rsd GLASS®
Governance Manager

Version 3.4

User Guide

Trademarks and Registered Names

All brand and product names quoted in this publication are trademarks or registered trademarks of their respective holders.

Notices

RSD GLASS Governance Manager is a software package property of RSD - Geneva, Switzerland that cannot be used without license.

RSD reserves the right to make any modifications to this product and to the corresponding documentation without prior notice or advice.

Manual: RSD GLASS Governance Manager - User Guide and Technical Reference version 3.4

Contents

Introduction

Information Governance Policies define how an organization should manage its content (and information) in order to comply with the requirements of laws, regulations, and internal operational needs. These policies cover the rules of behavior and handling of the various types of documents and Records that are used within the numerous processes in the organization.

The primary mission of the Records Management Program is to ensure that Records are retained in a reliable and authentic manner and are ultimately disposed of in accordance with applicable laws and regulations. It is also necessary to ensure that Records are accessible to all stakeholders within the enterprise.

IG Policies are a set of Record Class (RC) definitions along with the lifecycle policies and rules that must apply to the Records to which these classes are applied.

RSD GLASS Governance Manager is one of the main modules of RSD GLASS and enables the enterprise architecture team to enforce the corporate policies across geographies and jurisdictions, platforms and applications, repositories and data warehouses.

Once the Master Classification has been defined and deployed in the Business Units (BU's) using RSD GLASS Policy Manager, File Plans can be built through RSD GLASS Governance Manager.

This application defines how IG Policies are applied to content in the field. It includes traditional RM administration functions (as required by MoReq2 and DoD 5015.2) such as, but not limited to, Record Screening and Scheduling, Event-based Retention Administration, Vital Record reviews and Physical Record management. It also includes the notifications and approval workflows about upcoming disposition of Records.

The following introduction outlines the features and components of the product.

Topics covered:

Who uses RSD GLASS Governance Manager?

RSD GLASS Governance Manager is primarily used by the Business Unit Records Administrator. This is the person within the BU who has been assigned the responsibility of implementing and managing the Information Governance Policies. It is also destined for the IT Records Managers who oversee the correct functioning of the ILM process in the enterprise.

RSD GLASS Governance Manager Functionality

The following list gives an introduction to the main functionality of RSD GLASS Governance Manager.

- Creation of the File Plan (by the BU Record Administrator actor). The File Plan defines the organization of the folder or file structure within the Business Unit.
- Lifecycle management of Records, Metadata and Security based on the implemented IG Policies.
- Searching and navigating the folder structure of a File Plan in order to retrieve, display, print and export documents that it contains.
- Definition of security access rights to the various branches of the File Plan tree.
- Following the occurrence of a business event, the triggering of events both manually and automatically to start the retention of affected Records.
- Schedule and process the disposal of Records, depending on any prior authorization requirements.
- The capture of documents and reports for archiving, as well as the authoring of documents in MS Office format.
- Performing of electronic discovery and applying holds on Records on instruction from the Legal Counsel due to litigation actions.
- The management of physical archives for inclusion in the Lifecycle process of the enterprise.

What is a File Plan?

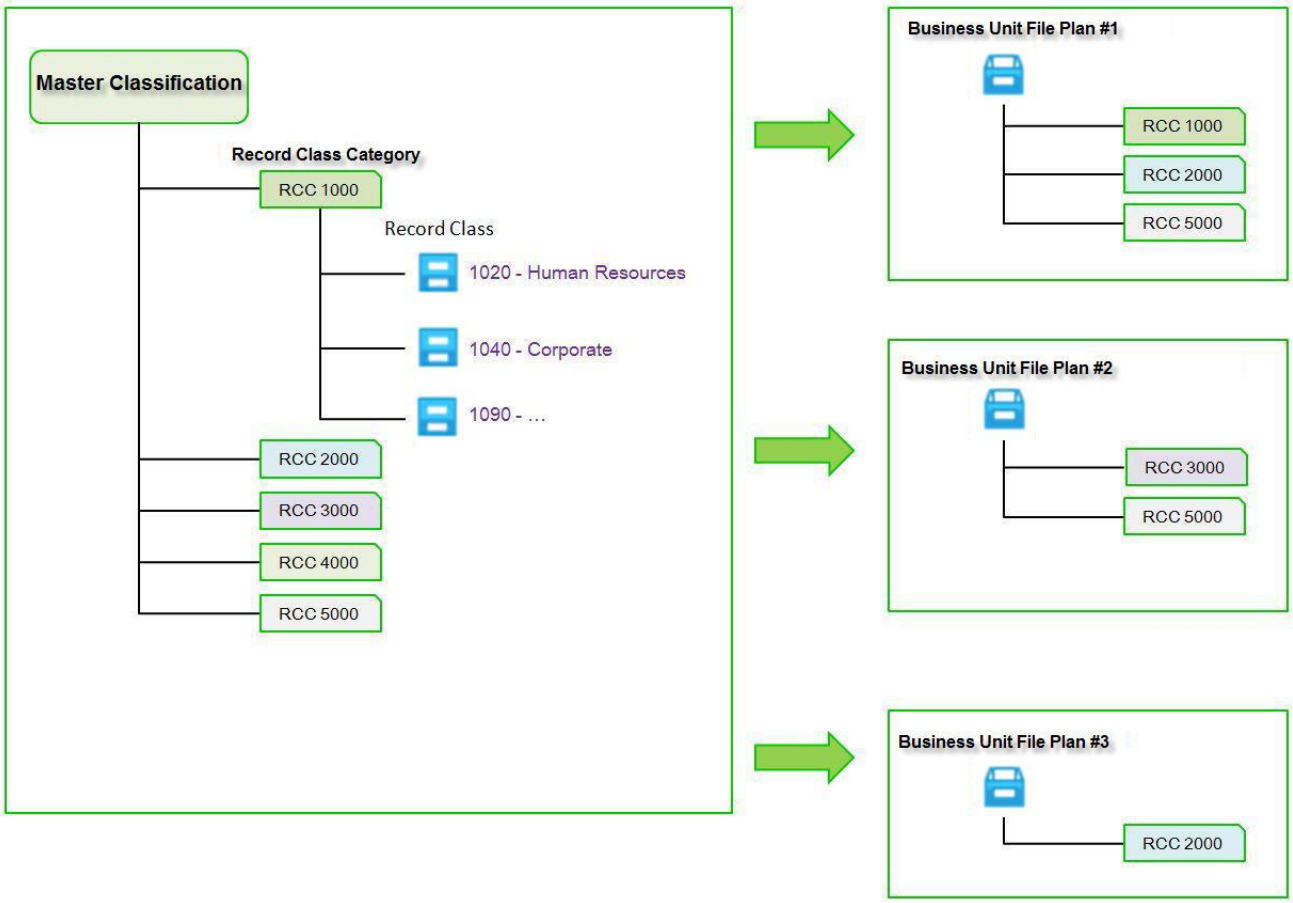
A File Plan is a structure composed of Record Classes selected from the Master Classification. It is used by the BU members to perform Record management tasks or for other specific business needs.

The Master Classification corresponds to the Records Retention Schedule of an enterprise and is composed of Record Classes that are organized in a hierarchical and coded structure.

The Master Classification represents the corporate reference list (hence master) of Record Classes along with the various Information Governance rules associated with them. It is the master list of Record Classes organized in a hierarchy of Master Record Classes. In large organizations, there might be multiple levels in the hierarchy.

A Business Unit is the generic name of an operational unit of employees responsible for a business activity. The Business Unit can be, for example, a department, a section or a location. The Master Classification is used to generate the Business Unit File Plans. File Plans are used to create the folder structure of a Business Unit.

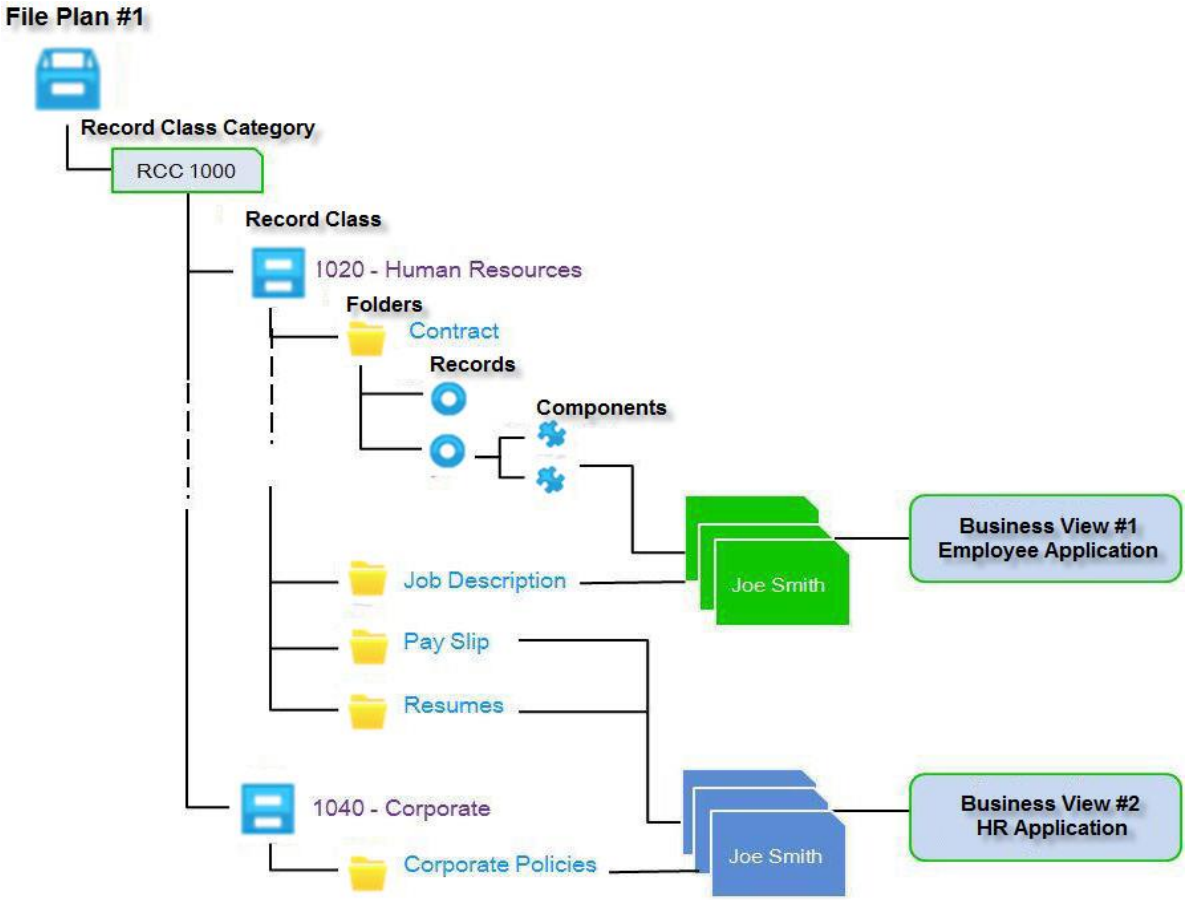
The Master Classification scheme generates the File Plan



What is a Business View?

A Business View is a way of viewing information from a File Plan sorted in a manner that best suits the user for his business activity. It is a subset of a File Plan that allows the user to access only information that he really needs for his particular line of expertise.

The File Plan generates the Business View



Finding your way around

Login

At the initial RSD GLASS Governance Manager Login panel you will be asked to supply your user login and password. Select the **Login** button.

The initial screen to appear after login is the 'Home' page. This Home page automatically displays all of the capabilities of the product according to the role of the user that has logged on. From the initial Home page you will be able to select from a list the File Plan that you wish to consult.

Information on common functionality

The following sections describe functionality that is common to various screens in RSD GLASS Governance Manager.

Sorting list data

By default, elements are listed in the order they have been inserted in the database, with the newest shown last.

How the sort functionality works:

- Clicking on a column header sorts the list according to the data in that column.
- A tool indicating the sort order is added to the right of the column header. To change the sort order, click again on the column header.
- The default is to sort the list on any single column.
- The sort criteria may be set to sort on multiple columns. If that is done, then clicking on a second column header re-sorts the list (sorting the data in the second column with respect to the first sorted column) and so on for any additional columns.

Sort tools:

- Indicates the column is sorted in ascending order. Click on the tool to change the sort order to descending.
- Indicates the column is sorted in descending order. Click on the tool to change the sort order to ascending.

Filtering list data

In order to locate information more easily in a list, it is possible to display only the rows of a list that contain a particular value in one or more columns.

How the filtering functionality works:

- Clicking on the filter icon in a column header displays a box where you may enter the filter criteria. This then limits the number of rows that are displayed. You can use wildcards like * or ? to match any sequence of characters or even a single character.
- This tool indicates that column filtering is applied on the column. To change the filter criteria, click again on the tool.

Required fields

A red asterisk (*) after a field name indicates that a field is required. Fields with no asterisk are optional.

Errors in fields

Fields outlined in red when saved are in error either, because they are required, or they contain illegal information. For example they may contain letters when a date in numbers is required. A red pop-out bubble indicates the nature of the error when the mouse pointer is moved over the field.

Picking from lists

There are two methods to move pre-existing elements from one list to another. Holding down the Ctrl key allows you to select multiple elements at the same time.

