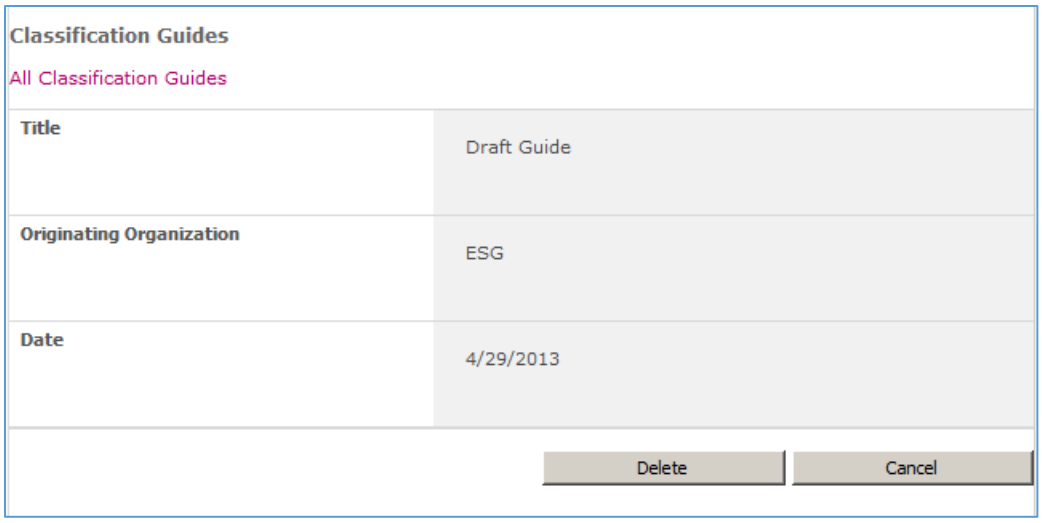


Figure 32 Delete Confirmation

3 Click **Delete** or click **Cancel** to return to the previous screen.

Creating, Editing and Deleting Classification Guide Topics

Each Classification Guide can have one or more topics associated to it. Each topic has its own default values that are selectable by users. If the topic contains a classification value, users can only select topics that correspond to their assigned Security Classification and those that are of lower rank.

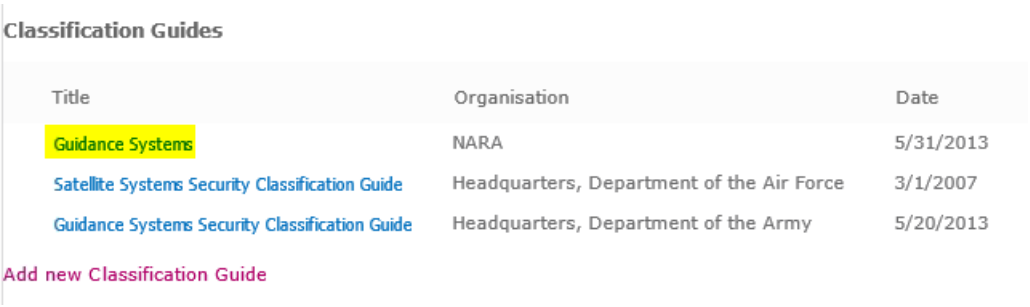


Figure 33 Classification Guide Selection

Creating a Topic

Follow these steps to create a classification guide topic:

1 From the Classification Guides list, click on any Guide. The screen refreshes and displays the topics associated with the guide.

2 Click **Add new Classification Topic** to add a topic to the guide.

3 Enter the title of the topic and an optional remark.

4 Click **Create**.

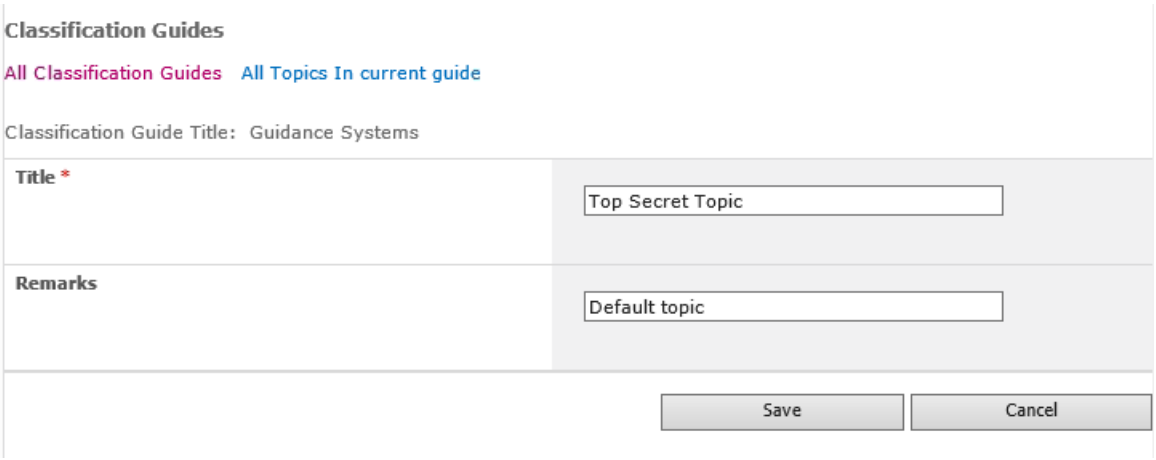


Figure 34 Creating a Classification Guide Topic

5 From the Topic view, click on the newly created topic to add default values to copy to the Classified Record's form if this Guide and Topic is selected in the **Derived From** section on the record's form.

6 Enter any needed value on the Topic form, if desired. In the following example, a Supplemental Marking, Classification value, Classified By value, Declassify On Date option,

and the date itself are set.

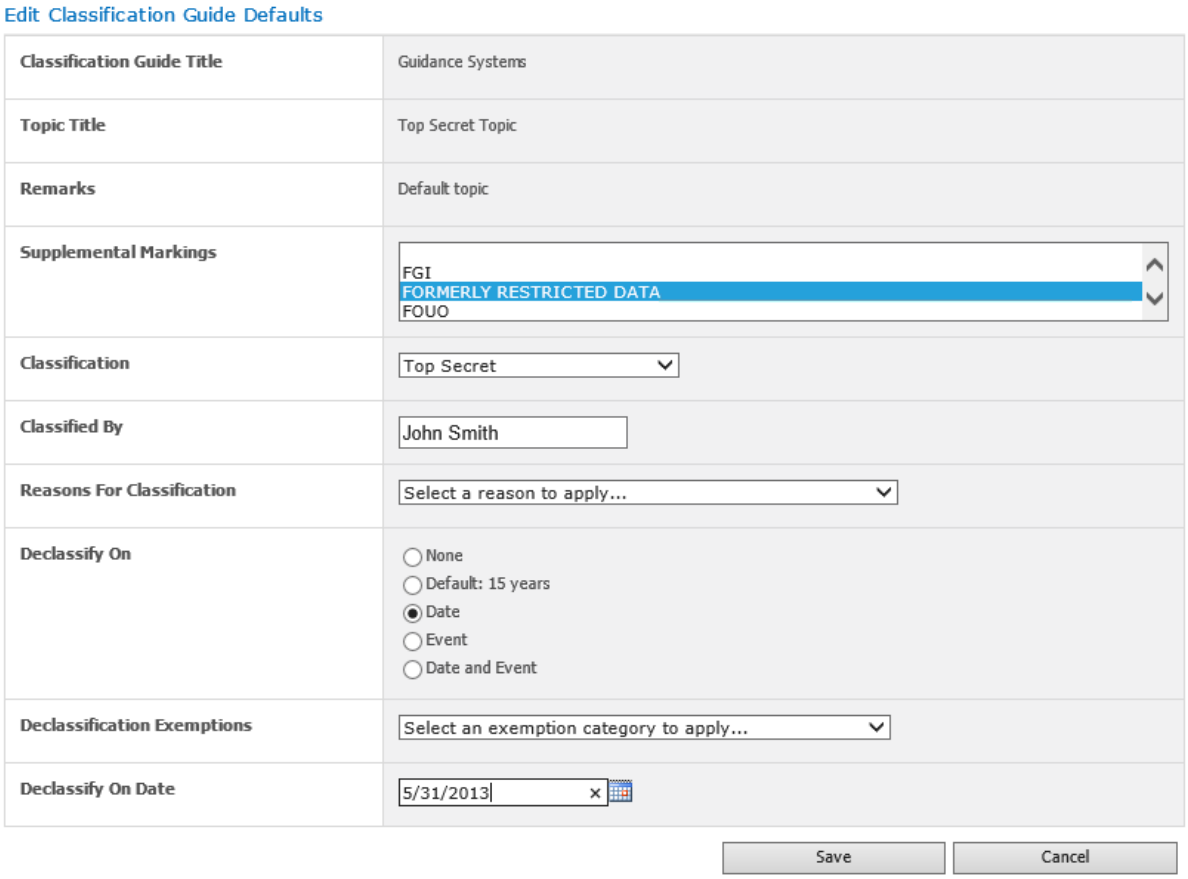


Figure 35 Entering Topic Values

7 Click **Save**. You can copy these values to the classified record's form.

Editing a Topic

Follow these steps to edit a classification guide topic:

