



IBM Enterprise Records 5.1: System Configuration

(Course code F179)

Student Notebook

ERC 1.0

Authorized



| **Training**

Trademarks

IBM® and the IBM logo are registered trademarks of International Business Machines Corporation.

The following are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide:

FileNet®

Initiate®

Redbooks®

WebSphere®

Windows and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Other product and service names might be trademarks of IBM or other companies.

November 2011 edition

The information contained in this document has not been submitted to any formal IBM test and is distributed on an “as is” basis without any warranty either express or implied. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer’s ability to evaluate and integrate them into the customer’s operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will result elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious, and any similarity to the names and addresses used by a real business enterprise is entirely coincidental.

© Copyright International Business Machines Corporation 2011.

This document may not be reproduced in whole or in part without the prior written permission of IBM.

Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Contents

Trademarks	v
Course description	vii
Unit 1. IBM Enterprise Records 5.1: System Configuration	1-1
Unit lessons	1-2
Lesson 1.1. Configure an object store for record declaration.	1-3
Configure an object store for record declaration	1-4
Activities that you need to complete	1-5
Overview: configure an object store as an RDOS	1-6
Configure an object store as an RDOS	1-8
Set the Can Declare property to True	1-9
Enable declaration from IBM FileNet Workplace	1-11
Demonstrations	1-12
Activities	1-13
Lesson 1.2. Create a record class	1-15
Create a record class	1-16
Activities that you need to complete	1-17
Overview	1-18
What is property mapping?	1-19
Configure property mapping	1-21
Set properties to be visible during record declaration	1-22
Create a record class	1-24
Activities	1-25
Lesson 1.3. Create links	1-27
Create links	1-28
Activities that you need to complete	1-29
What are links?	1-30
Link classes and their uses (1)	1-31
Link classes and their uses (2)	1-32
Enable editable link classes	1-34
Create links	1-35
Create a new link class	1-36
Activities	1-37
Lesson 1.4. Modify security	1-39
Modify security	1-40
Activities that you need to complete	1-41
Enterprise Records security	1-42
Enterprise Records uses Content Engine security	1-44
Modify security on a category	1-46
Control who can declare records from Workplace	1-47
Limit access to the FPOS from Workplace	1-48
Enterprise Records security roles	1-49
Security roles provide varying access levels	1-51

Use Security Script Wizard to modify security roles	1-53
Using other Content Engine security features	1-54
Activities	1-55
Lesson 1.5. Use security markings	1-57
Use security markings	1-58
Activities that you need to complete	1-59
What are security markings?	1-60
Marking values on records	1-61
Constraint masks and ACLs	1-63
How markings work with records	1-65
A closer look at a marking value	1-67
Hierarchical and list marking sets	1-68
Marking sets included in Enterprise Records	1-70
How to create and use markings	1-72
Demonstrations	1-73
Activities	1-75
Lesson 1.6. Export and import a file plan	1-77
Export and import a file plan	1-78
Activities that you need to complete	1-79
What is the File Plan Tool?	1-80
Overview of tasks	1-81
File Plan Tool modes	1-82
Configure the File Plan Tool	1-83
Target object store configuration requirements	1-84
Commands to export a file plan	1-85
Export scope options	1-86
Importing a file plan	1-87
Updating a file plan	1-88
File Plan Tool limitations	1-89
Activities	1-91
Glossary.....	A-1

Trademarks

The reader should recognize that the following terms, which appear in the content of this training document, are official trademarks of IBM or other companies:

IBM® and the IBM logo are registered trademarks of International Business Machines Corporation.

The following are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide:

FileNet®

Initiate®

Redbooks®

WebSphere®

Windows and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Other product and service names might be trademarks of IBM or other companies.

Course description

IBM Enterprise Records 5.1: System Configuration

Duration: 4 days

Overview

This course is for those who administer and maintain an IBM Enterprise Records system.

You work with a fully functioning IBM Enterprise Records system to practice the skills required for system configuration, administration, and system maintenance.

Audience

This course is for anyone who is planning to configure, maintain, or administer an IBM Enterprise Records system.

Prerequisites

F040: IBM FileNet P8 Prerequisite Skills 4.5

F042: IBM FileNet P8 Administration 4.5

Skills taught

After completing this course, you should be able to:

- Identify the capabilities of IBM Enterprise Records.
- Identify the role of IBM Enterprise Records in an enterprise compliance solution.
- Identify and search for records that are ready for disposition.
- Initiate disposition.
- Declare electronic records.
- Create a disposition schedule.
- Add alternate retentions.
- Work with file plan containers.
- Work with holds.
- Configure an object store for record declaration.

- Create a record class that allows property mapping from document to record.
- Enable editable link classes.
- Create and use a new link class.
- Modify security on a category.
- Control access to IBM Enterprise Records assets and functionality from IBM FileNet Workplace.
- Create and use a new marking set.
- Export and import a file plan.
- Configure multiple instances of Disposition Sweep.
- Configure an instance of Hold Sweep.
- Configure automatic destruction of records.
- Enable and configure auditing.
- View and export audit logs.
- Enable metadata retention on the file plan.
- Export and delete retained metadata from the production system.
- Automate record declaration.

Unit 1. IBM Enterprise Records 5.1: System Configuration

What this unit is about

This unit is for anyone who is planning to configure an IBM Enterprise Records system for use by records managers and users.

You work with a fully functioning IBM Enterprise Records system to practice the skills required for system configuration.

What you should be able to do

After completing this unit, you should be able to:

- Configure an object store for record declaration
- Create a record class that allows property mapping
- Enable editable link classes
- Create and use a new link class
- Modify security on a category
- Control access to IBM Enterprise Records assets and functionality from IBM FileNet Workplace
- Create and use a new marking set
- Export and import a file plan

How you will check your progress

- Successfully complete the activities in the Student Exercises book.

References

<http://publib.boulder.ibm.com/infocenter/p8docs/v5r1m0/index.jsp>

Note: for search terms, type the term exactly as shown, including quotation marks.

IBM Enterprise Records 5.1 Installation and Upgrade Guide can be downloaded from the following location:

<http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.ws?s?CTY=US&FNC=SRX&PBL=GC19-3248-00>

Unit lessons

This unit contains these lessons:

- Configure an object store for record declaration
- Create a record class
- Create links
- Modify security
- Use security markings
- Export and import a file plan

© Copyright IBM Corporation 2011

Figure 1-1. Unit lessons

F1791.0

Notes:

Lessons in this unit

This unit has 6 lessons. After the first lesson, each lesson relies on information and skills taught in the prior lessons. For best results, do these lessons in the sequence presented.

Configure an object store for record declaration – In this lesson, you configure an object store for record declaration.

Create a record class – In this lesson, you create a record class that allows property mapping from document to record.

Create links – In this lesson, you enable editable link classes and create and use a new link class.

Modify security – In this lesson, you modify security on a record category and control access to Enterprise Records assets and functionality from Workplace.

Use security markings – In this lesson, you create and use a new marking set.

Export and import a file plan – In this lesson, you export and import a file plan.

Lesson 1.1. Configure an object store for record declaration

Lesson

Configure an object store for record declaration



Why is this lesson important to you?

- You are helping the records manager add a new department to the file plan. The department has its own object store from which they declare records. In order for them to declare records, you must first configure their object store for record declaration.

© Copyright IBM Corporation 2011

Figure 1-2. Configure an object store for record declaration

F1791.0

Notes:

Configure an object store for record declaration

Activities that you need to complete

- Configure an object store for record declaration.

© Copyright IBM Corporation 2011

Figure 1-3. Activities that you need to complete

F1791.0

Notes:

Configure an object store for record declaration

Overview: configure an object store as an RDOS



- An object store must be record-enabled in order to declare its documents as records.
- Tasks to be completed:
 - Configure the object store as an RDOS.
 - Set the Can Declare property to True for all document classes to be declared.
 - Configure Site Preferences to allow declaring records on the RDOS.

© Copyright IBM Corporation 2011

Figure 1-4. Overview: configure an object store as an RDOS

F1791.0

Notes:

Help reference

- Search for "gs_configuring.htm"

Reference

You can download the IBM Enterprise Records 5.1 Installation Guide.pdf (the URL is provided at the beginning of this unit).

The meaning of ROS and RDOS

The Enterprise Records product and associated documentation use the term ROS, which stands for Record Object Store. However, records are **not** stored in an ROS, and this can lead to confusion with the file plan object store (FPOS), which is where the record objects are actually stored.

So in this course, an ROS is referred to as an RDOS, which stands for Record-enabled Document Object Store, to emphasize that **documents** are stored on it, not record objects.

File names and references in the product documentation, however, refer to ROS, so be aware of the different terms.

Configure an object store for record declaration

Configure an object store as an RDOS



Using IBM Enterprise Records web application:

1. IBM Enterprise Records > Configure > Object Store Configuration
2. Choose the object store.
3. Select ROS or both FPOS and ROS.

Using IBM Enterprise Records Configuration Manager

1. Locate and start configmgr.exe.
2. Create a new installation profile > object store configuration profile.
3. Connect to the Content Engine.
4. Edit the Configure Record Object Store task.
5. Run the task.

© Copyright IBM Corporation 2011

Figure 1-5. Configure an object store as an RDOS

F1791.0

Notes:

Help path

- IBM FileNet P8 Version 5.1 Information Center > Working with documents > Records management

You can use either the IBM Enterprise Records web application or the IBM Enterprise Records Configuration Manager to configure object stores for records management.

Configure an object store for record declaration

Set the Can Declare property to True

- Can Declare is a Boolean property of the Document class.
 - Added when you configure the object store as an RDOS
 - False by default
- This property must be set to True for each document class that you want to be declarable.
 - For efficiency, set only the needed document subclasses.
 - If a document parent class is configured, all subclasses can be set to inherit the configuration if desired.
- Configuration Manager always applies the Can Declare setting to subclasses.
 - Use the Configuration Manager only if you want the Can Declare property set to True for the specified class and all subclasses

© Copyright IBM Corporation 2011

Figure 1-6. Set the Can Declare property to True

F1791.0

Notes:

Help reference

- Search for "gs_configuring.htm"

On the RDOS, any document class must be made declarable in order to declare documents in that class. All of the documents that are added to the system that are part of that class are undeclarable until you make the class declarable. Then you can declare any of the documents in that class. To do this, you need to make changes to the class definition on the RDOS. When you configure an RDOS, a Can Declare property is added to the Document class and is inherited by all subclasses. By default, the default value of the Can Declare property is false. You must set the value to true on each class that you want to make declarable.

Limit the Document subclasses that are declarable

When you change the Can Declare property value, you have the option to propagate the change to all subclasses. If you set the Can Declare property to True on the root Document class, then all of the Document subclasses become declarable. Generally, however, it is

better to allow declaration only for those classes that are going to be declared. There are many configuration-related objects in an RDOS that you might not want to declare as records, such as search templates and workflow definitions. Be selective as to which classes you enable for record declaration.

