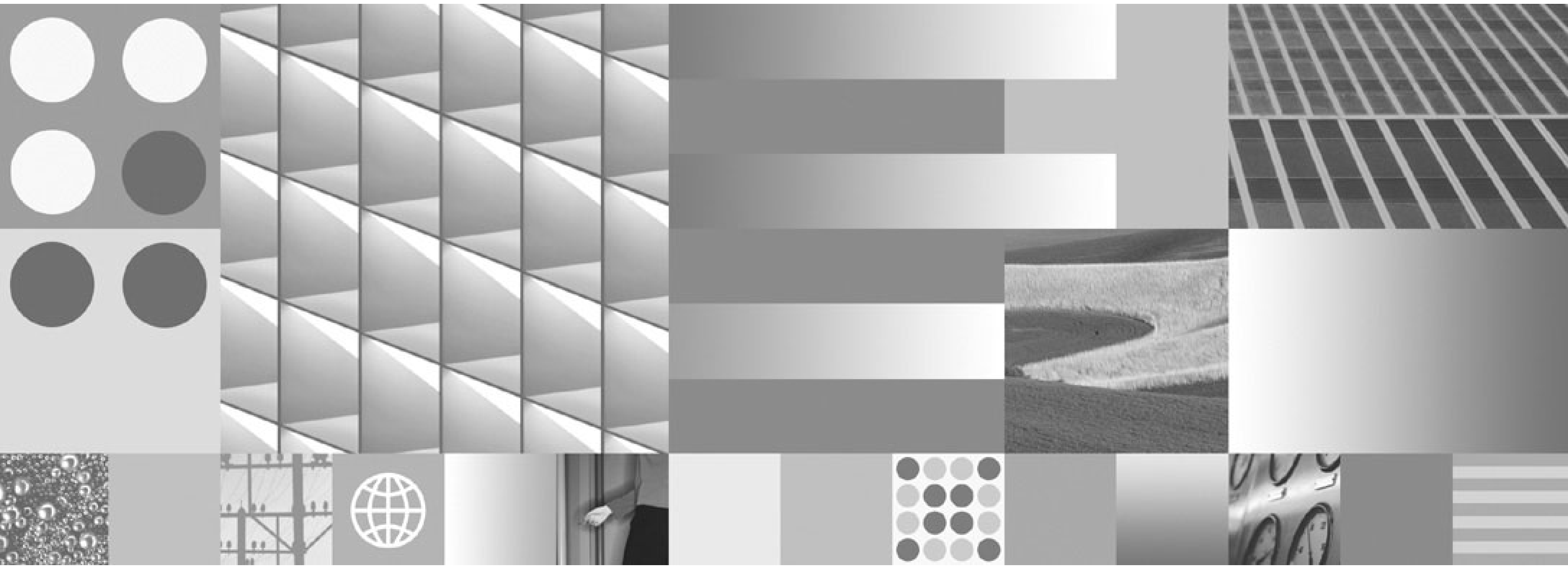
IBM FileNet Image Services Remote Admin Console

4.1.2

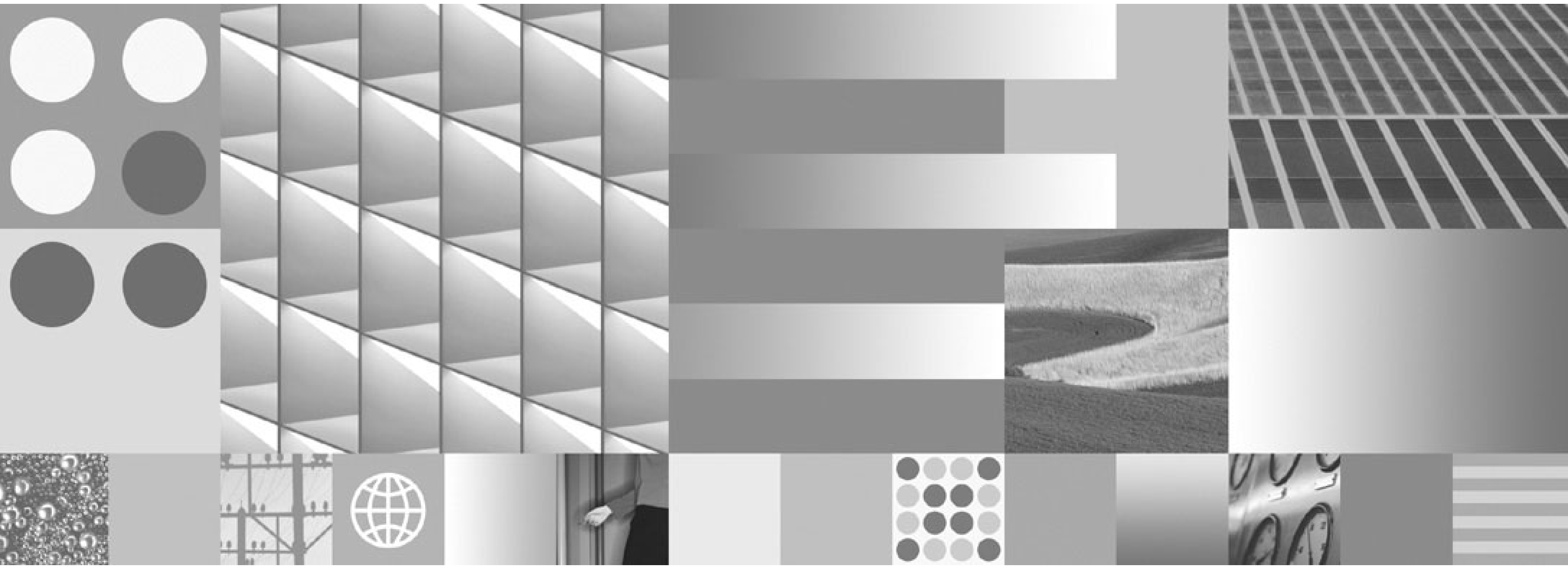


Remote Admin Console User's Guide

SC19-2684-00

IBM FileNet Image Services Remote Admin Console

4.1.2



Remote Admin Console User's Guide

SC19-2684-00

Note

Before using this information and the product it supports, read the information in "Notices" on page 210.

This edition applies to version 4.1.2 of IBM FileNet Image Services Remote Admin Console (part number 5724-R95) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

About This Manual

This manual describes how to use the Remote Admin Console (RAC) to perform various tasks on an Image Services System from a remote Windows®-based personal computer.

Chapter 1, "Remote Admin Console," on page 19 provides an overview of the FileNet® RAC system components.

Chapter 2, "Security Administration," on page 25 describes how to set up FileNet system security.

Chapter 3, "Database Maintenance," on page 107 describes how to create and modify indexes, document classes, and media families.

Chapter 4, "CFS Connector - IS Catalog Export Tool," on page 183 describes how to set default Content Engine (CE) object store mappings for a given IS document class and how to export existing document information associated with an IS document class to make it available for import by a CE system.

Chapter 5, "Database Server Connect," on page 189 describes FileNet RAC system support for the IBM® DB2® relational database.

Chapter 6, "Sample Scenarios," on page 198 presents some examples that can serve as general guides for using Remote Admin Console.

Document revision history

IS version	Date	Comment
4.1.2	Nov. 2008	Initial release.

Related Documents

The following installation and system administration documents are available:

- Remote Admin Console Installation and Configuration Procedures.
- Image Services System Administrator’s Handbook.

Conventions Used in this Manual

The following paragraphs discuss the ways in which we call your attention to information throughout this document.

Computer Output

Information you see displayed at the console (such as displays of file contents, system messages, or output from program execution) is shown in the following manner:

```
costa3(kehr)/home/kehr> fnlogon

FileNet user name: SysAdmin
FileNet password:
FileNet security service (CR = local service):
Program (CR = default shell):

 ------------------------------------------------------

   Name    : SysAdmin:costa3:FileNet
   Logon # : 274
   Last successful logon:
      time : Tue Jan 16 14:15:43 2003
      where: WS001@135.0/2.6:costa5:FileNet
   Last unsuccessful logon:
      time : Fri Jan 12 14:15:29 2003
      where: WS001@135.0/2.6:costa5:FileNet
      error: < 92, 2, 2 >
 ------------------------------------------------------

fnlogon: executing /bin/csh...
```

Lengthy output listings are bounded by bold lines.

File Paths

This manual applies to Windows Server platforms.

The term **FileNet local directory** refers to the Windows server directory \FNSW_LOC.

Cautions, Notes, and Tips

Three message types call your attention to important information:

CAUTION Signals possible damaging consequences of an action, such as loss of data or time.

Note Draws your attention to essential information you should read.

Tip Introduces an idea that might make your work easier.

Command Syntax

Command syntax definitions are indented:

```
fn_msg <errorspec>
```

Required Parameters

Parameters that require you to provide information are shown within angle brackets (< >). For example, for the following command:

```
fn_msg <errorspec>
```

you must substitute the name of a command for the parameter in angle brackets, such as:

```
fn_msg 126,0,103
```

Multiple Server Configurations

MultSv This flag indicates information for users with more than one server. WorkGroup users and other users with single-server configurations should ignore sections with this flag.

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.

1

Remote Admin Console

Overview

The Image Services Remote Admin Console (RAC) makes it possible to perform certain administrative functions of Image Services from remote Windows-based computers.

Traditionally, Image Services admin applications have been available only via the server console, which could only administer the domain hosted by the machine. The user had to use a remote access software product (for example, pcAnywhere, Exceed, or a UNIX® remote login) to run the IS admin applications on a target machine. With RAC, these applications have been repackaged as client-side programs based on a superset of the IS Toolkit, formally known as WorkFlo Application Library (WAL). IS Administrators who want to remotely administer these applications can install RAC on any PC that has computer connectivity to their Image Services server.

RAC can access the following as remote applications that can be used anywhere on your network:

- Security Administration as described in **Chapter 2, “Security Administration,” on page 25**.
- Database Maintenance as described in **Chapter 3, “Database Maintenance,” on page 107**.
- The CFS Connector - IS Catalog Export Tool as described in **Chapter 4, “CFS Connector - IS Catalog Export Tool,” on page 183**.

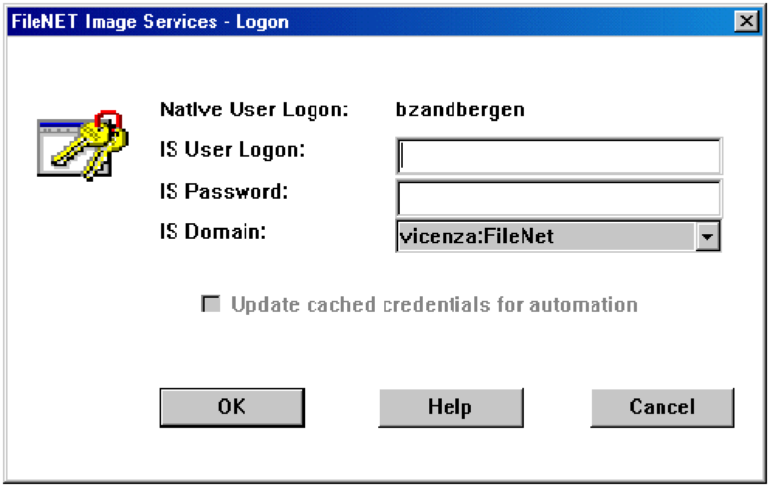
- Database Server Connect as described in **Chapter 5, "Database Server Connect," on page 189**.

Starting RAC

Install RAC according to instructions in the *Remote Admin Console Installation and Configuration Procedures*. To download this manual from the IBM support page, see **"Accessing IBM FileNet documentation" on page 17**.

Note The version of IS Toolkit (ISTK) must be the same as the version of Remote Admin Console (RAC), and **you must install ISTK on the target system before you install RAC**.