1 Click on the topic in the list and change any of the values on the topic's page.

2 Click **Save** to commit the changes.

Deleting a Topic

From the topic list, select the pull-down menu on the right and click **Delete**.

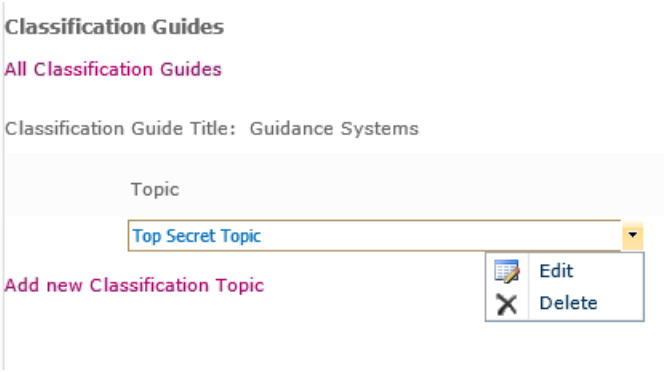


Figure 36 Deleting a Classification Guide Topic

Reasons for Classification List

The Administration Manager creates the Reasons for Classification Lists. Each line of the list represents reasons for classification and the entire list is presented to users when classifying a record. Multiple reasons can be selected from the list. Each line of the list can only contain one item. There must be a reason for each list item.

Notes
You must have RMA Records Manager privileges in order to create, edit, or delete Classification List entries. Without these permissions, you can view the entries in the Reasons for Classification, but you cannot change them. When you change (edit or delete) an entry on the Reason for Classification list, the original values in existing record values are not changed. However, if you edit the record and reapply a Reason for Classification, which has been changed since the item was created, the newest version of a Reason for Classification is applied to the Classified record.

To access the Reasons for Classification page to create, edit, or delete entries, select Reasons for Classification under the Lists section of the Quick Launch region. You can also access the page by selecting **Site Actions** -> **Site Settings** -> **Classified Records** -> **Reasons for Classification.**

Figure 37 Reasons for Classification Selection

Creating Entries

Entries in the Reasons for Classification List consist of both a Title and a Description. To create an entry, use the following procedure:

1 Open the **Reason for Classifications** page. The first time you open the Classification Reasons, no entries display. Click **Add new item** at the bottom of the list to create an entry.

2 Complete the **Title** and *Description* fields in the **Classification Reasons new item** menu.

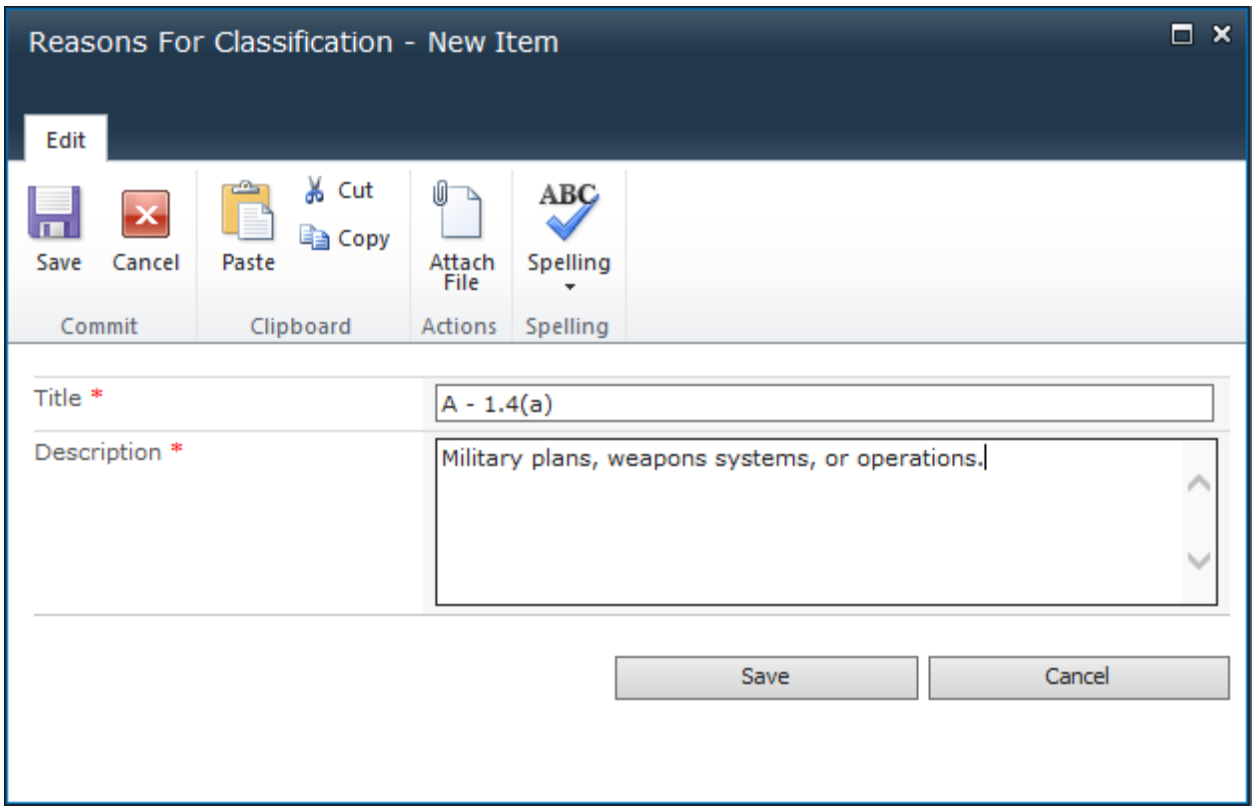


Figure 38 New Reason for Classification

3 Click **Save**.

4 Continue entering other Classification Reasons as needed.

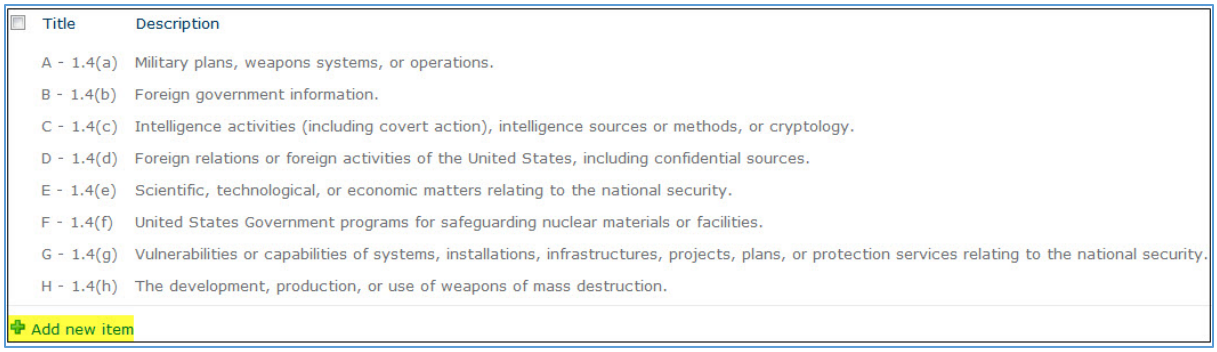


Figure 39 Classification Reasons

Editing Entries

This subsection explains how to edit Reasons for Classification list entries.