Existing documents not declarable as records

When an object store is configured to be an RDOS and the RecordsManager add-on is added to the object store, additional records-related properties are added to existing objects. For instance, the Can Declare property is added to existing documents, but the value of that property does not get set. Because it is a read-only property, these documents can never be declared as records because this property must be set to True in order for documents to be declared.

Configuration Manager

Configuration Manager does not allow you to complete the object store configuration until you choose a document class to make declarable. With the other method (using the Enterprise Records web application) you can configure the object store without making any document classes declarable. You use Content Engine Enterprise Manager to specify each class that you want to make declarable later. If you configure the object store using Configuration Manager, the Can Declare property value is applied to that class and all subclasses automatically. This method can save time if you want all subclasses of a specified document class to be declarable. However, if you do not want all of the subclasses to be declarable, do not use Configuration Manager to configure the RDOS. Instead, use the Enterprise Records web application to configure the RDOS. You can then configure the Can Declare property for each specific document class using Enterprise Manager.

Configure an object store for record declaration

Enable declaration from IBM FileNet Workplace

- Purpose: Allow declaration from the object store in IBM FileNet Workplace.
 - In IBM FileNet Workplace, the Declare as Record task is in the Actions menu.
 - This option is available only if the object store is configured as an RDOS in IBM FileNet Workplace.
 - You must configure this setting in Site Preferences.
- Where you enable declaration:
 - Site Preferences > Object Stores > *[your RDOS]* > Support Declare Records

© Copyright IBM Corporation 2011

Figure 1-7. Enable declaration from IBM FileNet Workplace

F1791.0

Notes:

Help reference

- Search for "rm_site_preferences.htm"

Configure an object store for record declaration

Demonstrations



- Set the Can Declare property on document classes.

© Copyright IBM Corporation 2011

Figure 1-8. Demonstrations

F1791.0

Notes:

Demonstration notes

Set the Can Declare property on document classes

1. In Enterprise Manager, set the Can Declare property on the base Document class of the Finance object store.
 - a. Do not propagate the change to the subclasses.
 - b. Remember that you must choose which document classes to enable explicitly.
2. Set the Can Declare property on the Email document class.
 - a. Because the Can Declare property is inherited from the root Document class, you need to select Inherited Properties in order to see that property listed.
 - b. Because there are no subclasses of the Email class, you are not asked if you want to propagate the changes to the subclasses.

Configure an object store for record declaration

Activities

In your Student Exercises

- Unit: IBM Enterprise Records 5.1:
System Configuration
- Lesson: Configure an object store for record declaration
- Activities:
 - Configure an object store for record declaration.

© Copyright IBM Corporation 2011

Figure 1-9. Activities

F1791.0

Notes:

Use your Student Exercises to perform the activities listed.

Lesson 1.2. Create a record class

Lesson

Create a record class

Why is this lesson important to you?

- Users in your company need to declare product documents as records. They need custom document property values to populate the record object automatically. Your task is to create a record class with custom properties that take the values of the originating document.

© Copyright IBM Corporation 2011

Figure 1-10. Create a record class

F1791.0

Notes:

Create a record class

Activities that you need to complete

- Create a record class that allows property mapping.

© Copyright IBM Corporation 2011

Figure 1-11. Activities that you need to complete

F1791.0

Notes:

Create a record class

Overview



- To create a record class with properties that map to the original document, do the following:
 1. Create property templates on the FPOS so that they map to properties on the RDOS.
 2. Configure property templates to be visible during declaration.
 3. Create a record class using these property templates.

© Copyright IBM Corporation 2011

Figure 1-12. Overview

F1791.0

Notes:**Help path**

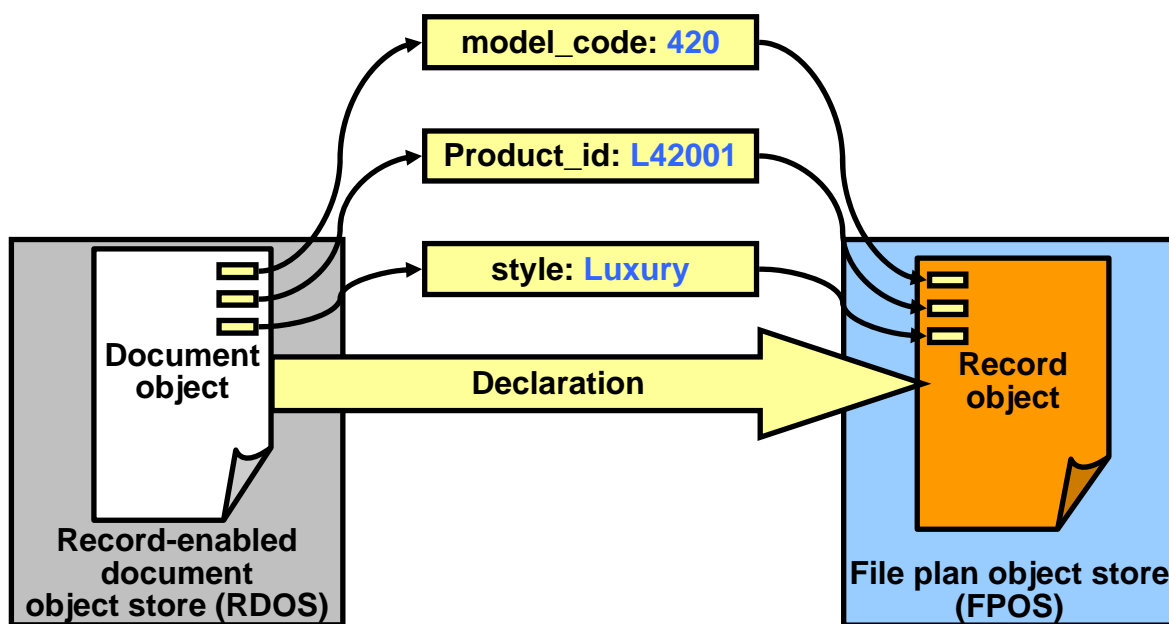
- IBM FileNet P8 Version 5.1 Information Center > Working with documents > Records management > Declaring records > Declare a record

Record properties with the same symbolic names as the properties of the originating document are automatically populated with the document values when the record is declared.

Create a record class

What is property mapping?

- You can map record properties so that they take the values of the originating document when the record is declared.



© Copyright IBM Corporation 2011

Figure 1-13. What is property mapping?

F1791.0

Notes:

Help path

- IBM FileNet P8 Version 5.1 Information Center > Working with documents > Records management > Configuring IBM Enterprise Records system > Configuring property synchronization

If an object store is enabled for records declaration, the documents stored in it can be declared as records. When a document is declared as a record, a new object is created in a special kind of object store called a File Plan Object Store (FPOS). This record object is then managed by the records management rules, disposition schedules, and other requirements of your company.

Property mapping is ordinarily done by IBM FileNet Workplace during declaration. If you are using a custom application for declaration, however, you need to configure the property mappings yourself.

Diagram

The diagram shows how document property values can be copied into the corresponding record properties during declaration.

Properties not synchronized between records and documents

Property mapping allows values to be passed from an originating document to a record during declaration. After a record is declared, the default behavior is that changes to property values on either the originating document or the record have no effect on the other object. This behavior can be modified by configuring property synchronization, which is described in the help path topic.

Create a record class

Configure property mapping

- IBM FileNet Workplace maps matching symbolic names automatically.
- One way to configure property mapping is to export the property templates on the RDOS and import them to the FPOS.
 - This procedure ensures that symbolic names are the same.

© Copyright IBM Corporation 2011

Figure 1-14. Configure property mapping

F1791.0

Notes:

Create a record class

Set properties to be visible during record declaration



- New property templates on the FPOS are not automatically visible in the Workplace record declaration wizard.
 - When you declare a document in IBM FileNet Workplace, new record properties are not visible by default, so their values cannot be set manually.
- Use Enterprise Manager to make a property visible during manual declaration.
 - Locate the property template in the FPOS.
 - Add *declare* to the property template Description field.
 - Separate *declare* from the rest of description with a comma.

© Copyright IBM Corporation 2011

Figure 1-15. Set properties to be visible during record declaration

F1791.0

Notes:

Help paths

- IBM FileNet P8 Version 5.1 Information Center > Working with documents > Records management > Managing classes and properties > Adding properties to classes
- IBM FileNet P8 Version 5.1 Information Center > Working with documents > Records management > Managing classes and properties > Customizing the display of properties

You do not need to enable declaration on property templates that existed when you initially configured the object store and record classes, but it is necessary to enable declaration for new custom record classes and property templates.

Adding *declare* to the property template description

A comma is needed to separate the word *declare* from other comments. If no other comments are listed in the Description field, you do not need the comma.

Both of the following formats allow the property template to be used during record declaration:

- Property_description,declare
- declare,Property_description

Create a record class

Create a record class



- The Record class is a subclass of Document on the FPOS.
- Two subclasses of Record exist:
 - Electronic Record
 - Marker Record (used for physical records only)
- To create a new record class, do the following:
 - Create a subclass of the Electronic Record class for electronic records.
 - Create a subclass of the Marker Record class for physical records.
 - Ensure that required properties are visible, if needed.
 - Ensure that record properties are mapped to the document properties if applicable.

© Copyright IBM Corporation 2011

Figure 1-16. Create a record class

F1791.0

Notes:**Help path**

- IBM FileNet P8 Version 5.1 Information Center > Working with documents > Records management > Managing classes and properties > Creating subclasses

You can use Enterprise Manager to create a new subclass of the Record, RecordFolder, or RecordCategory class and associate various properties with the subclass. However, the newly created subclass is not visible in the Enterprise Records user interface.

Create a record class

Activities

In your Student Exercises

- Unit: IBM Enterprise Records 5.1:
System Configuration
- Lesson: Create a record class
- Activities:
 - Create a record class that allows property mapping.

© Copyright IBM Corporation 2011

Figure 1-17. Activities

F1791.0

Notes:

Use your Student Exercises to perform the activities listed.

Lesson 1.3. Create links

Lesson

Create links



Why is this lesson important to you?

- The records manager at your company needs a way to associate product description document records with their technical specifications and marketing documents. When she attempts to create a link, however, she receives a message stating that the link class is read-only. Your task is to enable editable IBM Enterprise Records link classes so that she can add links.
- Your company performs various tests on each product before releasing it. Each test has its own detailed results record. Additionally, all of the test results for a product are tabulated in a single, summary record. Your task is to allow the individual test result records to be linked to the summary record so that all the components of the test package can be found easily.

© Copyright IBM Corporation 2011

Figure 1-18. Create links

F1791.0

Notes:

Create links

Activities that you need to complete

- Enable editable link classes.
- Create and use a new link class.

© Copyright IBM Corporation 2011

Figure 1-19. Activities that you need to complete

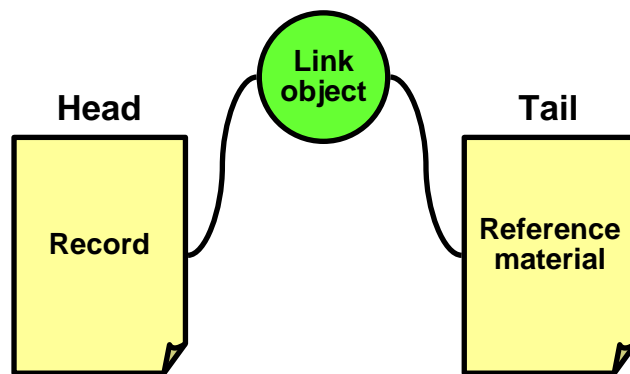
F1791.0

Notes:

Create links

What are links?