After RAC has been installed, start RAC by selecting Start> Programs> FileNet> IS Remote Admin Console. The following dialog box appears:



FileNET Image Services - Logon

Native User Logon: bzandbergen

IS User Logon:

IS Password:

IS Domain: vicenza:FileNet

□ Update cached credentials for automation

The **IS User Logon** and **IS Password** are created by the FileNet Security Administration program. All users of FileNet software require Image Services user names which are not the same as operating system user names. All users require an operating system user name (shown as the **Native User Logon** on the logon screen). The **Native User Logon** displays the operating system logon information.

Note RAC and IS IDM can run concurrently on the same workstation as long as the **same** IS User logs on to both applications. RAC and IDM also allows different IS users to log on concurrently on **different** workstations.

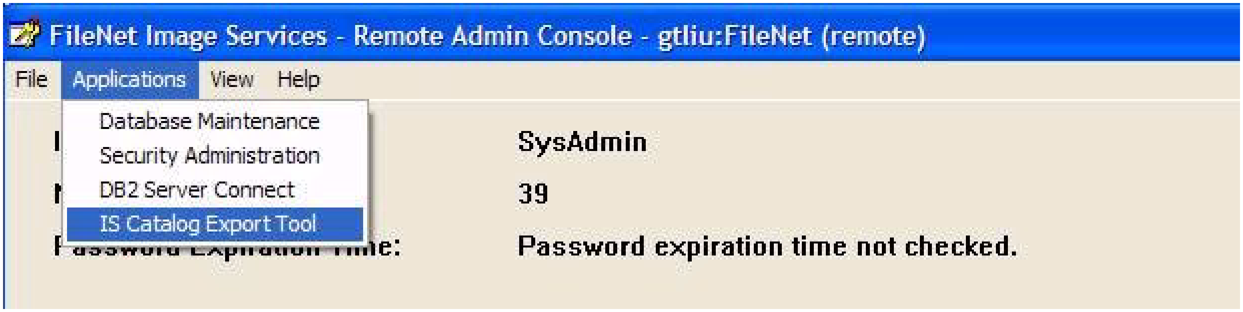
The **Update cached credentials for automation** feature is not supported with RAC.

After RAC has been installed on your PC, the **IS Domain** field is initially blank. The IS Domain field should be in the form Name:Organization. Make sure your RAC PC can access the IS Domain. When you access RAC next time, the most recently used domain name will be the default value.

A **Help** button provides information on the Logon window fields.

Remote Admin Console Main Window

After you have successfully logged on to an Image Services domain, the Remote Admin Console main window title bar appends the domain and organization to the Application Executive title.



SysAdmin

39

Password expiration time not checked.

You can now select Security Administration, Database Maintenance, DB2 Server Connect or CFS Connector - IS Catalog Export from the Applications menu.

Software

The Image Services software consists of applications and services. Applications forward user requests to FileNet software services. The system administration applications available from your RAC PC are:

System Administration Applications

Application	Description
Security Administration	See **Chapter 2, “Security Administration,” on page 25** to create user accounts for the FileNet software as well as set up security attributes.
Database Maintenance	Sets up and maintains your index database. See **Chapter 3, “Database Maintenance,” on page 107** to create and modify indexes, document classes, and media families. You can use the reporting features of Database Maintenance to obtain information about user indexes, document classes, and media families. Database Maintenance also includes several special-purpose tools.
CFS Connector - IS Catalog Export	See **Chapter 4, “CFS Connector - IS Catalog Export Tool,” on page 183**. This chapter describes how to set default Content Engine (CE) object store mappings for a given IS document class and how to export existing document index information associated with an IS document class to make it available for import by a CE system.
Database Server Connect	See **Chapter 5, “Database Server Connect,” on page 189**. This chapter describes FileNet RAC system support for the IBM DB2 relational database.

Online Help

The RAC help system provides a table of contents, keyword search capabilities, hypertext links, and browse sequences.

The Help pull-down menu contains these options:

Help Menu Option	Function
Contents	Display table of contents for online help
Search for help on	Search for a particular help topic
How to use help	Instructions for using online help
On Context Help	Display a help window related to the currently-active window
About	Display information about the current version of Image Services software

Commands

RAC provides the following commands: fn_msg, wal_ipc and stamp. For usage information on each command, refer to the *Image Services System Tools Reference Manual.* To download this manual from the IBM support page, see **"Accessing IBM FileNet documentation" on page 17**.

Printing

You can print reports to any Windows-based printer that has been configured for your PC. (These are printers that have been set up through Windows printing.)

2
Security Administration

Overview

Remote Admin Console (RAC) enables you to use the Security Administration application to control user logons, passwords, devices, and the group memberships that determine access to system data and functions (menu options).

Basic Concepts

Security Administration is governed by a set of basic concepts that apply to a number of different parts of the system. When you understand these concepts, the interactions between the different parts of the Security Administration system are easier to understand.

Security Object

Users, groups, and devices are security objects. You can apply most security characteristics to users, groups, and devices.

User

A user is a security object that can log on and perform tasks.

Group

A group is a security object to which you can assign one or more users, devices, or other groups. Some group assignments confer membership; other group assignments, such as those of administrative or session groups, do not confer membership. A group cannot log on or perform tasks. You define data objects with groups or users, including (ANYONE) or (NONE), with read, write, and append/execute permissions.

Device

The two major types of security devices are:

- Terminals
- Printers and fax servers

Terminal security controls logons and data access from the terminal.

Printer and fax server security controls access to print and fax devices. Setting up printer and fax security is a two-step process. You must configure the printer and fax on the server using the Configuration Editor first. Then you can set up printer and fax security.

Permission

Permission is the privilege granted to a security object to perform certain tasks. Each security object has permissions based on its own definition, as well as the definition of the system and the groups of which the object is a member. The extended memberships and override capabilities of the requesting user, groups, and devices control permissions.

Administrator

An administrator is a user assigned special privileges to perform security tasks affecting users, groups, and devices. The four administrative attributes are: supervisor, principal, group, and password. By assigning various combinations of administrative attributes to different users, you can provide checks and balances in your security system.

Membership

You can assign membership for users and devices in one or more groups. A user or device inherits the permissions of all groups of which the user or device is a member. You can assign a group membership in one or more groups. The group inherits the permissions of all groups of which it is a member.

Extended Membership

A user is a member not only of the groups to which the user is assigned, but also to any groups to which those groups are, in turn, assigned. Use extended membership with caution. Be certain you know who is a member, directly or through extended membership, when you expand privileges by assigning one group to another.

You can use group membership to control who can log on from which terminals, access which data, and use which print and fax devices. A security object may belong to any number of groups, either directly or through extended membership. For example, if a user is a member of group A, and group A is a member of groups B and C, and group C is member of groups D and E, then the user is a member of groups A, B, C, D, and E. Through extended membership, the user inherits the permissions of **all** these groups and can perform tasks that require permissions beyond those explicitly assigned to group A.

Administrative Domain

Any user with administrative attributes can manage his own administrative group and any other administrative group of which he is a member. This is the user's administrative domain.

Session

A session is a single logon occurrence. You can assign users to a session group, allowing addition or modification of logon privileges for an entire group of users at once. Assigning a session group is optional.

Data Object

Documents, folders, and annotations are data objects. You can assign security to these objects through the groups, granting them read, write, and append/execute privileges using the Database Maintenance program (see Document Security in the *Image Services System Administrator's Handbook*). To download this handbook from the IBM support page, see **"Accessing IBM FileNet documentation" on page 17**.

Override

The system override attribute causes the security object’s attributes to be used instead of the system attributes in certain instances. Attributes for which overrides apply are: device security, time use restrictions, security logging, and maximum concurrent sessions.

You can set system overrides for groups, users, and devices. Permission to perform a given task depends on how you set these overrides for the user, the terminal, any other device required, and the extended group membership of the user, terminal, and device.

You can reserve the ability to permit groups, users, or devices to override the system defaults for SysAdmin or grant it to other administrators.

Template

Templates are security objects with default attributes to assist you in creating users, groups, and devices. When you create a user, group, or device, it inherits its attribute values from its template. You can customize the three templates provided by Security Administration.

Expiration

Expiration makes a user, group, or terminal unusable after exceeding the time set by an administrator. You may also set user accounts to an expired status if the user does not renew a password when required or if he has exceeded the permitted failed logon attempts. The system does not delete an expired security object, which the appropriate administrator can reactivate.

Logging

The system writes security logs daily and keeps them for 28 days. On the 29th day, the system overwrites the oldest security log. To view security logs, select Events Log from the System pulldown menu. Note that security logs are different from system event logs.

Security Database

The security database sec_db0 is a multi-keyed file (MKF) database that contains security information for:

- the FileNet system
- each object (user, group, device)
- each direct membership occurrence
- each function name and class
- each database logon

The system stores security information with its related data. For example, the system stores document security along with the document indexing information in the index and permanent databases; it stores annotation security in the permanent database.

System Security

As SysAdmin, you can set the default security for the FileNet system. You can use the system default settings provided with the system or you can modify the default system security. See Set Up FileNet System Security in the *Image Services Administrator’s Handbook*. To download this handbook from the IBM support page, see **"Accessing IBM FileNet documentation" on page 17**.

Group Security

A group is a security object to which you can assign one or more users, devices, or other groups. A group cannot log on or perform tasks. You create a group and assign security objects to the group for one of two reasons:

- To permit an administrator to set values for several security objects at once
- To grant the object certain privileges held by the group, such as access to devices, data objects, and functions

The system reserves the following groups for special uses:

- (NONE)
- (ANYONE)
- SysAdminG
- AuditG
- FieldServiceG
- OperatorG

For details, see **"Reserved Groups" on page 32**.

The following group assignments have special meaning:

- Primary Group Assignment
- Administrative Group Assignment
- Session Group Assignment

For details, see **“Group Assignments” on page 33**.

Administrative and session group assignments do not provide membership privileges in the group.

Reserved Groups

The following table describes the six reserved security groups: (NONE), (ANYONE), SysAdminG, and AuditG, FieldServiceG, and OperatorG.

Reserved Group	Description
(NONE)	A group name used to specify that no one has access to an object except SysAdmin and members of SysAdminG. The group name is in all caps and includes the parentheses.
(ANYONE)	A group name that you use to specify that everyone has access to the object. The group name is in all caps and includes the parentheses.
SysAdminG	The name of the group whose members can read, write, and append/execute all documents, annotations, folders, queues, procedures, and so forth, on the system. This group is a member of all groups.
AuditG	The name of the group whose members can read, but not write or append/execute, all documents, annotations, folders, queues, procedures, and so forth, on the system.
FieldServiceG	A group created only for compatibility with previous releases. FieldServiceG has no special permissions.
OperatorG	A group created only for compatibility with previous releases. OperatorG has no special permissions.

Refer to **“Group Assignments” on page 33** for the meaning of (NONE) and (ANYONE) when assigned as administrative, primary, or session groups.

Members of the SysAdminG and AuditG groups have no power to create and activate users, assign them to groups, modify their attributes, or change passwords unless the members also have the corresponding administrative attributes. See **“User Security and Administrative Attributes” on page 37**.

Group Assignments

You can make users, devices, and groups members of an unlimited number of groups. In addition, you can make three special types of group assignments: administrative, primary, and session.

Administrative Group Assignments

The system assigns every security user, device, and group to an administrative group. An object’s administrative group determines which security administrators can perform administrative tasks for the object (for example, activating an expired account). An object’s administrative group also determines which administrators can perform administrative tasks for the object’s extended membership and data object access.

