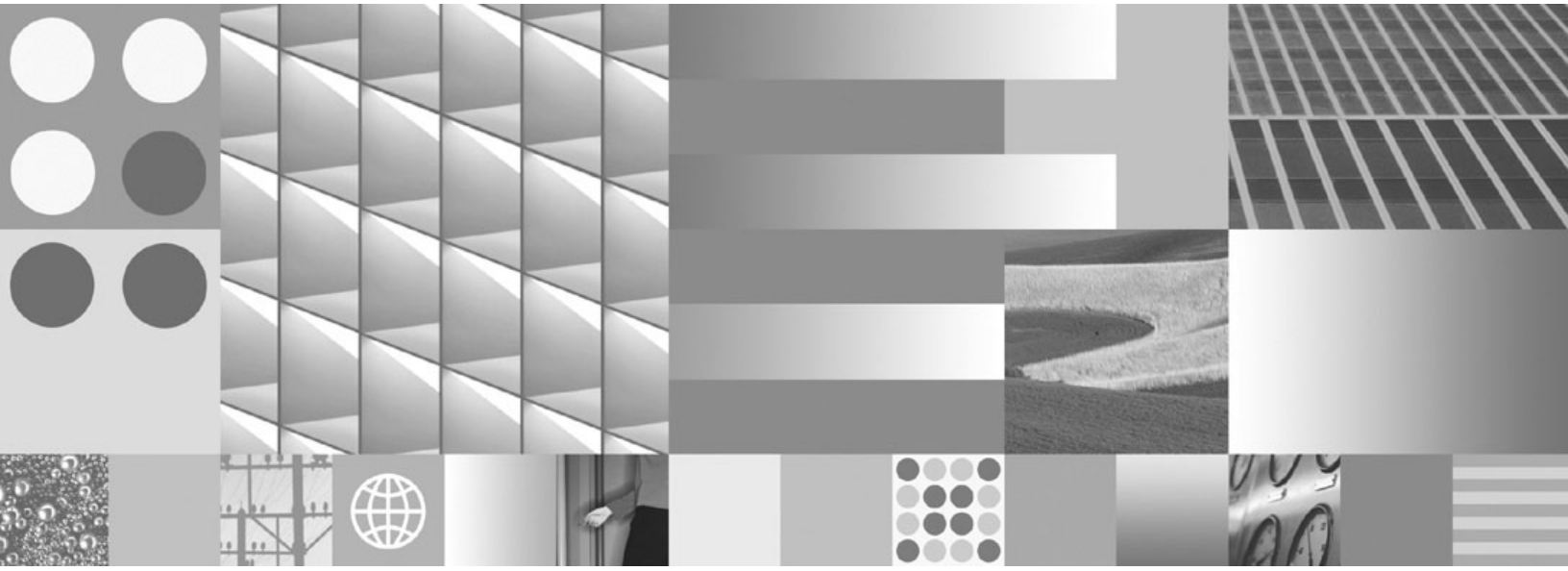
IBM FileNet Image Services

4.1.2

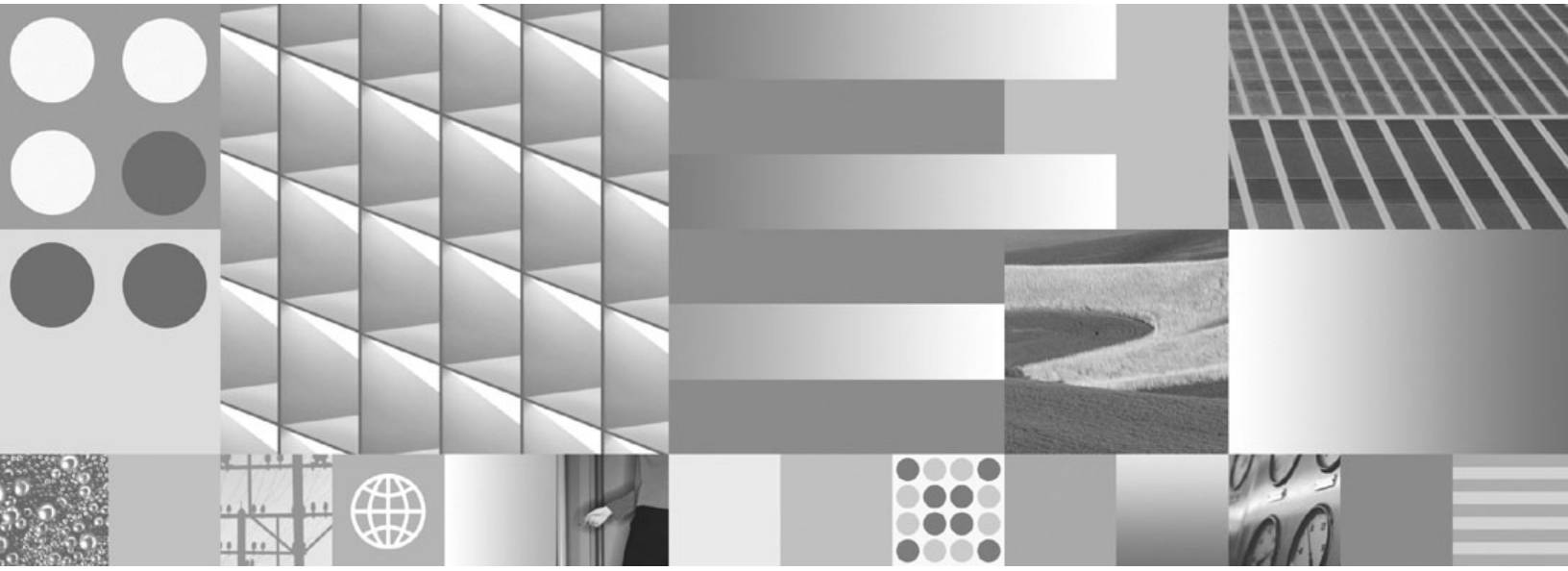


Implementing Enhanced LDAP Security

SC19-2678-00

IBM FileNet Image Services

4.1.2



Implementing Enhanced LDAP Security

SC19-2678-00

Note
Before using this information and the product it supports, read the information in "Notices" on page 17.

This edition applies to version 4.1.2 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 LDAP Security

This document provides instructions for exporting user and group information from an LDAP (Lightweight Directory Access Protocol) server and re-importing it into an Image Services system.

Because information technologies are constantly advancing, security has become one of the major areas that require constant improvement. Image Services tools that export and import LDAP data have been enhanced to keep pace with these demands.

The algorithm that creates LDAP passwords has been redesigned to provide greater security. This improvement, along with other security-related enhancements, ensures that Image Services software continues to provide a solid, robust, high level of security to its customers.

This latest enhancement adds two columns of data to the Image Services security database table. One column contains the name of the LDAP Server and the other contains the IP address of the LDAP Server. Adding these columns provides the ability to import users from multiple LDAP servers.

Audience

Everyone who accesses Image Services through LDAP unified logon needs to follow this procedure to implement enhanced LDAP security.

You do not need to continue with this procedure if you do not use LDAP unified logon or have not implemented the LDAP unified logon environment.

Document revision history

IS version	Date	Comment
4.1.2	Nov. 2008	Initial release.

Accessing IBM FileNet Documentation

To access documentation for IBM® FileNet® products:

1. Navigate to the Information Management support page (**www.ibm.com/software/data/support**).
2. Select the appropriate IBM FileNet product from the “Select a category” list.
3. On the Product Support page, click **Documentation** and then click **Product Documentation**.
4. On the Product Documentation page, locate the document you need, then cick the icon in the appropriate release column to access the document.