- A link is an object that represents a relationship between two other objects.
 - Use links to reference or associate related records and information.
 - Examples: Notes, attachments, source documents
- A link can have its own properties.
 - Example: The link properties can give information about the relationship between the linked objects.
 - Security can be set to control access to the link object.
- A link has head and tail properties.
 - The head and tail point to different objects.
 - Example: The head of a link can reference a record while the tail references a document.
 - You can get to the head or tail from the other object through the link.



© Copyright IBM Corporation 2011

Figure 1-20. What are links?

F1791.0

Notes:

Help reference

Search for: "manage_links.htm"

You can create links between IBM Enterprise Records entities and other Content Engine objects in Workplace. A record can share links with other records, documents, and record folders.

Only authorized users are allowed to change or delete links.

Create links

Link classes and their uses (1)

- The Links class is a subclass of *Other Classes*
- Link subclasses include the following:
 - Extract Link: Used for referencing sources of document extracts.
 - Record See Also Link: Relates records with related content.
 - Record Folder See Also Link: Establishes a link between two related folders or a record and a folder.
 - Reference Link: Associates records with their references.
 - Rendition Link: Associates records with renditions of documents in different software formats.
 - Hybrid Folder Link: Establishes a relationship between a hybrid folder and a physical or electronic folder.
 - Record Copy Link (for internal use only): Establishes an association between the original record and different copies of the original.

© Copyright IBM Corporation 2011

Figure 1-21. Link classes and their uses (1)

F1791.0

Notes:

Help reference

- Search for: "class_descriptions.htm"

Link retention and deletion

When a linked record is deleted, all associated links of that record are also deleted.


When you relocate, transfer, or export records, all links between records are retained.

Other internal link types

Record Hold Link: Record Hold Link is a subclass of the RM Link class. It establishes an association between a record entity that is on hold and the hold itself. This link is used for internal processing and is not visible in the Enterprise Records user interface.

RM Folder Hold Link: RM Folder Hold Link is a subclass of the RM Link class. It establishes an association between an Enterprise Records folder entity that is on hold and the hold itself. This link is used for internal processing and is not visible in the Enterprise Records user interface.

Create links

Link classes and their uses (2)


Link name	Head	Tail
Extract Link	Record	Document
Hybrid Folder Link	Generic object	Generic object
Record Copy Link	Record	Record
Record Folder See Also Link	Generic object	Generic object
Record Hold Link	Record	Record Hold
Record See Also Link	Record	Record
Reference Link	Record	Document
Rendition Link	Generic object	Generic object
RM Folder Hold Link	RM Folder	Record Hold

© Copyright IBM Corporation 2011

Figure 1-22. Link classes and their uses (2)

F1791.0

Notes:

The target head or tail class can be a class or its subclasses. Therefore, it is possible to use a Reference Link between two record objects because Record is a subclass of the Document class.

Predefined link types and their respective head and tail object types

For the Extract Link type, the head is a Record object and the tail is a Document object.

For the Hybrid Folder Link type, the head is a generic object and the tail is a generic object.

For the Record Copy Link type, the head is a Record object and the tail is a Record object.

For the Record Folder See Also Link type, the head is a generic object and the tail is a generic object.

For the Record Hold Link type, the head is a Record object and the tail is a Record Hold object.

For the Record See Also Link type, the head is a Record object and the tail is a Record object.

For the Reference Link type, the head is a Record object and the tail is a Document object.

For the Rendition Link type, the head is a generic object and the tail is a generic object.

For the RM Folder Hold Link type, the head is an RM Folder object and the tail is a Record Hold object.

Create links

Enable editable link classes



- Enable editable link classes so that users can add links.
- Enable them in IBM FileNet Workplace Site Preferences:
 - Site Preferences > Object Stores > *file plan object store*
 - Add Link Class > RM Link > *link subclass*
- Use these link class settings to configure user access:
 - Include Subclasses
 - Allow Create
 - Allow Modify
 - Allow Delete

© Copyright IBM Corporation 2011

Figure 1-23. Enable editable link classes

F1791.0

Notes:**Help reference**

- Search for: "set_add_link_class_pref.htm"

Create links

Create links



- Create links in Enterprise Records using the Action menu of the selected object.
- Set properties.
 - Choose the link class.
 - Choose object to link to.
 - Name and describe the link.
 - Set link property values, if applicable.
- Set security.

© Copyright IBM Corporation 2011

Figure 1-24. Create links

F1791.0

Notes:**Help reference**

- Search for: "create_a_see_also_link.htm"

When choosing an object to link to, you can use My Search from within the Create Link wizard.

Create links

Create a new link class



- Create new link classes in Enterprise Manager.
- Create a subclass of Other Classes > Link > RM Link.
- Add properties and define default values.

© Copyright IBM Corporation 2011

Figure 1-25. Create a new link class

F1791.0

Notes:

Create links

Activities

In your Student Exercises

- Unit: IBM Enterprise Records 5.1:
System Configuration
- Lesson: Create links
- Activities:
 - Enable editable link classes.
 - Create and use a new link class.

© Copyright IBM Corporation 2011

Figure 1-26. Activities

F1791.0

Notes:

Use your Student Exercises to perform the activities listed.

Lesson 1.4. Modify security

Lesson

Modify security



Why is this lesson important to you?

- The records manager at your company has a list of security requirements for different record categories that she needs you to implement. Your task is to make security changes to meet these requirements.
- You also need to limit who has access to the FPOS and who can declare records from IBM FileNet Workplace.

© Copyright IBM Corporation 2011

Figure 1-27. Modify security

F1791.0

Notes:

Modify security

Activities that you need to complete

- Modify security on a category.
- Control access to assets and functionality from Workplace.

© Copyright IBM Corporation 2011

Figure 1-28. Activities that you need to complete

F1791.0

Notes:

Modify security

Enterprise Records security



- Enterprise Records uses security features from the Content Engine.
 - Default instance security determines the initial security settings for a container or record.
 - The Enterprise Records data models assign inheritable default instance security to categories.
 - Records inherit security settings from a security parent, allowing security to be controlled from the category level.
 - Record objects serve as security proxies for the original electronic documents.
 - Supplemental security markings can be configured and used to secure access to individual records.

© Copyright IBM Corporation 2011

Figure 1-29. Enterprise Records security

F1791.0

Notes:

Help reference

- Search for: "managing_security.htm"

Record objects as security proxies for the source document

When a document is declared as a record, the record object takes over security on the original document by adding additional proxy security settings on the document object. These proxy security settings are evaluated when the document object is accessed.

Some security proxies can conflict with IBM Enterprise Records. Before you declare documents as records, remove any security proxies that are already in effect on the document.

Strategies for controlling access to records

Determine security requirements during the planning phase.

- Set default instance security before file plan creation.

Start by securing the categories.

- Categories are the primary mechanism for controlling access.
- Modify security on each category to control the access to the records in that category.

You can use markings to further restrict access to individual records.

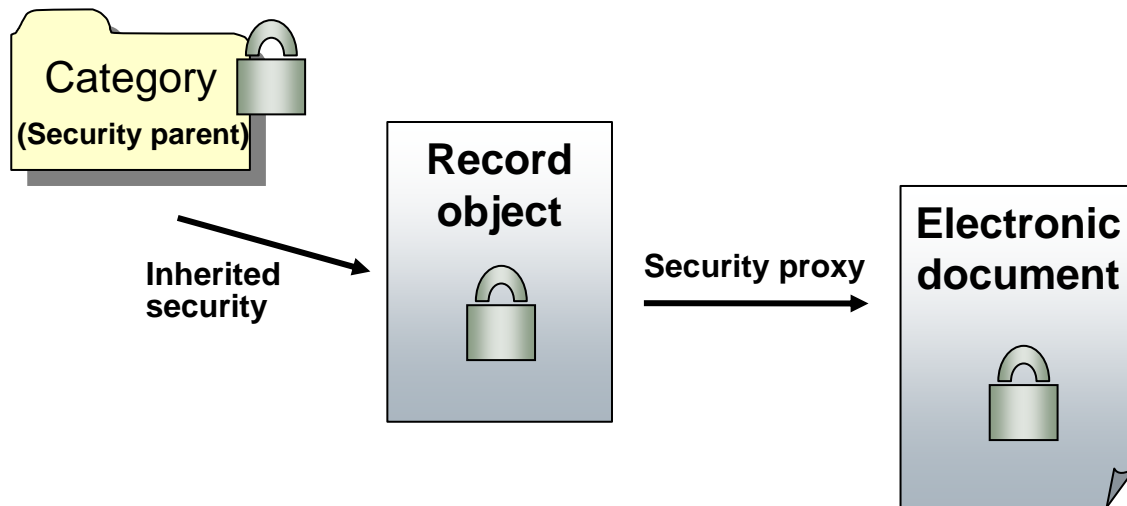
- Security markings are covered in the next lesson.

To learn more about design considerations for setting up security on a records management system, refer to the chapter on security in the IBM Redbooks publication *Understanding IBM FileNet Records Manager*. This publication is available through the IBM support website and on your student system at C:\Reference Materials\.

Modify security

Enterprise Records uses Content Engine security

- Records are primarily secured by category.



© Copyright IBM Corporation 2011

Figure 1-30. Enterprise Records uses Content Engine security

F1791.0

Notes:**Help reference**

- Search for: "object_security.htm"

Record security

When the declaration process files a record into a container, the record inherits the security of the parent container, known as the security parent. If you use Workplace to declare the record into multiple containers, the security parent is the first record container that is selected.

The post-import script FPOS_PostImport_datamodel.vbs, which is run when importing a data model into an object store, sets the Default Instance Owner for the Record class, and its subclasses Electronic, Email, and Marker, to NULL. When a user declares a record with the Record class or a subclass, the record inherits the Default Instance Owner property of the class, which is set to NULL. When the Owner property is NULL, Enterprise Records does not grant any special access rights to any user. Therefore, a record creator does not have administrative rights to the record and cannot modify the security of the record.

You can use Enterprise Manager to change the owner to a specific user or group by modifying the Default Instance Owner on the Record class or a subclass. However, Enterprise Records applies the change only to records created after the change. The change is not applied to any existing records.

Modify security

Modify security on a category



- Access to records in the category is restricted based on the security settings of the category.
- You can modify the direct security on a category:
 - When adding a new category, use the page that allows you to set security.
 - On an existing category, modify security by using the property page for security.
- Changes to security at the category level are propagated to all inheriting children.
 - Record security is computed only when the record is accessed.
 - Therefore, because the security on a record is inherited, security changes to the category affect the security of the inheriting records the next time that they are accessed.