- Select the item and holding down the left mouse button drag the item to the list,
- or use the or buttons to move selected items between two lists.

Selecting your Governance Manager environment

Once you have logged into the Governance Manager environment in order to either create a new File Plan or to access an existing File Plan, it is possible to access a different File Plan by selecting the name of the new environment from the Home page.

Setting up your RSD GLASS Governance Manager environment

The following sections describe the elements of RSD GLASS Governance Manager that should be setup prior to starting to use the application.

Topics covered:

Content Repositories

Defines the location of the content repositories accessed by the RSD GLASS applications where information is archived. Over and above the three predefined connections supplied with the default installation (RSD GLASS Repository, CMIS and Java Content Repositories) it is possible to make use of a range of connectors developped by RSD that enables you to access existing data stored in environments such as SharePoint, FileNet and Documentum. A separate document describes how to install, configure and use these drivers.

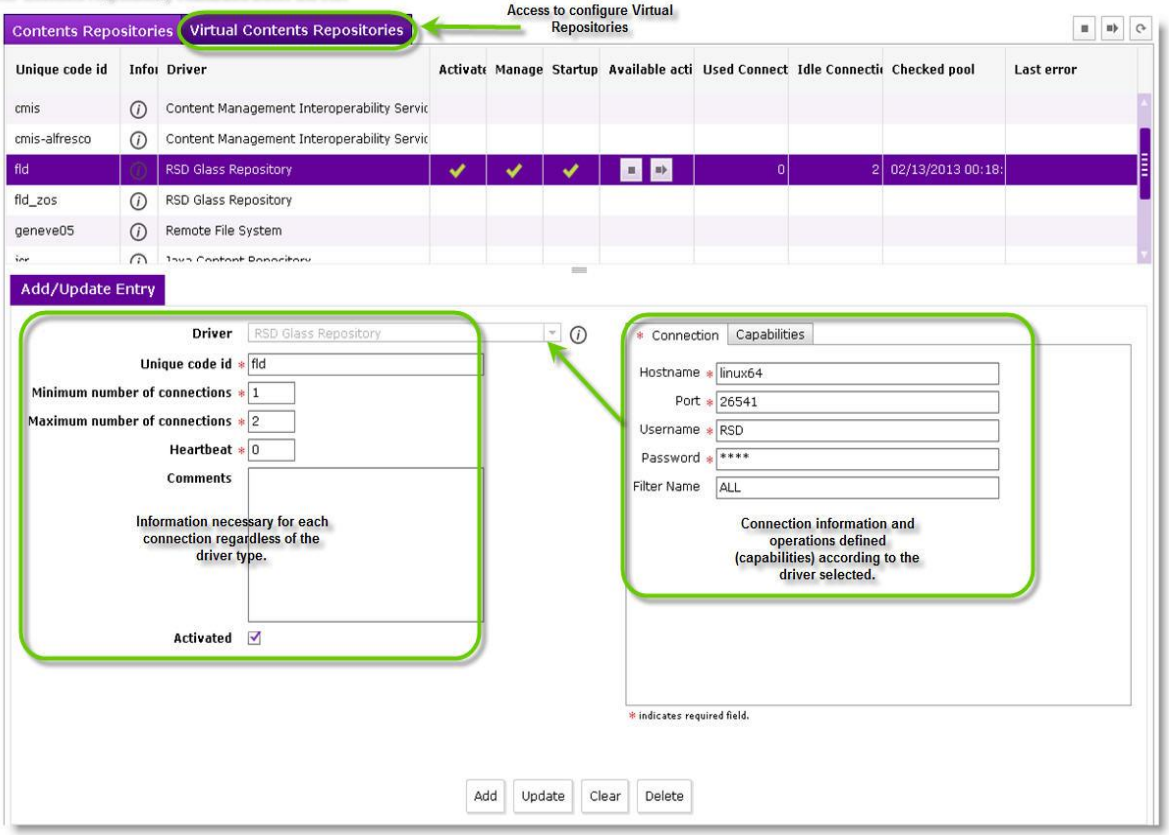
As well as content being stored in online repositories, it is also possible, if configured, to store physical paper archives in boxes. These boxes are archived in off-site repositories or warehouses and managed by the logistics team using the RSD GLASS Physical Records module.

Virtual repositories may also be defined. For further information see "Virtual Repository definition" on page 15.

How to setup access to Repositories

- From the Settings menu, select the 'Content Repository' menu item.
- Select the name of the driver from the dropdown box and configure the dynamically displayed driver-related options according to your needs.

The Content Repository Administration screen



Three predefined connections are supplied with the default installation: RSD GLASS Repository, CMIS and Java Content Repositories. A fourth connector, RSD GLASS Physical Records, may be added by installing the additional driver. Each of these repositories needs to be configured to reflect your environment and to be activated.

For each of the content repositories defined the following common information should be supplied:

Arguments	Information
Unique code id	The name given to the content repository.
Minimum Nb Connections	The minimum number of connections that can be made to the repository.
Maximum Nb Connections	The maximum number of simultaneous connections that can be made to the repository.
Heartbeat	Interval, in seconds, between two connectivity tests.
Activated	Permissible values: true or false. If false, the repository cannot be used.

Driver-specific connection information

RSD GLASS Repository

Arguments	Information
User	The user name used for authentication.
Password	The password for the user name used for authentication.
Host	The host name or the IP address of the RSD GLASS Repository.
Port number	The IP port number of the RSD GLASS Repository.
Filter name	The name of the folder to use in the RSD GLASS Repository. If none is specified, the default RSD GLASS Repository filter is applied.

Java Common Repository (JCR)

Compliance with all libraries that implement the JCR 1.0 interface. The connector works with the http layer mode.

Arguments	Information
User	The user name used for authentication.
Password	The password for the user name used for authentication.
Host	The host name or the IP address of the JCR content repository.
Port number	The IP port number of the JCR content repository.
Path	The Path of the service.
Class name	The class name of the JCR driver.

Example:

Jackrabbit in a Linux environment:

```
Host = linux64
Port Number = 8081
User = adminId
Password = admin
Path = /rmi
Class Name = org.apache.jackrabbit.rmi.repository.URLRemoteRepository
```

Content Management Interoperability Services (CMIS)

Compliance with all repositories that implement CMIS 1.0 (May 2010). The connector works with the http soap layer mode.

Arguments	Information
User	The user name used for authentication.
Password	The password for the user name used for authentication.
Host	The host name or the IP address of the CMIS content repository.
Port number	The IP port number of the CMIS content repository.
Path	The base path of the web services end-points.
Security action	The security authentication mode. Permissible values: None, UsernameToken, Timestamp or UserNameTokenAndTimeStamp. Default: No.
http authentication	The http authentication method. Permissible values: Yes, No. Default: No.

Examples:

CMIS Fileshare on a Linux environment:

```
Host = linux64
Port Number = 8080
User = test
Password = test
Path = /cmis/services/ObjectService
CMIS Repository ID = test
Security Action = UsernameToken
```

Alfresco on a Linux environment:

```
Host = alfresco
Port Number = 8080
User = admin
Password = admin
Path = /alfresco/cmis/services/ObjectService
CMIS Repository ID =  6e53974b-ec85-4425-9cbc-c633f94c3f5c
Security Action = UsernameTokenAndTimestamp
```

Sharepoint:

```
Host =  spscmis01.rsd.com
Port Number = 80
User =  Administrator
Password = XXXXXXXX
Path = /_vti_bin/cmis/soap/ObjectService.svc
CMIS Repository ID =  82a7f6b4-c868-4f45-b362-72c1731f765b
Security Action = None
Http Authentification = Yes
```

RSD GLASS Physical Records

No supplementary arguments are necessary to configure the RSD GLASS Physical Records module driver. Note, however, in the following section when configuring the Virtual Repository for this driver that certain arguments are obligatory.

Repository Capabilities

Each of the four possible repository connector types has different capabilities. When selecting one of the drivers from the list, these capabilities are listed dynamically in the Glass Repository Capabilities tab. You may then select those that you wish to enable for this specific connector.

The following table lists the actions that it is possible to perform on each Repository Connector type.

Repository Connector	Read Content	Write Content	Navigation	Create Folder	Delete Node	Declare/ Undeclare content	Hold/ Resume content	Dispose content	Relocate content	Store physical archive
RSD GLASS Repository	X	X	X	X	X (1)	X	X	X	X	
JCR	X	X	X	X	X					
CMIS	X	X	X	X	X					
Physical Records		X (2)	X (3)		X (4)	X (5)	X (6)	X (7)		X (2)

(1) Delete Folder Name and Document
(2) Adds a physical component to a Box
(3) Lists Boxes
(4) Deletes a physical component from a Box
(5) Declares a physical component in a Box
(6) Holds / Resumes a physical component in a Box
(7) Disposal of a physical component in a Box

Virtual Repository definition

Virtual content repositories point to real repositories and may have a more restrictive filter defined than the physical repository. When a Repository definition is created, a Virtual Repository definition is automatically generated. Two Virtual Repository definitions may have the same Repository definition entry and the same connection information.

Arguments	Information
Unique Code ID	The name given to the virtual content repository.
Referenced repository ID	The name of the real content repository.
Storage Level	The default Storage Level set for the content when catalogued (as opposed to when uploaded) into the File Plan. Different Storage Levels have previously been set for the Storage Level system Metadata configured in the Master Classification of the RSD GLASS Policy Manager environment that your File Plans and Business Views are based upon.

The Context, Compression, Encryption, Capabilities, Integrity and Compliance Rules tabs are available to configure and possibly limit the scope of how the Repository is used.

- Context - used to specify the name of a defined filter. In the case where you are configuring an RSD GLASS Physical Records it is necessary to give the Contract Unique Code. This code is created and managed in the RSD GLASS for Physical Records module in the Settings section.
- Compression - the method used to possibly compress documents. Optional. Possible values: gzip, bzip2.
- Encryption - Encryption Key and Encryption method used to encrypt documents. Optional. Possible values: aes, DES-EDE, blowfish.
- Integrity - If enabled, allows you to automatically verify the integrity of the data stored in the virtual repository. Note that manual integrity checks are still allowed. Possible values: Enabled, Disabled. For more information, see "Managing the Integrity of information stored in your RSD GLASS environment" on page 44.
- Compliance Attributes - Each virtual repository may be qualified with additional compliance system metadata. This allows you in RSD GLASS Policy Manager to create Compliance Rules on Record Classes. Compliance rules may be used to manage how and where data is stored according to the needs of the enterprise. The following qualifying attributes may be set on a virtual repository:

  Minimum storage level, Maximum storage level, Repository Compliance level, Repository Native Encryption, Repository Hosting, Supported Component Type, Repository Location.

  Note that the options provided in the dropdown lists need to have previously been configured in the RSD GLASS Policy Manager environment. A set of 'Compliance' type Metadata need to have been setup to reflect the different levels, locations and options in your enterprise's environment.

  RSD GLASS Policy Manager 'Compliance' Metadata:

componentTypes	Component Types	Compliance
nativeRepositoryEncryption	Native Repository Encryption Readiness	Compliance
repositoryHosting	Repository Hosting	Compliance
repositoryLocation	Repository Location	Compliance
repositoryComplianceLevel	Repository Compliance Level	Compliance
storageLevel	Storage level	Compliance

Scheduler

When a new File Plan is generated in your RSD GLASS Governance Manager environment, four jobs are created and set to automatically run. One of these jobs determines if there are any lifecycle Actions that need to be performed. The second job is used to initialize the workflows to approve the execution of scheduled actions. A third job is created that computes statistics for use in the 'Scheduled Actions Execution' functionality, see "Scheduled Actions Execution" on page 38.

A fourth job performs automatic integrity checks. See "Managing the Integrity of information stored in your RSD GLASS environment" on page 44.

How to configure the Scheduler

- From the Settings Menu, select the Scheduler menu item.

Using the Scheduler

A list of jobs is displayed that correspond to the number of File Plans contained in your RSD GLASS environment. When selecting the name of a job, its details are displayed.

The Cron expression field represents a set of times used to schedule the execution of the job.

It is possible to configure the Cron expression field to specify complex time combinations such as "At 8:00am every Monday through Friday" or "At 1:30am every last Friday of the month".

An extra field (Execution Time) is visible if it is an 'Integrity check' scheduler. This field allows you to limit to the specified number the time in minutes that the integrity check will run.

Cron Expression configuration

Cron expressions are comprised of 6 required fields and one optional field separated by white space. The fields are described as follows:

Field name	Allowed Values	Allowed Special Characters
Seconds	0-59	, - * /
Minutes	0-59	, - * /
Hours	0-23	, - * /
Day Of Month	1-31	, - * ? / L W
Month	1-12 or JAN-DEC	, - * /
Day of Week	1-7 or SUN-SAT	, - * ? / L #
Year (optional)	empty, 1970-2099	, - * /

The '*' character is used to specify all values. For example, "*" in the minute field means "every minute".

The '?' character is allowed for the day-of-month and day-of-week fields. It is used to specify 'no specific value'. This is useful when you need to specify something in one of the two fields, but not the other.

The '-' character is used to specify ranges For example "10-12" in the hour field means "the hours 10, 11 and 12".