Note
You must be in the RMA Records Manager group to edit Reasons for Classification entries.

1 Open the Reason for Classifications page. The list of Reasons for Classification displays.

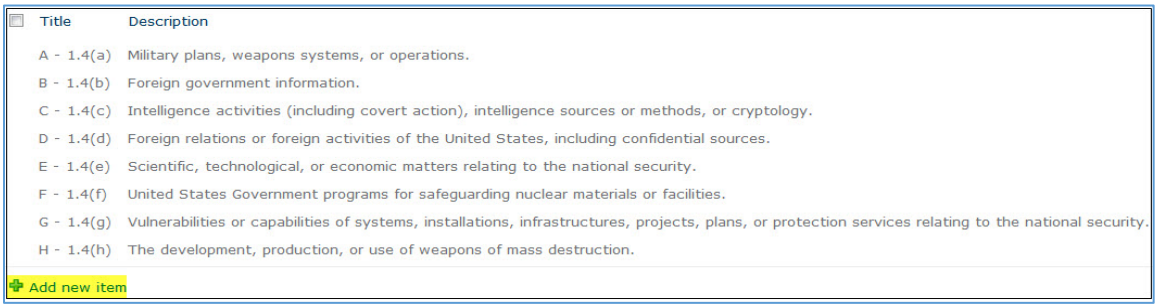


Figure 40 Reasons for Classifications

2 Click on the entry you want to edit and click **Edit Item** in the header ribbon. The Reasons for Classification window displays your selection.

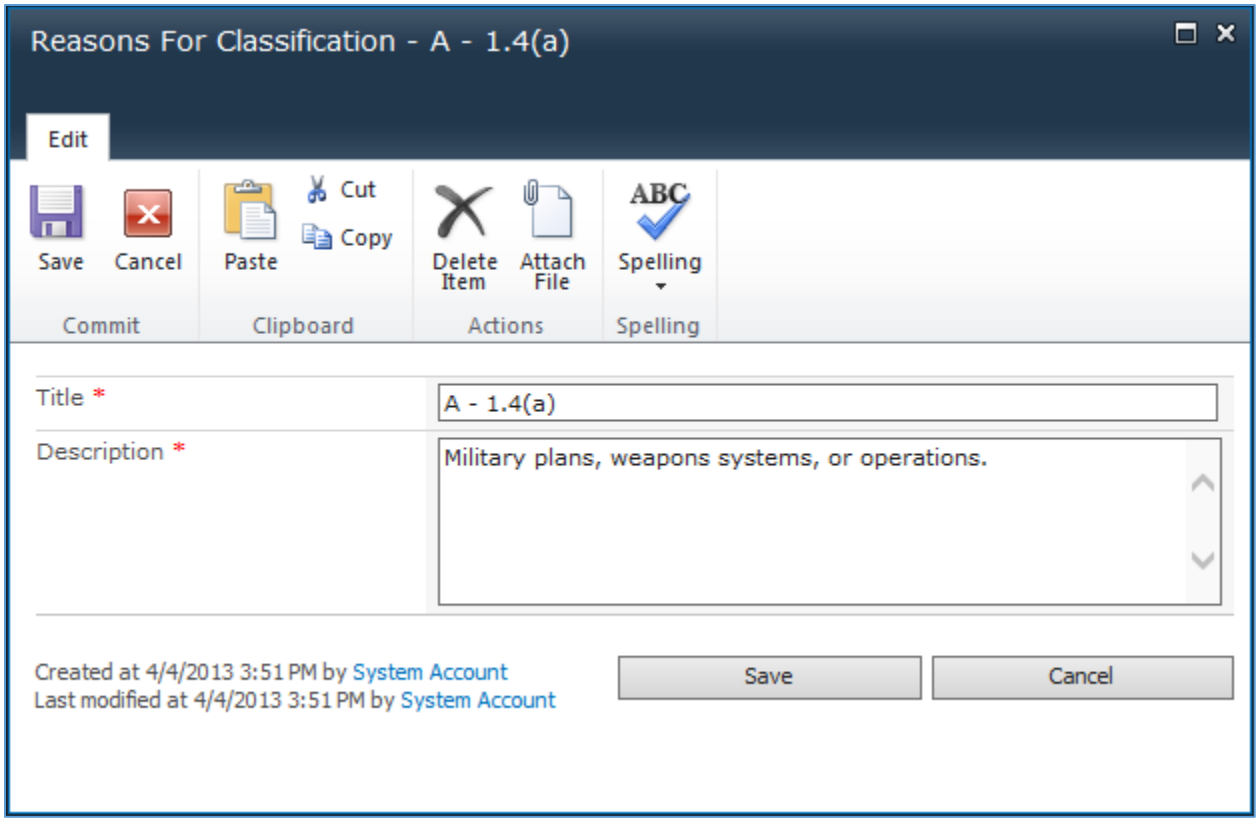


Figure 41 Edit Reasons for Classification

3 Make changes to the **Title** and **Description**.

4 Click **Save**.

Deleting Entries

This subsection explains how to delete Reasons for Classification entries.

1 Open the Reason for Classifications page. The list of Reasons for Classification displays.

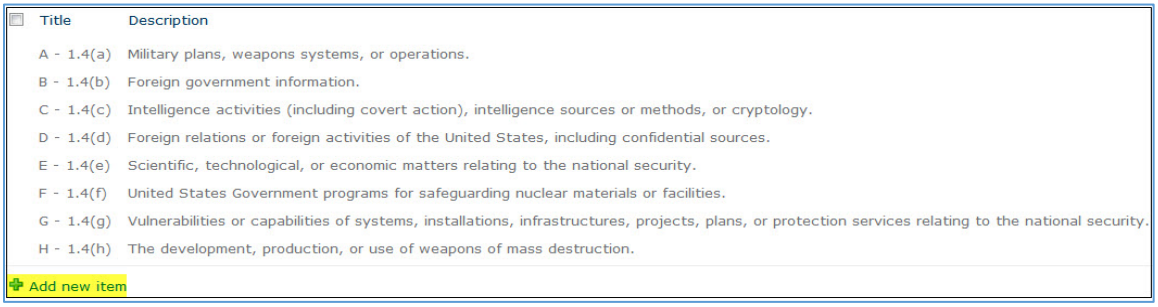


Figure 42 Reasons for Classifications

2 Select the entry you want to delete and click **Delete Item** in the header ribbon. If you want to delete all entries, select the rectangle beside **Title**.

3 When the dialog box asking if you are sure you want to delete displays, click **Yes**. The entry is deleted.

Declassification Exemptions List

When a user creates a classified record, an exemption category is mandated if the declassification date selected exceeds the automatically calculated date for this process. The automatic date is determined by the value entered in "Default Declassification Timeframe" in the Manage Timeframes window in the Classified Records section. See "Managing Timeframes Setup**"** for additional instructions on how to use Timeframes.

Notes
You must be in the RMA Records Manager group to create, edit, or delete Classification Exemptions entries. Without this permission, you can view the entries in the Classification Exemptions but you cannot change them. When you change (edit or delete) an entry on the Classification Exemptions List, the original values in existing record values are not changed. However, if you edit the record and reapply a Classification Exemption, which has been changed since the item was created, the newest version of a Classification Exemption is applied to the Classified record.

- To access the Declassification Exemptions page to create, edit, or delete entries, select Declassification Exemptions under the Lists section of the Quick Launch region.
- You can also access the page by selecting Site Actions -> **Site Settings** -> **Classified Records** -> **Declassification Exemptions**.

Figure 43 Declassification Exemptions Selection

Creating Entries

Entries in the Exemption category consist of both a Title and a Description. To create an entry, use the following procedure:

1 Open the Declassification Exemptions page. The first time you open the Declassification Exemptions, no entries display. Click **Add new item** at the bottom of the list to create an entry.