© Copyright IBM Corporation 2011

Figure 1-31. Modify security on a category

F1791.0

Notes:

Modify security

Control who can declare records from Workplace

1. Go to Workplace Site Preferences > Access Roles.
2. Create an access role that contains only the security groups that need to declare records from Workplace.
 - Be sure to remove the default group #AUTHENTICATED-USERS from the access role.
3. Go to Workplace Site Preferences > Actions.
4. Assign the access role to the record declaration actions.
 - These actions are not available in the Action menus for users who do not belong to the access role.
- Be sure to configure both actions that declare records.
 - Declare as Record
 - Declare Versions as Record

© Copyright IBM Corporation 2011

Figure 1-32. Control who can declare records from Workplace

F1791.0

Notes:

Help paths

- IBM FileNet P8 Version 5.1 Information Center > Working with documents > Working with documents with Workplace XT > Site preferences > Access roles preferences
- IBM FileNet P8 Version 5.1 Information Center > Working with documents > Working with documents with Workplace XT > Site preferences > Actions preferences

Modify security

Limit access to the FPOS from Workplace



1. Go to Workplace Site Preferences > Access Roles.
2. Create an access role that contains only the security groups that need access to the file plan object store in Workplace.
3. Go to Workplace Site Preferences > Object Stores > *[object store]*.
4. Under Object Store Access, click *Select access roles*.
5. Click the access role that you defined.
- Result:
 - The object store is not available in Workplace for users who are not members of the access role.

© Copyright IBM Corporation 2011

Figure 1-33. Limit access to the FPOS from Workplace

F1791.0

Notes:

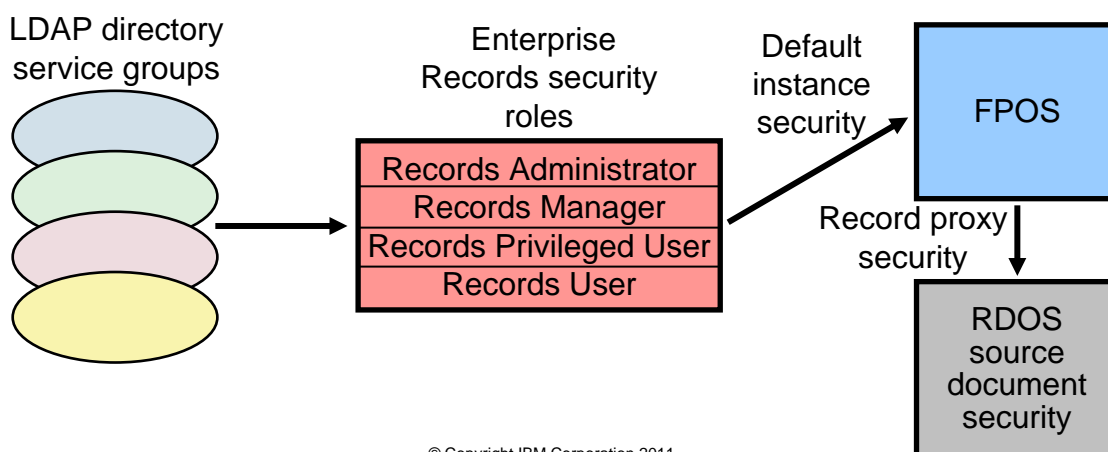
Help path

- IBM FileNet P8 Version 5.1 Information Center > Working with documents > Working with documents with Workplace XT > Site preferences > Object store preferences > Object store access

Modify security

Enterprise Records security roles

- Directory service security groups are mapped to Enterprise Records security roles.
- Enterprise Records security roles are used to set default instance security on categories and records in the FPOS.
- Security is applied to documents in the RDOS by the records.



© Copyright IBM Corporation 2011

Figure 1-34. Enterprise Records security roles

F1791.0

Notes:

Help reference

- Search for: "rm_security_roles.htm"

Help path

- IBM FileNet P8 Version 5.1 Information Center > Install additional IBM FileNet P8 products > Installing additional IBM FileNet P8 products > IBM Enterprise Records Installation and Upgrade > Configuring IBM Enterprise Records after installation > Configuring security for the file plan object store (FPOS)

Diagram

The diagram shows the relationship between LDAP directory service groups and Enterprise Records security roles, and how those roles are applied to objects in the FPOS and RDOS.

When a data model is applied, required properties and classes are added to an FPOS to make it compliant with a particular standard.

The security roles shown are for the Base data model. These four standard roles represent the most common, broad access levels required by most organizations.

Enterprise Records security roles

Enterprise Records security roles provide a convenient way of mapping common roles to functional access rights. The predefined roles are based on records management standard practices.

Security roles are defined by the data model specified when defining an FPOS. When the roles are applied, the default instance security is configured on the FPOS.

Managing the roles

- Use directory service tools to administer the groups that have been mapped to the Enterprise Records security roles. Because security is computed only when an object is accessed, changes made to the LDAP group membership apply to the affected objects immediately (except for possible directory service caching delays).
- Use the Security Script Wizard to change the mappings to the LDAP groups. Changes of this kind apply only to the Enterprise Records classes and new objects. Existing record objects and containers are not affected.

Location of role names in Enterprise Records and IBM FileNet Content Manager

- You see the security role names in the Security Script Wizard in the Enterprise Records web application.
- In all other places, you see the LDAP group names associated with the roles instead of security role names.

Important: Enterprise Records security roles are not the same as Workplace access roles.

Modify security

Security roles provide varying access levels

- User roles are mapped to specific security settings.
 - The roles for the Base data model are shown.
 - DoD Classified data model also has Classification Guide Administrator role.

Role	Summary of access rights
Records Administrator	Full access including access to administrative functions in Workplace and Enterprise Manager
Records Manager	Full control, which includes deleting records and containers, modifying properties, and configuring all aspects of a file plan
Records Privileged User	Privileged access, which includes modifying properties of records and folders and adding new folders and volumes
Records User	Limited access which typically includes record declaration and retrieval, and filing records into other categories or folders

© Copyright IBM Corporation 2011

Figure 1-35. Security roles provide varying access levels

F1791.0

Notes:

Help reference

Search for "rm_security_roles.htm"

Help path

- IBM FileNet P8 Version 5.1 Information Center > Installing additional IBM FileNet P8 products > IBM Enterprise Records Installation and Upgrade > Planning IBM Enterprise Records installation > IBM Enterprise Records security > IBM Enterprise Records security roles

Base data model roles and access rights

Note: This list of all the capabilities of each role is not comprehensive.

Records Administrator – Members in this role have full access including access to administrative functions in Workplace and Enterprise Manager.

Records Manager – Members in this role have full control, which includes deleting records and containers, modifying properties, and configuring all aspects of a file plan.

Records Privileged User – Members in this role have privileged access, which includes modifying properties of records and folders and adding new folders and volumes.

Records User – Members in this role have limited access which typically includes record declaration and retrieval, and filing records into other categories or folders.

Important: Do not assign more than one Enterprise Records security role to a user. When you are explicitly denying permissions to a user, the assignment of more than one role to a user results in the role with the least access taking priority. For the same reasons, do not assign a user to multiple groups that have different Enterprise Records security roles. Do not assign #AUTHENTICATED-USERS to the Records User role because it negates the permissions needed by users assigned as Records Managers, Records Reviewers, and Records Administrators.

The access rights granted to users in these roles vary slightly based on the data model. You assign groups (and possibly users) to security roles as part of configuring each FPOS in your environment.

Modify security

Use Security Script Wizard to modify security roles

- The Security Script Wizard allows the security role mappings to be modified on an FPOS.
 - The FPOS infrastructure, including default instance security and security on classes, is modified.
 - Security on existing record objects and containers is **not** modified by running the Security Script Wizard.
- Run the Security Script Wizard in Enterprise Records to do the following:
 - Update the security of all the Enterprise Records-related classes in the FPOS.
 - Define the default instance security for the Enterprise Records-related classes.
 - Assign the selected users and groups the access rights available to the security role to which they are mapped.
- Only a GCD administrator can run the Security Script Wizard.

© Copyright IBM Corporation 2011

Figure 1-36. Use Security Script Wizard to modify security roles

F1791.0

Notes:

Help path

- Install additional IBM FileNet P8 products > Installing additional IBM FileNet P8 products > IBM Enterprise Records Installation and Upgrade > Configuring IBM Enterprise Records after installation > Configuring security for the file plan object store (FPOS)

Modify security

Using other Content Engine security features



- You can combine other Content Engine security features.
 - Example: Direct security on entities other than categories
 - Example: Security policies
- You can modify direct security on entities other than categories.
 - Directly on folders or volumes
 - Directly on record objects
- Be aware of the possible complexity.
 - Try to use category security and markings if possible.
 - Use direct security on folders only if needed.
 - Avoid manipulating direct security on records if possible.

© Copyright IBM Corporation 2011

Figure 1-37. Using other Content Engine security features

F1791.0

Notes:**Help path**

- IBM FileNet P8 Version 5.1 Information Center > Security > IBM FileNet P8 security > Security overview

Modify security

Activities

In your Student Exercises

- Unit: IBM Enterprise Records 5.1:
System Configuration
- Lesson: Modify security
- Activities:
 - Modify security on a category.
 - Control access to assets and functionality from Workplace.

© Copyright IBM Corporation 2011

Figure 1-38. Activities

F1791.0

Notes:

Use your Student Exercises book to perform the activities listed.

Lesson 1.5. Use security markings

Lesson

Use security markings

Why is this lesson important to you?

- The records manager and solution designer at your company have determined that marking sets are going to be used in implementing security in your records management system. Your task is to create and implement the marking sets to meet their requirements.

© Copyright IBM Corporation 2011

Figure 1-39. Use security markings

F1791.0

Notes:

Use security markings

Activities that you need to complete

- Create and use a new marking set.

© Copyright IBM Corporation 2011

Figure 1-40. Activities that you need to complete

F1791.0

Notes:

Use security markings

What are security markings?



- Security markings are an optional feature.
 - They are used only to provide additional constraints to the regular security settings on an object.
 - Markings are used by Enterprise Records.
- Markings are special property values that control access to individual objects.
 - Marking values have associated security constraint masks.
 - Users can access an object if they meet the criteria set by the instance security and the constraint mask of the marking value.
- A marking set is a collection of mutually exclusive marking values.
- Markings are used to model security in terms of codes, levels, or categories.
 - Hierarchical marking set example: Top Secret, Secret, Confidential, Unclassified

© Copyright IBM Corporation 2011

Figure 1-41. What are security markings?