The ',' character is used to specify additional values. For example "MON, WED, FRI" in the day-of-week field means "the days Monday, Wednesday, and Friday".

The '/' character is used to specify increments. For example "0/15" in the seconds field means "the seconds 0, 15, 30, and 45". And "5/15" in the seconds field means "the seconds 5, 20, 35, and 50". Specifying '*' before the '/' is equivalent to specifying 0 as the value to start with. For each field in the expression, there is a set of numbers that can be turned on or off. For seconds and minutes, the numbers range from 0 to 59. For hours 0 to 23, for days of the month 0 to 31, and for months: 1 to 12. The "/" character simply helps you turn on every "nth" value in the given set. Thus "7/6" in the month field only turns on month "7", it does NOT mean every 6th month, please note that subtlety.

The 'L' character is allowed for the day-of-month and day-of-week fields. This character is shorthand for "last", but it has different meanings in each of the two fields. For example, the value "L" in the day-of-month field means "the last day of the month" - day 31 for January, day 28 for February on non-leap years. If used in the day-of-week field by itself, it simply means "7" or "SAT". But if used in the day-of-week field after another value, it means "the last xxx day of the month" - for example "6L" means "the last Friday of the month". When using the 'L' option, it is important not to specify lists, or ranges of values, as you'll get confusing results.

The 'W' character is allowed for the day-of-month field. This character is used to specify the weekday (Monday-Friday) nearest the given day. As an example, if you were to specify "15W" as the value for the day-of-month field, the meaning is: "the nearest weekday to the 15th of the month". So if the 15th is a Saturday, the trigger will fire on Friday the 14th. If the 15th is a Sunday, the trigger will fire on Monday the 16th. If the 15th is a Tuesday, then it will fire on Tuesday the 15th. However if you specify "1W" as the value for day-of-month, and the 1st is a Saturday, the trigger will fire on Monday the 3rd, as it will not 'jump' over the boundary of a month's days. The 'W' character can only be specified when the day-of-month is a single day, not a range or list of days.

The 'L' and 'W' characters can also be combined for the day-of-month expression to yield 'LW', which translates to "last weekday of the month".

The '#' character is allowed for the day-of-week field. This character is used to specify "the nth" XXX day of the month. For example, the value of "6#3" in the day-of-week field means the third Friday of the month (day 6 = Friday and "#3" = the 3rd one in the month). Other examples: "2#1" = the first Monday of the month and "4#5" = the fifth Wednesday of the month. Note that if you specify "#5" and there is not 5 of the given day-of-week in the month, then no firing will occur that month. If the '#' character is used, there can only be one expression in the day-of-week field ("3#1,6#3" is not valid, since there are two expressions).

The legal characters and the names of months and days of the week are not case sensitive.

NOTES:

Support for specifying both a day-of-week and a day-of-month value is not complete (you'll need to use the '?' character in one of these fields).

Overflowing ranges is supported - that is, having a larger number on the left hand side than the right. You might do 22-2 to catch 10 o'clock at night until 2 o'clock in the morning, or you might have NOV-FEB. It is very important to note that overuse of overflowing ranges creates ranges that might not make sense.

Record Owner

A list of Record Owners can be setup in RSD GLASS Governance Manager. The Record Owner is used in RSD GLASS Governance Manager when creating a new Record entry, File Plan or Folder, for example.

Creating new Record Owners

- From the Settings menu, select the Owner menu option.
- A list of previously created 'Owners' is displayed at the top of the screen.
- Setup the rule to define the new Owner from the User, Group and Role selection boxes.
  You may specify either, a User, a Role or a Group. You may also specify a Role and a Group at the same time, but it should be noted that a user must be part of both Role and Group lists to be considered an Owner.

Legal Cases

The Legal Case sets the perimeter for disposal holds that can be set on Record Classes, RC Categories, Folders, Records and Components. See "Managing Legal Cases" on page 42 for a description of the Legal Case functionality.

Creating Legal Cases and Legal Holds

- From the Settings menu, select the Legal Cases menu option.
- In order to be able to set a litigation hold on an element in your File Plan, you need to setup 'Legal Cases' that must contain one or more 'Legal Holds'. "Managing Legal Cases" on page 42 describes the various aspects of Legal Case and Hold creation.

Integration Tools

Various tools are available in the RSD GLASS Governance Manager environment that facilitate the task of importing, exporting and moving content between repositories. The following list gives an overview of the functionality provided by these tools.

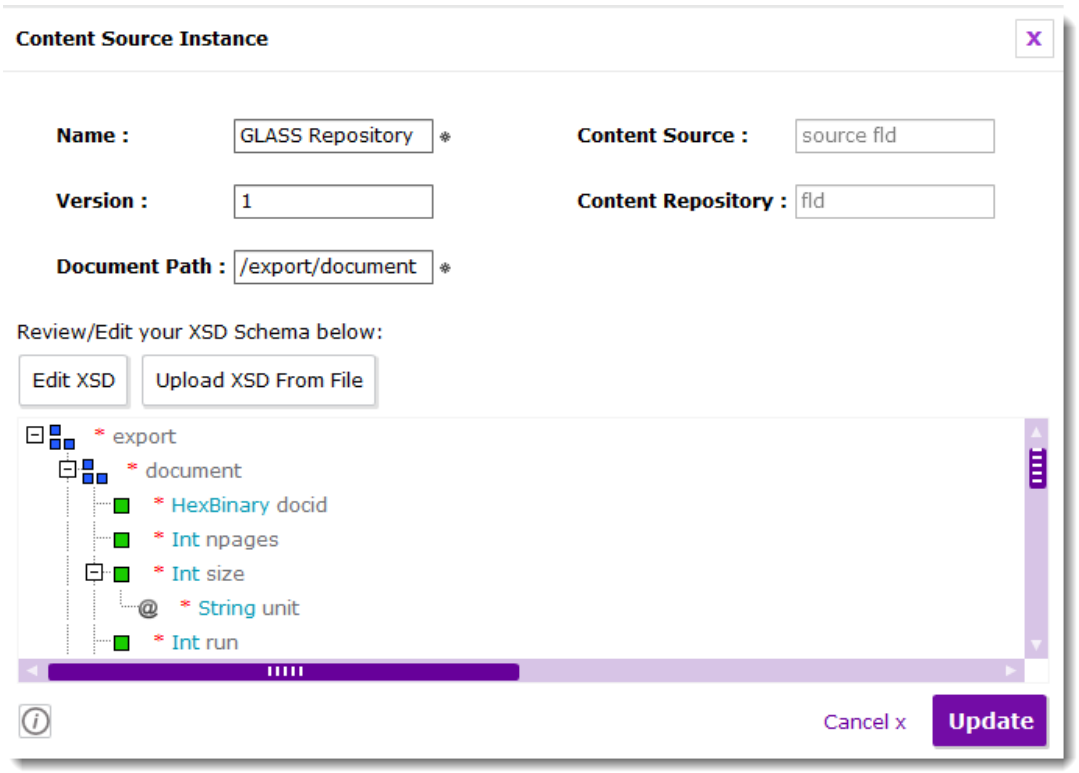
- "The 'Schema Manager' tool". Manages the data sources and the associated schema definitions for sets of documents stored in external content repositories.
- "The 'Mapping to RSD GLASS' tool". Used to map Metadata available in an external content repository to pre-existing Metadata defined in RSD GLASS. These mappings may be used either during the bulk import process, or, for example, when filing a new document from your ECM system interactively into RSD GLASS. This eases the import of information as you will not have to re-enter Metadata and can make use of existing information contained in the third party content repository. For example, the ‘invoice number’ in Sharepoint, seamlessly becomes the ‘invoice number in RSD GLASS.
- "Classification Rules". It is possible to create classification rules allowing you to pre-classify elements that will become Records: ‘Record Candidates’. These Rules may be used either during the bulk import process, or, for example, when filing a new document from your ECM system interactively into RSD GLASS. This can be inserted directly into the File Plan in the Record Class indicated in the rule or a choice of various record classes may be proposed where the user may select the required record class location.

- Import Simulation" Allows you to test and correct your mapping and classification rules on small example XML files before performing the bulk import process.
- "The 'RSD GLASS Mapping to Repository' tool". Used to map Metadata from RSD GLASS to an external content repository. Has two uses. The first use facilitates the upload of new documents from GLASS to an external repository. The second facilitates the move of content between external repositories, for example, between Sharepoint and RSD Folders. These mappings allow the end user not to have to worry about how to input system metadata, as, for example, when uploading content to an RSD Folders repository the Folder Type, Doc Type will be automatically filled in.

The 'Schema Manager' tool

Manages the data sources and associated XML schema definitions for sets of documents stored in external content repositories. This is used in the 'Mapping to RSD GLASS' and 'Classification Rules' functionality.

- From the Integration Tools menu, select the 'Schema Manager' menu item.
- To create new Content Sources: to the left of the screen select the name of the Content Repository you wish to associate to the Content Source from the dropdown box. Give the name you wish and select the 'Add' button.
- To add the schema to the Content Source, select the 'Add' button in the 'Content Source Instance creation form' to the right of the screen. The following screen allows you to configure the uploading or pasting of an XML schema definition to be used as the source. The metadata listed in the XSD file will be used as a reference for the creation of mappings and classification rules.
- The document path must be selected from one of the Metadata listed in the XSD file. It represents the looping XML element that qualifies the exported document. You are recommended to set the relevant one for bulk importing documents.

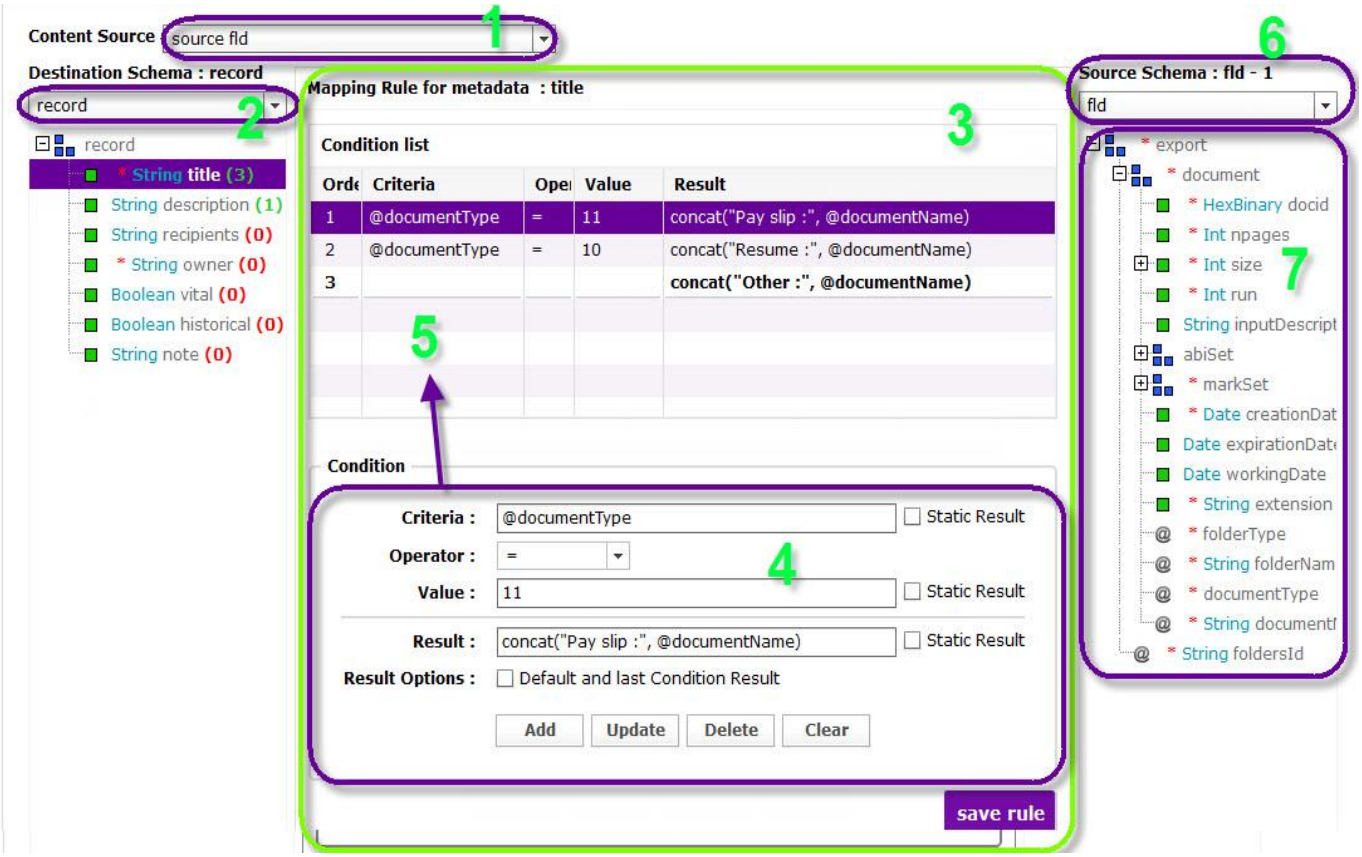


The 'Mapping to RSD GLASS' tool

Used to map RSD GLASS Metadata from an external content repository. Allows you to create mapping rules for each element of any File Plan that will be be used to feed business metadata.

The process uses the schemas created in the 'Schema Manager' tool for sources of data.