IBM FileNet Education

IBM provides various forms of education. Please visit the IBM Information Management support page at (**www.ibm.com/software/data/support**).

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 IBM 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.

Starting Points

For this upgrade, your IS system must already be running one of these releases of Image Services:

- **IS 4.0 SP5 FP2 or higher**
- **IS 4.1.1 or higher**
- **IS 4.1.2 or higher**

These releases of Image Services contain the updated versions of the **cranuser**, **fn_ldif_xfer**, and **LDAP_import** tools, which are used in the following procedure.

Backward Compatibility

Due to the potentially large number of servers and clients involved, you might need an extended period of time to accomplish this update. Because of this, the IS server software is compatible with both the old and new client passwords. During this transition phase, IS will allow LDAP users to log on using either their old or new password.

When all servers and clients have been updated, you can easily turn off the backward compatibility feature.

Back Up the System

Before implementing Enhance LDAP Security, make a complete backup of your system configuration. For complete information on making system backups refer to:

- *Image Services System Administrator's Companion for UNIX*
- *Image Services Enterprise Backup and Restore User's Guide*
- *Image Services Third-Party Backup/Restore Guidelines*

To download these documents from the IBM support page, see **"Accessing IBM FileNet Documentation" on page 8**.

Update the Image Services System

On the Image Services server, re-export and re-import all LDAP users using the LDAP tools. During the re-import process, you must specify the **f** option to force the password to be recalculated and updated. This process needs to be done only once.

If you are an ISRA (Image Services Resource Adapter) customer who supports anonymous logon, you must recreate the IS anonymous user using the **cranuser** tool. You must specify the **s** and **a** options.

If you used the **fn_ldif_xfer** tool to create the XML input file, you must run **fn_ldif_xfer** again for all LDAP users. You must also specify the **s** and **a** options.