A security object’s administrative group is inherited from the administrator who created the object. Only SysAdmin can delete an administrator or change the administrative group of a security object. If the administrative group is (NONE), only members of SysAdminG can administer the object. If the administrative group is (ANYONE), anyone with administrative attributes can administer the object. Although the administrative group is assigned to the object, the object does **not** become a member of the administrative group.

You can set up your security system with the same groups as membership groups and administrative groups. However, you may want to create certain groups that are used only as administrative groups.

Primary Group Assignments

Every user is assigned one primary group and becomes a member of that primary group. The primary group assigned to a user determines who has access to various data objects created by that user. The data objects affected by a user's primary group include the following:

- annotations, notes, and highlights created through your desktop application
- folders
- WorkFlo systems, procedures, and queues
- forms and signatures on forms

Note The document class security controls access to user-generated documents and batches, rather than the user's primary group.

The default primary group for users is (NONE). If you leave (NONE) as the primary group for a user, then no one except SysAdmin and members of SysAdminG has access to data objects the user creates. You can change a user's primary group to (ANYONE). All folders, annotations, and WorkFlo queues then created by the user are accessible to everyone. Permissions for existing data objects created by a user are not changed when the user's primary group changes.

If the user's primary group is changed, the user retains membership in the original primary group, while acquiring membership in the new primary group. The administrator who assigns the primary group can assign any group in the administrator's administrative domain (see **"Administrative Domain" on page 28**). The primary group for a group is itself, by definition, and the group's primary group assignment cannot be changed.

Session Group Assignments

The administrator assigns every user to a session group (groups and devices do not have a session group). The purpose of the session group is to permit an administrator to control logon privileges, such as logon times and expirations, for a group of users. By assigning a particular session group to several users, the administrator can add or modify logon privileges for the entire session group at once.

A session group assignment does not affect a user whose system attributes are set to override the system defaults, since the user values always override the session group values. The default session group is (NONE), which is equivalent to not having a session group. (ANYONE) cannot be assigned as a session group. The session group is assigned to the user, but the user does **not** become a member of the session group.

Tip To prevent users from logging on when you need to perform a task such as defining indexes (see Define an Index in the *Image Services System Administrator's Handbook*), put all the users in a session group and expire the session. To download this handbook from the IBM support page, see **"Accessing IBM FileNet documentation" on page 17**.

Group Deletions

Before deleting a group, you need to be aware of what kind of data access or logon restrictions the group is providing to users. For example, if you delete the group that has read access to many of the documents on your system, many users would no longer have access to the documents they need.

If you delete a group functioning as a session group, then users that formerly had logon restrictions might suddenly have no restrictions or no access, depending on their override capabilities.

When you delete an object’s primary group, that object’s primary group reverts to (NONE), but membership in the group is not revoked.

Before deleting a group, you can review its members and see what groups it is a member of. However no report shows you which objects depend on the group as a session or primary group.

You should not delete an administrative group without first using the Re-Assign Administrative Groups function. If you are not SysAdmin, then you must ask SysAdmin to run the Re-Assign Administrative Groups function. See Reassign Objects to a Different Group in the *Image Services Administrator’s Handbook* for details. To download this handbook from the IBM support page, see **“Accessing IBM FileNet documentation” on page 17**.

If SysAdmin deletes an administrative group, the group attribute becomes (NONE) for all objects to which this administrative group had been assigned.

Deleting an administrative group has the following effects on the administrators for whom it was their administrative group:

- The principal administrator can still create objects but no administrator can see any of the objects.
- Only SysAdmin can administer objects with the group attribute (NONE).
- Reports (summary, detail, extended membership) are blank. Administrators can still view current logons and event logs.

Note You cannot delete the reserved groups: SysAdminG, AuditG, FieldServiceG, and OperatorG.

User Security and Administrative Attributes

If you are SysAdmin (or if the Allow System Override system default is checked), you can allow a particular user to override system defaults. For example, that user could set logon times which are different from the system default.

Many user permissions are granted through direct and extended group membership. A user is a member of the following groups:

- Primary group
- All groups of which you explicitly make the user a member
- All groups of which the explicitly assigned groups are members through extended membership

Always be aware of the extended membership of any group you make a user a member of.

Note Assigning an administrative or session group to a user does not give the user membership within that group.

The two broad classes of users are:

- Administrative users
- Nonadministrative users

Administrative users are distinguished by the assignment of one or more administrative attributes: Supervisor, Principal, Group, and Password. You can assign one or more administrative attributes to a user.

Four attributes give a user administrative abilities:

Administrative Attributes

Attribute	Description
Supervisor	Can update and delete security objects and log off users. Can manage users, groups, and devices belonging to the supervisor's extended group membership. Only an administrator with the supervisor attribute can view event logs and activate user accounts by turning off the expired status.
Principal	Can add security objects and log off users. When a principal creates a security object, that object automatically acquires the administrative group of the principal administrator. This group determines which administrator can manipulate the object. When a principal administrator without the supervisor attribute creates a new security object, the object is set to an expired status. A principal administrator without the group attribute cannot set or change a user's primary group.

Administrative Attributes

Attribute	Description
Group	Can add members to and delete members from groups and functions, as long as the members are in the administrator’s extended group membership.
Password	Can add or update passwords of non-administrative users within the administrator’s extended group membership. Unless the password administrator also has the supervisor attribute, the user must be expired by a supervisor before the password administrator can change the password.

Some changes can be made only by administrators with a combination of attributes or by the SysAdmin user. SysAdmin is a special user with all administrative privileges and membership in all groups. Attributes are assigned on the Add User and Update User dialog boxes.

Only SysAdmin can create, modify, and delete administrative users. Administrative users cannot modify each other’s characteristics.

In a small installation, one or two administrators might perform all administrative functions. The SysAdmin user can also perform these functions. In a large installation, one administrator might be in charge of keeping passwords and would need only the Password attribute. Another administrator might be in charge of creating and updating users and would need Principal and Supervisor attributes.

Since group membership determines what security objects users can access, you could divide responsibilities for group memberships among several administrators who understand the details of their groups and can assign people to the appropriate groups. Administrative attributes do not control access to data objects, such as documents, folders, annotations, or queues. Only group memberships allow access to data objects.

Document Security

For each data object (document, folder, annotation) you can assign the following access privileges:

- User or group name that has read access
- User or group name that has write access
- User or group name that has append/execute access

The meanings of these access types depend on the data object. You control access to data objects by putting the appropriate users in the groups that you assign to each type of access.

Document Classes

Batches and documents acquire security attributes from their document class. A newly created document class uses (ANYONE) for each type of access (read, write, append/execute). To secure documents in this class, change the security attribute to an appropriate user or group name.

Specify the security attributes for the documents in a document class when you create the class. If you change security for a class after committing documents to it, documents already committed have the old security attributes which differ from documents committed after the change.

Note You cannot change security attributes for committed documents on a FileNet RAC system.

Each annotation, margin note, and highlight has its own security attributes. See **"FileNet Notes" on page 41**. In addition, each tab has its own security attributes. See **"Tabs" on page 42**.

Uncommitted Batches

Batches acquire security attributes from their document class. Operators who scan, index, reassemble pages, commit batches, or delete uncommitted batches need read, write, and append/execute permissions.

Folders

When a user creates a folder, the system assigns permission to read, write, and append/execute to the user's primary group. To see or perform any operation on the folder, a user must belong to that group. You can change the group. You cannot set append/execute for folders on a PC workstation. Your desktop application automatically uses the group with write access as the group name for append/execute.

FileNet Notes

Each FileNet note (which includes annotations, margin notes, and highlights) has three security attributes: read, write, and append/execute access rights. When a user creates a FileNet note, permission to read, write, and append/execute is assigned to the user's primary group. The system checks note access rights when the user accesses notes in a display dialog box.

Tabs

Each tab has three security attributes: read, write, and append/execute access rights. When a user creates a tab, permission to read, write, and append/execute is assigned to the user's primary group. The system checks tab access rights when the user toggles between notes and tabs in a display dialog box.

Note When users **without** a primary group create folders, notes and tabs, those objects will have access rights set to the user, not the group. If that user should be deleted from the security database, no other users will be able to access those objects.

Function Security

Function Security controls access to the Image Services system administrative applications. These applications can be restricted to specific Security Administration defined users and/or groups which can be logically mapped to specific roles or functions within an organization. For finer granularity control, specific functions within the administrative applications can also be restricted. For example, a particular night shift operator's role may only allow for accessing specific functions within the Storage Library Control application. All other Image Services administrative applications would be locked out for this user. This user's role would be mapped to a specific Security Administration defined user or group. This user or group would only be linked with the specific Storage Library Control functions that apply to this person.

Although RAC only provides direct access to the Security Administration and Database Maintenance applications, you can set up Function Security for all Image Services administrative applications through RAC. The Function Security that's set up for Database Maintenance will apply to users and groups that logon through RAC as well as through the Image Services Application Executive (on the server). The Function Security that's set up for applications, such as Storage Library Control and Background Job Control, will only apply to users and groups that logon through the Image Services Application Executive. For example, in RAC, you can define access to the Storage Library Control application to a specific Security Administration defined group. When someone that is not a member of this group logs on to the Image Services Application Executive (on the server), they will not see the Storage Library Control program listed under the Applications menu.

Relationship Between Roles and Tasks

A role is defined as a function access that performs a specific task(s). Roles are basically derived from Function Codes. There is a role associated with each function code. The text describing what the role does is called the Function Name.

For example, dbmaint is a function code that is used for controlling access to the Database Maintenance application.

Function Code:	dbmaint
Function Name or Role:	Database Maintenance

A function code is always associated with a role or function name. A role is always associated with a function code.

The Security Administration function menus provide a high-level, user-friendly interface. Each role that a user activates enables one or more tasks for a particular application. In most cases, each role can perform only one task. However, there is one special occasion where a role (function code) allows users to perform multiple tasks:

Role	Allowable Task
Enable/Disable Storage Library	Enable/Disable Media Enable/Disable Library Enable/Disable Slot Enable/Disable Grippers Enable/Disable Drive

Listed below are the Application Level and specific Feature Level functions that can be activated through Function Security.

Note This is a fixed Feature Level Role set that is built into the IS administration applications.

Application Level Role	Feature Level Role
Database Maintenance	Archiving Utilities Delete Doc/Folder Update Document Security Update Retention Parameters Define/Update Index Rename Index Build Retrieval Key Drop Retrieval Key Define/Update Cluster Index Report Build Menu Define/Update Class Class Report Define/Update Family Family Report
Security Administration	NONE. Security Administration has built-in function access. Only administrators can access most functions, and what is accessible depends on each administrator's attributes. See **"Built-in Security Attributes (Security Administration Application)" on page 49**.

Application Level Role	**Feature Level Role**
Storage Library Control	Detailed Surface Info Pending Surface Requests Media Space Usage Local/Foreign IDs Create Doc Header File Enable/Disable Storage Library Change Media Type Media Family Info Change Family Name Local Statistics Remote Committals Respond to RSVP Delete Info Message Configure Library screen Insert Media Eject Media Preformat Media Slot Drive Map Media Surface Summary Calibrate Library Identify Media in Library Write Services Information Eject Media by Location Delete RSVP MSAR Backup

Application Level Role	**Feature Level Role**
Background Job Control	Incorporate Foreign Media Manually Incorporate Foreign Media Copy Documents Copy Documents Using File Copy Annotations From Database to Media Consolidate Media Erase Media Rebuild Media Import Documents From Media Create Archive Database Import Archive Image Service Find Open Documents Completed Jobs Results of Find Open Documents Modify Status of Background Job Delete Log of Completed Job MSAR Convert Migrate Documents

Application Level Role	**Feature Level Role**
Cache Export/Import	Export Cache Objects Show Cache Objects Import Cache Objects Cache Backup Program
COLD Main Menu	Define Background Template Define Channel Control File Define Report Format Define Import Job Preview Documents Import Documents View Import Log

Application Level Role vs. Feature Level Role

It is important to understand that application level roles control access to feature level roles (menu options). Think of an application level role as a gate. When the gate is closed (application not launchable), none of its associated feature level roles can even be accessed. When the gate is open, all feature level roles behind that particular gate are now accessible and further security function checking may be imposed.