2 Enter the required information in the appropriate fields.

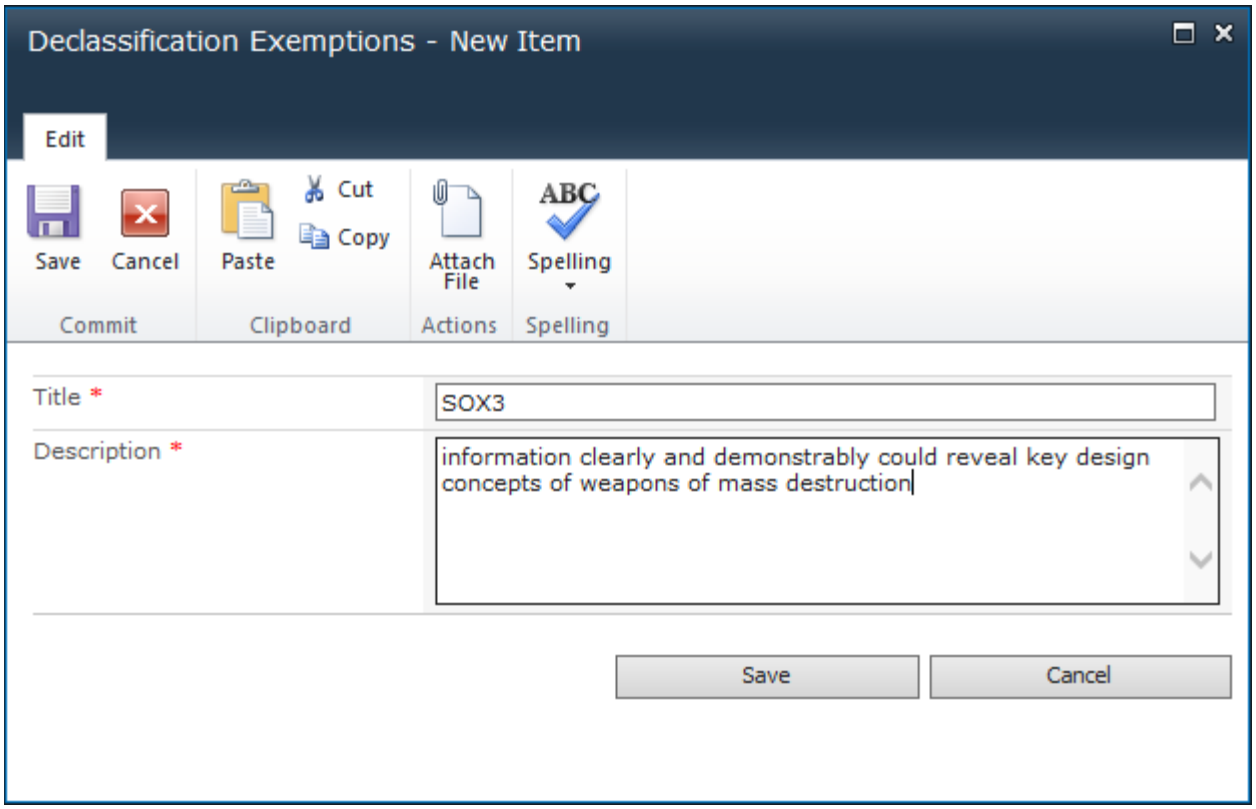


Figure 44 New Declassification Exemption

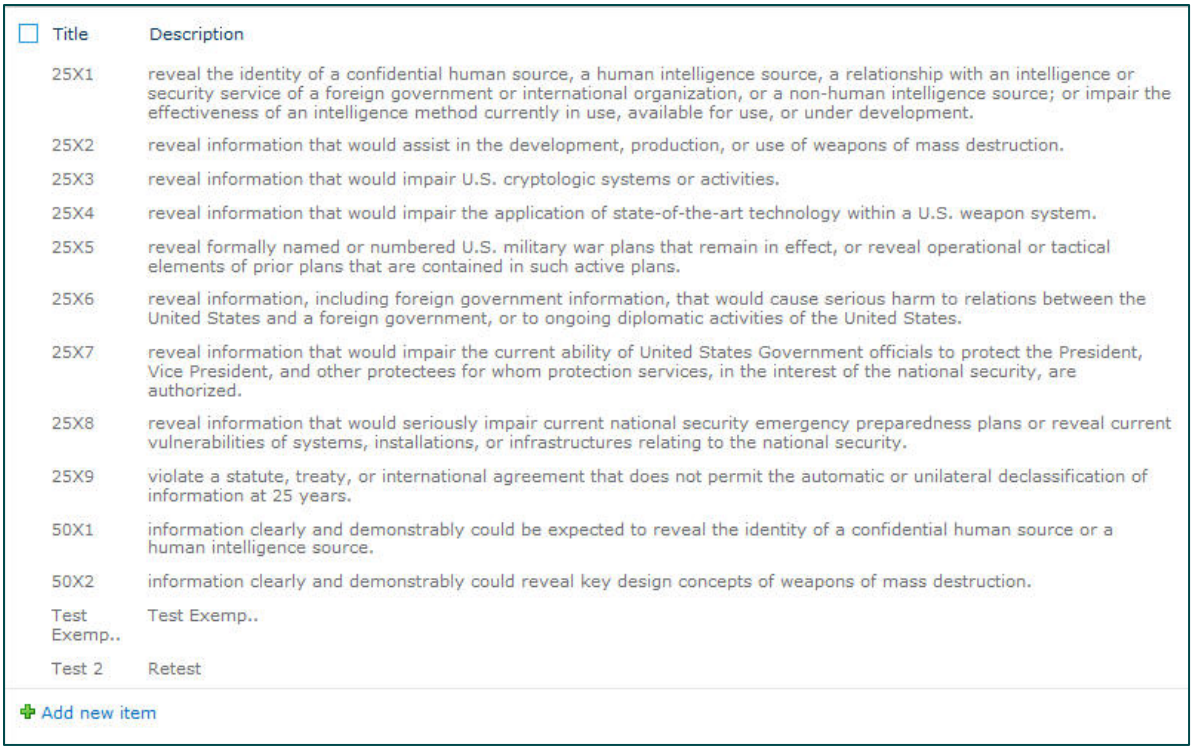
3 Click **Save**.

Editing Entries

This subsection explains how to edit Classification Exemptions entries.

Note
You must be in the RMA Records Manager group to edit Classification Exemptions entries.

1 Open the Declassification Exemptions page. The list of Exemption Classifications displays.



Title	Description
25X1	reveal the identity of a confidential human source, a human intelligence source, a relationship with an intelligence or security service of a foreign government or international organization, or a non-human intelligence source; or impair the effectiveness of an intelligence method currently in use, available for use, or under development.
25X2	reveal information that would assist in the development, production, or use of weapons of mass destruction.
25X3	reveal information that would impair U.S. cryptologic systems or activities.
25X4	reveal information that would impair the application of state-of-the-art technology within a U.S. weapon system.
25X5	reveal formally named or numbered U.S. military war plans that remain in effect, or reveal operational or tactical elements of prior plans that are contained in such active plans.
25X6	reveal information, including foreign government information, that would cause serious harm to relations between the United States and a foreign government, or to ongoing diplomatic activities of the United States.
25X7	reveal information that would impair the current ability of United States Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized.
25X8	reveal information that would seriously impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, or infrastructures relating to the national security.
25X9	violate a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at 25 years.
50X1	information clearly and demonstrably could be expected to reveal the identity of a confidential human source or a human intelligence source.
50X2	information clearly and demonstrably could reveal key design concepts of weapons of mass destruction.
Test Exemp..	Test Exemp..
Test 2	Retest

Add new item

Figure 45 Declassification Exemptions List

2 Click on the entry you want to edit and click **Edit Item** in the header ribbon. The Reasons for Classification window displays your selection.