- From the Integration Tools menu, select the 'Mapping to RSD GLASS' menu item.



1 Content Source as defined in the 'Schema Manager'.

2 List of destination schema metadata for which rules need to be created. The destination schema to the left represents the *typable* metadata listed for a given group of properties. The metadata with a red star are mandatory within the group to be able to insert an entity qualified by this group. The number (X) indicates that the mapping rule for the metadata is made of X conditions.

Note that:

- If a group does not contain any *typable* Metadata it appears as empty.
- The following Metadata Groups are not displayed: Security, storagescale, volume, recordClass, workspace.

3 For each metadata there is only one rule to configure as described in this section.

4 The Condition form lets you create, update, remove the condition for the currently selected rule.

5 The Condition list shows the list of conditions for the rule. These conditions will be executed in sequential order. Once a condition is met, the value is used and the following conditions are ignored. Items may be moved up or down in the list by 'dragging and dropping' them in the desired order.

Argument	Explanation
Criteria	Text input field that may be generated dynamically from the value of the element selected from the 'source tree'.
Operator	Possible values: exists, = , !=, >, >=, <, <= , contains, starts-with, ends-with
Value	Text input field that may be generated dynamically from the value selected from the 'source Schema'. Equal to true if 'exists' operator is selected.
Results	Text input field that may be generated dynamically, or manually when the 'static result' option is checked.

6 Content Source schema as configured in the 'Schema Manager'.

7 Metadata displayed according to the source selected. The Criteria, Value and Result text input arguments of the Condition form may be filled in by drag and drop action from a metadata node value.

The 'RSD GLASS Mapping to Repository' tool

Used to export Metadata information from an RSD GLASS file plan to Metadata used in an external Content Repository.

When an RSD GLASS content needs to be moved or an upload to be performed, a mapping of metadata is needed to create the link between the destination content repository and the source RSD GLASS metadata from the File Plan.

The source schema on the right of the screen shows all existing metadata referenced by GLASS and sorted by File Plan.

The destination schema to the left represents the metadata listed for a given content repository where we wish to move or upload content. The metadata with a red star are mandatory to be able to have the content repository accept the move or upload of content.

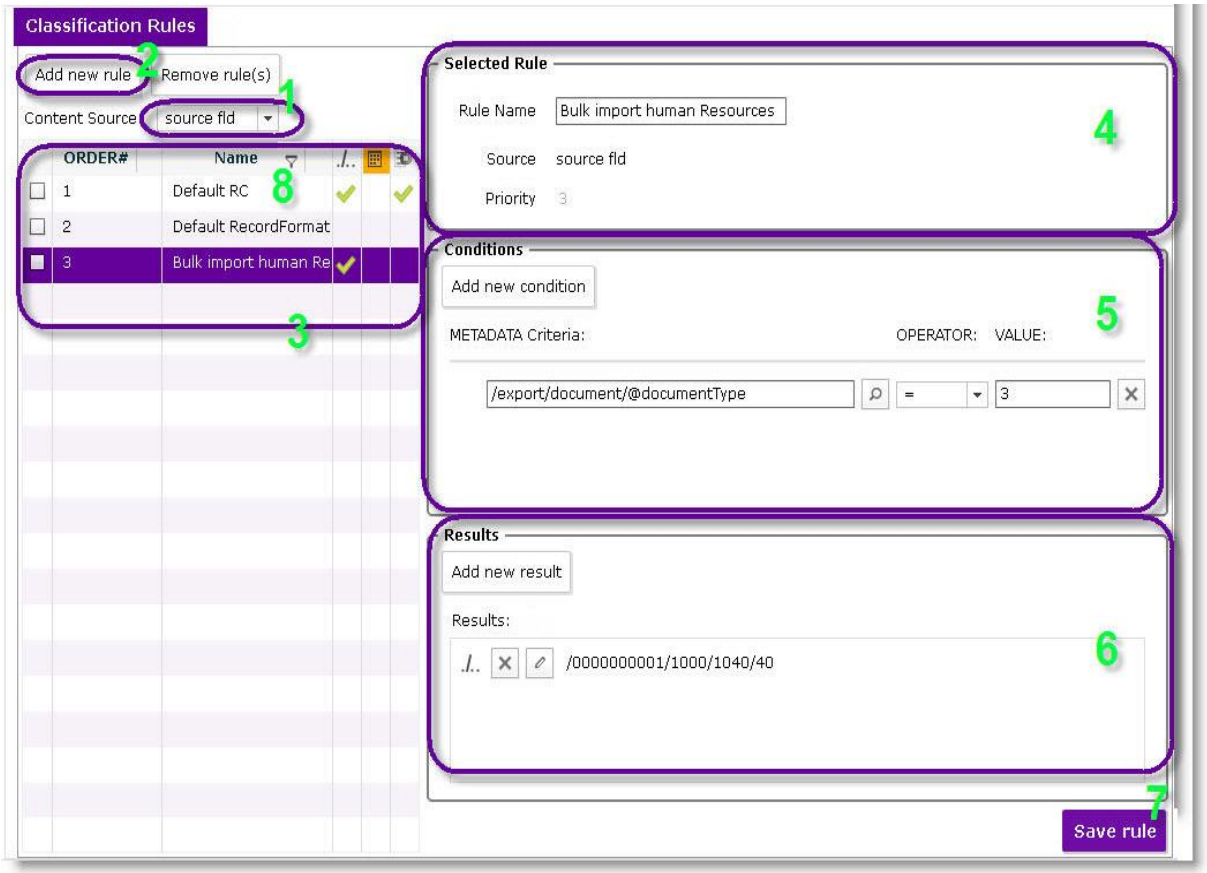
The 'Mapping to RSD GLASS' tool on page 7 contains an explanation of how to create the mapping rules.

Classification Rules

This tool allows you to setup, for each content repository in your environment, a set of automatic classification rules to be used when importing documents into your File Plan. These rules may be used either when performing the bulk import of documents using the RSD GLASS web services or when importing documents interactively or automatically from external ECM environments.

How to use the 'Classification Rules' Tool

- From the Integration Tools menu, select the 'Classification Rules' menu item described following.



1 From the dropdown list, select the name of the Content source environment where 'Record Candidates' will be created (using the Classification Rules you are setting up).

2 Select the 'Add new rule' button to initiate a new rule screen.

3 The list of previously created Classification Rules for the Content source selected above. Items may be moved up or down in the list by 'dragging and dropping' them in the desired order. To remove a Classification Rule, mark the checkbox to the left of the Rule and select the 'Remove rules" button above.

4 When naming a Classification Rule be sure to give a name relevant to its purpose.

5 The Condition list shows the list of metadata conditions for the rule. ALL conditions must be met in order for the rule to be executed. To see the list of metadata on which the condition may be set click on the button. Select the name of the Metadata from the list proposed, then set the details of the condition that must be met. In our example condition, in order for the rule to be executed the 'document type' metadata on the document must be '3'.

6 The Results list.

Note that if you are performing a bulk import using the RSD GLASS web services, only the first element in the results list will be used. If there are any other 'results' in the list they will be ignored. However, when using the Classification Rule to import a document from an external ECM environment, the Results list will be displayed in order for the user to select the location where the document will be sorted.

Full qualified code	Either directly in File Plan by selecting the Full Qualified Code of the location, or by using metadata to place manually.
Date	Date of the Record that enables the selection of the suitable version of the Record Class. Default value: current date
Record Format	The record format. Default value: ERCD (Electronic Record)

Both the date and Record format are either entered manually or composed using Metadata.

Note that a classification rule is made up of the three different results types (a full qualified code, a date and a record type). Different rules may be created to specify any of the three results types and these rules will then be processed together to generate a classification rule. Furthermore, if the 'date' and 'record format' result types are not set the default values will be used.

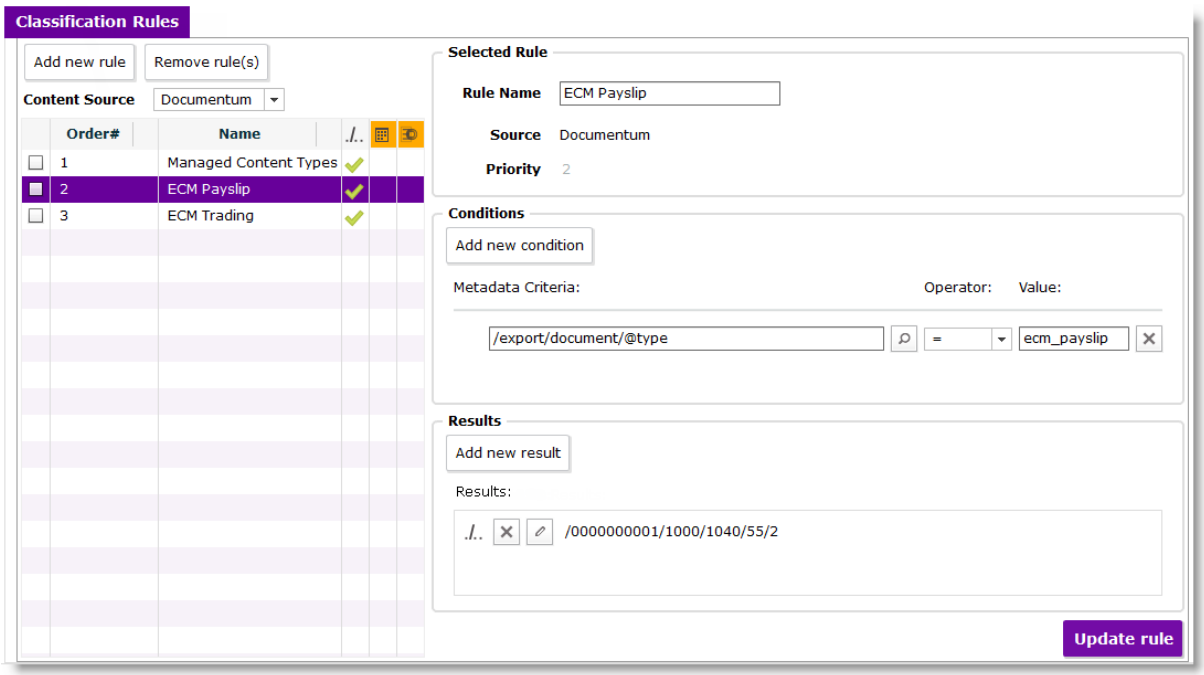
7 Once you have configured the required settings for the classification rule, you may save it by selecting the 'save rule' button.

8 The filter button may be used to search and sort for elements contained in the field. "Filtering list data" on page 10.

Classification Rule examples

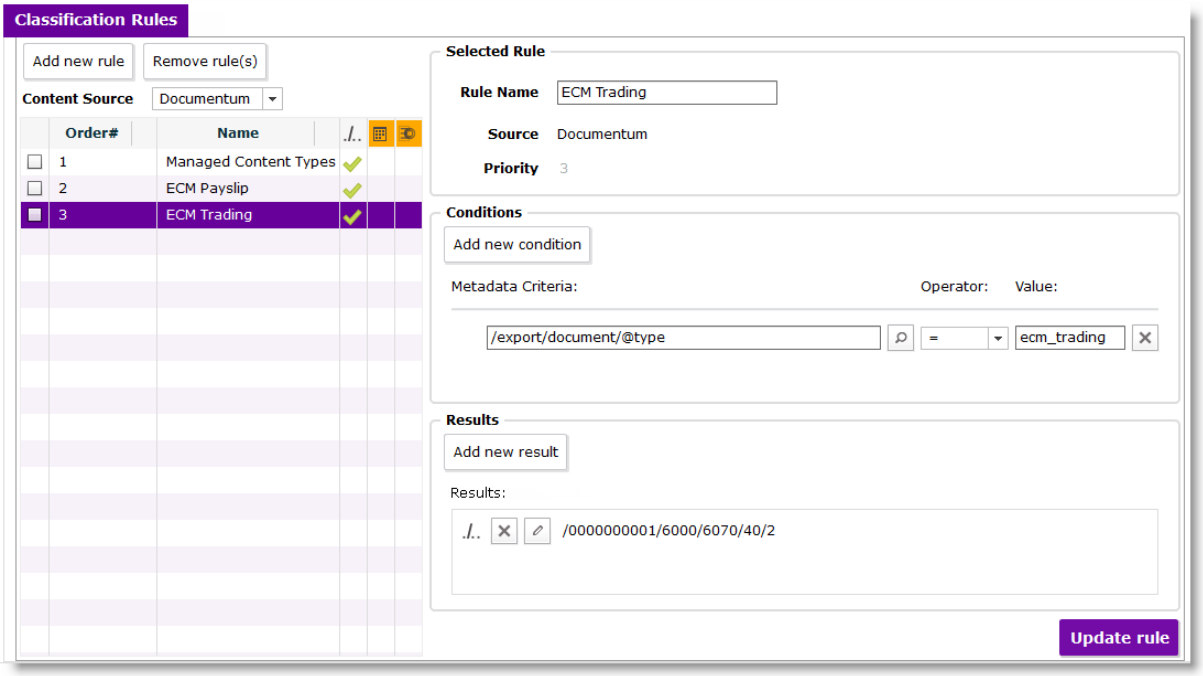
The following simple example illustrates how certain types of documents stored in a Documentum repository may be classified in your File Plan. The following screen shows the classification rule necessary to file 'ecm_payslip' Documentum documents in the HR > Payslip Record Class. A second rule files 'ecm_trading' documents into the Investment > Trade Records Record Class.