In general, responsibility-based access control (RBAC) should be achieved by activating application level roles only. However, in order to fully take advantage of function security, feature level roles should also be activated. See **Chapter 6, “Sample Scenarios,” on page 198** and **“Best Practice” on page 50**.

Built-in Security Attributes (Security Administration Application)

In the table starting on **on page 45**, there are no feature level roles listed for the Security Administration application. This is because the Security Administration application has built-in security levels that are not part of functional security. The four major security attributes SUPERVISOR:Supervisor, PRINCIPAL:Principal, GROUP:Group and PASSWORD:Password are entirely controlled within the Security Administration application itself.

Default Behavior

The default behavior for Image Services is that if a role hasn't been activated, then anyone has access to the role. This is determined by the global setting **Allow Access to Undefined Functions** in the **Default Security Settings** window which is enabled by default. When a role is activated, everyone who should have access to it needs to be specifically added to that role (either directly or by group reference). Therefore, when a function is activated for the first time, anyone that is not included in the function's access list will lose access to that function. A suggestion is to initially put [ANYONE] in the controlled list until you are comfortable that all authorized groups and users have been accounted for. If a role is activated, but with no members, then no one has access to that role except for SysAdmins.

When the global setting **Allow Access to Undefined Functions** is unchecked (OFF), no one is allowed access to unactivated roles. Granting access to a user is done by making the user a member of the activated role. Setting up function security in this manner is a much more cumbersome process, since all functions must be specifically activated.

Special user: SysAdmin

SysAdmin is a special user who has access to all roles regardless of the state of the global setting.

Best Practice

In general, the best practice is to always apply security against groups or roles. Add users to one or more groups as appropriate. Only in special cases should security be granted directly to a user.

New System Considerations

It is very important for you to understand the usage, power, scope and features of RBAC. Please read **“Default Behavior” on page 49** before setting up function security on your system. It is suggested that you create a sample scenario where a test user and group are given certain roles to understand how function security operates.

If a new system is being set up, it is easy to suggest what some common roles might be (for example, data center operator, application developer, help desk, application user, and application manager). In general, establish groups to support roles that exist in the company. Based on the needs of each group, function access should be activated to support the desired level of security and appropriate groups added to each function. New installations should activate each of the major application function names with the user [ANYONE] placed in each application function where it is appropriate for anyone to run the program. Each user should be assigned his own user ID and each user ID should be placed into the appropriate group(s).

Existing System Considerations

If an Image Services system already has function codes activated, all previously entered function codes now appear as function names. In the **Activate Function Name** window, which is displayed via the Function pulldown menu, you are no longer required to enter a precise function code. Instead, you can choose from a list of roles. If you had previously entered incorrect function codes, these invalid function codes will be appended with the string **Unsupported Function** in the **Deactivate Function...** window and the **View Functions and Members...** window. The best thing for you to do is to delete these invalid codes.

RBAC is backward compatible with function codes. Although it is strongly recommended that users adapt to function names because they are more descriptive, users who prefer to see function codes as they did previously can still do so by enabling the Toggle Function Code Display option via the Function pulldown menu.

Note You may want to refer to Appendix A, Function Codes in the *Image Services Administrator's Handbook* for a full listing of these codes. To download this handbook from the IBM support page, see **"Accessing IBM FileNet documentation" on page 17**.

An administrator with an existing system must be careful, depending on what aspects of the system he wishes to control. Often on pre-existing systems, users are allowed access to any undefined function codes and probably have no function names activated. This means everyone can run anything assuming they can access the IS server. Once they activate a function, only those people who are in groups added to the function (or who are added to the function directly) are able to run the application associated with the function name. Unless you already have a good mapping of roles to groups, you may encounter some initial difficulty in resolving which groups and or individuals should be granted access. Defining new groups and then adding existing users and groups to them could be the cleanest way to address this.

General Considerations

In the following two examples you should define function access names for all administrative applications:

- Allow access only to Security Administration by help desk personnel.
- Allow access only to Storage Library Control related functions by data center operators.

Any application without an activated function name is open for use by anyone by default. So, for example, to exclude the help desk personnel from everything except Security Administration means that all application level functions should be activated. The help desk role-based group would be added only to the **Security Administration** function name. Similarly, the data center operator group is added only to the **Storage Library Control** function name (and probably also to the **Background Job Control** function name).

In day-to-day usage, administrators need to set up users and groups carefully. It is best to handle security control through groups, so choose functions that a group has access to when the group is created.

Device and Terminal Security

To use device security for printers and fax servers, your support representative enables security while configuring the device through the System Configuration Tools (see the System Configuration Tools online help). You need to know which names have been assigned to each printer or fax server.

Terminals, printers, and fax servers are members of groups and must have a common group membership. However, printers and fax servers are not subject to time restrictions and cannot be expired.

When you add a terminal, the system prompts you for a string name and the TCP/IP address of the device. The purpose of the address is to provide a unique name for the terminal. The address you specify here is not used for networking.

If you enable terminal security at the system default level, you must assign each workstation to a group appropriate for the users who need to use the workstation. If you do not enable terminal security at the system default level, then all devices are freely available to anyone unless you override the system defaults and turn on terminal security at another level.

If terminal security is enabled, a user’s extended group membership is compared to the terminal’s extended group membership to determine if the user has permission to log on at that terminal.

Password Controls

You can require that passwords be a minimum length (0 to 8 characters) or contain one or more nonalphabetic characters. You can also set them to expire after a configurable number of days (with an optional grace period with warnings to the user). Passwords are always encrypted within the security database.

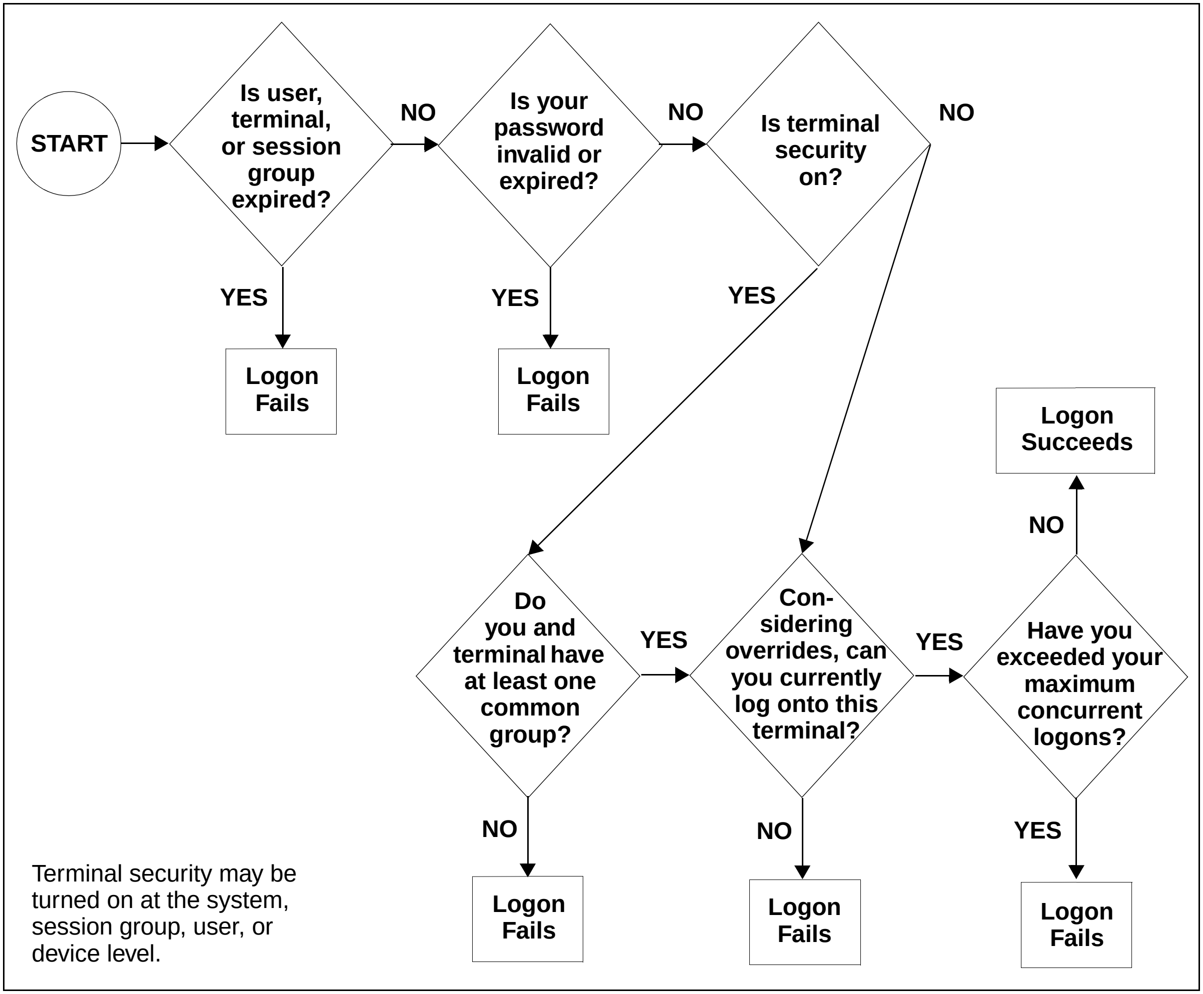
Users can change their own passwords with the Change User's Password option (see **"Set User Passwords" on page 73**).

If you change the minimum password length in the system defaults (see Default Security Settings in the *Image Services Administrator's Handbook*) to greater than zero, the next time a user changes a password, the No Password checkbox is disabled and the new password must match the new requirements.

To download the *Image Services Administrator's Handbook* from the IBM support page, see **"Accessing IBM FileNet documentation" on page 17**.

Logon Process

The following flowchart illustrates the logon process.


START
Is user, terminal, or session group expired?
NO
YES
Logon Fails
Is your password invalid or expired?
NO
YES
Logon Fails
Is terminal security on?
NO
YES
Logon Succeeds
NO
Do you and terminal have at least one common group?
YES
NO
Logon Fails
Con-sidering overrides, can you currently log onto this terminal?
YES
NO
Logon Fails
Have you exceeded your maximum concurrent logons?
YES
Logon Fails

Terminal security may be turned on at the system, session group, user, or device level.

Start the Security Administration Application

For detailed information on starting, setting up, planning and other Security Administration topics see the *Image Services System Administrator's Handbook*. To download this handbook from the IBM support page, see **"Accessing IBM FileNet documentation" on page 17**.

Set Up Group Security

You create all groups, including groups assigned as primary, session, and administrative groups, in the same way. Before creating groups, review the group template settings.

Note To avoid confusing group names with user names, adopt a naming convention, such as ending all group names with an uppercase G, to distinguish groups from users in reports and event logs.

You must have certain administrative attributes to perform administrative tasks affecting groups. You must have the Principal attribute to create groups, the Supervisor attribute to update groups, and the Group attribute to add members to groups. Administrative attributes are discussed in detail in **"User Security and Administrative Attributes" on page 37**.

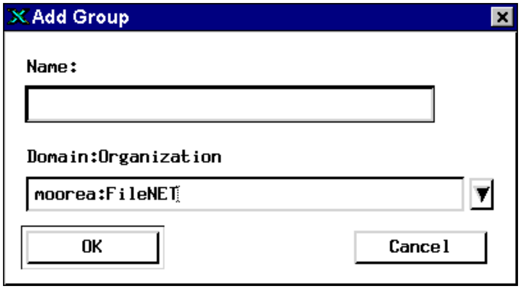
The System Administrator can perform any and all administrative tasks for all groups.