F1791.0

Notes:

Help references

- IBM FileNet P8 Version 5.1 Information Center >Security > IBM FileNet P8 security > Authorization > Markings
- Search for "security_markings.htm"

Help path

- Install additional IBM FileNet P8 products > Installing additional IBM FileNet P8 products > IBM Enterprise Records Installation and Upgrade > Planning IBM Enterprise Records installation > IBM Enterprise Records security > Security markings

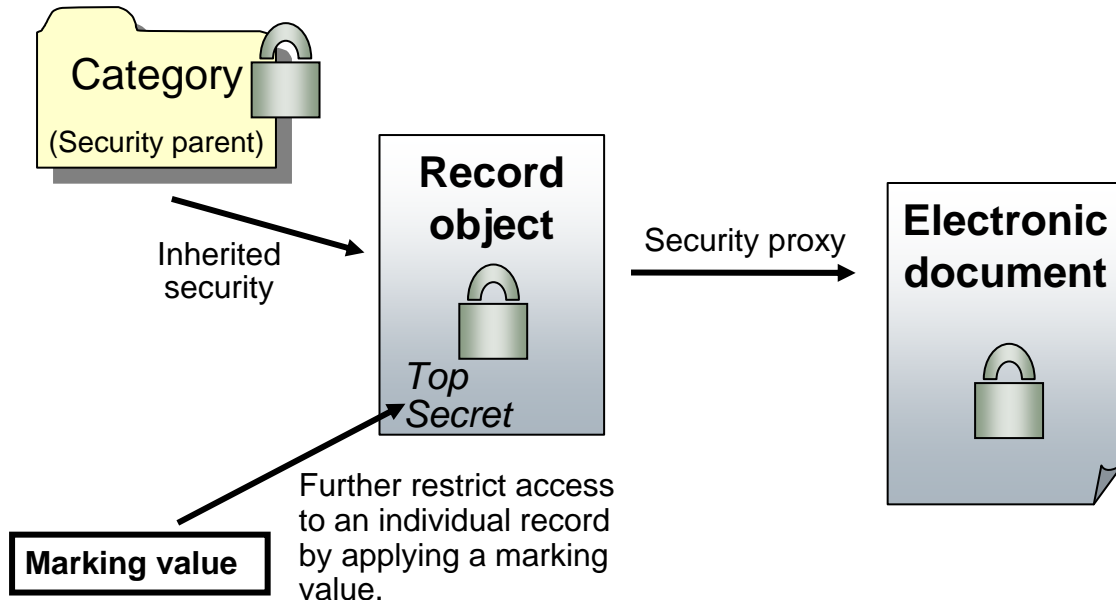
Markings are objects that combine metadata behavior with access control behavior in a way that allows access rights to an object to change by changing a property value.

Markings are defined at the FileNet P8 domain level in Enterprise Manager.

Use security markings

Marking values on records

- A marking value further restricts access to a record.



© Copyright IBM Corporation 2011

Figure 1-42. Marking values on records

F1791.0

Notes:

Markings do not replace conventional access permissions on a record, but are used in conjunction with them in determining access rights.

A category, acting as a security parent, is generally the primary control mechanism for records within that category. However, marking values can be assigned to records on an individual basis to further restrict access.

If a record has one or more markings applied to it, then access to that record is granted only if it is granted by both the Access Control List (ACL) permissions and by the markings. Remember that the ACLs of records generally include permissions inherited from the records category.

Access checking process

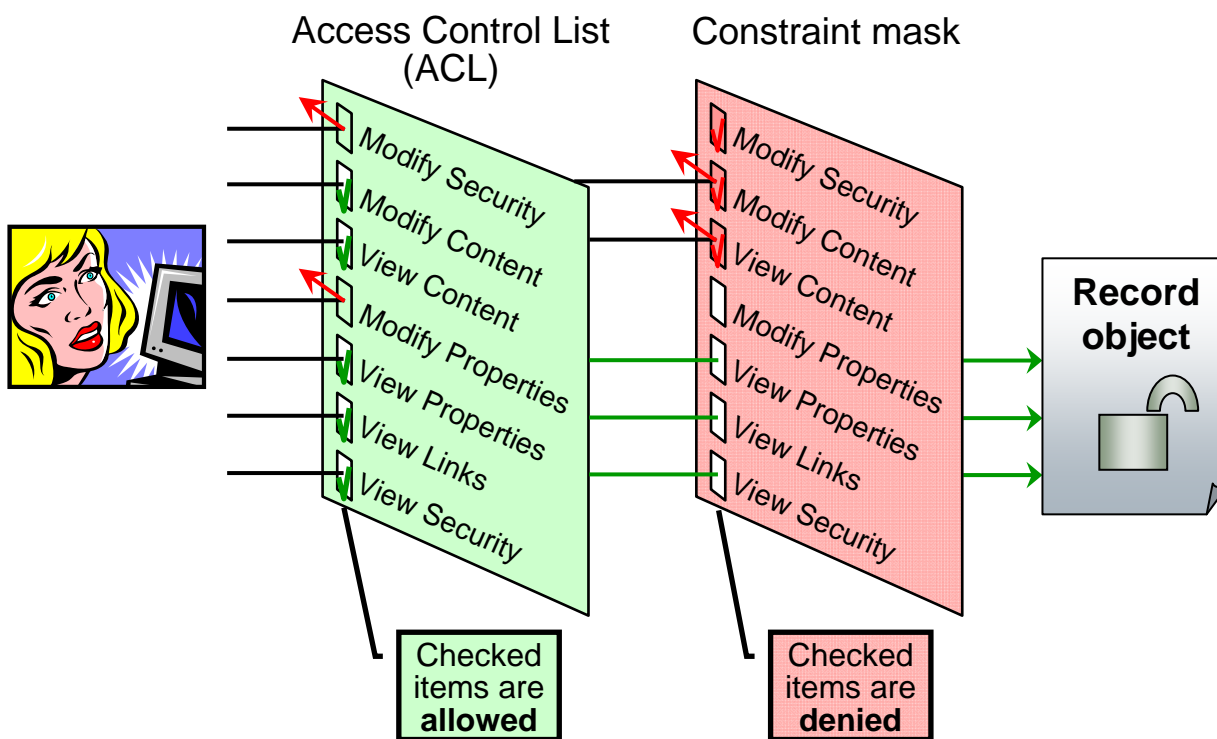
1. A user or process tries to access an object.
2. The Content Engine resolves the ACL of the object to determine who can access the object and what those users can do.

3. If a user has access based on the ACL, the Content Engine then determines whether that user has access based on the marking security definition and constraint mask.

Although it is possible to create markings on folders and categories, the containers do not pass marking security on to contained objects. The result is that, although you cannot see an area of the file plan to which you are denied by markings, you can still search for and potentially retrieve the contained records.

Use security markings

Constraint masks and ACLs



© Copyright IBM Corporation 2011

Figure 1-43. Constraint masks and ACLs

F1791.0

Notes:

Help path

- IBM FileNet P8 Version 5.1 Information Center > Security > IBM FileNet P8 security > Authorization > Markings > Constraint Mask

Diagram

The diagram shows an example of evaluating security for a user who does not have the Use Marked Objects permission for a marking value. Some individual security rights are allowed by the ACL of the record. Then the restrictions imposed by the constraint mask are applied. For a user to be able to access the record, the user must be allowed access by both the ACL and the constraint mask.

For security principals that have the Use Marked Objects right granted for that marking value, the constraint mask is ignored.

Constraint mask analogy

Think of a constraint mask as a barrier with holes in it. The holes allow users who have access to an unmarked object to continue to have access. You can plug those holes by

checking the items in the constraint mask, thus denying them access that they might otherwise be granted by the ACL.

It is important to remember that check marks mean different things in different interfaces. In the ACL, check marks are permissions. In the constraint mask, they are denials

Note that marking sets work only to deny access, which is why the constraint mask uses the Deny approach, and the checked rights are denied.

Use security markings

How markings work with records



- The use of markings requires adding a marking property to the record class.
- The property holds a marking value that is defined as part of a marking set.
- When the marking value is assigned to the object, the particular constraint mask associated with that marking value is applied to the object.
 - Users listed in the specific marking value who have been given Use Marked Objects permission are exempt from its constraint mask.
 - Everyone else is subject to the constraint mask.
- Marking property values can be assigned only by users authorized by the associated marking.
 - Example: A user with Secret level access to a record cannot set the marking value to Top Secret.

© Copyright IBM Corporation 2011

Figure 1-44. How markings work with records

F1791.0

Notes:

For a marking set to affect record security, a property on that record class must be associated with the marking.

How markings work

1. A marking set is defined, containing several possible values called markings.
2. Each marking value contains a set of access permissions that define who can assign that specific value to an object property, who can modify or remove that specific value, and, when it is assigned, who has access to the object it is assigned to.
3. The marking set is assigned to a property definition on a class such that the value of that property must be one of the markings defined by the marking set.
4. Values can be assigned only by users authorized by the associated marking, and access to the object is restricted based on the marking when it is applied.
5. A marking property on a record contains one value from a marking set, which specifies the constraint mask and which users, if any, are exempt from that mask.

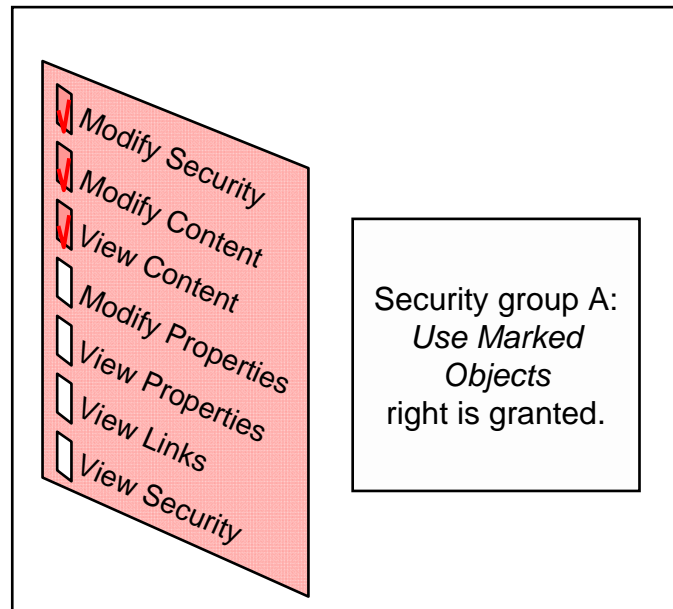
Multiple marking properties can be assigned to a single class, and they are all used to determine the final access to the object. The collection of all markings actually being applied to a particular object is displayed by Enterprise Manager as the *active markings* for the object.

Use security markings

A closer look at a marking value

- A marking value identifies both a constraint mask and a list of security principals.
- In this example, security group A is granted the Use Marked Objects permission.
- Group A is exempt from the constraint mask when a record has a property with this marking value.
- All other users are subject to the constraint mask.

A marking value



© Copyright IBM Corporation 2011

Figure 1-45. A closer look at a marking value

F1791.0

Notes:

Help path

- IBM FileNet P8 Version 5.1 Information Center > Security > IBM FileNet P8 security > Authorization > Markings > Marking security: Add, Remove, Use

Diagram

A marking value contains both a constraint mask and a list of security principals who might be exempt from that constraint mask. The constraint mask for that marking value is ignored for the security principals who are granted the Use Marked Objects right on the Security tab.

