IBM FileNet Image Services
Version 4.2

Implementing Enhanced Document Security

SC19-3295-00

IBM FileNet Image Services
Version 4.2

Implementing Enhanced Document Security

SC19-3295-00

Note

Before using this information and the product it supports, read the information in "Notices" on page 23.

This edition applies to version 4.2 of IBM FileNet Image Services (product number 5724-R95) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Implementing Enhanced Document Security 7

Implementing Enhanced Document Security

A higher level of document security has been implemented in IBM® FileNet® Image Services. This document provides instructions for establishing the new security for document classes, documents, folders, and WorkFlo queues on all relational database management systems supported by Image Services: Oracle, DB2, and MS SQL Server.

This upgrade is not mandatory. The procedures described in this document are optional for systems that use single-byte character sets, such as US7ASCII, for indexing.

Important Enhanced Document Security is only supported on site-controlled (full-use) relational databases.

Document revision history

Image Services version	Date	Comment
4.2	May 2011	Initial release.

Accessing IBM FileNet documentation

To access documentation for IBM FileNet Image Services products:

1. On the **www.ibm.com** website, enter “Image Services Documentation” in the search box on the menu bar.
2. Select **IBM - Product Documentation for FileNet Image Services** from the list of search results.

IBM FileNet education

IBM provides various forms of education. Please visit the IBM Training and Certification for IBM software page at **/www.ibm.com/software/sw-training**.

Feedback

We value your opinion, experience, and use of our products. Please help us improve our products by providing feedback or by completing a consumability survey.

Documentation feedback

Send comments on this publication or other FileNet Image Services documentation by e-mail to **comments@us.ibm.com**. Be sure to include the name of the product, the version number of the product, and the name and part number of the book (if applicable). If you are commenting on specific text, include the location of the text (for example, a help topic title, a chapter and section title, a table number, or a page number).

Product consumability feedback

Help us identify product enhancements by taking a Consumability Survey (**http://www-306.ibm.com/software/data/info/consumability-survey/**). The results of this comprehensive survey are used by product development teams when planning future releases. Although we are especially interested in survey responses regarding the most recent product releases, we welcome your feedback on any of our products.

The survey will take approximately 30 minutes to complete and must be completed in a single session; there is no option to save a partially completed response.

Background

FileNet Image Services supports Read, Write, and Append/ Execute security access rights for document classes, documents, folders, and WorkFlo queues. The security information for each of these entities is contained in a field that is twelve bytes long and that must be encrypted before it is written to the index database. This security information must be decrypted whenever it is read or queried.

The FileNet algorithm that encrypts and decrypts the security information stores data in the high order bit (the 8th-most significant bit) of each byte in the security information field. This is acceptable when the Image Services system is using the single-column US7ASCII character set because the high order bit of each byte is not being used by the character set. However, if a different character set is being used, the high order bit for encrypting and decrypting the security attributes might conflict with the character translation used by the Oracle, DB2, or MS SQL Server relational database management system.

As a result, the security attributes might not be assigned correctly, and Image Services might interpret unexpected access privileges as ANYONE when they are retrieved from the database.

The new security schema

Three new integer columns were added to the FileNet reserved area of the index (or WorkFlo queue) database during the upgrade to Image Services 4.0 SP3 or later to support the enhanced security schema. These new columns will be used to hold the appropriate security information, independent of any

character set constraints. An added benefit of using integer data is that no encryption is required.

Table Name	Database	Previous Security Access Column Name	New Security Access Column Names
DOCTABA	INX	f_accessrights	f_accessrights_rd f_accessrights_wr f_accessrights_ax
DOCUMENT_CLASS	INX	f_accessrights	Same as above
FOLDER	INX	f_accessrights	Same as above
FOLDER_TABS *	INX	f_accessrights	Same as above
WQS_WORK-SPACES	Workflow Queue	ws_access (workspace security)	ws_access_rd ws_access_wr ws_access_ax
WQS_QUEUES	Workflow Queue	q_descacc (description security)	q_descacc_rd q_descacc_wr q_descacc_ax
		q_contentacc (content security)	q_contentacc_rd q_contentacc_wr q_contentacc_ax

* FOLDER_TABS is an obsolete table.

Prerequisites

Image Services version

Before you begin this update, verify that your Image Services system meets the following minimum software requirement:

Image Services 4.1.2 FP6 or higher
Image Services 4.1.1 FP10 or higher

Avoiding ORA-1555 “Snapshot Too Old” messages (Oracle only)

During the migration you might see ORA-1555 errors in the event log. These messages indicate that Oracle undo (rollback) records are being overwritten because either the undo_retention parameter is not set large enough (with System Managed Undo) or the rollback segment is too small (with traditional rollback segments.).

To avoid this error, for System Managed Undo, you can either increase the undo_retention parameter, increase the undo tablespace, or both. If you use traditional rollback segments, enlarge the rollback segment space.

Important This error is not an issue for DB2 or MS SQL Server because there are no rollback segments or undo tablespaces. The “Snapshot Too Old” error does not apply to these relational databases.