Stop the Image Services Software

As the FileNet software user, such as **fnsw**, stop all Image Services processes by entering:

WIN

```
initfnsw -y stop
killfnsw -D -y
```

UNIX

```
initfnsw -y stop
killfnsw -DAy
```

Upgrade the System to the Appropriate IS Fix Pack

You must install the appropriate Image Services Fix Pack that is referenced in **“Starting Points” on page 10**. The Fix Pack installs modules that are essential for implementing the security upgrade. At this time, download the latest Fix Pack.

Recreate ISRA Anonymous Users

ISRA users who support anonymous logons must recreate the IS anonymous users using the **cranuser** tool. Refer to the description of **cranuser** in the *IS System Tools Reference Manual*. To download this document from the IBM support page, see **"Accessing IBM FileNet Documentation" on page 8**.

For example:

WIN

cranuser /hidm1 /sldaphost /a10.55.14.25

UNIX

cranuser -hidm1 -sldaphost -a10.55.14.25

The LDAP server name and its IP address will be used in the recalculation of the encrypted password.

Export the LDAP Users

Export the LDAP users using the ldap_exp tool, the tool that exports users, groups, and group memberships from an LDAP-based directory service, such as Microsoft Active Directory. Refer to the description of the **ldap_exp** tool in the *IS System Tools Reference Manual*. To download this document from the IBM support page, see **"Accessing IBM FileNet Documentation" on page 8**.

Convert LDIF Files to XML Format

IS users who used the **fn_ldif_xfer** tool to create the XML input file, must run **fn_ldif_xfer** again for all LDAP users. Refer to the description of the **fn_ldif_xfer** tool in *IS System Tools Reference Manual*. To

download this document from the IBM support page, see **"Accessing IBM FileNet Documentation" on page 8**.

For example, as the FileNet software user, such as **fnsw**, the command you enter might look like this:

WIN

```
fn_ldif_xfer  /imy.ldif  /ofilenet.xml  /tmsft  /sWinter   /a10.14.5.63
```

UNIX

```
fn_ldif_xfer  -imy.ldif  -ofilenet.xml  -tsun  -sSunspot  -a10.14.5.66
```

Import the LDAP Users

Import the LDAP-based security information into the IS Security Service. This step takes the XML formatted input file and updates the Image Services security database. Refer to the description of the **LDAP_import** tool in the *IS System Tools Reference Manual*. To download this document from the IBM support page, see **"Accessing IBM FileNet Documentation" on page 8**.

For example, as the FileNet software user, such as **fnsw**, the command you enter might look like this:

WIN

```
LDAP_import   /h<server1>  /i<userlist>.xml  /f
```

UNIX

```
LDAP_import  -h<server1>  -I<userlist>.xml  -f
```

The **f** option forces the password encryption to be recalculated and updated with a stronger algorithm.

Update the Client Systems

After the IS server has been updated, you can upgrade all of the client systems, either as a group or one at a time. Due to a potentially large number of client systems, the installation of the updated client applications may require an extended period of time. Because of this concern, the IS server has backward compatibility. The client can log on using either the old or new password. During this transition phase, IS will allow LDAP users to log on using either password.

It is also possible that you may have a large number of IS servers to support. Fortunately, all the enhancements made in IS software are de-coupled from the client enhancements. This means that a mixture of old and new client applications will work with a mixture of old or new IS root servers at the same time.

Your client application suite can be one of the following:

- ISRA
- IDM Desktop, WebServices, Open Client
- Siebel Connector
- eProcess

Back Up the System

When the Image Services update is finished, make a complete backup of your system configuration. For complete information on making system backups refer to:

- *Image Services System Administrator's Companion for UNIX*
- *Image Services Enterprise Backup and Restore User's Guide*

- *Image Services Third-Party Backup/Restore Guidelines*

To download these documents from the IBM support page, see **"Accessing IBM FileNet Documentation" on page 8**.

Important It's especially important to make a backup after this update to the MKF Security database. Earlier backups cannot be restored after the database has been modified.

Return to Production Mode

Now that you've finished updating the MKF Security database, you can place your Image Services system back in normal operation. There should be no change in operation or performance at your current Image Services release level.

Disable Backward Compatibility

After all IS servers and client applications have been upgraded to use the enhanced LDAP security, you can disable the backward compatibility support.

Log onto the Image Services Root/Index server as a member of the fnsw group, such as **fnsw**,

Then use the touch command to create the following trigger file. For example:

touch /fnsw/local/noldapfb.trg

The existence of this trigger file will prevent LDAP users from using their old passwords.

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 Director of Licensing
IBM Corporation
North Castle Drive Armonk, NY 10504-1785
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:

IBM World Trade Asia Corporation
Licensing

2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, 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 Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites 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.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is

available on the Web at "Copyright and trademark information" at **www.ibm.com/legal/copytrade.shtml**.

FileNet is a registered trademark of FileNet Corporation, in the United States, other countries, or both.

Microsoft and Windows 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 may be trademarks or service marks of others.

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.

Program Number: 5724-R95

Printed in USA

SC19-2678-00