Bypassing markings and the Use Marked Objects right

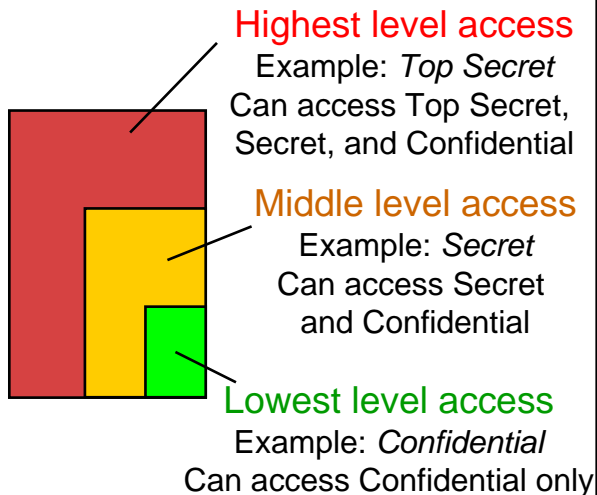
The Use Marked Objects access right is set on the Security tab of the of the Property page of a marking value and determines whether the presence of the marking on a record constrains access to that record for a user. If a user has Use Marked Objects permission for the marking value, access to the record is not constrained by that marking.

Use security markings

Hierarchical and list marking sets

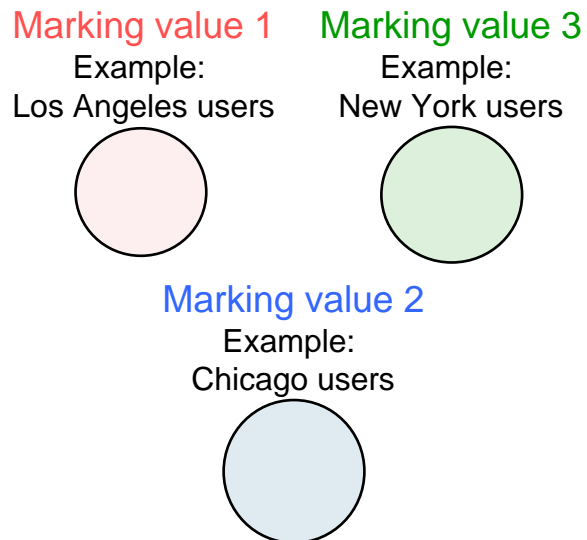
- Hierarchical marking sets

- Security principals given access in a marking value have access to the lower levels in the hierarchy.



- List marking sets

- Each marking has its own, independent access.



© Copyright IBM Corporation 2011

Figure 1-46. Hierarchical and list marking sets

F1791.0

Notes:

Help path

- IBM FileNet P8 Version 5.1 Information Center > Security > IBM FileNet P8 security > Authorization > Markings > Hierarchical and Non-hierarchical

Hierarchical marking sets can be assigned only to single-valued properties.

Nonhierarchical marking sets, also called list marking sets, can be assigned to either single or multi-valued properties.

Hierarchical marking permission rules

1. *Allow* permissions affect markings downward in the hierarchy. That is, an *Allow* permission placed on a superior marking is implicitly present on inferior markings.
2. *Deny* permissions affect markings upward in the hierarchy. That is, a *Deny* permission placed on an inferior marking is implicitly present on superior markings.
3. *Deny* permissions take precedence over *Allow* permissions.

Diagram

In the hierarchical marking set example, the Top Secret group has the highest level of access. Members can access Top Secret records, as well as all levels below. The Secret group has the middle level of access, and can access only the Secret and Confidential records. The Confidential group has the lowest level of access, and can access only the Confidential records.

In the list marking set example, the three marking values control access independently of the other marking values. The Los Angeles users group is allowed access by Marking value 1, the Chicago users group is allowed access by Marking value 2, and the New York users group is allowed access by marking value 3.

Use security markings

Marking sets included in Enterprise Records



- These marking sets are created for the entire FileNet P8 domain when an object store is configured as an FPOS.
 - Prevent IBM Enterprise Records Entity Deletion (DoD and Base data models)
 - Supplemental Marking (DoD and PRO data models)
 - Security Categories (DoD Classified data model)
 - Security Categories (PRO data model)
- You specify the data model when you configure the FPOS.

© Copyright IBM Corporation 2011

Figure 1-47. Marking sets included in Enterprise Records

F1791.0

Notes:

Help path

- IBM FileNet P8 Version 5.1 Information Center > Working with documents > Records management (See Types of IBM Enterprise Records Installations)

A data model is an Enterprise Records component that you configure or import into an FPOS. It adds required properties and classes to an FPOS to make it compliant with a particular standard.

Prevent RM Entity Deletion

For Base and DoD installations, the Prevent RM Entity Deletion hierarchical marking set prevents users who are not in the Records Administrators or Records Managers security roles from deleting entities, including file plans, record categories, record folders, volumes, and records. Because the Prevent RM Entity Deletion marking set is used internally by Enterprise Records, do **not** modify this marking set.

The marking set includes the following marking values:

- **Default:** This marking value is the default marking that Enterprise Records applies to file plans, record categories, record folders, volumes, and records.
- **Prevent Delete:** Enterprise Records applies this marking when an entity is placed on hold. When this marking is applied, the entity cannot be deleted by anyone, including members of the Records Administrators and Records Managers security roles. (These groups do not have the Use Marked Objects permission.)

Use security markings

How to create and use markings



- Create and name the marking set in Enterprise Manager.
 - To create or modify markings, you must have GCD administrator access.
- Designate the marking set as a list or hierarchical type.
- Name and define the possible marking values within the set.
 - Define the constraint mask for each value.
 - Set the security parameters for each value.
- Create a new marking property for that marking set and add it to a record class.
- When a record is added using that class, assign the desired marking value to the marking property of the record.

© Copyright IBM Corporation 2011

Figure 1-48. How to create and use markings

F1791.0

Notes:

Markings are defined at the FileNet P8 domain level in Enterprise Manager.

To create or modify markings, you must have GCD administrator access. After a marking set is created, it is potentially available for use with all object stores in the domain.

However, properties that use the marking set are specific to their object store.

Use security markings

Demonstrations



- Examine the marking set used for records on hold.
- Create a list type marking set.

© Copyright IBM Corporation 2011

Figure 1-49. Demonstrations

F1791.0

Notes:

Demonstration notes

Examine the marking set used for records on hold

1. Open the Properties page of the Prevent RM Entity Deletion marking set in Enterprise Manager.
2. Select the Prevent Delete value and click Edit. This value is the marking value used when records are on hold.
3. Go to the Constraint Mask tab and verify that only the Delete right is denied.
4. Go to the Security tab and verify that the groups listed do not have the Use Marked Objects permission. Therefore, even these administrative users cannot delete an object that has this marking value.
5. Click Edit for the Default marking value. Verify that administrative records users have the Use Marked Objects permission. Verify that other record users do not have the Use Marked Objects permission.

6. Look at a record that is not on hold and confirm that it has the Default marking value.
7. Place the record on hold and verify that the marking value is set to Prevent Delete.

Create a list type marking set

1. Create a list marking set with three marking values.
 - a. For each value, set the constraint mask to deny users from making any modifications to properties or content.
 - b. Set the security to give members of a particular security group full control on the marking value.
 - c. Allow the Administrator full control on each marking value.
2. Create a property template of String type that uses the new marking set.
 - a. Be sure to add the word *declare* to the Description property so that the property is visible during declaration.
 - b. Make the property a multi-valued property, and select the *Unique and unordered values* option.
3. Create a record class that is a subclass of Electronic Record. Add the new marking property that you created to the class.
4. Test the marking.
5. Declare a document as a record using the new record class.
 - a. Assign one marking value to the marking property.
 - b. Sign in to the IBM Enterprise Records web application as a user who is a member of the security group that was granted Use Marked Objects permission for the marking value that you assigned to the property. Verify that this user can modify properties of the record. Note that the user **cannot** change the marking property to any other marking value.
 - c. Sign in to the IBM Enterprise Records web application as a user who is **not** a member of the security group that was granted Use Marked Objects permission for the marking value that you assigned to the property. Verify that this user **cannot** modify properties of the record.
6. Sign in to Enterprise Records as Administrator and add a second marking value to the marking property.
7. Sign in to Enterprise Records as a user who is a member of both of the security groups that are associated with the two marking values. Verify that you can modify properties of the record.
8. Sign in to Enterprise Records as a user who is a member of only one of the security groups that are associated with the two marking values. Verify that you **cannot** modify properties of the record.

Use security markings

Activities

In your Student Exercises

- Unit: IBM Enterprise Records 5.1:
System Configuration
- Lesson: Use security markings
- Activities:
 - Create and use a new marking set.

© Copyright IBM Corporation 2011

Figure 1-50. Activities

F1791.0

Notes:

Use your Student Exercises to perform the activities listed.

Lesson 1.6. Export and import a file plan

Lesson

Export and import a file plan

Why is this lesson important to you?

- The company records manager has created a file plan on a development system and has verified that it works as designed. You must now move the file plan into a production environment. You need to use the File Plan Import and Export tool to do this task.

© Copyright IBM Corporation 2011

Figure 1-51. Export and import a file plan

F1791.0

Notes:

Export and import a file plan

Activities that you need to complete

- Export and import a file plan.

© Copyright IBM Corporation 2011

Figure 1-52. Activities that you need to complete

F1791.0

Notes:

Export and import a file plan

What is the File Plan Tool?



- The File Plan Import and Export Tool is a Java program for importing and exporting file plans.
 - Also called the File Plan Tool
 - Does not support records, volumes, security information
- File Plan Tool uses an XML file to complete the import and export processes.
- The tool can be run the following ways:
 - Start the tool from a command line Java executable.
 - Start the tool with either the FilePlanTool.bat (Windows) or FilePlanTool.sh (UNIX) command file.

© Copyright IBM Corporation 2011

Figure 1-53. What is the File Plan Tool?

F1791.0

Notes:

Help reference

- Search for "fileplan_import_export.htm"

Export and import a file plan

Overview of tasks



1. Configure the File Plan Tool.
2. Export the file plan data.
 - Export the metadata.
 - Export the file plan.
3. Configure an object store.
 - Configure the object store as an FPOS.
 - Configure the security.
4. Import the file plan data.
 - Import the metadata.
 - Wait 5 minutes for the custom class and property metadata to be refreshed.
 - Import the file plan.

© Copyright IBM Corporation 2011


Figure 1-54. Overview of tasks

F1791.0

Notes:

Export and import a file plan

File Plan Tool modes

- 
- **Configure**
 - This mode opens a window that allows you to specify required information, such as the server name and administrator password.
 - **Export**
 - This mode is used to create a compatible and compliant XML file that you can import to another environment.
 - **Import or Update**
 - These modes import a specified XML file into an environment.
 - **Validate**
 - This mode is used to verify that an XML file is compatible with the IBM FileNet P8 XML schema and complies with the XML standard.

© Copyright IBM Corporation 2011

Figure 1-55. File Plan Tool modes

F1791.0

Notes:

You can run the tool in Update mode to make minor modifications after the initial import of a file plan, and you can distinguish subsequent updates from the initially imported XML files.