Example 1



- Select the Documentum Repository from the drop down box
- Create a new Rule with the Rule Name "ECM Payslip"
- Create the Condition by selecting METADATA Criteria /export/document/@type using the criteria picker, OPERATOR '=', VALUE 'ecm_payslip'
- Define a new Result by selecting 00000000001/1000/1040/55/2 using the result picker. This corresponds the the HR > Payslip Record Class. The type is 'Full Qualified Code' and by 'File Plan'.
- Save the Rule
- Repeat for the second Classification Rule example: Name 'ECM Trading' with the Condition VALUE 'ecm_trading'. The same results settings should be set for the /0000000001/6000/6070/40/2 (Investment>Trade Records>Trade Records) Record Class.

Example 2



Import Simulation

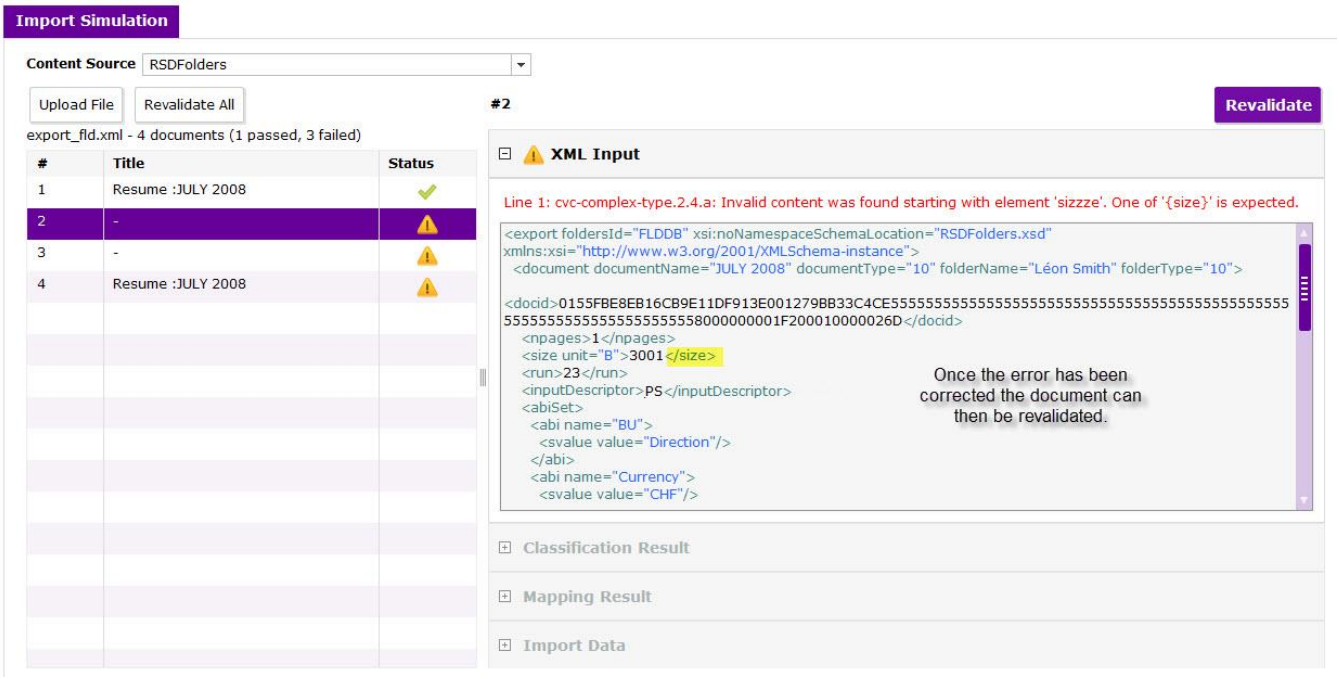
Once you have setup your 'Mapping to RSD GLASS' and 'Classification Rules' as explained above, this 'Import Simulation' tool allows you to test and at the same time correct your mapping and classification rules on small example XML files. The process is as follows:

- Select the Content source.
- Upload the XML file.
- Correct errors.
- Revalidate corrected entries.
- Once all errors are corrected you will be able to perform the bulk import process.

The following example shows the list, to the left, of four example documents uploaded in the XML file for simulation purposes. The four documents uploaded are listed to the left of the screen and the last three contain errors. The second document in the list contains an error in the XML input entry. Once the error is corrected it can be 'revalidated' and the Status of the document changes to .

The panel to the right of the screen displays the four different areas where potential errors need addressing.

Note that in order to correct Classification and Mapping Result errors, you may switch between the 'Mapping to RSD GLASS' and 'Classification Rules' menu entries and correct the settings.



Batch Management

Batch jobs are processes (either importing records or re-indexing data) that are grouped and run automatically at given times during the day. The Batch management tools allow you to oversee the progress of the two different types of batch jobs possible in the RSD GLASS Governance Manager environment:

- "Batch Import Jobs"
- "Batch Re-indexing Jobs"

Batch Import Jobs

- From the Settings - Batch Management menu, select the 'Import Batch Jobs' menu item. A list of the last actions or execution of each job is displayed.

  The bottom of the screen gives an overview, including a pie chart, of the status of the total amount of jobs in the list.

  By selecting the ⓘ button in the Action column you may display the details of this execution of a particular job.

  The following sections describe the four tabs available from the details screen.

Note that the Bulk Import process is described in depth in the following manuals:

- the RSD GLASS 'Operations Guide' ('Bulk Import' section);
- the RSD GLASS Governance Services 'Management Guide and Technical Reference' for the related connector ('Bulk export' or 'Information referencing' sections).

Job steps

Lists details of the various steps that might have been executed in the job.

Created nodes

Displays details and number of nodes that may have been created in the file plan when the document was imported.

If, for example, you wish to remove nodes that have been created incorrectly or to start the import job from scratch, you may select the 'Delete created nodes'.

Import document

Gives details of the document being imported, displayed in XML format. This document may be edited (and saved) in order to, for example, correct any errors or add missing obligatory information. Once this has been done, you may simulate the execution of the import to ensure that it is correct.

Simulation

The simulation process allows you to simulate what might have gone wrong in each sequence. Once you have seen the details of the potential errors it is possible to edit and save in the 'Import document' tab.

For example, if a document has a missing obligatory salary metadata, it would be possible to insert the salary information by hand then verify that the added information is correct by performing a simulation. Once this correction and simulation have been performed you may reschedule the bulk import command line procedure to recover the missing document.

Batch Re-indexing Jobs

- From the Settings - Batch Management menu, select the 'Batch Re-indexing Jobs' menu item. A list of the last actions or execution of each job is displayed.

  The bottom of the screen gives an overview, including a pie chart, of the status of the total amount of jobs in the list.

  By selecting the  button in the Action column you may display the details of this execution of a particular job.

  The following section describes the tab available from the details screen.

Job steps

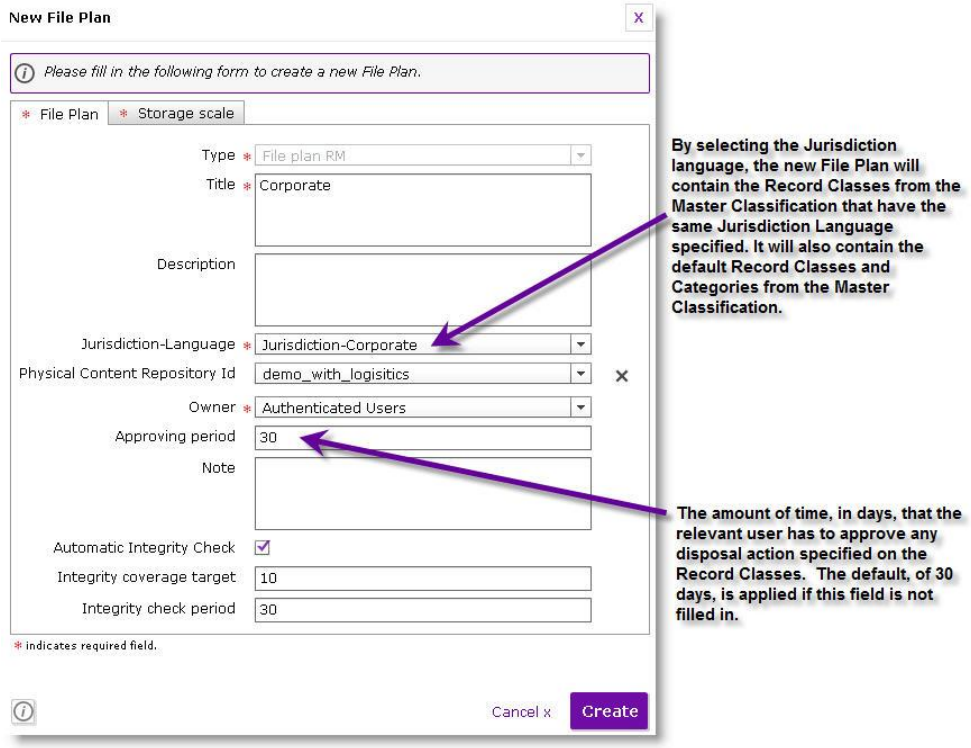
Lists details of the various steps that might have been executed in the job.

File Plan Creation

See "What is a File Plan?" on page 7 for a description of File Plans.

There are two methods of creating a new File Plan either: from the home screen, or from the File Plan Menu by selecting the 'New File Plan' option

Fill in the desired information in the New File Plan screen and click on the 'Create' button to confirm your choices:



Once the new File Plan has been created it is displayed to the right of the Master Classification that it is based upon. The File Plan contains the default Record Classes and Categories from the Master Classification. For information on how to setup and manage your newly created File Plan, see "Managing your File Plan" on page 31.

Storage scale tab

Allows you to configure a list of one or more Content Repositories where the File Plan may reside along with the storage scale that you wish to use in connection with this Content Repository. This enables you to fine tune the management of storage space in your enterprise environment.

Integrity check settings

"Managing the Integrity of information stored in your RSD GLASS environment" on page 44 describes the process of verifying that components in your File Plan remain unchanged. To be able to perform automatic checks these three options need to be configured on File Plan creation (or later by editing the Metadata of the File Plan).

The Content Repository where the data resides needs to be correctly configured to enable the automatic integrity check service. This service needs to be set on the Virtual content repository or repositories used to store data. For more information, see "Virtual Repository definition" on page 15.

The 'Integrity coverage target' is the percentage of the components in the File Plan to be covered by the integrity check during the number of days specified in the 'Integrity check period' box. In the screen example above, 10% of components in the File Plan will be checked over a period of 30 days.

Business View Creation

See "What is a Business View?" on page 8 for a description of Business Views.

How to setup Business Views

- As a Business View is a different way of displaying information in a File Plan, you need to open the File Plan that you wish to use as the basis for your new Business View.
- From the Business View menu, select the New Business View menu.
- Fill in the desired fields and click on the 'Create' button to confirm your choices. Note that the Classification code is automatically filled in using information from the Title field. This may be overwritten.

For information on how to setup and manage your newly created Business View, see "Managing your Business View" on page 35.

Working with RSD GLASS Governance Manager

Topics covered:

Browsing or Editing?

There are two ways of working with your File Plans or Business Views in RSD GLASS Governance Manager: either in the Browse or Edit Modes.

The Editing mode enables you to manage your File Plan (or Business View) in order to define the Record Classes it should contain and to configure who can access it. This is described in the section Managing your File Plan, below.

The Browsing mode allows the authorized users to navigate the File Plan, search for Metadata and Record content, as well as performing such actions as editing or adding of Metadata, performing legal hold on Records, adding new Records or Folders.

When initially opening RSD GLASS Governance Manager the user finds himself by default in the Browse mode. All of the functionality described above and provided in this Browse mode is covered by the application RSD GLASS client and is documented in the RSD GLASS client - User Guide.

How to browse or edit a File Plan or Business View

- Access a File Plan in 'edit' mode by selecting the 'Edit' item from the File Plan menu.
- Access a File Plan in 'browse' mode by selecting the 'Browse' item from the File Plan menu.
- Access a Business View in 'browse' mode by opening it in the RSD GLASS client interface.
- Access a Business View in 'edit' mode by selecting the 'Edit Business View' item from the Business View menu.