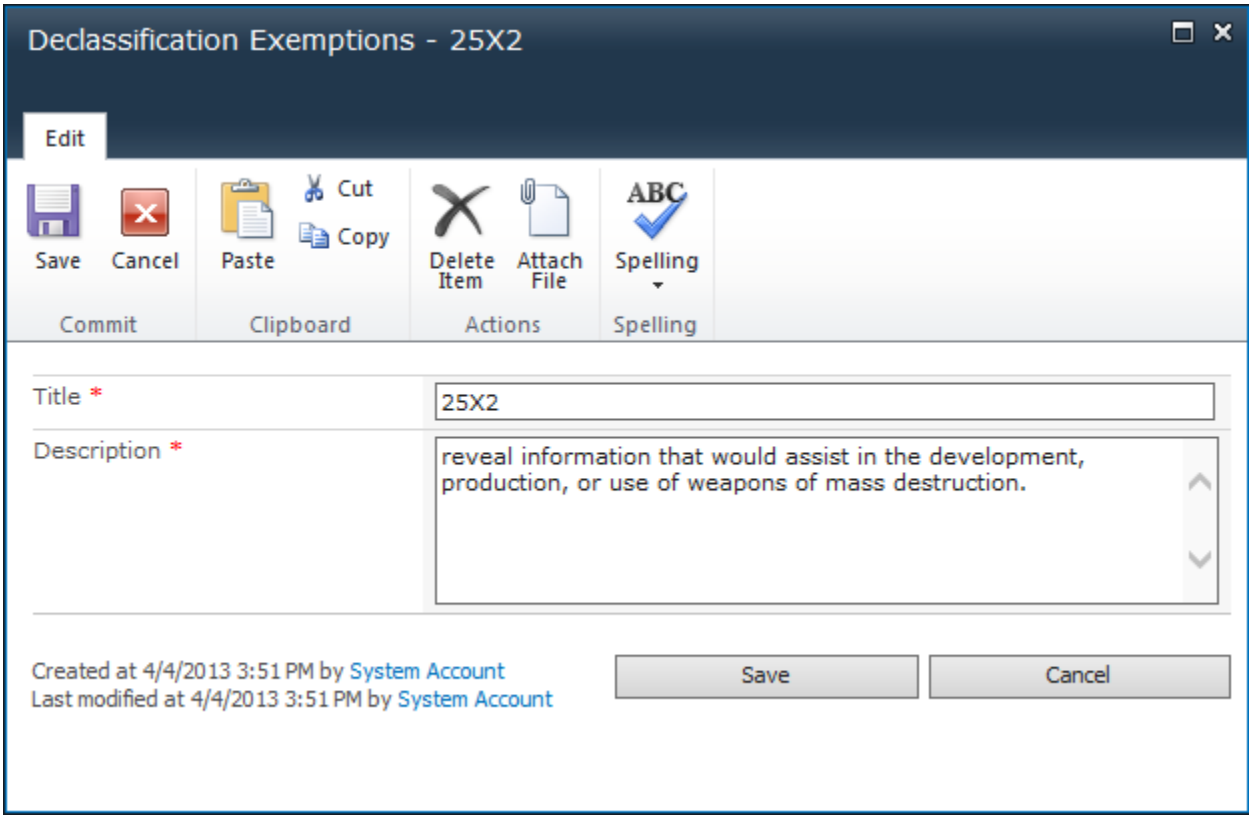


Figure 46 Edit Declassification Exemption

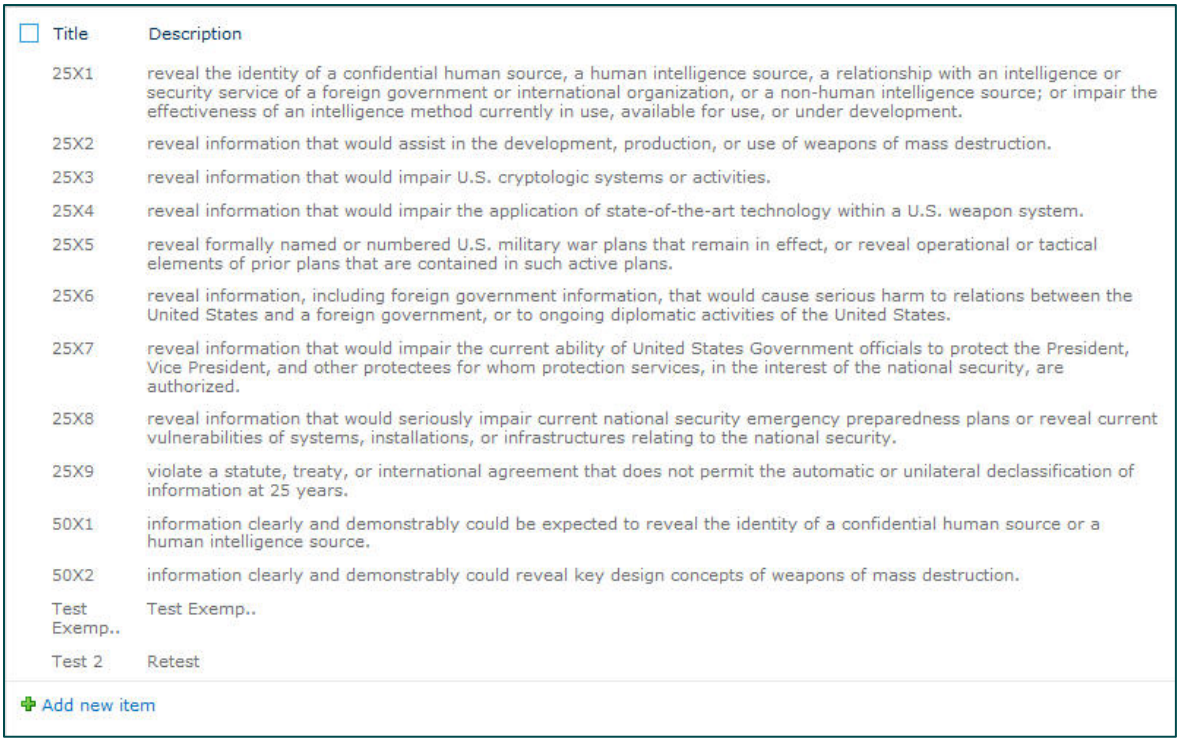
3 Make changes to the **Title** and **Description**.

4 Click **Save**.

Deleting Entries

This subsection explains how to delete Classification Exemptions entries.

1 Open the Declassification Exemptions page. The list of Exemption Classifications displays.



Title	Description
25X1	reveal the identity of a confidential human source, a human intelligence source, a relationship with an intelligence or security service of a foreign government or international organization, or a non-human intelligence source; or impair the effectiveness of an intelligence method currently in use, available for use, or under development.
25X2	reveal information that would assist in the development, production, or use of weapons of mass destruction.
25X3	reveal information that would impair U.S. cryptologic systems or activities.
25X4	reveal information that would impair the application of state-of-the-art technology within a U.S. weapon system.
25X5	reveal formally named or numbered U.S. military war plans that remain in effect, or reveal operational or tactical elements of prior plans that are contained in such active plans.
25X6	reveal information, including foreign government information, that would cause serious harm to relations between the United States and a foreign government, or to ongoing diplomatic activities of the United States.
25X7	reveal information that would impair the current ability of United States Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized.
25X8	reveal information that would seriously impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, or infrastructures relating to the national security.
25X9	violate a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at 25 years.
50X1	information clearly and demonstrably could be expected to reveal the identity of a confidential human source or a human intelligence source.
50X2	information clearly and demonstrably could reveal key design concepts of weapons of mass destruction.
Test Exemp..	Test Exemp..
Test 2	Retest

Add new item

Figure 47 Declassification Exemptions List

2 Select the entry you want to delete and click **Delete Item** in the header ribbon. If you want to delete all entries, select the rectangle beside **Title**.

3 When the dialog box asking if you are sure you want to delete displays, click **Yes**. The entry is deleted.

Grading Classified Records

Records can be scheduled for re-classification when an authorized user changes the Upgrade On, Downgrade On, or Declassify On fields, or alternatively, when the Current Classification level is manually changed.

Upgrading:

- Changing the Current Classification field from a lower security classification to a higher one
- When classified records are moved up in the hierarchy; for example, from "Secret" to "Top Secret"

Downgrading:

When classified records are moved down in the hierarchy, for example, from "Top Secret" to "Secret"

Note
You cannot downgrade a record to the lowest level classification, as this is regarded as declassification.

Declassifying:

When classified records are moved down in the hierarchy to the lowest level of classification

This chapter explains the roles, functionality, and requirements for grading classified records. For specific information on grading procedures, see the *Gimmal Classified Records User Guide*.