Add or Update Groups

To add or update a group, select Add Group or Update Group from the Security Administration window's Groups menu. You must have the Principal attribute to add groups and Supervisor attribute to update group memberships.

1 Select Add Group or Update Group from the Groups menu.

a If you select Add Group, the following dialog box displays.



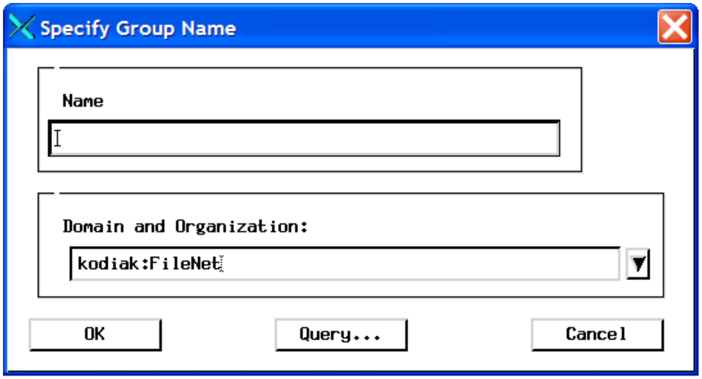
Name:

Domain:Organization
moorea:FileNET

Enter the new group name in the dialog box and click OK.

b To update a group, perform the following steps.

- Select Update Group from the Group menu to display the Specify Group Name dialog box.



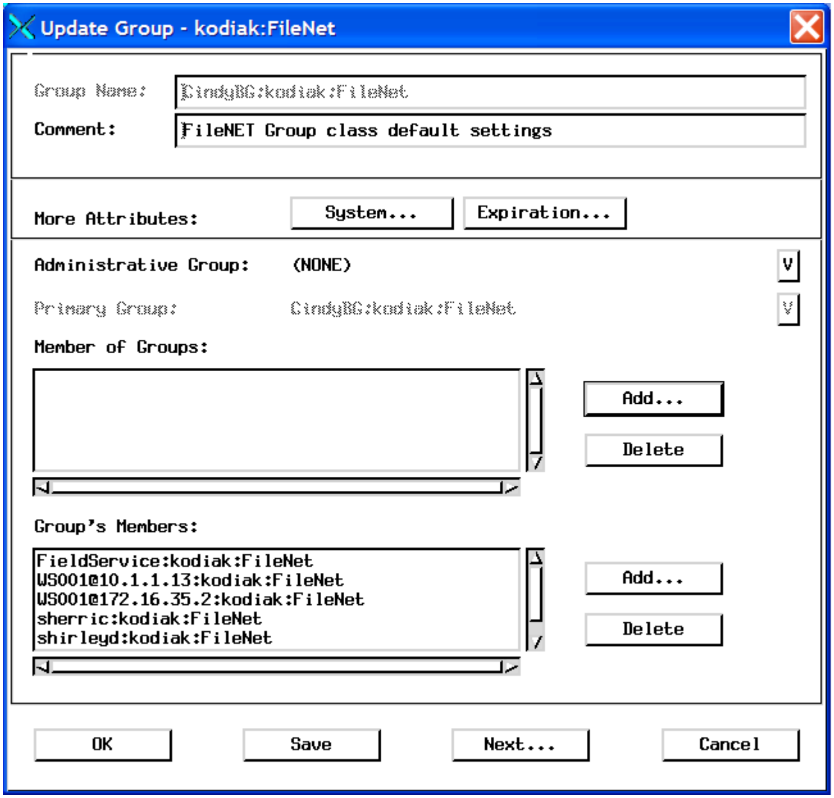
Domain and Organization: kodiak:FileNet

- Enter the group name in the Name field or click Query to search for the group name. See **“Using the Query Feature to Select a Group Name” on page 65**.

Note The Domain and Organization field information you specify will only be utilized if you enter a name and click OK. It is not passed on to the Query function.

- Click OK. The Update Group dialog box appears.

2 Make your selections and entries in the Update Group dialog box that displays.



Update Group - kodiak:FileNet

Group Name: CindyBG:kodiak:FileNet

Comment: FileNET Group class default settings

Administrative Group: (NONE)

Primary Group: CindyBG:kodiak:FileNet

Member of Groups:

Group's Members:

```
FieldService:kodiak:FileNet
WS001@10.1.1.13:kodiak:FileNet
WS001@172.16.35.2:kodiak:FileNet
sherric:kodiak:FileNet
shirleyd:kodiak:FileNet
```

3 To add your group to another group:

a Click Add next to the Member of Groups list.

b Enter the group name in the Name field or click Query to search for the group name. See **“Using the Query Feature to Select a Group Name” on page 65**.

c Click OK. The group appears in the Member of Groups list.

4 To delete your group from another group:

a Select the group in the Member of Groups list.

b Click Delete.

5 To add a member to the group:

a Click Add next to the Group’s Members list.

b Enter the group name in the Name field or click Query to search for the group name. See **“Using the Query Feature to Select a Group Name” on page 65**.

c Click OK. The group appears in the Member of Groups list.

Note that you may add only one member at a time. Repeat this step to add another member to the group.

6 To delete a member from a group:

a Select the group in the Group’s Members list.

b Click Delete.

7 Once you are finished:

a Click OK to accept your changes and close the dialog box.

b Click Save to save your changes and leave the dialog box open.

c Click Next to clear the changes from the dialog box and make more changes (be sure you save any changes you want to keep before clicking Next).

d Click Cancel to close the dialog box without making any changes.

The following table describes the options in the Add (or Update) Group dialog box.

Add (or Update) Group options

Option	Description
Group Name field	Displays the group name in object:domain:organization format.
Comment field	Contains up to 79 characters of user-specified text. The default is: FileNet Group class default settings.
System button	Click the System button to display the System Attributes dialog box (see Override Security Object Defaults in the *Image Services Administrator's Handbook*). To download this handbook from the IBM support page, see **"Accessing IBM FileNet documentation" on page 17**.
Expiration button	Click the Expiration button to display the Expiration Date dialog box. See Override Account Expiration Date in the *Image Services Administrator's Handbook*. To download this handbook from the IBM support page, see **"Accessing IBM FileNet documentation" on page 17**.
Administrative Group field	Displays the administrative group name of the administrative user who created the group. Only SysAdmin can view or change the administrative group assignment.
Primary Group field	Displays the name of the group you created or updated. You cannot edit this field.
Member of Groups listbox	List all the groups that the group you are adding/updating is an extended member of (see **"Extended Membership" on page 27**).
Add button	Click Add to display the Group Selection List. You can choose from this list or enter a search pattern. When you enter the search pattern, a group (in the Group Selection List) which matches the search pattern is automatically highlighted. Click OK when you've selected the group to add.
Delete button	Select the member to remove from the group and click Delete.
Group's Members listbox	Lists the members of the group selected in the Member of Groups list.

Add (or Update) Group options

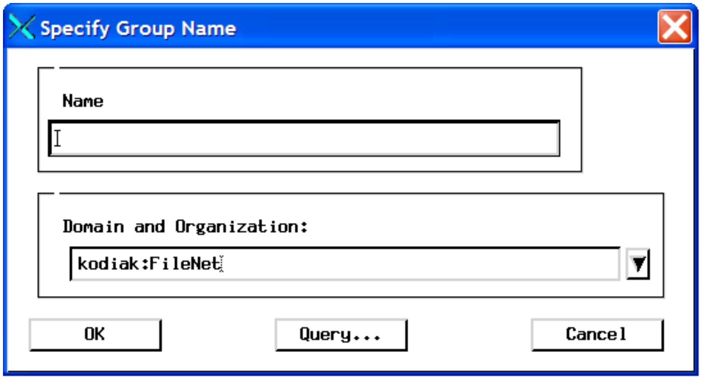
Option	Description
Add button	Click Add to display a list of security objects. Select those you want to be members of the group you are creating or updating and click OK.
Delete button	Select the member to remove from the group and click Delete.

Delete Groups

The procedure you use to delete a group depends on the group's assignment: Administrative, Primary or Session. (see the Image Services System Administrator's Handbook for more information).

To delete a Primary or Session group

1 Select Delete Group from the Group menu to display the Specify Group Name dialog box.



kodiak:FileNet

You can delete only one group at a time.

2 Enter the group name in the Name field or click Query to search for the group name. See **"Using the Query Feature to Select a Group Name" on page 65**.

Note The Domain and Organization field information you specify will only be utilized if you enter a name and click OK. It is not passed on to the Query function.

3 Click OK. The Delete Group dialog box appears.

4 Click OK to delete the selected group.

Note You cannot delete the reserved groups: SysAdminG, AuditG, FieldServiceG, and OperatorG.

To delete an Administrative Group

1 To reassign the objects belonging to this group to another administrative group, run Reassign Administrative Groups (see the Image Services System Administrator's Handbook for more information).

2 Follow the directions for deleting a Primary or Session group.

Update Group Membership

Group administrators can add members to and delete members from groups they administer. They can also make a group a member of another group, delete it from a group, or add a selected group in their administrative domain to other groups. If you have both group and supervisor attributes, you can use Update Group Membership to perform both kinds of functions.

1. Select Update Group Membership from the Groups menu.

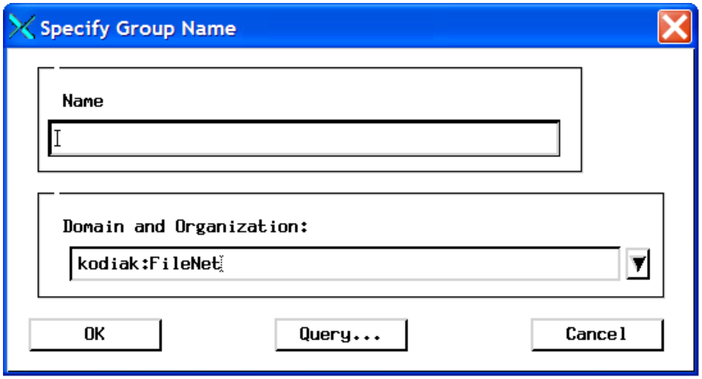
2. Enter the group name in the Name field or click Query to search for the group name. See **"Using the Query Feature to Select a Group Name" on page 65**.

3. The Update Group Membership dialog box appears. You can now add or delete groups and members. For more information, see **"Add or Update Groups" on page 56**.

Rename Groups

An administrator with the Supervisor attribute can rename groups in his administrative domain.

1. Select Rename Group from the Groups menu to display the Specify Group Name dialog box.



Specify Group Name

Name

Domain and Organization:

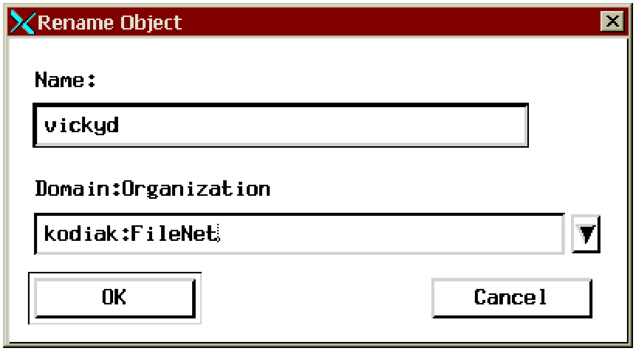
kodiak:FileNet

2. Enter the group name in the Name field or click Query to search for the group name. See **"Using the Query Feature to Select a Group Name" on page 65**.

Note The Domain and Organization field information you specify will only be utilized if you enter a name and click OK. It is not passed on to the Query function.