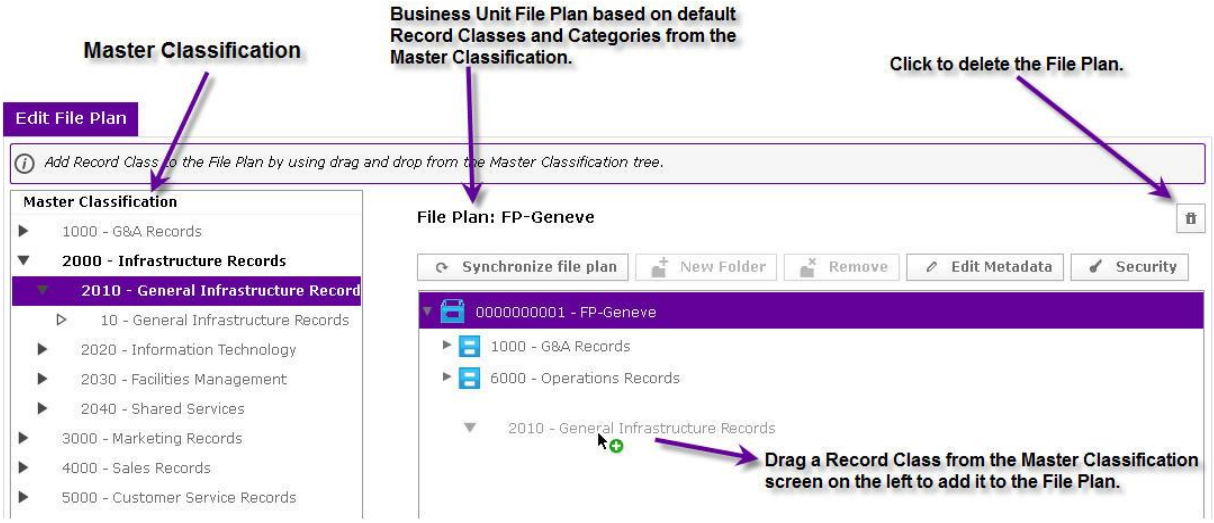
Note that it is not possible to 'browse' a Business View from the RSD GLASS Governance Manager interface, only from the RSD GLASS client interface.

Managing your File Plan

This section of the documentation describes the various elements involved in the management of the Business Unit File Plan. In order to do this you need to ensure that you are in the File Plan Edit mode of RSD GLASS Governance Manager.

Adding Record Class definitions

Additional Record Classes may be added to the File Plan from the Master Classification, according to the requirements of the Business Unit (as shown below).



Note, however, that is not possible to remove the default RCs from the File Plan.

Adding Folders

In order to add Folders to your File Plan you need to:

- Access the File Plan in 'edit' mode by selecting the Edit item from the File Plan menu.
- Select the level of the File Plan where you wish to add the Folder.
- Click on the 

button to display the 'Create New Folder' screen.
- The tabs and details to be completed for the new Folder depend on the Metadata options of the current node.

Editing metadata

In order to edit the Metadata details of your File Plan you need to:

- Access the File Plan in 'edit' mode by selecting the Edit item from the File Plan menu.
- Select the node where you wish to edit the Metadata.
- Click on the 

button to display the 'Metadata edition' screen.
- The tabs and details displayed depend on the Metadata options of the current node.

Refreshing/synchronizing your File Plan

When new versions of Record Classes have been generated, or new Record Formats have been created in the RSD GLASS Policy Manager application it is necessary to 'refresh' your File Plans to reflect the changes.

- Access the File Plan in 'edit' mode by selecting the Edit item from the File Plan menu.
- Click on the 

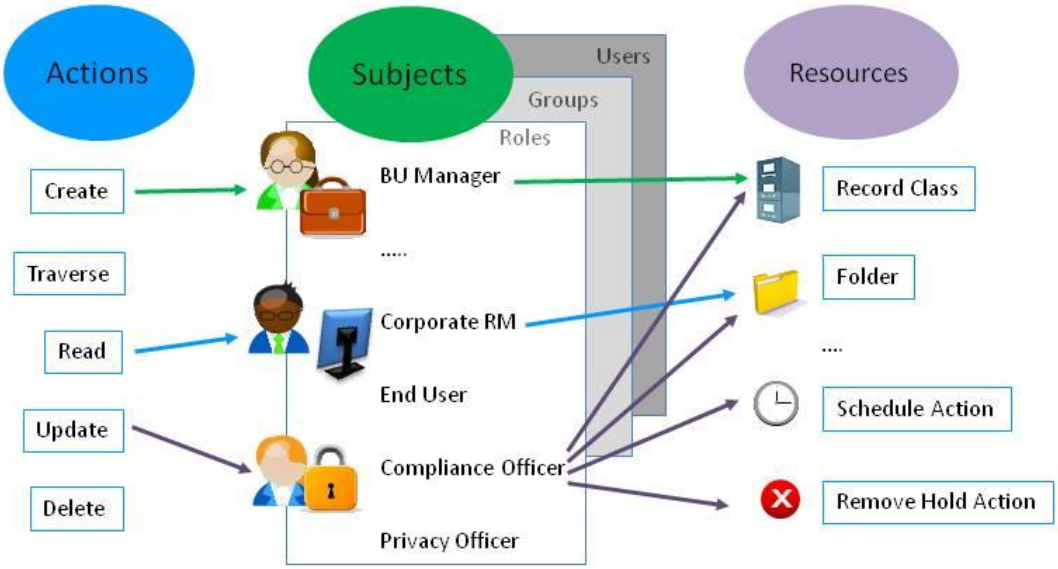
button to refresh the File Plan.

Security

Users are associated to specific roles depending on their business role in the enterprise. Initial access to all RSD GLASS applications and their functionality is configured in the RSD GLASS Admin Center tool.

Further security is added in Governance Manager by defining access control at all levels of the File Plan, from the File Plan itself down to the lowest Folder. It is performed by allowing or denying permission by subject, resource and by action type. See diagram below that illustrates the process.

A list of rules, called an Access Control List (ACL), is established that determine which subjects can perform which actions on which resources, at and under, the current node (as long as child node ACLs do not override them).



Managing Access Control Lists (ACL)

In order to manage rules contained in the ACL you need to:

- either

  (1) access the File Plan in 'edit' mode (to manage ACLs on the File Plan down to the Folder), or

  (2) access the File Plan in 'browse' mode (to manage ACLS on the Record or Component).
- Select the element that you wish to determine the access rules.
- Click on the Security button at the top of the File Plan tree to display the 'Manage ACL' screen. A list of previously defined rules is displayed.
- Either edit a rule or select the + Add Rule button to display the 'Rule Edition' screen.
- Select the 'Effect of the Rule' by selecting Allow or Deny.
- Specify the details of the Rule in the three tabs:

  Actions Select the Action that the users will be permitted to perform on the Resources. Select the button to apply the Rule to all actions or select from the list of Create, Traverse, Read, Update, Delete. Rules denying the action Traverse are used to limit any action on child nodes.

  Subjects Subjects are the users who will perform the Action. Select the button to apply the Rule to all Subjects or select from the list of Roles, Groups or Users depending on the granularity you desire in the access rights.

  Resources Resources are the elements that a user may request to perform an Action upon: the node, child node type, or node capability. For example, a child node type (Record Class, Folder, etc), the specific node the ACL is on (This Node), or a capability of the ACL's node or its child nodes (Hold action, etc). See the following list of all resources.

Resources and possible actions

Resource	create	read	update	delete	traverse
Business View	x	x	x	x	
Record Class	x	x	x	x	x
Folder	x	x	x	x	x
Record	x	x	x	x	x
Component	x	x	x	x	
Metadata	x	x	x	x	
ACL either/		x			
or	x	x	x	x	x
Hold Action	x			x (unhold)	
Open/Close Action	x (close)		x (open)		
Declare Action	x				
Trigger Action	x				
Schedule Action		x	x		
Execute Action	x				
This node	x	x	x	x	x
RM File Plan View		x			
Data Integrity			x		
Search settings		x	x		
Client settings	x	x	x	x	
Batch Job		x			
Record Date			x		
'Owner' Metadata			x		
Move action	x				
Declared Record				x	
Reclassification	x				
Box Withdrawal	x				
Business Item		x	x	x	

LegalCase/LegalHold resources and possible actions

Resource	create	read	update	delete	traverse
Legal Hold	x	x	x	x	
ACL either/		x			
or	x	x	x	x	x
Hold Action	x				
Close Action	x				
This node	x	x	x	x	

Note: If no rules match for a legal hold ACL, the legal case ACL will be used.

ACL evaluation rules

The following conditions must be met in order for an authenticated user to perform an action on a resource:

1. Using RSD GLASS Admin Center, the type of the requested resource must be permitted for the subject's role and the module of the requested resource in Policy Manager.

2. The Action TRAVERSE must be permitted on all parent ACLS, if there are any. In other words, for the resource on which you want to control the access, the action TRAVERSE must not be denied on any of the parent node ACLs.

3. For Records and Components only in Governance Manager and GLASS client, the Policy Manager RC security metadata (if any) must match that of the resource. To reach a permitted component, its parent record must be permitted.

4. ACL rule evaluation. The rules are automatically split into deny/permit rules for: users, groups, roles, any subject; and evaluated in the following order:

Rules for:

deny owner, permit owner

deny users, permit users,

deny groups, permit groups,

deny roles, permit roles (an optional condition on the group may be defined),

deny any subject, permit any subject

If no particular rule matches for a given ACL, the ACLs of the parent nodes will be evaluated in order from child to parent until a matching rule is found.

The result (Permit or Deny) of the matching rule is used only if the other controls do not evaluate to deny. If no matching rule is found in any ACL, access is denied.

Managing your Business View

This section of the documentation describes the various elements involved in the management of the Business View. In order to do this you need to ensure that you are in the Business View Edit mode of RSD GLASS Governance Manager.

A Business View is able to reference Record Classes from only one File Plan. A Business View can be made of one or more Record Classes related to one or more activities. It can be used to rapidly access working documents and would typically contain a few bottom level Record Classes or even just a number of folders with frequently consulted information.

A Business View has its own set of access rights: permissions are inherited from File Plan but you can reduce the scope of these inherited permissions.

It is possible to add folders to a Business View that can be used to aggregate and organize Records of different sources. Records can be grouped from different Record Classes by using a metadata. If a folder is described by a distinctive metadata, for example, then the value can be used to regroup Record and Folder entries. This way a Business View may group Records having the same distinctive metadata value. e.g. an employee ID number metadata may be used to sort all information on one specific employee.

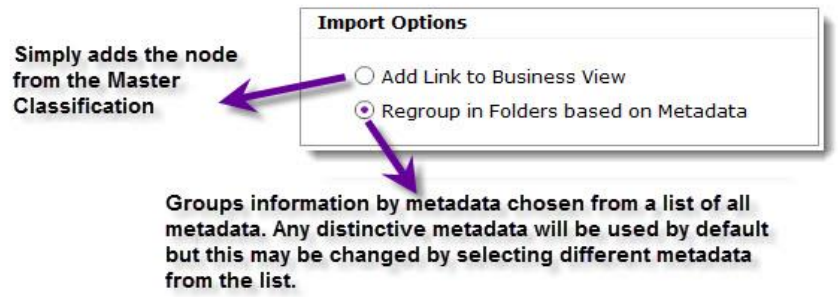
Adding Record Class definitions

Once a Business View has been created, Record Classes need to be added from the File Plan to the Business View, according to the requirements of the department or team who will be using it.

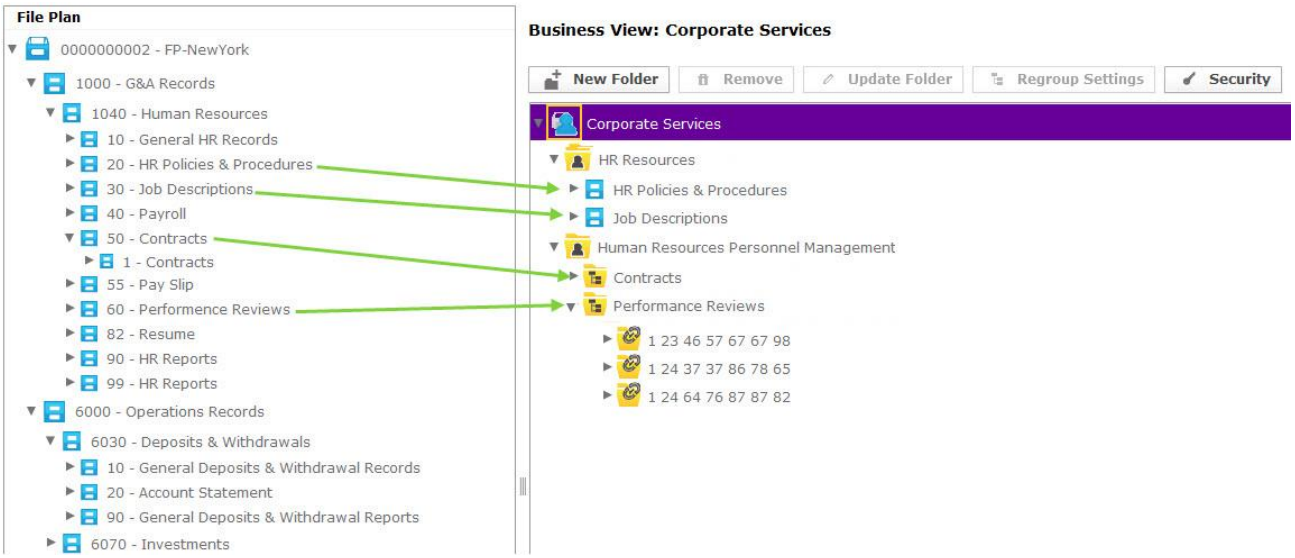
Drag Record Classes from the File Plan on the left of the screen to the Business View on the right ensuring to select the required 'import options' to determine how the Record Class information is displayed in the Business View.

These 'import options' allow you to select if information is grouped into a certain folder structure.