Roles

Roles are the grouping of resource permissions defined for the application. Users must be assigned to roles in order to have functional access to the classified records. The roles include:

- Records Management Application (RMA) Applications Administrator
- Records Manager
- Security Officer
- Typical User

The RMA Records Manager must set up initial classifications.

Functional Privileges and Requirements

Table 1 helps determine who in your organization should have what functional privileges.

Table 1 Functional Privileges

User Type	Functional Access
Security Officer	Upgrade, downgrade, declassify, and review classified records. Request the RMA automatically calculate a new "Declassify On" date based on changes to the "Declassify On" timeframe. Input and manage classification guides. Enter or update Exemption Category of classified records.
Records Manager	Transfer and expunge declassified records from the classified repository. Map the fields of a classification guide to the record metadata fields. Select which metadata fields to capture. Delete the record history audit after filing as a record.
RMA Records Manager	Maintain the "Declassify On" timeframe. Restrict access to records by setting up user accounts and access control lists.

Table 2 lists the requirements for the Classified Record fields.

Table 2 Classification Population

Component	Required for Population
Initial Classification	Mandatory
Current Classification	Mandatory
Reasons for Classification	Mandatory only when "Classified By" is not blank or null.
Classified By (also called classification authority)	Mandatory if "Derived From" field is blank or null.
Derived From	Optional; mandatory if "Classified By" field is blank or null.
Declassify On	Mandatory for all but restricted data or formerly restricted data (the declassify trigger can be a date, an event, an exemption category and date, or a combination of dates and events)

Table 3 provides the Downgrading, Reviewing, and Regrading information.

Table 3 Downgrading, Reviewing, and Regrading Population

Component	Required for Population
Downgrade On	Optional (the downgrade trigger can be a date, an event, or a combination of dates and events).
Downgrade Instructions	Mandatory if "Downgrade On" is populated
Reviewed On	Optional
Reviewed By	Mandatory if "Reviewed On "is populated.
Downgraded On	Automatically filled in on the server.
Downgraded By	Mandatory if "Downgraded On" is populated
Declassified On	Automatically filled in on the server.
Declassified By	Mandatory if "Declassified On" is populated.
Upgraded On	Automatically filled in on the server.
Reasons for Upgrade	Mandatory if "Upgraded On" is populated.
Upgraded By	Mandatory if "Upgraded On" is populated.

Classified Records Timer Jobs

Classified Records installs SharePoint timer jobs with the product that run in the background and process items. The product contains the following timer jobs: Declassify and Downgrade Records Evaluation Timer Job, Declassify and Downgrade Records Timer Job, and Declassify Transfer Timer Job.

Figure 48 Classified Records Timer Jobs

Note
If a record changes and is declassified, its effective declassification date is immediately set.

Declassify and Downgrade Records Evaluation Timer Job

This timer job runs through each of the classified records, looking for records that:

1 Have declassify set to an event, or default declassification time

2 Have a downgrade set to an event

This job sets the effective downgrade or effective declassify date and time once there is an actual value that can be determined. It can be scheduled or run by choosing the Quick Link that security officers can run to re-evaluate. This timer should be run before the Declassify and Downgrade Records Timer Job to ensure that records are evaluated according to the latest default classification time and up-to-date events.

Declassify and Downgrade Records Timer Job

This timer job is run to perform the declassification or downgrade of classified records that have reached their effective dates. This timer job actually performs the downgrades/declassifications and sets the updated properties. This timer job should be run after the evaluation timer job.

Declassify Transfer Timer Job

This timer job looks for classified records that have been declassified. It configures the transfer of those declassified records, based on the transfer settings that are configured through a link in the site settings. After you run this timer job, you can see the entries in the scheduled transfers. This timer job must be run before the standard Gimmal Transfer timer job, which actually performs the transfers that have been configured.

Note
You must configure the Declassify Transfer Export screen for the Declassify and Downgrade Records Evaluation and Declassify and Downgrade Records Timer jobs to export properly.

Restricted Records Cleanup Timer Job

The Restricted Records Cleanup Timer Job validates and removes invalid record relationships and is disabled upon installation. If you plan to use record relationships, you must enable the job.

Running the DoD Declassification Report

As records are declassified, they are not automatically purged from the repository. The reports are kept in the system in a "declassified" state and deemed as unclassified (rank 0). The Records Manager runs this report and can purge records that have been declassified by the system. The exported records can be archived or alternatively imported into a public system as they are no longer considered as having classified information.

Running the Report

Records managers follow these steps to run the DoD Declassification Report:

1 Display the Declassification Reporting page by selecting **Site Actions** -> **Site Settings** -> **Classified Records** -> **Declassification Reporting**.

Figure 49 Declassification Reporting Selection

The Declassification Reporting page displays.

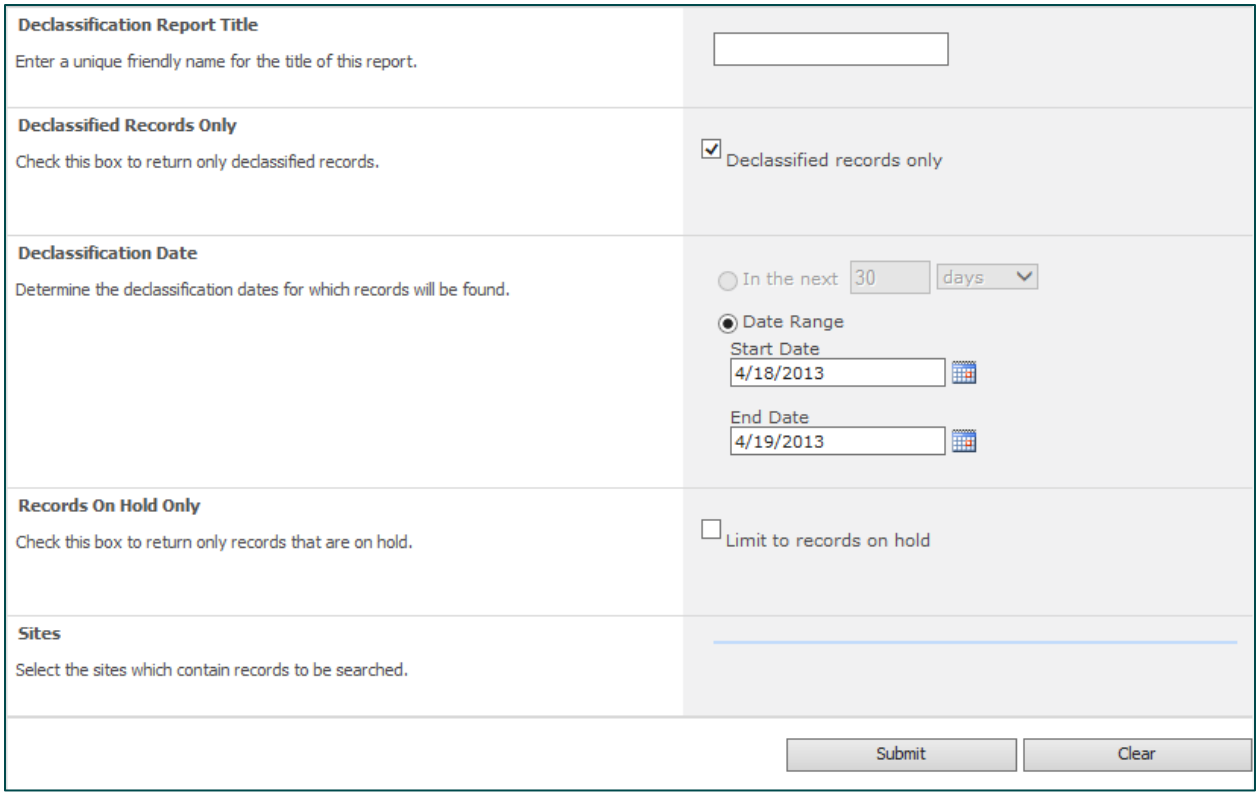


Figure 50 Declassification Reporting Page

2 Enter the title of the report in **Declassification Report Title**.

3 If you want the report to include all classified records in the system, uncheck the **Declassified records only** checkbox.