3 Click OK. The Rename Group dialog box appears.

4 Enter the new group name in the Rename Object dialog box and click OK.


Rename Object

Name:

vickyd

Domain:Organization

kodiak:FileNet

Using the Query Feature to Select a Group Name

If you aren't sure of the group's name, click Query to search by name. The Query for User Name dialog box appears. You have two options for searching by name:

- Choose Select All and click Submit. Select a name from the Match List and click OK.
- Choose By Name, enter a number in the Number in Match List field and enter one or more characters in the Name field. These characters should match the name you are searching for. Click Submit. Select a group name from the Match List and click OK.

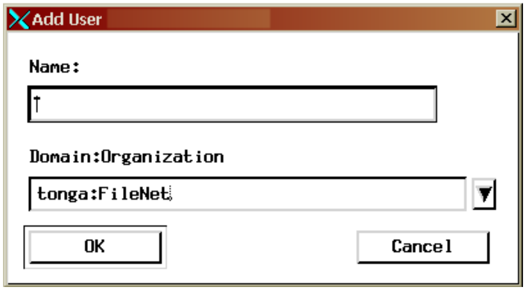
Set Up User Security

After you set up your system security defaults and create groups, you are ready to add users. Only users can log on and perform tasks. The system provides a user template, which you can modify. A new user created by a principal administrator has an expired status. An administrator with the Supervisor attribute must activate the logon account by changing the expired status. If you create a new user without a password, an administrator with the Password attribute must set the password for the user before the user can log on.

Add and Update Users

Follow this procedure to add a user.

1 Select Add User to display the following dialog box.



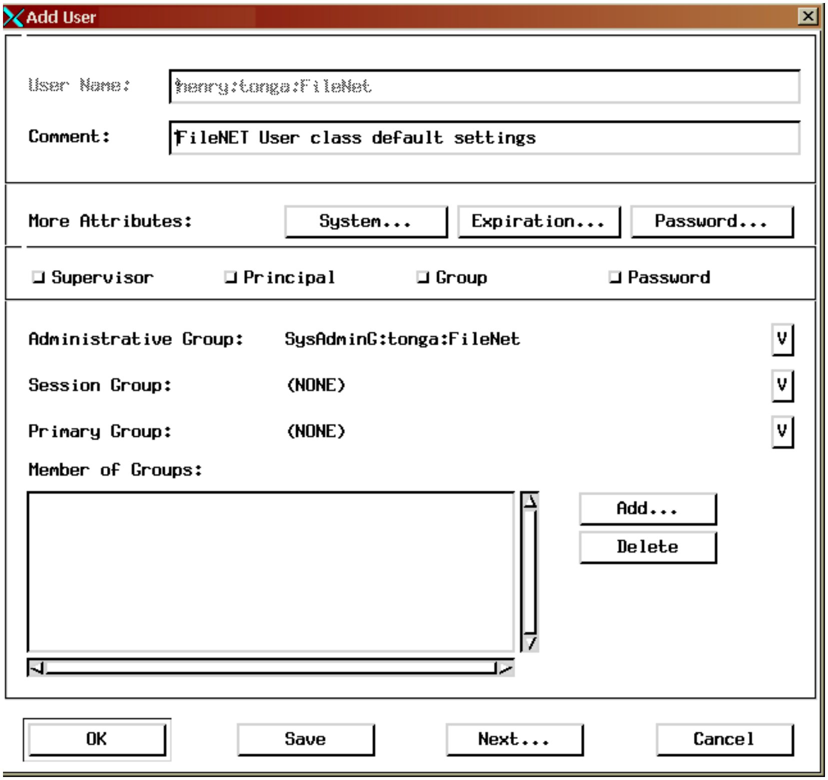
Name:

Domain:Organization

tonga:FileNet

Enter the new group name in the dialog box and click OK.

2 A dialog box similar to the following displays.



Add User

User Name: henry:tonga:FileNet

Comment: FileNET User class default settings

More Attributes:

□ Supervisor □ Principal □ Group □ Password

Administrative Group: SysAdminG:tonga:FileNet

Session Group: (NONE)

Primary Group: (NONE)

Member of Groups:

3 Change the default information as appropriate for the user (see “Add User Options” table below).

The new user inherits the administrative group attribute from the administrator.

Note The attributes you can give a user depend on your administrative attributes. For example, if you have the Principal attribute, you can only create the user and change the Comment.

4 Click OK to accept your changes and close the dialog box.

- Click Save to save your changes and leave the dialog box open.
- Click Next to clear the changes from the dialog box and make more changes (be sure you have saved any changes before clicking Next).
- Click Cancel to close the dialog box without making any changes.

The following table describes the options on the Add User dialog box.

Add User Options

Option	Description
User Name	The user name in object:domain:organization format. This field is grayed because you entered it in the previous dialog box and cannot change it here.
Comment	Contains up to 79 characters of user-specified text. Default text is: “FileNet User class default settings.”
System button	See Override Security Object Defaults in the *Image Services Administrator’s Handbook*.
Expiration button	See Override Account Expiration Date in the *Image Services Administrator’s Handbook*. To download this handbook from the IBM support page, see **“Accessing IBM FileNet documentation” on page 17**.

Add User Options, Continued

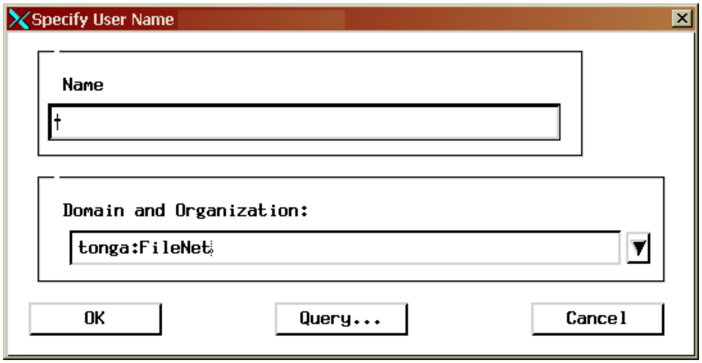
Option	Description
Password button	See Set Up Terminal and Device Security in the *Image Services Administrator's Handbook*. To download this handbook from the IBM support page, see **"Accessing IBM FileNet documentation" on page 17**.
Supervisor	SysAdmin checks this box to assign Supervisor status. Grants permission to update security objects.
Principal	SysAdmin checks this box to assign Principal status. Allows the user to create, but not update, security objects.
Group	SysAdmin checks this box to assign Group status. Allows the user to make an object a member of a group.
Password	SysAdmin checks this box to assign Password status. Allows the user to change other users' passwords within the administrator's extended membership.
Administrative Group	The name of the administrative group of the administrator who created the user. Only SysAdmin sees this field.
Session Group	Lists groups when Group box is checked. When a Session Group other than (NONE) (the default) is assigned, logon controls of the session group apply to the user, unless the user can override system default privileges. The user is not made a member of the session group.
Primary Group	Lists groups when Group box is checked. The primary group determines the default security access and can be changed. The primary group determines who has access to data objects, such as folders or annotations (but not documents), created by the user. The user is made a member of the primary group. The default is (NONE).
Member of Groups	Lists all the groups this user is a member of.

Add User Options, Continued

Option	Description
Add button	Displays the Group Selection List, which contains the same selection as the list button for Primary Group. Select from the list or enter a search pattern. When you enter the search pattern, a group in the list which matches the search pattern is automatically selected.
Delete button	Deletes groups from the Member of Groups list. Select the groups to delete from this list and click the Delete button.

Follow this procedure to update a user's properties.

1 Select Update User from the User menu to display the Specify User Name dialog box.



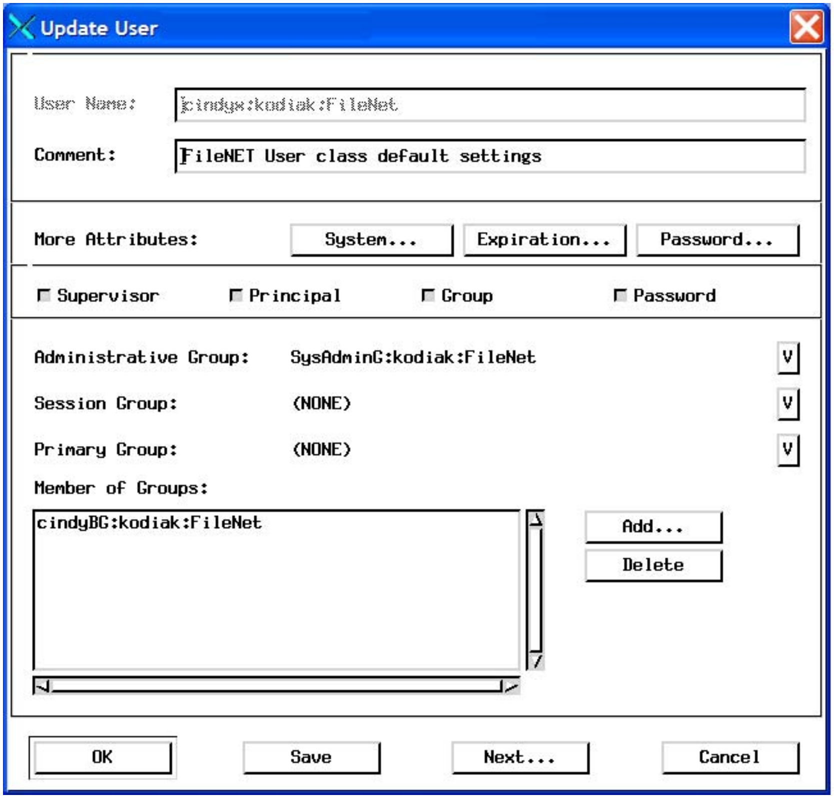
tonga:FileNet

2 Enter the user name in the Name field or click Query to search for the user name. See **"Using the Query Feature to Select a User Name" on page 83**.

Note The Domain and Organization field information you specify will only be utilized if you enter a name and click OK. It is not passed on to the Query function.

3 Click OK. The Update User dialog box appears.

4 Make your selections and entries in the Update User dialog box that displays. See the table **“Add User Options” on page 68** for more information on the various fields.



Update User

User Name: cindyx:kodiak:FileNet

Comment: FileNET User class default settings

More Attributes:

☐ Supervisor ☐ Principal ☐ Group ☐ Password

Administrative Group: SysAdminG:kodiak:FileNet

Session Group: (NONE)

Primary Group: (NONE)

Member of Groups:
cindyBG:kodiak:FileNet

5 To add the user to a group:

a Click Add next to the Member of Groups list.

b Enter the group name in the Name field or click Query to search for the group name. See **“Using the Query Feature to Select a Group Name” on page 65**.

c Click OK. The group appears in the Member of Groups list.

6 To delete the user from a group:

a Select the group in the Member of Groups list.

b Click Delete.

7 Once you are finished:

a Click OK to accept your changes and close the dialog box.

b Click Save to save your changes and leave the dialog box open.

c Click Next to clear the changes from the dialog box and make more changes (be sure you save any changes you want to keep before clicking Next).

d Click Cancel to close the dialog box without making any changes.

Set User Passwords

Selecting Change User's Password from the Users menu displays the Change User Password dialog box. This dialog box will be slightly different for password administrators than for other users.

For users who do not have password administrator privileges, the Change User Password dialog box will only allow them to select the "No Password" option or enter a new password.

For password administrators, the Change User Password dialog box will contain the additional option, "Password Never Expires". For more information on the "Password Never Expires" option, refer to **"User Expiration Exclusion" on page 75**.

For all users, when you enter a new password, you must enter it twice. If the second entry does not match the first, you receive an error message that the password was not changed because the verification failed.

Note Windows Server users, when you make changes to a user password, you must then run Application Executive and refresh that user's password information for unified logon.