For the purposes of this update, you can double the undo_retention setting or double the size of the rollback segments.

After the migration is successful, return the undo_retention setting or rollback segments to their original values.

Verifying the security schema currently in use

A parameter in the Image Services configuration database (CDB) file indicates whether the newly enhanced multi-column security has been enabled:

1 = original single-column security is in effect.
2 = enhanced multi-column security is in effect.

This parameter was automatically added to the CDB file in Image Services 4.0 SP3 and higher releases. The default value is 1.

To determine the current state of the CDB parameter, enter:

fn_util mlb_get_state

The current security state displays:

multi_cols_security = 1

The original single-column security is still in effect. Continue with the following sections to enable the enhanced multi-column security.

multi_cols_security = 2

The enhanced multi-column security is already in effect.

Backing up the Image Services server

Stopping the Image Services software

Server Types Perform the steps in this section on **all** Image Services servers.

Beginning with Application servers, then Storage Library servers, and finally the Root/Index server, stop the Image Services software on all servers in the system. Follow the steps in the appropriate section:

- **"On UNIX Servers:" on page 13**
- **"On Windows Servers:" on page 14**

On UNIX Servers:

1. Make sure the Image Services software is completely shut down on all servers by entering at each server:

   initfnsw -y stop
   killfnsw -DAy

2. Make sure no fnsw processes are running. Enter:

   ps -elf | grep fnsw

   Kill any remaining fnsw processes:

   kill -9 *ProcessID*

3. Make sure no MasterSnmpd processes are running. (You only need to perform this step on HP-UX and Solaris servers.)

   On HP-UX and Solaris servers, enter:

   ps -elf | grep MasterSnmpd

Kill any remaining MasterSnmpd processes:

kill -9 ***ProcessID***

4 If the Image Services Toolkit is also installed on this UNIX server, shut down all Image Services Toolkit applications, then enter:

wal_purge

5 Skip to the next section, **"Backing up the current Image Services software and data" on page 14**.

On Windows Servers:

1 Open a Command Prompt window.

2 Make sure the Image Services software is completely shut down on all servers by entering at each server:

initfnsw -y stop
killfnsw -D -y

The killfnsw command also stops the Image Services ControlService.

3 Stop the SNMP process by entering:

net stop "SNMP"

Backing up the current Image Services software and data

Server Types Perform the steps in this section on **all** Image Services servers.

As a safeguard, make a backup of the current Image Services software and data using your preferred method.

For complete information on performing a system backup, refer to the “Backup” chapter in one of the following documents:

- ***System Administrator’s Companion for UNIX***
- ***System Administrator’s Companion for Windows Server***

Updating the Index Database

Server Types

Perform the steps in this section on these Image Services servers:

Root/Index server during a Dual server update.

Root/Index/Storage Library server during a Combined server or Entry server update.

Application server with WorkFlo Queue services, SQL services, or VWServices.

Stopping Archive Logging (optional)

On Oracle and DB2 systems, you can optionally stop Archive Logging, if it is currently active. For each database record that is modified during this upgrade, an entry is written in the archive log. To reduce the size of the archive log, consider stopping Archive Logging for the duration of this upgrade.

The Database Administrator is responsible for turning off Archive Logging.

Starting the relational database

Verify that the relational database is up and running. If necessary, ask the Database Administrator to start the RDBMS database.

Using the fn_util mlb_mig_sec_cols command

The **fn_util mlb_mig_sec_cols** command invokes the internal **migr_sec_cols** tool, which in turn spawns multiple instances of the **dbupgade** tool to copy the security information for all the database tables listed in **"The new security schema" on page 9**. The original security information is not changed in any way. After the migration is completed, and after the enhanced schema is enabled, any new security information will be added only in the new database columns.

Syntax

fn_util mlb_mig_sec_cols [-n #] [-o] [-l]

where:

-n # specifies the number of dbupgrade instances. The minimum, which is also the default, is two instances. The maximum is eight instances

-o overrides or remigrates security data to the new security columns. This option causes all security data to be migrated, even if it has already been migrated before. If this option is not present, security data is only migrated to unpopulated new security columns.

-l logs the progress of the migration. This option causes fn_util mlb_mig_sec_cols to create log files in the following directories:

/fnsw/local/tmp/mib (UNIX)
C;\fnsw_loc\tmp\mib (Windows)

If you do not specify this option, no logging occurs.

Usage

To speed the migration process, **fn_util mlb_mig_sec_cols** can run as many as eight instances of **dbupgrade** simultaneously. If you have a very large index database, you might run a maximum of eight instances by using the following command:

fn_util mlb_mig_sec_cols -n 8

To also create log files, you would enter:

fn_util mlb_mig_sec_cols -n 8 -l

To run only six dbupgrade instances and to overwrite the security that was already migrated during a previous run, you would enter:

fn_util mlb_mig_sec_cols -n 6 -o

Multiple instances

When you specify the -n option to run multiple instances of the dbupgrade tool, the migr_sec_cols tool, which is invoked by fn_util mlb_mig_sec_cols, logs onto the relational database and determines the total number of rows in the DOCTABA table, it determines the minimum and maximum document ids in DOCTABA, and then it calculates how many rows each instance should process. Each dbupgrade instance processes as close to the same number of rows as possible.