Export and import a file plan

Configure the File Plan Tool

- The first time that you run the File Plan Tool, you must configure it.
`FilePlanTool -mode configure` (Windows)
- Set the following required configuration options.
 - CE server name
 - File plan object store name
 - Mode (Export, Import, or Update)
 - Web URL
 - EJB URL
- If File Plan Tool fails to run, open `fileplantool.bat` using a text editor and verify the following settings are correct:
 - Web Application Service provider (WebSphere, WebLogic, JBoss)
 - `NAMING_PROVIDER_URL` has the correct CE server and port.
 - `EXT_DIRS` includes the correct JRE path.

© Copyright IBM Corporation 2011

Figure 1-56. Configure the File Plan Tool

F1791.0

Notes:

Web Service URL

Specify the Content Engine Web services web address in this field in the format `http://<content engine server>:<port>`. Example: `http://hqdemo1:9080`

EJB URL

Specify the web address of the Enterprise Java Bean transport to the Content Engine in this field. See the help path listed for the different format required for each supported web application server.

When you configure the File Plan Tool, entries in certain fields define default values that are used the next time the tool is run. For example, when you enter the file plan object store name, the File Plan Tool performs the subsequent actions on that object store.

Export and import a file plan

Target object store configuration requirements



- Create the target object store first.
- The correct data model must be imported to the object store.
 - The data model must match the data model of the exported file plan.
 - The National Archives Records Administration (NARA) properties must exist on the destination object store if they exist on the source object store.
- Assign security roles on the object store before importing.
- Export and import custom properties and classes in a separate XML file before you import the rest of the file plan.

© Copyright IBM Corporation 2011

Figure 1-57. Target object store configuration requirements

F1791.0

Notes:

When you configure an object store to be an FPOS, you can select whether or not to install National Archive Records Administration (NARA) properties. If you select yes, additional electronic record subclasses are installed. If you export a file plan with NARA properties to an FPOS for which NARA properties do not exist, the import fails. If you are not sure whether the file plan has the NARA properties installed, you can look at the installed add-ons on the source object store using Enterprise Manager. Select the object store and click All Tasks > Install AddOn to see which of the add-ons are installed on that object store.

Export and import a file plan

Commands to export a file plan

- If you have custom properties, export the metadata.

```
FilePlanTool -mode export -fileplan "File Plan" -o  
c:\metadata.xml -scope metadata
```

- Export the file plan.

```
FilePlanTool -mode export -fileplan "File Plan" -o  
c:\fileplan.xml
```

- Use the **scope** option if you are exporting metadata or if you are exporting only part of a file plan.
- Guidelines
 - Use double quotation marks around the file plan name if it includes spaces.
 - Use file names that indicate whether the XML file is for the file plan or the exported metadata.

© Copyright IBM Corporation 2011

Figure 1-58. Commands to export a file plan

F1791.0

Notes:

The **-scope metadata** option is not the same thing as a standard metadata export using Enterprise Manager. You must use the **-scope metadata** option if you have custom properties to export with the File Plan Tool.

Export and import a file plan

Export scope options



- You can select a scope for the file plan export in order to do the following:
 - Separate a large file plan into smaller pieces.
 - View and edit smaller export files.
 - Import a large file plan incrementally.
- Scope options
 - metadata
 - robject
 - includecategory
 - excludecategory
 - includecategories
 - excludecategories

© Copyright IBM Corporation 2011

Figure 1-59. Export scope options

F1791.0

Notes:

Use the full path for the record category name. For example: `"/Cat0/Cat01/Cat03"` for Cat03

Includecategory specifies which record category is to be exported.

Use Includecategories to export multiple record categories.

Use Excludecategory to exclude the record category from the export.

Use Excludecategories to exclude record categories from the export.

Use the inclusion options to define the initial scope from which you can use the exclusion options.

Category scope options do not export the Enterprise Records objects. You must use the `robject` option to export Enterprise Records custom objects.

You can use a combination of include and exclude scope options.

Export and import a file plan

Importing a file plan

- If you have custom properties, first import the metadata.

```
FilePlanTool -mode import -f c:\metadata.xml
```

- **Important:** Wait 5 minutes after you import the metadata before you continue to allow the metadata cache to be cleared.

- Import the file plan.

```
FilePlanTool -mode import -f c:\fileplan.xml
```

- When importing, you can set the **-reimportoption** value.
 - Skip: Skip over any existing entities.
 - Replace: Replace any existing entities.
 - None: Like Skip except that it reports a warning in the exception log.
 - Default value is None.

© Copyright IBM Corporation 2011

Figure 1-60. Importing a file plan

F1791.0

Notes:

After you import the metadata, you must wait 5 minutes before you import the file plan because the old metadata is still cached. The cache time-to-live is 5 minutes, after which time the cache is cleared.

Reimport option

Use the **-reimportoption** value to specify the behavior of the add action in the XML file. The option determines what happens when the File Plan Tool adds an object that already exists. During the initial import, use the **Skip** option. In case of failure and during the second attempt at importing the same file plan, use the **Skip** option to avoid reimporting entities that have been successfully imported. If the second attempt fails, you might want to use the **Replace** option.

Scope mechanism not used during import

In Import mode, the tool does not use the scope mechanism, but looks at an XML tag to determine what to import.

Export and import a file plan

Updating a file plan



- Use the update mode to make minor changes after the initial importation of a file plan.

```
FilePlanTool -mode update -f c:\fileplan.xml  
-reimportoption replace
```

- You must specify Update as the InputMode attribute of the FilePlan tag in the XML file.

© Copyright IBM Corporation 2011

Figure 1-61. Updating a file plan

F1791.0

Notes:

Help path

- Search for "file_plan_import_export_tips.htm"

In this example, the `reimportoption` value is set to `replace`. This setting causes existing objects to be replaced with new ones. If your update to the file plan does not replace existing data but adds more data to it, you might choose to use another reimport option, such as `Skip` in order to save time.

Export and import a file plan

File Plan Tool limitations

- You must first export and then import custom properties in a separate XML file before you import the rest of the file plan.
- The File Plan Tool does not support exporting or importing the following objects:
 - Records
 - Volumes
 - Documents
 - Security information, markings
 - Workflow definitions
- No rollback mechanism is supported.
- The tool does not support exporting and importing properties with a null value.
- The data model in the target object store must be the same as the one in the source object store.

© Copyright IBM Corporation 2011

Figure 1-62. File Plan Tool limitations

F1791.0

Notes:

Security on the new file plan

The security of the imported file plan is based on default instance security.

Workflow definitions

If you have workflow definitions that are used by other objects, you need to export the workflow definitions first.

File Plan Tool export file format

The File Plan Tool can use only XML files in a specific format. This format does not match the XML files generated by Enterprise Manager during metadata exports, so you cannot use these XML files with the tool.

Exporting and importing properties with a null value

Properties with a null value cannot be imported. For example, if a phase of a disposition schedule with no retention period is exported and then the disposition schedule is imported into another object store, the retention period is **not** updated to null.

Manually creating XML files

You can manually create and import an XML file that includes schedule inheritance, alternate retentions, disposal triggers, and dynamic or conditional holds. You can find more information about this subject by following the *File Plan XML Schema* link in the help path.

Export and import a file plan

Activities

In your Student Exercises

- Unit: IBM Enterprise Records 5.1:
System Configuration
- Lesson: Export and import a file plan
- Activities:
 - Export and import a file plan.

© Copyright IBM Corporation 2011

Figure 1-63. Activities

F1791.0

Notes:

Use your Student Exercises to perform the activities listed.

Glossary

A

action

See disposition action.

aggregation

Part of an internal event trigger that determines which type of IBM Enterprise Records entity is affected by the disposition action. For example, depending on the aggregation level, a disposition schedule can destroy a single record or an entire folder at one time. When the aggregation level is a container, the action affects all of the entities at that level or below.

alternate retention

An alternate retention period applied to entities that meet specified conditions. In IBM Enterprise Records, multiple alternate retentions can be defined in the same disposition phase. For example, if records are kept in multiple countries, each country might have different laws regarding retention. Records can be retained in each country using a retention interval based on a country property.

See also disposition schedule and disposition phase.

auto destroy

Permanently deletes or destroys records without the use of a workflow. The record removal is immediate when it has reached the end of the retention schedule.

B

box

A container that provides a mechanism to model physical entities that contain other physical entities. Derives from the PhysicalContainer class. See PhysicalContainer.

C

catalog

When declaring a record, the step in which the record class and file plan location are specified.

charge-out

In physical records management, the checking out of a physical record from its home location. This action is handled by the Physical Record Management (PRM) workflow.

charge-in

In physical records management, the checking in of a physical record to its home location. See also charge-out.

classification guide

Security classification guides (SCG) are available only in a DoD Classified data model. Persons with Original Classification Authority can delegate the authority to classify information by creating guidelines to be used by authorized derivative

classifiers. Only users assigned to the Classification Guide Administrator security role can create or modify security classification guides.

classified

When using the DoD Classified data model, a record can be defined as a classified record upon declaration. Classified records have special access restrictions in addition to normal record security.

compliance

Acting in accordance with certain accepted standards, laws, and guidelines.

conditional hold

See dynamic hold.

container

An IBM FileNet P8 folder. In IBM Enterprise Records, a container can be a folder, category, box, volume, or hybrid folder. All of these containers are subclasses of the RM Folder class, which is a subclass of Folder.

See folder.

cutoff

The event that signifies the end of the active period of an entity and the start of disposition.

Cut Off workflow

A workflow that is launched by the cutoff event. The purpose of the Cut Off workflow is to ensure that the records manager reviews the entity after the cutoff trigger and approves the cutoff date. The different phases of the disposition schedule start only after approval of the cutoff date.

D

data model

A template for a file plan object store, to be compliant with certain records management standards. The data model can include metadata and security features. When a new file plan object store is created, a data model must be chosen. Four data models are available:

Base: Satisfies the requirements of most corporations.

Department of Defense (DoD): Includes the properties required by version 2 of the DoD standard (DoD 5015.2)

Department of Defense Classified (DoD Classified): Includes the properties required by version 2 of the DoD Classified standard (DoD 5015.2) for managing classified records

Public Records Office (PRO): Includes the properties required by the PRO 2002 standard.

declare

The act of creating a record object. Declaration and cataloging happen simultaneously. Declaration can be manual or automatic.

declassification review sweep

See sweep processes.

default retention

The phase retention period that applies if either no alternate retentions are specified or if the entity does not meet any alternate retention conditions.

destruction

The removal of the record and the object of the record from the system. For electronic documents, both the record object and the document object are deleted. For physical objects, the record object is deleted. Optionally, the metadata of destroyed records can be retained after the record itself is destroyed, providing a record of the destruction of the record.

discovery

In law, the pretrial phase in a lawsuit in which each party can request documents and other evidence from other parties or compel the production of documents and other evidence using the legal system.

disposal phase

A part of a disposition schedule that controls the retention of entities in a particular state for a specified time period and the disposition action that is performed at the end of the retention period. Also called a phase or a disposition phase. Each phase has a phase retention period and a phase action.

disposition phase

See disposal phase.

disposition

Actions performed on a record after cutoff. Disposition is applied through disposition schedules that are created in IBM Enterprise Records and associated with containers. Disposition includes one or more disposal phases. Each phase has a phase retention period and a disposition action that occurs at the end of that retention period.

disposition action

An action performed on entities after the cutoff is reached or when their retention period in a disposal phase is over. For vital records, it is a periodic review. Disposition actions are created in IBM Enterprise Records. Each action is associated with a workflow. Some examples of actions include Destroy, Review, Export, Transfer, and Vital Review. Actions need to be initiated manually when the retention period of the phase is over. Each phase has an associated disposition action. Each disposition action (except auto destroy) is associated with a disposition workflow. Also called phase action.

disposition hold

A temporary suspension of disposition processing. A hold can be created and then applied to an entity or group of entities. Each hold is for a specific use and can be applied to several entities at one time. In addition, an entity can be placed on several holds at the same time.

disposition schedule

Disposition instructions that specify how long to keep the entity and how to dispose of it. In IBM Enterprise Records, a disposition schedule has

one or more disposition phases. Disposition schedules are created in IBM Enterprise Records and associated with containers. The disposition schedule is inherited by all contained elements within the container, but applies only to the entity type specified by the aggregation.

disposition sweep

See sweep processes.

disposition workflow

A workflow that is associated with a disposition action that automates that part of the disposition process. IBM Enterprise Records comes with several workflows. Examples of disposition workflows include Destroy, Export, and Interim Transfer.