4 In the **Declassification Date** section, select the **Date Range**. If you chose to include all classified records in step 3, you can also select **In the next X days/months/years**.

5 If you want the report to only include records on hold, click the **Limit to records on hold** checkbox.

6 In the **Sites** section, select the sites you want to search for these records.

7 Click **Submit**. The screen updates with a message that you can retrieve the report from the Declassification Reports list.

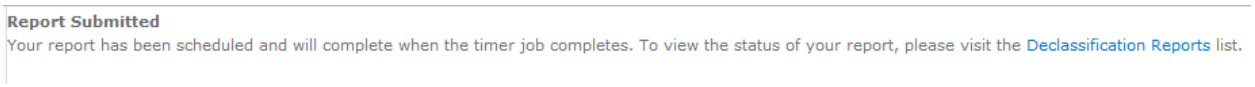


Figure 51 Declassification Reports Selection

8 To retrieve the report, click Declassification Reports in the message. To retrieve the report at any other time, select **Declassification Reports** from the **Lists** quick menu.

Purging Declassified Records

Once the Security Officer creates a Declassified Report, the Records Manager purges and exports the records from the system. Once a report displays a status of Completed, you can view it.

The report allows you to export the list of results to a CSV file and allows the Records Manager to purge declassified records from the system. Purging permanently destroys the record (content and metadata) from the system. As part of the declassification process, a transfer of the record (its binary and its metadata) is performed. It is intended that the declassified record is purged from the classified records system and the "transfer copy" can be imported into another system (a non-classified system).

Note
Be sure to export items before you purge!

The Records Manager follows these steps to purge declassified records:

1. Display the Declassification Reports by selecting **Declassification Reports** under the **Lists** section of the **Quick Launch** region.

Figure 52 Declassification Reports Selection

The Declassification Reports page displays.

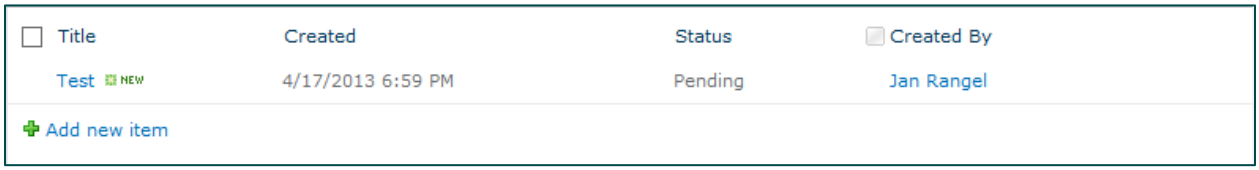


Figure 53 Declassification Reports Page

2 Click on the report to view the results of the declassification reporting.

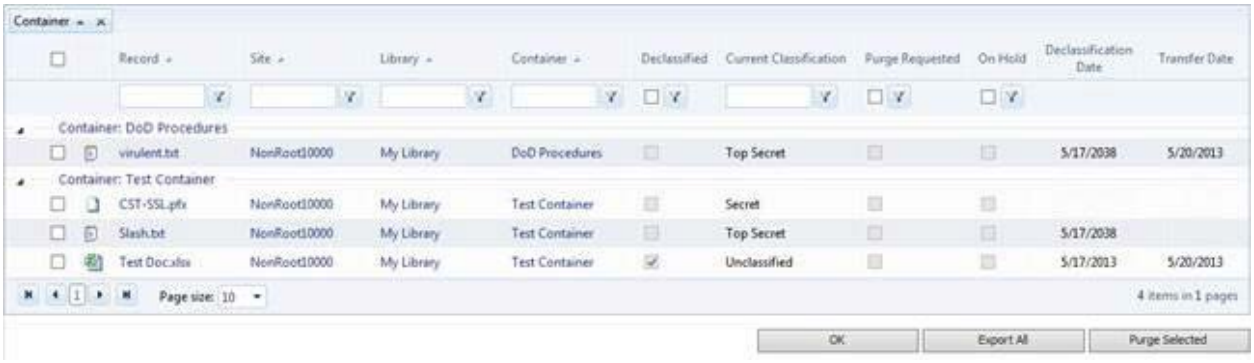


Figure 54 Declassification Report

3 Click **Export** to create a CSV file of the report results that you can open in a spreadsheet program.

4 Select one or more records in the report and click **Purge**. A justification window displays as confirmation, which is also included in the audits of the purge.

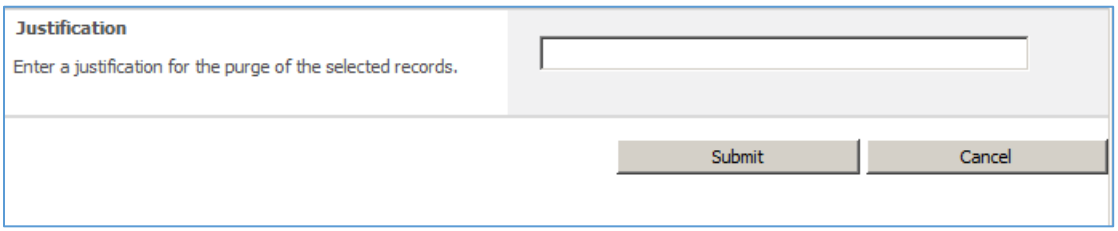


Figure 55 Justification for Purge

You can click **Cancel** to return to the previous screen without making any changes.

5 Click **Submit** to queue up the documents for purge. The system returns to the previous screen, but each record that was selected for the purge displays a checkmark in the **Purge Requested** column.

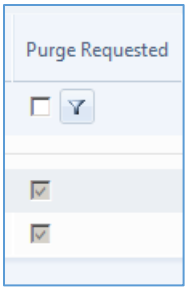


Figure 56 Records with Purge Requested

Once the purge timer job and associated disposition workflow complete, the records that were purged are no longer in the system (or in the Declassification report).

Transferring Classified Records

When classified records are declassified either manually or by a schedule, the system can be configured to transfer the metadata and the content of the classified record to a specific network location.

Configuring Transfer Export

You can schedule two timer jobs for transferring records: "Gimmal Compliance Suite - Declassify Transfer Timer Job" and the "Gimmal Compliance Suite - Transfer Timer Job." Both jobs can be scheduled to suit the organization's individual needs. This exported record can be brought back into the system or can be imported into a non-classified system.

Setting Transfer Export

Follow these steps to set the transfer export:

1 Select **Site Actions** -> **Site Settings** -> **Classified Records** -> **Declassification Transfer Export** to set the transfer export type, mappings file, and network location.

2 Choose the **Transfer Export Type** and the **Schema Mappings File** to use for the transfer.

Note
If the File entry is blank, you must first configure the Mapping File following the "Transfers" section in the Compliance Suite User Guide.

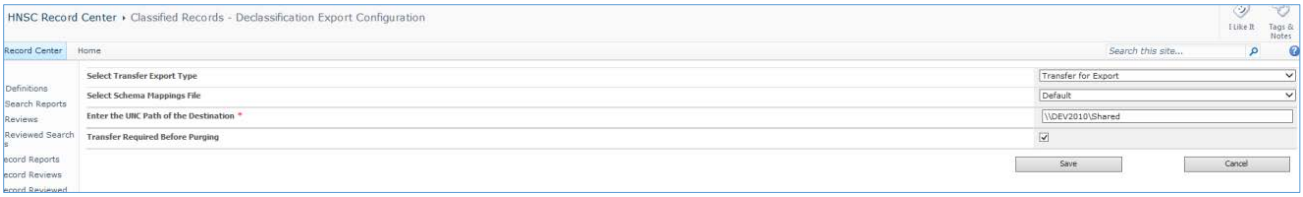


Figure 57 Declassification Transfer Export

3 Select a **Destination Transfer Path** to save the exported files and indicate whether you want a **Transfer Required Before Purging**.

4 Click **Save**.

Whenever a classified record is declassified, it is exported to the location specified in Figure 57 using the mappings that were specified. This is performed by the previously scheduled

timer jobs automatically or can be manually done by running the Declassify Transfer Timer Job followed by the Transfer Timer Job.