Import options when adding Record Classes to a Business View



If using the **'Regroup in Folders based on Metadata'** option, values used in metadata are used to group information in a folder. You will be prompted to select the metadata options that will be used to create these business folders. If there are any distinctive metadata, they will be selected by default but can be changed. For example if an employee ID number is used as distinctive metadata a folder will be created using his ID number and will contain all the Records in the Record Class with the same distinctive metadata.



Business Folder types

- Folder already existing in the File Plan and dragged over the Business View as is.
- Created using the 'New Folder' button, as explained below.
- Created using 'Regroup in Folders based on Metadata' import option.
- Folder created automatically from Metadata, in the example above the Metadata is the employee ID number.
- Created using the 'Add link to Business View' import option.

Adding Folders

In order to add Folders to your Business View you need to:

- Access the Business View in 'edit' mode by selecting the Edit item from the Business View menu.
- Select the level of the Business View where you wish to add the Folder making sure that it is below the root level of the Business View.
- Click on the 

button to display the 'Create New Folder' screen.
- The tabs and details to be completed for the new Folder depend on the Metadata options of the current node.

Managing Information Lifecycle

RSD GLASS Governance Manager automatically identifies information and Records eligible for lifecycle rules such as disposal, declassification, deletion of search index, etc.

The Record lifecycle is managed automatically by deleting eligible Records:

- for which disposition is set to automatically destroy in RSD GLASS Policy Manager,
- that are marked for destruction by disposition authority following the execution of the Record Disposition process.

Metadata lifecycle is managed through the automatic deletion of Metadata Groups at the different stages of the Record lifecycle whilst at the same time including the possibility to keep Metadata at the Record disposition stage.

Governance Manager covers the Security lifecycle by automatically:

- declassifying (or downgrading) elements,
- transferring and expunging declassified elements from the repository.

The following sections describe the functionality that oversees this information lifecycle management.

Scheduled Actions

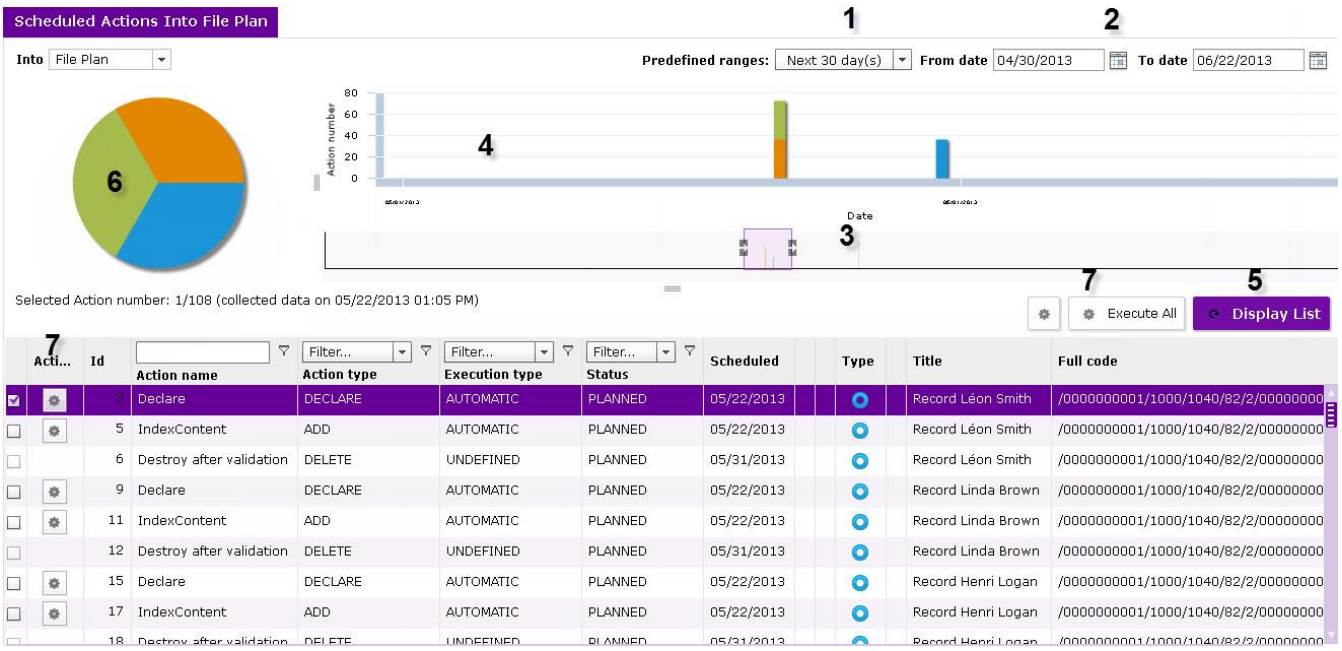
Following the occurrence of business events, ILM events are triggered automatically either through integration between business applications and the RSD GLASS environment or through events triggered automatically through the RSD GLASS Governance Manager scheduler. These business events trigger the Lifecycle Actions that are scheduled to be performed on information and Records in your environment.

The RSD GLASS Governance Manager interface provides a list of these scheduled actions. This list can be used to monitor the correct functioning of the enterprise IG policies.

How to access the list of Scheduled Actions

- From the Lifecycle Management menu, select the Scheduled Actions menu.

The Scheduled Actions screen



Working with the Scheduled Actions interface

1. Select the date range of the scheduled actions you wish to monitor either
   - from the dropdown 'Predefined ranges' list (1 in diagram, above), for example, 'Next 30 days', or
   - using the calendar tool (2 in diagram, above) to specify a 'From date' and a 'To date', or
   - using the sliding ruler (3 in diagram, above) to increase or reduce the date range.

   The bar chart (4 in diagram, above) displays the number of actions per day during the date range selected.
2. Click on the 'Display list' button (5 in diagram, above) to populate the list below which will display details of actions that have or will have taken place during the date range specified in the previous step.

   The pie chart (6 in diagram, above) displays the number of actions during the period sorted by 'Action name'. One of the pie sections might show, for example, that there are eight 'Destroy after validation' actions to be carried out during the next 30 days (displayed as a percentage of the total number of actions to be performed during this period).

Once the list is populated it is possible to execute any of the actions that should have taken place in the past and for some reason had not been executed, maybe due to a litigation hold, for example. To do so, tick the select box in to the left of the action you wish to execute - then click on the 'Execute' button (see 7 in diagram, above). Alternatively, execute individual scheduled actions by selecting the 'Execute' button in the 'Action' column of each scheduled action.

Scheduled Actions Execution

A results-based view of the scheduled Actions is available for consultation and possible execution.

- From the Lifecycle Management menu, select the Scheduled Actions Execution menu option.

The top of the screen displays statistics that are generated at a scheduled moment during the day as configured using the Scheduler functionality. These statistics display, for a predefined number of periods of time - the last seven days, for example - the number of scheduled actions in their various states (suceeded, in error, etc).

Note that the list may be empty if the statistics scheduler job has never been run.

 Selecting this button displays a list below giving you quick access to its contents. It should be noted that the figures in the bottom list are given in real-time and may differ to those in the precalculated list at the top of the screen.

 Allows you to execute, one by one in the list, all the actions that are scheduled.

Triggering Events manually

Even if the majority of events and actions are scheduled to take place automatically, the RSD GLASS Governance Manager interface provides a way of manually triggering business events that in turn launch the scheduling of actions to be performed on affected Records.

How to trigger events

- From the Lifecycle Management tab, select the Trigger Event menu option.

A dropdown list displays the possible events that may be triggered. All events will have fields that need information in order to be triggered. In an example where the event to be triggered is the moment an employee leaves the company, then you might need to provide the employee ID number.

Once the event has been triggered a list of a hundred possible Actions that are scheduled to take place will be displayed.

If you tick the 'Simulation mode' tick box before triggering the event, the list displays the actions that *would* be scheduled to take place (if not in simulation mode).

Viewing events that have been triggered

It is possible to view a list of events that have already been triggered. This history of triggered events is filtered according to the Event Type. The list displayed may be sorted, for example, according to one of the three possible event statuses: Suceeded, Failed and Pending.

How to trigger events

- From the Lifecycle Management menu, select the Trigger Events Results menu option. From the 'List of Events' dropdown box, select the Event Type that you wish to display.

Approval Actions

The RSD GLASS Governance Manager interface provides a to-do list of Actions that the logged in user is required to perform. For example, a Security Officer might need to approve the declassification of a security level on a certain set of Records.

How to approve Actions

- From the Lifecycle Management tab, select the Approval Actions menu option.

The list displayed contains the Actions for which the logged in user is required to provide their approval.

When selecting an Action it is possible to:

Approve	Once the Action is approved it no longer appears in the list.
Review	Review the selected Actions and possibly define a new review date and review action.
Pause	Indefinitely.
Resume	Resumes a previously Paused Action and approves the Action.
Hold	Perform a legal Hold on the element.

Initiate Approval Process

The RSD GLASS Governance Manager interface provides a way of manually starting the Approval Process in the event that it is not initiated automatically.

How to initiate the approval process

- From the Lifecycle Management tab, select the Initiate Approval Process menu option.

Once the Approval Process has been initiated a list of Approval Actions that need to be performed will be displayed.

If you tick the 'Simulation mode' tick box before initiating the approval process, the list displays the Approval Actions that *would* be scheduled to take place (if not in simulation mode).

Moving the contents of your RSD GLASS environment

Documents associated to Records may be moved as part of their potentially decades-long lifespan across several content repositories. This moving process is achieved through the configuration of system Metadata on the File Plan, Record Class or Folder elements. These Metadata settings, along with the Lifecycle choices set when Record Classes are created, allow you to define how content is moved according to the milestones reached along its lifespan.

Managed content may be migrated at a given period of time to a different supported content repository as organizations want and need to consolidate content declared as records out of their production systems and into stable, scalable and economical archives.

Various scenarios can be imagined along the lifespan of a document where a change of stockage might be needed. For example, when:

- an employee retires, all the employee related documents be moved to an archive repository;

- ten years after their creation, record related documents be moved to a less expensive archive repository;

- decommissioning a given content repository that generates a need to move content to another system;

- automated business processes of content items associated to RSD GLASS records should be moved to another business application.

How to move content

In order to setup your RSD GLASS environment to be able to move content, it is necessary to perform the following steps.

1. In the RSD GLASS Policy Manager that is the basis for your File Plans and Business Views, you need to ensure that the Storage Level Metadata is correctly setup. This Storage Level Metadata needs to be configured to reflect the different levels of storage that are used in our RSD GLASS environment. A set of enumeration values between 0 and 999 may be used to reflect the different phases that a document may be moved through during its lifecycle.
   - From the RSD GLASS Policy Manager interface select the Tools / Metadata menu option.
   - Select the predefined system Metadata called 'Storage Level'.
   - Select the link to 'Enumeration values defintion'. This is where you need to specify the levels of storage for each potential phase in the lifecycle of documents in your RSD GLASS environment. These levels will be used by the Lifecycle Action 'Move' that will use a Metadata value to define where content will be moved. Content will be uploaded to the content repository tied to the highest storage level. A default value needs to be selected from the levels specified.

     For example:

     999 -> on-line local fast storage
     500 -> near-line bulk storage
     0 -> archive
2. Now that the Storage Level Metadata structure has been put in place, a set of Lifecycle Actions have to be created that correspond to the move to the different storage levels phases used in the Storage Level Metadata. For example, to move content from on-line local fast storage to near-line bulk storage. A 'Move' Action can also be configured without a specified storage level. The value of the storage level will be decremented by 1 (until it reaches 0).
   - From the RSD GLASS Policy Manager interface select the Tools / Lifecycle Action menu option.
   - Create a new Lifecycle Action of Type 'Move' and select the Storage Level Metadata options for the move you wish to create. Following our previous example, you would select the 'near-line bulk storage' as you wish to move content from online local fast storage to near-line bulk storage. For more information on the creation of Lifecycle Actions, see the RSD GLASS Policy Manager User Guide.

     Repeat this step for all the storage level moves required in your environment.
3. The lifecycle defined on Record Classes should now be configured to make use of the Lifecycle Action used on Content.
   - From the RSD GLASS Policy Manager interface, when creating Record Classes, particular attention should be taken when setting up the Lifecycle rules in the Lifecycle tab of the Record Class.
   - Ensure to configure the Action that corresponds to the move you wish to setup, for example the option that moves content from on-line local fast storage to near-line bulk storage.

     See the RSD GLASS Policy Manager User Guide for more information on the creation and setup of Record Classes.

   This now concludes the setup needed in the RSD GLASS Policy Manager. The following functionality continues in the RSD GLASS Governance Manager.
4. At this stage you need to configure the storage options for your File Plan, Record Classes and Folders.
   - From the RSD GLASS Governance Manager or RSD GLASS client interface, select the File Plan, Record Class or Folder that you wish to configure.
   - From the Metadata accordion on the right of the screen, select the Edit Metadata option and select the Storage Scale tab.
   - As described in the RSD GLASS client User Guide ('Defining where information is stored' section), specify the details for each Storage level on the dedicated content repository.

Once these four steps have been put into place, the combination of Storage Level settings and Lifecycle Actions will automatically move content at the various milestones in the lifespan of information. These moves may be checked and overseen through the Lifecycle Management menu using the Scheduled Actions functionality.