Background processing

Each dbupgrade instance processes its own section of the database. Regardless of how many dbupgrade instances are running, each instance automatically updates 1000 records before committing them to the database.

The size of the database and the hardware and network configuration determine the amount of time this command might run.

For example, a database containing a million rows might take a few minutes or so to finish. Also, the command typically performs faster on a local database than on a remote database.

Starting the migration

Enter the **fn_util mlb_mig_sec_cols** command with options that are appropriate for your system. For example:

```
fn_util  mlb_mig_sec_cols  -n 6  -l
```

Progress is not shown on the screen, so please be patient. You can monitor the log files to determine the progress of the migration. The system prompt displays when the migration is finished.

Stopping and restarting the migration

You can safely interrupt the migration at any time and resume processing at a later time.

When you run the **fn_util mlb_mig_sec_cols** command more than once, the migration always starts from the beginning of the database and checks every row in each table.

- If changes have been made to the original document security, and you therefore need to specify the -o (overwrite) option, the new multi-column security is updated with new values.
- If no changes have been made to the original security, and if the original security is the same as the new multi-column security. those database rows are bypassed. Thus, the impact on system performance is minimal.

Important If any dbupgrade instances or processes are still running in the background after you interrupt the migration, fn_util mlb_mig_sec_cols will abort when you restart the migration. You might

have to terminate them using available system command before you can restart the migration.

Viewing the system event log

View the system event log to make sure the **dbupgrade** tool completed successfully. Use the **vl** (view log) command by entering:

vl

Tip Oracle only: ORA-1555 errors during the migration indicate that Oracle undo (rollback) records are being overwritten. You can either increase the undo_retention setting in the Oracle initialization parameter file, or contact the Database Administrator to temporarily increase the size of the rollback segments.

For the purposes of this update, you can double the undo_retention setting or double the size of the rollback segments.

After the migration is successful, return the UNDO_RETENTION setting or rollback segments to their original values.

See Oracle documentation for more information.

Enabling multi-column security

When the migration is finished, enable the new multi-column security by entering:

fn_util mlb_enable

This command sets the multi_cols_security indicator in the Configuration Database to “2” – enabled.

Tip The migration must be completely finished before you enable the multi-column security. After you enable this feature, fn_util mlb_mig_sec_cols will not run.

Verifying the new security schema

To verify that the new security schema has been enabled successfully, enter:

fn_util mlb_get_state

You should see:

multi_cols_security = 2

A value of “2” indicates that the new multi-column security has been enabled.

Restarting Archive Logging (Oracle and DB2 only)

On Oracle or DB2 systems, if you stopped Archive Logging at the beginning of this procedure, you can start it again now.

The Database Administrator is responsible for starting Archive Logging.

Updating additional relational databases

Return to the beginning of this section, **“Updating the Index Database” on page 15**, and repeat the procedure on each Image Services server that has a relational database.

After you have updated all the servers with relational databases, continue with the next section.

Starting the Image Services software

Server Types Perform the steps in this section on **all** Image Services servers.

Beginning with the Root/Index server, start the Image Services software on all servers in the system.

1 Start the Image Services Task Manager.

- On UNIX servers: As **fnsw** user, open the FileNet Image Services Task Manager window by entering:

  Xtaskman &

- On Windows servers: From the **Taskbar**, point to **Programs**, **FileNet Image Services**, **Server Applications**, and click the **Task Manager** icon.

2 To bring up the FileNet software, click **Start**.

System messages display in the Current Status pop-up window as FileNet software starts up.

3 When the FileNet software is up and the **Close** button is highlighted, click the **Close** button to close the Current Status window.

4 View the Event Log window to make sure there are no error messages.

5 After viewing the Event Log, chose **Exit** from the File menu to close the Event Log.

6 Repeat the steps in this section on each Image Services server.

Backing up the system

After you have finished defining security for document classes, documents, and WorkFlo queues, you need to make a full system backup.

Important Backups that were made prior to this security update cannot be restored after you have changed the security schema, unless you want to revert to the single-column security schema. It is

essential that you make new backups of all Image Services software and data now.

For complete information on performing a system backup, see the “Backup” chapter of these documents:

- ***System Administrator’s Companion for UNIX***
- ***System Administrator’s Companion for Windows Server***.

Returning to production mode

The new Document Security upgrade has been successfully implemented. You can return the FileNet Image Services system to normal operation.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Corporation
J74/G4
555 Bailey Avenue
San Jose, CA 95141
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

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 an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at **www.ibm.com/legal/copytrade.shtml**.

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

UNIX is a registered trademark of The Open Group in the United States and other countries.

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

U.S. Patents Disclosure

This product incorporates technology covered by one or more of the following patents: U.S. Patent Numbers: 6,094,505; 5,768,416; 5,625,465; 5,369,508; 5,258,855.

Product Number: 5724-R95

Printed in USA

SC19-3295-00