See also disposition action.

document

An object saved in an object store that has properties and security and can additionally have content, versions, lifecycles, and subscriptions. Documents are instances of the Document class or one of its subclasses.

dynamic hold

Refers to the ability to specify conditions for entities to be placed on hold. A scheduled Hold Sweep process determines if any entities meet the conditions of the holds. If so, the hold is applied automatically. Also called Conditional hold.

E

electronic record folder

A folder used for declaring records having electronic data.

entity

A generic term that can apply to a record object or an IBM Enterprise Records container.

event

In IBM FileNet Content Engine, a change in the metadata that, when specified in an event subscription, initiates an event action. For example, an event can be the addition of a document to a folder. The event action might be to declare that document as a record. In IBM Enterprise Records, an event is used to trigger the start of the disposition process or, in the case of vital record review, to trigger the vital review action. See also event action, event subscription, and event trigger.

event action

In IBM FileNet Content Engine, a script or workflow that the Content Engine runs, as defined in a subscription. Event actions can be used to launch workflows and to declare records.

event subscription

In IBM FileNet Content Engine, a definition of conditions required to initiate an event action. An event subscription specifies the class to which the subscription applies, the event that must occur (such as adding a document or changing a property value), and the event action that is triggered.

See also event action.

event trigger

In IBM Enterprise Records, an event that triggers the start of the disposition process. Each event trigger has a condition. When an event occurs that meets the condition, Disposition Sweep marks the entity as being ready for disposition. Several types of event triggers can be configured in IBM Enterprise Records: internal events, external events, recurring events, and predefined date events. In addition, a calendar date in the disposition schedule can be defined to be the cutoff trigger. Also called a trigger, cutoff trigger, or disposal trigger.

external event

An event that occurs outside the system, but that can directly impact the cutoff and disposition of entities. For example, a change in administration might delay disposing of unnecessary or old records. External event triggers are similar to predefined date events, except that the date field is not a required property, which means that the trigger can be created without knowing the future date of the event.

F**file plan**

In IBM Enterprise Records, a container hierarchy that defines the organization of records. The file plan also determines the security and disposition of contained entities. Entities can inherit security and disposition from the parent container in the file plan.

file plan object store (FPOS)

An object store that hosts a file plan. The administrator must create an FPOS by importing the appropriate data models and performing other configurations. After the FPOS is configured, the records manager can create the file plan on it.

FPOS

See file plan object store.

folder

In IBM FileNet Content Engine, an object that can contain other objects. In IBM Enterprise Records, a container that contains record volumes. *See also* volume.

H**hold**

See disposition hold.

hold sweep

See sweep processes.

I**IBM Enterprise Records**

An add-on product to the FileNet P8 system that has special record management capabilities. A records management application (RMA) as defined in the DoD standard 5015.2.

interim transfer

Temporarily transfers records to some other

location. The original record remains in the IBM Enterprise Records system until final disposition occurs.

interim transfer workflow

A workflow that ensures that the home location of a physical entity and location of an electronic entity are changed to the specified location at the end of the retention period of a phase. The records manager must approve the interim transfer of each entity. Before approving the interim transfer of a physical entity, the records manager must ensure that the physical entity has been manually transferred to the new location.

internal event

An event trigger that refers to a change in the metadata of an entity. These events are triggered automatically when the specified condition is fulfilled. For example, the system can track when a volume closes and trigger cut off and disposition at that time. An internal event acts on the type of entity specified in the aggregation field. *See also* event trigger.

N**naming pattern**

Specifies rules used to automatically generate names when new containers are added to a file plan. For example, a container naming pattern can be used to automatically ensure that each new container has a unique category ID. Naming patterns consist of one or more pattern levels that apply to an entire level in the file plan hierarchy (for example, the tree diagram of the file plan). *See also* record pattern.

O**offset**

An optional time gap between the event trigger and cutoff.

P**permanent record**

A record that has been identified as having sufficient historical or other value to warrant continued preservation by the organization beyond the time that it is normally required for administrative, legal, or fiscal purposes.

phase

See disposal phase.

PhysicalContainer

A container used for declaring records for physical items.

physical record

Metadata describing a physical object like paper, tapes, compact disks, and so on.

physical record folder

A container used for declaring records for physical items, such as paper records. A physical folder is a virtual entry for a paper folder.

predefined date event trigger

In IBM Enterprise Records, an external event trigger with a required date field.

R**RDOS**

See record-enabled document object store.

record

A file that references and contains information about another electronic file (document) or a physical object. A record is created to place the document or physical object under corporate or governmental control. The record specifies how the document or object is to be stored, accessed, and, optionally, disposed of. A record is metadata.

record-enabled document object store (RDOS)

An object store that has been configured to allow record declaration. Electronic documents on an object store that is not configured as an RDOS cannot be declared as records.

Note: Do not confuse the RDOS and the FPOS. In *ecm_help* and in the *IBM Enterprise Records Installation and Upgrade* guide, RDOS is called ROS. For the IBM Enterprise Records courseware, the word *document* was added to emphasize the distinction between the RDOS, in which documents are stored, and the FPOS, in which record objects are stored.

record pattern

Used to constrain the names of new records to a pattern that is associated with the container. It is similar to a naming pattern except that it does not generate names, only constrains them. Users must be careful when adding records to a container with a record pattern because the pattern does not allow declaration if the record name is not compliant with the pattern. Care must be exercised when using record patterns with automated declaration.

See *also* naming pattern.

records manager

An IBM Enterprise Records security role, the duties of which include setting up the file plan, triggers, and disposition schedules. Sometimes referred to as a records management professional, or records officer.

records management system

Any system for managing records. In the IBM Enterprise Records courses, a records manager system includes the file plan, disposition schedules, naming patterns, record classes and properties, locations, workflows, and anything else that can be created for records management.

records administrator

An IBM Enterprise Records security role, the duties of which include setting up security, object stores, document and record classes, and metadata.

records reviewer

An IBM Enterprise Records security role (in the PRO data model), the duties of which include reviewing entities that are ready for disposition, declaring records, and performing basic

record-related operations, such as filing or copying records. In the DoD and Base data models, this person is called a Privileged User.

records user

A IBM Enterprise Records security role, the duties of which include declaring and viewing records.

retention period

At a high level, how long to keep a record. In IBM Enterprise Records, a part of a disposition phase that specifies the length of time between cutoff and the phase action. A disposition schedule can have several phases of retention, each with its own retention period. Total retention time is equal to the retention period of the final phase of disposition. The retention period is always relative to cutoff, not to the end of a prior phase. For example, if a review phase is set for one year after cutoff and the second phase is set for a year after the review, then the phase retention period for the second phase is two years (after cutoff).

retention schedule

See disposition schedule.

record types

A categorization of records that has a unique disposition schedule. Record types are used when a group of records existing in a record container needs to have a disposition schedule that is different from the one currently associated with the container. Usually, record types are used when some records must be destroyed before the rest of the records in the container. If a record type has a longer retention than other records in the container, the container is placed on hold until all the records are ready for disposition.

recurring event

Events that recur automatically after a specified time interval. They are used to trigger periodic reviews of vital records. For example, a recurring event called Monthly review with a specified frequency of one month can be created to cause a monthly review of the associated entity.

See *also* Vital records.

ROS

See record-enabled document object store.

S**screening workflow**

A workflow that prompts a reviewer to decide if the disposition of an entity should proceed before executing workflows associated with its disposition phase. Screening is optional and is specified when a disposition phase is created.

spoliation

The willful or accidental destruction of a record prior to its scheduled destruction.

sweep processes

Daemon processes that are scheduled to run at appropriate times in the business day. Sweeps carry out automatic operations, depending on their configurations.

Disposition Sweep calculates disposition-related properties, launches the Vital Review workflow,

and launches the Cut Off workflow where applicable. Disposition Sweep can optionally be configured to perform the auto destroy action.

Hold Sweep finds entities that satisfy the conditions for dynamic holds and applies the hold to those entities.

Declassification review sweep applies only to classified records for which the Declassify On Date or Declassify On Event values are not specified. IBM Enterprise Records uses the Default Declassification Timeframe to declassify these records.

sweep profile

A customized configuration for a sweep process that is saved as a separate file. Multiple sweep profiles provide a way to run sweep processes using different configuration settings without having to reconfigure the sweep process each time.

T

transfer

The act or process of moving records from one location to another, especially from the location the record is used to offsite storage facilities or NARA (National Archives and Records Administration).

transfer mapping file

An XML file that maps IBM FileNet Content Engine property names to XML property names. IBM Enterprise Records Transfer tool includes this file when importing or exporting IBM Enterprise Records entities. When you transfer records and record folders while they are still active, the transfer mapping capability tracks the entities by the organizations receiving and originating the entities.

trigger

See event trigger.

V

vital records

Records that are deemed by an organization as important enough to require periodic review. Whenever a recurring review event occurs, the vital records review workflow associated with the event is launched.

volume

A volume (also record volume) serves as a logical subdivision of a record folder. A folder can contain one or any number of volumes. A volume has no existence independent of the folder. A volume cannot contain a subfolder or another volume.

W

workflow

A business process to accomplish a task. In IBM FileNet BPM (Business Process Management), workflows are automated managed by the IBM FileNet Process Engine. IBM Enterprise Records includes several workflow definitions for performing records management tasks, including the

following: screening, cutoff, and disposition actions.

workflow definition

An electronic representation of the activities and resources required to accomplish a business process. The workflow definition acts as a processing template that the IBM FileNet Process Engine uses each time the workflow runs, routing the work to the specified participants, along with data, attachments, and other information needed to complete the activities.

Z

ZeroClick

Describes the ability to automatically declare records without user involvement. Example: a document is declared as a record automatically when it is added to an IBM FileNet Content Engine folder. A record can also be declared as part of a workflow. IBM Content Collector can direct IBM Enterprise Records to declare e-mail messages as records automatically.