Over and above this programmed automatic move that is part of the contents legal lifecycle, it is possible using a set of web services to move content between different content repositories. This move functionality is performed by the product administrator, for example, when decommissioning a content repository and setting up a new environment. These web services are described in the Public WebServices Reference Guide.

Managing Legal Cases

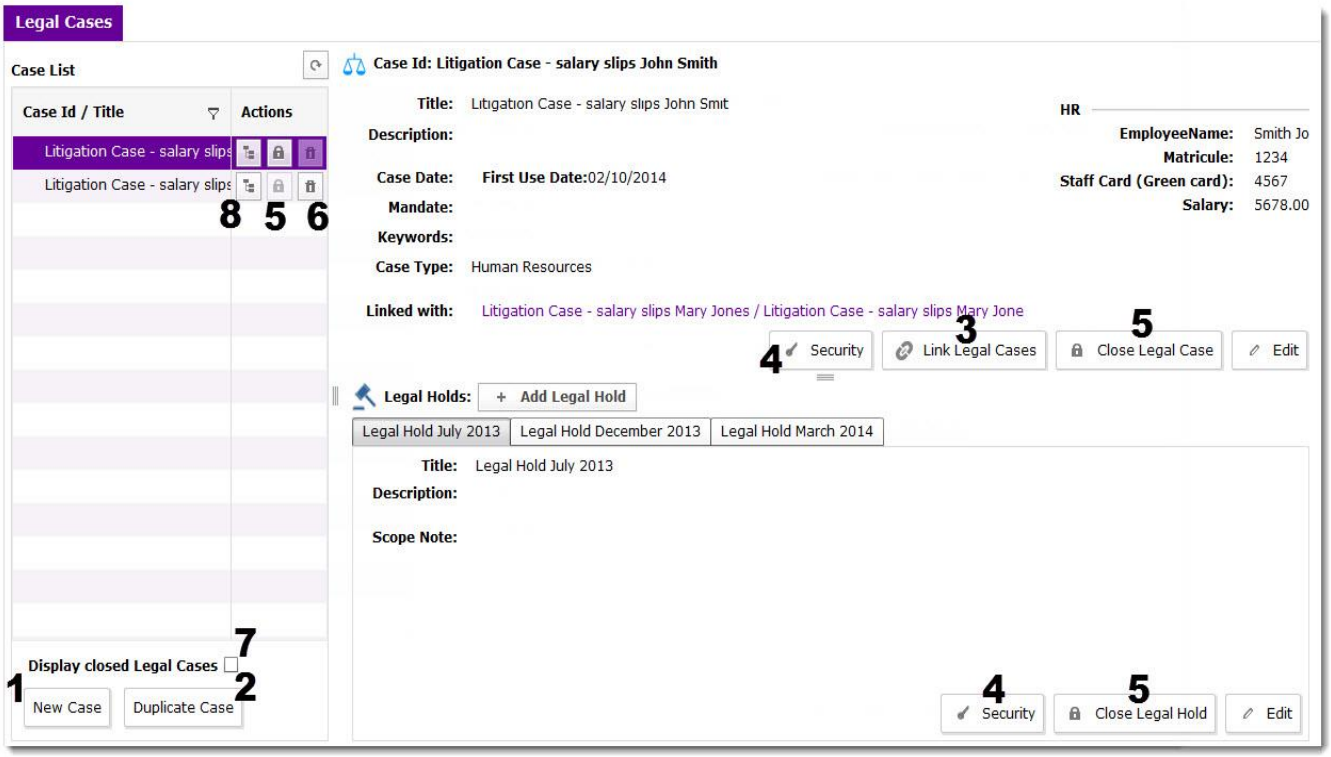
The Legal Case sets the perimeter for disposal holds that can be set on Record Classes, RC Categories, Folders, Records and Components. Disposal holds are an important and necessary part of modern records management. A hold is a legal or other administrative order that interrupts the normal disposal process and prevents the destruction of some of an organisation's records while the disposal hold is in place.

Where the hold is associated with a record individually it prevents the destruction of that record while the hold remains active. Once the disposal hold is released the record's disposal process continues.

Where the hold is associated with a Record Class, Category or Folder it prevents any element that it may contain, or that is a descendant, from being destroyed. This applies equally to new elements that are added after the hold has already been associated with the Class, Category or Folder.

For example a Legal Case might be setup to hold all the salary slips of a particular employee during a certain litigation period.

The following screen shows the Settings / Legal Cases menu option. The different functionalities it contains are numbered and described in the following sections.

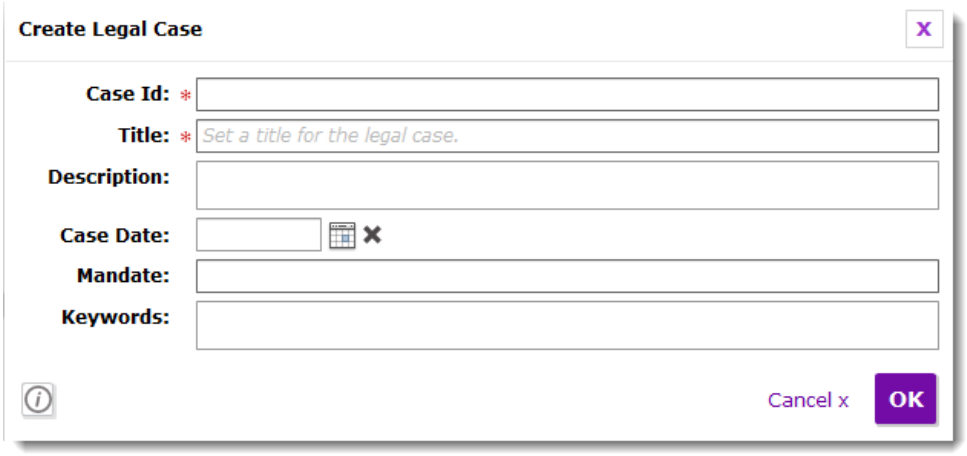


1. Creating Legal Cases and Legal Holds

When Creating a new Legal Case you will initially be prompted to select the name of the Type of Legal Case you wish to setup. Typical examples of Legal case types might be: Appeal cases, Bankruptcy cases, Class action cases, Copyright/trademark cases, Criminal cases, Custody cases, Divorce cases, Environmental cases, Foreclosure cases, Fraud cases, Gender equality cases, Patent infringement cases, Worker's Compensation cases, Workplace harassment cases, Tax Audits and Disputes.

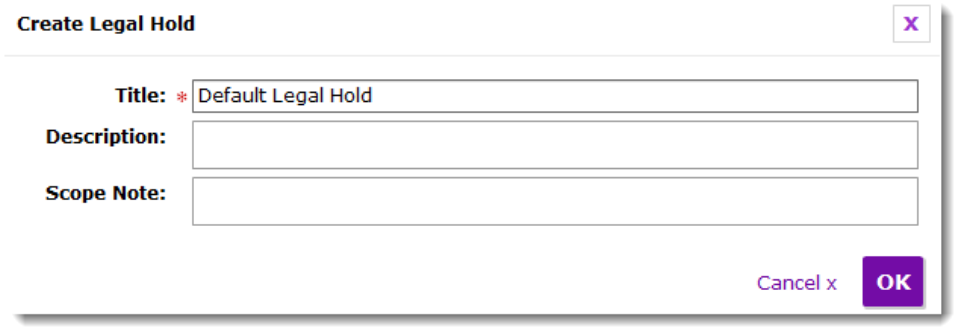
Note that these Legal Case Types are defined in the RSD GLASS Policy Manager application that your File Plan or Business View is based upon.

You will then have to complete the arguments that describe the case along with a mandatory Case ID and Title:



Note that there may also be additional metadata fields to be filled in. These supplementary metadata fields are according to the Legal Case Type upon which the Case is based.

After supplying details on the Legal Case, you will then be prompted to create at least one Legal Hold within the Legal Case.



Once the Legal Case has been created, you will be able to add extra Legal Holds to the Case by selecting the 

button. Hold names within a Case must be unique.

A Case always needs to contain a Hold for it to be able to be assigned.

2. Duplicating a Legal case

A duplicate Legal case may be created that is based on an existing Case but with a new unique Case ID. Any ACL security settings are not duplicated.

3. Linking Legal Cases

It is possible to link Legal Cases in order to be able to easily browse and navigate between related subjects.

4. Assigning security to a Legal Case and Legal Hold

ACL security settings determine who is able to administrate and access cases so that the case can only be managed be those with the correct clearance or competencies. "Security" on page 32 for an explanation of how to manage the Security options.

Business users should not necessarily be aware of any litigation in process. Therefore without the correct security settings a user will not even be able to see that a hold has been set on an element.

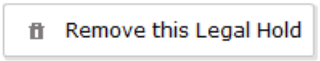
5. Closing a Legal Case and Legal Hold

When you close a case, the holds it contains will be closed too and all related items will be released.

6. Deleting a Legal Case and Legal Hold

It is possible to delete a Legal case when it has not been used, in other words none of the Legal Holds its contains has ever been associated to an element.

Equally, any Holds other than the initially created default Hold may be removed if they have never been associated to an element.



7. Displaying Closed Legal Cases

When you close a Legal Case it remains visible for consultation and the elements it contains are no longer 'held'.

8. Browsing the contents of a Legal Case

Selecting the  button allows you to browse the Legal holds contained within the Legal Case. You may then navigate and display all the details of the individual holds.

Managing the Integrity of information stored in your RSD GLASS environment

Data integrity checking is the process of verifying that data in the RSD GLASS environment remains unchanged wherever it may be stored. The process uses hash values on data which can be compared to determine whether the data was altered. A hash value is a numeric value of a fixed length that uniquely identifies data. By comparing hash values assigned to data between two different points in time it is possible to see if a document has been changed.

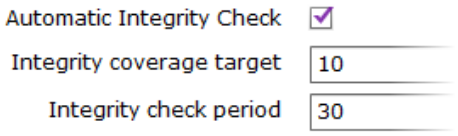
The RSD GLASS solution provides two ways of checking the integrity of data. The first is a manual process on individual components in the File Plan. The second is an automatic check that can be programmed to take place at a specified time and interval. See:

- "Manual integrity check on individual components"
- "Automatic integrity check on the file plan"

To set up the automatic checking of data integrity the following steps need to be performed:

- The Content Repository where the data resides needs to be correctly configured to enable the automatic integrity check service. This service needs to be set on the Virtual content repository or repositories used to store data. For more information, see "Virtual Repository definition" on page 15.
- The File Plan needs to be configured to enable the automatic integrity check services. Select the Menu File Plan / Edit, the select the 'Edit Metadata' button.

  The 'Integrity coverage target' is the percentage of the components in the File Plan to be covered by the integrity check during the number of days specified in the 'Integrity check period' box. In the following example, 10% of components in the File Plan will be checked over a period of 30 days. The documents checked are selected randomly from the File Plan.



This may also be setup when a File Plan is initially created. See "File Plan Creation" on page 28.

It should be noted that the manual check process is always enabled.

Note that when in 'Browse' mode it is possible to view the status and history of Integrity Checks on the File Plan, by selecting the root of the File Plan and displaying the 'Integrity' panel to the right.

Automatic integrity check on the file plan

Once your RSD GLASS environment has been correctly configured to perform the checks as described above, the 'Integrity Check Error Management screen' provides you with an overview of any discrepancies found during the automatic check process.

The 'Integrity Check Error Management' screen

- Access the 'Lifecycle Management' menu and select the 'Integrity Check Error Management' menu option. The list displayed contains any errors found between compared hash values on data between two different points in time therefore indicating that a document has been changed.

  The following items describe possible actions that may be performed.

Re-check selected components

Performs a manual check on one or more selected documents from the list.

Error Approval Options

- 'Update hash values' allows you to generate new hash values once you have determined and justified the reason behind a change in a component.
- 'Mark component as Exception' is a way of indicating that a component is no longer part of the integrity check process.

Manual integrity check on individual components

It is possible to perform an integrity check on individual components contained in a File Plan and Content Repository. Manual integrity checks are always enabled and do not need any prior configuration before being performed.

- Whilst in the 'browse' mode (by selecting the 'Browse' item from the File Plan menu), select the component that you wish to check. The 

button may be clicked. The resulting status will be displayed.

  If the integrity check fails, the actions 'Re-check selected components', 'Update hash values' and 'Mark component as Exception' will be available to be performed (as in the 'Integrity Check Error Management' screen previously described in "Automatic integrity check on the file plan" on page 45.
- The 'Integrity' panel to the right of a component displays the details of the status of the integrity of the component as well a history of the integrity checks performed.

Managing Physical Records

In order to manage the filing, maintenance and lifecycle of paper Records, RSD GLASS provides an effective solution that manages the 'Boxes' containing your paper archives.

Physical archives must be stored in such a way that they are accessible whilst at the same time safeguarding them against environmental damage. Paper documents that are typically stored in a filing cabinet in an office are now safely stored and managed in standardized boxes located in secure off-site Warehouses.

The functionality contained in the 'Physical Archives' menu of RSD GLASS Governance Manager interface is fully documented in the RSD GLASS client User Guide.

The RSD GLASS Physical Records module is the working tool of the logistics department that manages the transport of Boxes to and from off-site Warehouses or Repositories.