Extensible Password Authentication

Extensible password authentication in IS provides the ability to enforce stringent password validation rules and create customized password validation rules.

- **Mandatory Password Change** - The default security setting "Password Change Upon Reset" forces a user to change their password before logging in. This is required after the System Administrator has reset the users password.

- **User Expiration Exclusion** - excludes specific users from the password expiration rules.
- **Custom Password Validation** - provides the ability to enforce more stringent, customized password validation rules.

  The customer is responsible for providing a shared library defining the custom password validation rules. The library must have a single entry point designed to enforce restrictions on user passwords.

Note The external shared library is not included with Filenet software. For complete information on creating your own customized password validation library, contact your service representative.

Mandatory Password Change After Reset

After the System Administrator resets a users password, and if “Password Change Upon Reset” is checked for this user, the user must reset their password before the next log in. This applies to all clients and administrative tools. The check box "Password Change Upon Reset" is located in the Security Administration Default Security Settings dialog. For more information on default settings, see the *Image Services System Administrator’s Handbook*. The default value for this feature is false. To download this handbook from the IBM support page, see **“Accessing IBM FileNet documentation” on page 17**.

This system-wide setting can only be changed by System Administrators.

Note System Administrators are exempt from the requirement to change their password after reset.

User Expiration Exclusion

The Change User Password dialog is shared by both password administrators and users when changing a password. The dialog has two different configurations based upon the type of user.

Both SysAdmin and password administrators will see the "Password Never Expires" check box on the Change User Password dialog box. They can set this value for other System Administrators and users. If this box is checked, the System Administrator or user will be excluded from the password expiration rules.The default value for the "Password Never Expires" field is false.

Users who are not system administrators can access the Change User Password dialog box but will only have the option to change their password.

Note When a password administrator sets the “Password Never Expires" option for a user, and the system wide "Password Change Upon Reset" flag is set, the user will not be required to change their password.

Custom Password Validation

For added security, you can create a custom password validation function that can check for any set of conditions your installation requires.

For example, you may want users to have passwords that contain at least one numeric or one non-alphanumeric character. This feature allows for any type of password check and can vary widely from customer to customer.

Note System Administrators can create passwords that are exempt from the custom password validation rules. However, all other users are subject to password validation and must have passwords that comply.

To enable customized password validation, you must create a shared library to validate the user's new password. The IS software will load this shared library if it exists and the feature is enabled.

The customized rules validate the password and return either an OK or an INVALID. The IS system performs the external password check on all new passwords and password updates. This check requires that the password be re-entered if it is declared INVALID by the external shared library.

Note If you change the Enable Custom Validation setting, you must restart the IS software before the change will take effect.

Enable/Disable Custom Library Validation

The shared external shared library feature must be enabled from the default security settings dialog. The default value is false, which means the external library will not be loaded or used for password validation.

Shared Library Entry Point

After you've enabled Custom Password Validation, the Image Services software uses the following entry point to link to your custom shared library:

```
error_typ   SEC_ext_validate_pwd(
      char *username,
      char *password
int  action)   (Where action is ADD, UPDATE, DELETE)
```

where:

username is a null terminated string. The maximum length is 40 bytes.

password is an unencrypted null terminated string. The maximum length is 8 bytes.

You must create your own custom library function to do specialized checks. For Unix systems, the library will have the name **libSEC_ext_valid_pwd**. For Windows systems, the library will have the name **SEC_ext_valid_pwd**. The file extension varies between platforms:

AIX®	no extension
HP-UX	**.sl**
SUN	**.so**
Windows	**.dll**

For custom password validation, a valid password returns:

EXTERNAL_AUTH_PASS_OK 0

An invalid password returns:

EXTERNAL_AUTH_PASS_INVALID	-1

The IS software uses the action parameter to identify the type of password change. The valid values for the action parameter are:

EXTERNAL_AUTH_PASS_ADD	1
EXTERNAL_AUTH_PASS_UPDATE	2
EXTERNAL_AUTH_PASS_DELETE	3

Important For security reasons, you must restart the IS software after enabling the external shared library feature or making changes to the shared library itself.

Note The external shared library is not included with the FileNet software. For complete information on creating a customized password validation library, contact your service representative.

Update Users

To update an existing user, perform the following steps.

1. Select Update User from the Users menu to display the Specify User Name dialog box.
2. Enter the user name in the Name field or click Query to search for the user name. See **“Using the Query Feature to Select a User Name” on page 83**.

Note The Domain and Organization field information you specify will only be utilized if you enter a name and click OK. It is not passed on to the Query function.

3 Click OK. The Update User dialog box appears.

4 Update user values and click OK.

Only a System Administrator with the Supervisor attribute has access to the Expiration button. System Administrators with Supervisor and Principal rights can access the Session Group field. If system overrides are allowed, the System button is enabled.

Changing the Name of the fnsw User

Programmable Security Objects provide the ability to change the standard FileNet software user name **fnsw**.

Important The task of changing any security object should be done with great caution. Before you actually change the fnsw user name, analyze your system, and if you can avoid changing this security object, do so.

If you decide to change this security object, review the new tools available to work with programmable security objects: fn_pso_driver, fn_pso_podf_admin and fn_pso_switch in the *Image Services System Tools Reference Manual.* To download this manual from the IBM support page, see **“Accessing IBM FileNet documentation” on page 17**.

Delete Users

A System Administrator with the Supervisor attribute can delete users.

1. Select Delete User from the Users menu to display the Specify User Name dialog box.

2. Enter the user name in the Name field or click Query to search for the user name. See **"Using the Query Feature to Select a User Name" on page 83**.

Note The Domain and Organization field information you specify will only be utilized if you enter a name and click OK. It is not passed on to the Query function.

3. Click OK to delete the user.

Update User Membership

A System Administrator with the Group administrative attribute can make a user a member of one or more groups. A System Administrator can also specify a user's group membership in the Create and Update dialog boxes.

1. Select Update User Membership from the Users menu to display the Specify User Name dialog box.
2. Enter the user name in the Name field or click Query to search for the user name. See **"Using the Query Feature to Select a User Name" on page 83**.

Note The Domain and Organization field information you specify will only be utilized if you enter a name and click OK. It is not passed on to the Query function.

3 Click OK. The Update User Membership dialog box appears.

Depending on your attributes, certain fields may not display.

4 To add a user to a group:

a Click Add to display the Specify User Name dialog box.

b Enter the user name in the Name field or click Query to search for the user name. See **"Using the Query Feature to Select a User Name" on page 83**.

c Click OK.

You may add only one user to the group at a time.

5 To delete a user from a group:

a Select the group in the Member of Groups list.

b Click Delete.

c Click OK.

6 Once you are finished:

a Click OK to accept your changes and close the dialog box.

b Click Save to save your changes and leave the dialog box open.

c. Click Next to clear the changes from the dialog box and make more changes (be sure you save any changes you want to keep before clicking Next).

d. Click Cancel to close the dialog box without making any changes.

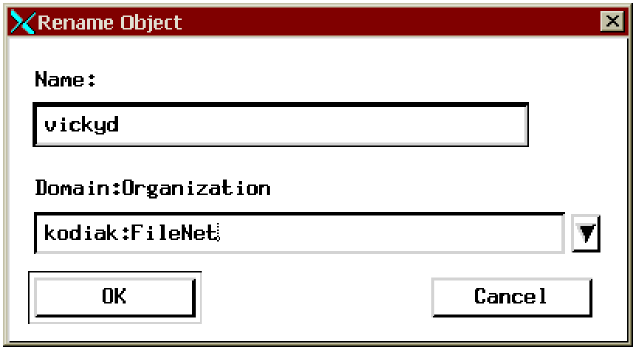
Rename Users

An administrator with the Supervisor attribute can rename users.

1. Select Rename User from the Users menu to display the Specify User Name dialog box.
2. Enter the user name in the Name field or click Query to search for the device name. See **“Using the Query Feature to Select a User Name” on page 83**.

Note The Domain and Organization field information you specify will only be utilized if you enter a name and click OK. It is not passed on to the Query function.

3. Click OK. The Rename User dialog box appears.
4. Enter the new user name in the Rename User dialog box and click OK.



Rename Object

Name: vickyd

Domain:Organization kodiak:FileNet

Using the Query Feature to Select a User Name

If you aren’t sure of the user’s name, click Query to search by name. The Query for User Name dialog box appears. You have two options for searching by name:

- Choose Select All and click Submit. Select a name from the Match List and click OK.
- Choose By Name, enter a number in the Number in Match List field and enter one or more characters in the Name field. These characters should match the name you are searching for. Click Submit. Select a device name from the Match List and click OK.

Set User’s Database Logon

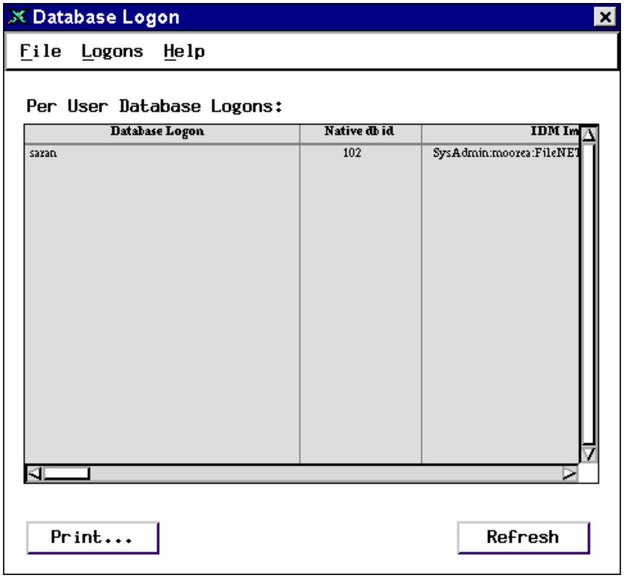
If you have a full-use database license, you can use the Database Logons window to map an RDBMS user to an Image Services user for using embedded SQL commands on a PC.

Note An RDBMS user must already exist before you can map it to an Image Services user.

You can set up the database logon permissions in several ways:

- Set individual database logons (one-to-one)
- Set a single database logon for several users (many-to-one)
- Set a combination of one-to-one and many-to-one logons

Select Database Logons from the Users menu to display the Database Logons window.



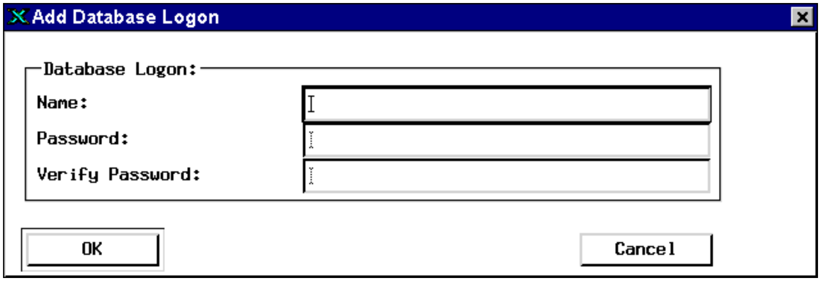
Per User Database Logons:

Database Logon	Native db id	IDM Im
saran	102	SysAdmin:moorea:FileNET

Add Database Logon

If you are the FileNet system administrator or if you have the Principal attribute (see the table **“Administrative Attributes” on page 38**), you can add database logons.

1 Select Add Logon from the Logons menu to display the Add Database Logons dialog box:



2 Enter a database logon name.

3 Enter and verify a password.

4 Click OK to accept your entry or Cancel to close the dialog box without making any changes.

Update Database Logon Password

If you are the system administrator or if you have the Password attribute (see the table **“Administrative Attributes” on page 38**), you can update the logon password.