5 To verify that the item was queued for transfer and to see its progress, click **View and Delete Scheduled Transfers**. From this interface, you can view the parameters of the transfer; view any exception, restart, or delete completed jobs.

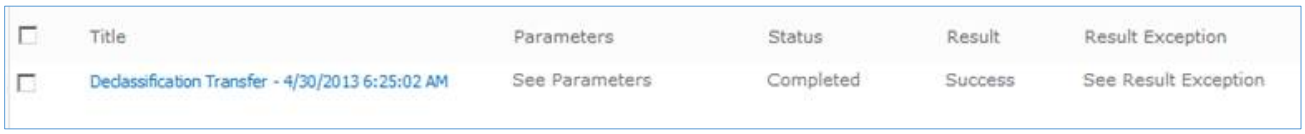


Figure 58 View Scheduled Transfers

Resetting Selected Item to Pending State

1. Select **Reset** from the menu.

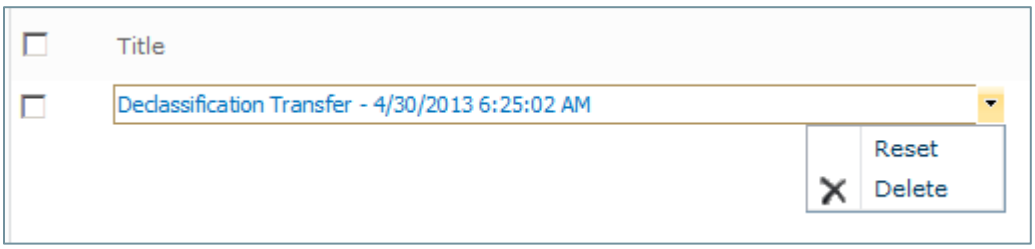


Figure 59 Resetting an Item to a Pending State

A warning message displays.

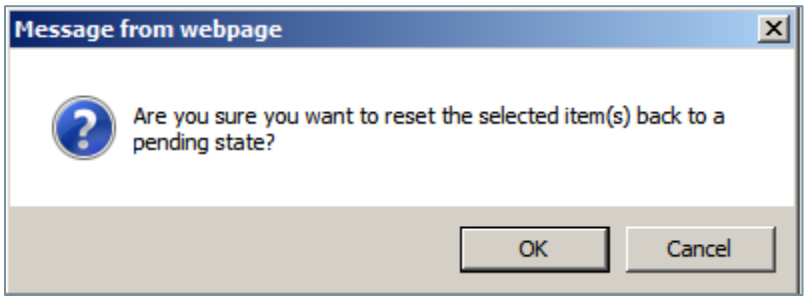


Figure 60 Reset Warning Message

2 Click **OK** to continue or **Cancel** to abort the operation.

Once reset, the item's status changes to pending and the item is transferred when the timer jobs are run again.

Deleting an Entry from Transfer List

1 Click the pull-down menu next to the item and choose **Delete**. A warning message displays.

2 Click **OK** to proceed or Cancel to abort the operation.

The entry no longer displays in the list once deleted.

Viewing Parameters for Transfer or Errors

1 Click **See Parameters** next to any item in the list to view the transfer settings.

2 Click **See Result Exception** next to any item in the list to display any errors.

Note
Ensure all declassified records are transferred before re-running the Declassification Timer job. Otherwise, the declassified records are re-queued in the next transfer.

Nonstandard Content Types

Organizations often possess documentation records that must be classified but are not standard content (RMA records). Enabling classification on a non-standard content type adds the required columns to that content type. Enabling classification on a parent content type also adds the required columns to all derived content types.

Classifying Nonstandard Content Types

Follow these steps to classify content that is nonstandard:

1 Display the Enable Classification on Content Types page by selecting **Site Actions** -> **Site Settings** -> **Classified Records** -> **Classify Non-Standard Content Types**.

Figure 61 Classify Non-Standard Content Types Selection

The Enable Classification on Content Types page displays.

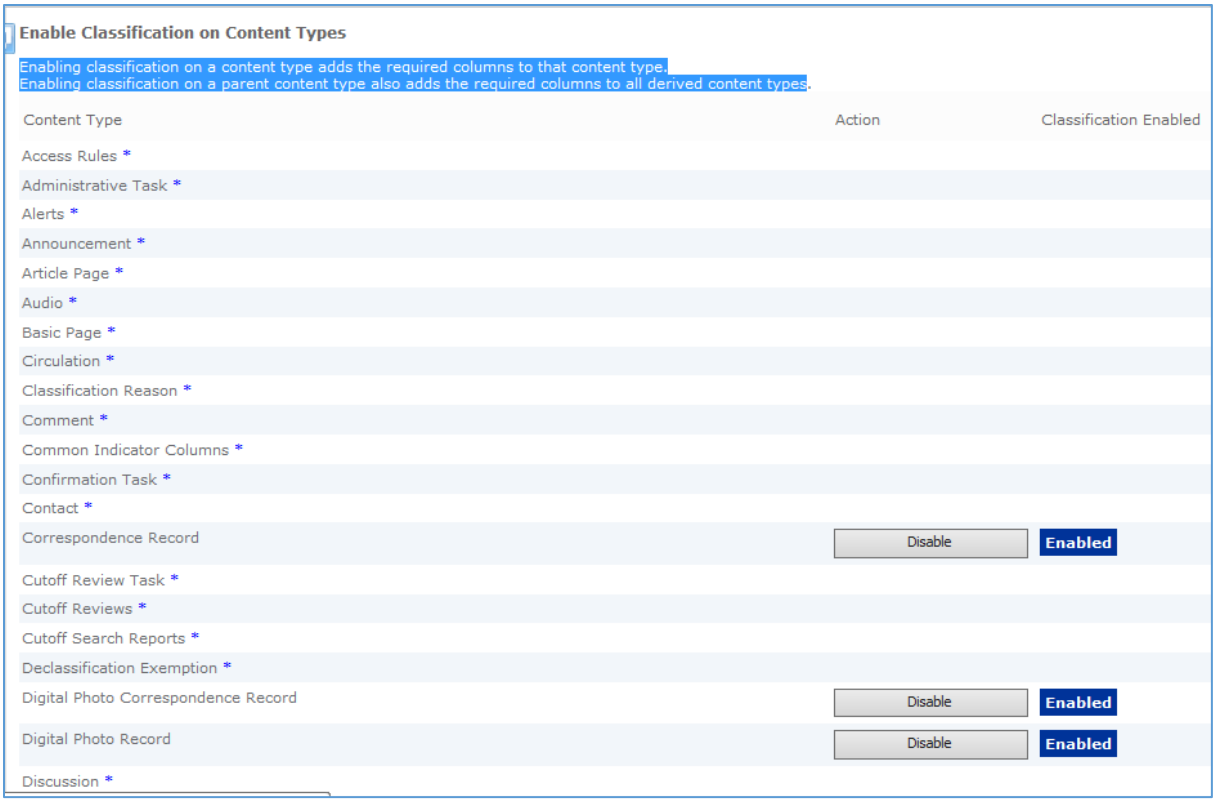


Figure 62 Enable Classification on Content Types Page

2 Click **Enable** next to the content types for which you want to enable classification.

Glossary

The following terms are used in this guide:

- Classified Records – Contain information that is not public. These records become public after a specified period of time. There can be separate repositories for classified and public records. Once records are declassified, they are expunged and transferred to a public accessible repository.

- Security Classifications – Special types of Supplemental markings placed on a Classified Record. Available values are selected from a security trimmed list called initial classification and current classification on the classified record form. The initial classification value serves as a marker while the current classification locks down the classified record to only those user's that have equal or higher access (called a rank value) for the entry selected.

- Conditional Mandatory Elements – Certain attributes when entered on the records form will cause other metadata elements to become mandatory as a result.

- Classification Guides – The guides provide a template that automatically populates certain metadata attributes on the classified records form when selected.

- Working Papers – Documents that contain classified information that must be protected and, as a result, have Security Classifications and optional Supplemental markings applied to them. They also have a finite existence if they are not declared as classified records as they are purged from the system after a set period of time that is by default 180 days but configurable by an administrator