1 Select a user name to update from the Database Logons window.

2 Select Update Logon from the Logons menu to display the Update Database Logons dialog box.

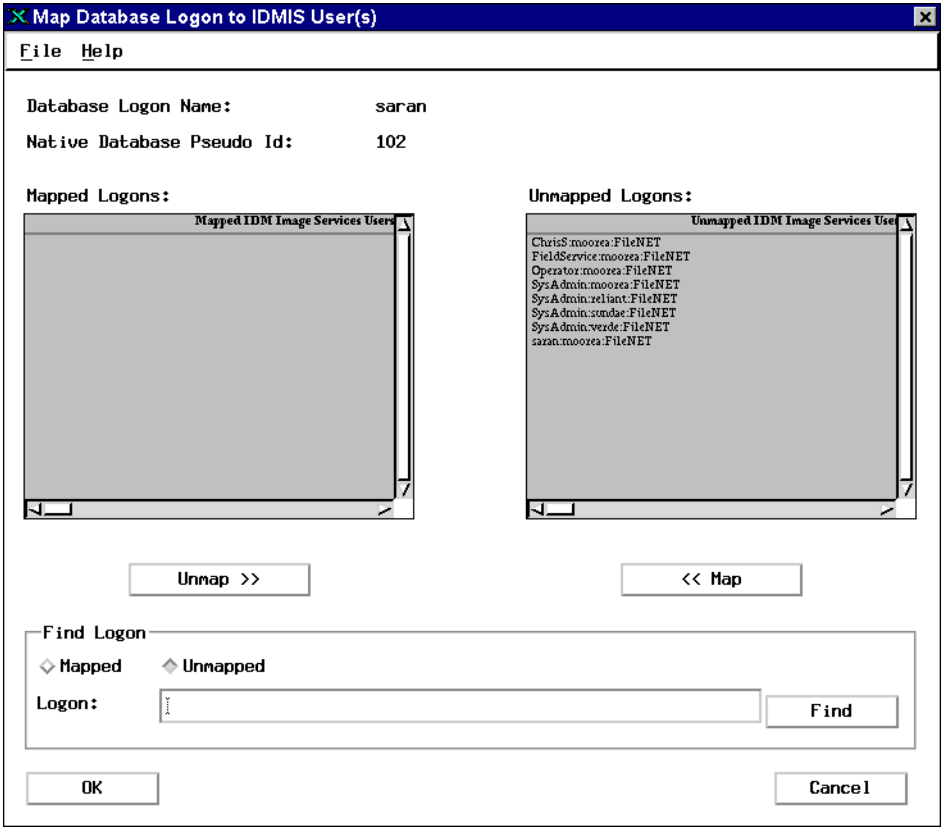
3 Enter and verify the new password.

4 Click OK to accept your entry or Cancel to close the dialog box without making any changes.

Map Database Logon to Image Services Users

If you are the system administrator or have both the Principal and Supervisor attributes (see the table **“Administrative Attributes” on page 38**), you can map the database logons to Image Services users.

1. Select a database logon from the Database Logons window.
2. Select Map Logon to Image Service Users from the Logons menu to display this window:



Database Logon Name: saran

Native Database Pseudo Id: 102

ChrisS:moorea:FileNET
FieldService:moorea:FileNET
Operator:moorea:FileNET
SysAdmin:moorea:FileNET
SysAdmin:reliant:FileNET
SysAdmin:sundae:FileNET
SysAdmin:verde:FileNET
saran:moorea:FileNET

3 To find a particular user:

a Check the Mapped or Unmapped radio button.

b Enter the name in the Logon field.

c Click the Find button and the list scrolls to the entered name.

4 To map a user to or unmap a user from a database logon:

a Select a name from the Unmapped Image Service Users or Mapped Logons list.

b Click the Map button to move the name to the Mapped Logons list or click the Unmap button to move the name to the Unmapped Image Services Users list.

5 When you finish all your selections, click OK to accept the changes or Cancel to close the window without making any changes.

Delete Database Logon

If you are the system administrator or if you have the Supervisor attribute (see the table **"Administrative Attributes" on page 38**), you can delete a logon name.

1 Select a name to delete from the Database Logons window.

2 Select Delete Logon from the Logons menu.

3 Click Delete at the prompt to delete the name, or click Cancel to close the prompt without deleting the name.

Set Up Document Security

Document security is determined when you set up your document classes in the Database Maintenance application. See the discussion under **"Document Security" on page 40** and Create Document Classes in the *Image Services System Administrator's Handbook*. To download this handbook from the IBM support page, see **"Accessing IBM FileNet documentation" on page 17**.

Set Up Function Security

Use function security to identify which functions (menu items, buttons) are to be secured, then assign members to those functions, making them available only to those users. Members can be user names or group names.

You can assign functions in two ways:

- To define a function and make it available to everyone, assign the group (ANYONE).
- To define a function and make it available to a restricted set of users, make the users members of the groups you assign to the function.

Security Administration has built-in function access. Only administrators can access most functions, and what is accessible depends on each administrator's attributes.

CAUTION Background Job Control's Erase Media function permits erasing optical media even if the media contain open documents. You may prefer to restrict this potentially hazardous function to a select few administrators. You can use the functional security feature to accomplish this.

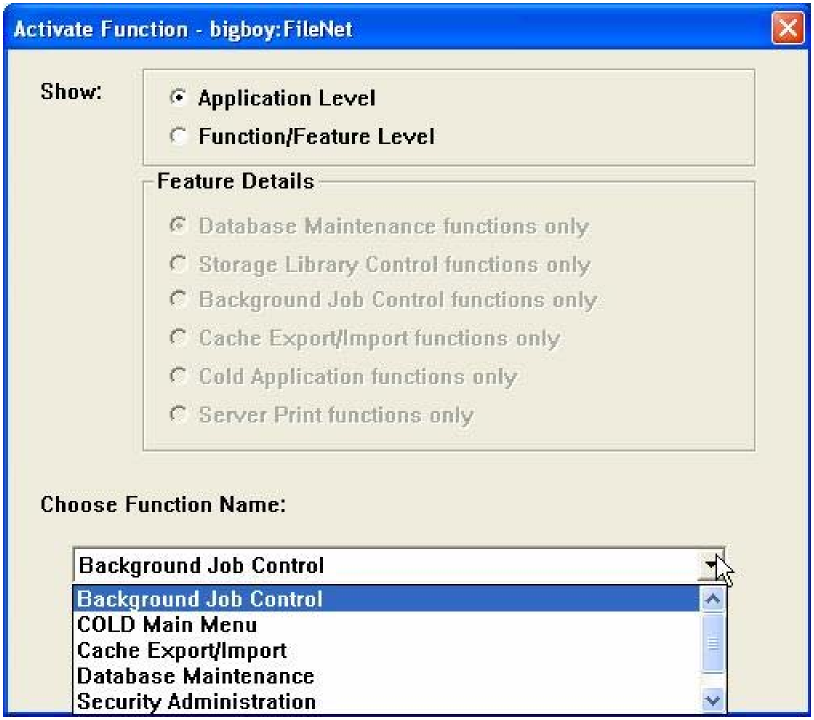
Activate Function Name

Only a System Administrator can assign user or group-specific functions. To activate a function name:

1 Select Activate Function Name from the Functions menu.

2 Next to the Show field, you have two choices:

- Select the Application Level option and go to Step 3.



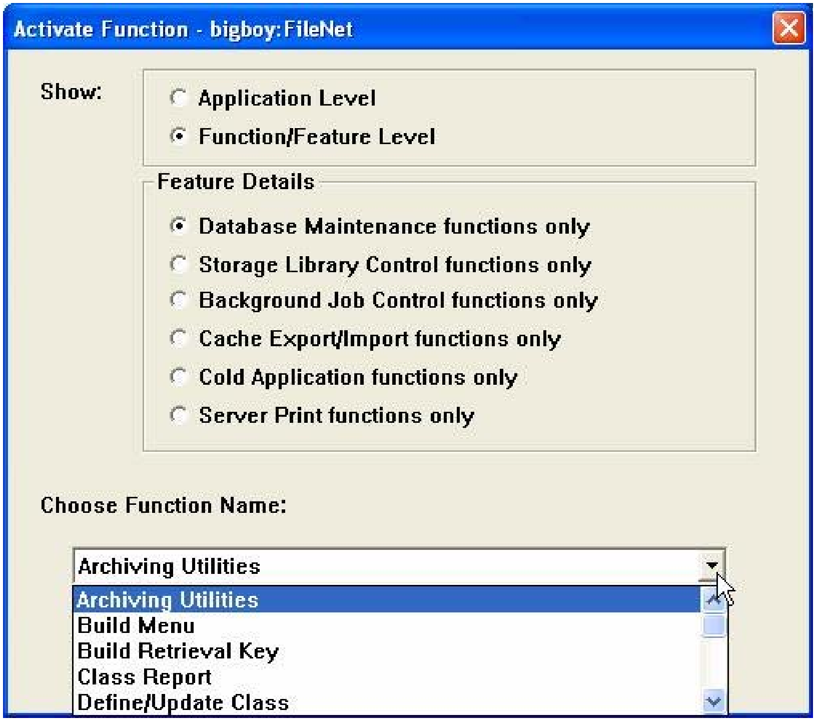
Activate Function - bigboy:FileNet

Show:
● Application Level
○ Function/Feature Level

Feature Details
● Database Maintenance functions only
○ Storage Library Control functions only
○ Background Job Control functions only
○ Cache Export/Import functions only
○ Cold Application functions only
○ Server Print functions only

Choose Function Name:
Background Job Control

- Select the Function/Feature Level option. The Feature Details area becomes active.



Activate Function - bigboy:FileNet

Show:
○ Application Level
● Function/Feature Level

Feature Details
● Database Maintenance functions only
○ Storage Library Control functions only
○ Background Job Control functions only
○ Cache Export/Import functions only
○ Cold Application functions only
○ Server Print functions only

Choose Function Name:
Archiving Utilities
- Archiving Utilities
- Build Menu
- Build Retrieval Key
- Class Report
- Define/Update Class

This area allows you to select a specific function feature within an application to assign to a Group or User. Selecting any one of these Feature Details provides you with a variety of function name options to select in Step 3.

3 Select the desired function name you want to secure in the Choose Function Name pulldown and click OK.

4 Click Add to display a list of user and group names.

5. Select one or more names to give those users or members of the group access to the function.

6. Click OK to save the function and close the window; click Save and Next to save and continue adding more functions; click Cancel to close the window without saving.

Update Function Membership

Only a System Administrator can update existing function membership. To update function membership:

1. Select Update Function Members... from the Functions menu.

   This displays a list of function names.

2. Choose the function you want to update and click OK.

   A dialog box similar to that shown for adding functions displays, showing the current members.

3. To add more members, click Add... and choose one or more names from the list.

4. To delete members, select them from the Function’s Members list and click Delete.

5. To save the update and close the dialog box, click OK.

   To save and continue updating more functions, click Save and Next. To close the dialog box without saving, click Cancel.

View Functions and Members

Choose View Functions and Members... to see a list of the functions defined and the members assigned to them. For a System Administrator, the complete list will display.

Deactivating a Function

Only a System Administrator can deactivate a function. To deactivate a function:

1. Select Deactivate Function... from the Functions menu and the list of defined functions displays.

2. Select one or more functions you want to deactivate and click OK.

   A popup dialog box asks you to confirm your selection.

3. Click OK to deactivate the selected functions or Cancel to exit the dialog box without saving.

Set Up Terminal and Device Security

A new system has three default logon names: SysAdmin, FieldService, and Operator. The passwords are SysAdmin, FieldService, and Operator, respectively.

You can place a group membership requirement on a printer or fax server. You must know the name the printer or fax server was assigned when configured through the System Configuration Editor. You cannot assign logon times or expirations on a printer or fax server. Until you turn on terminal security, everyone has access to all terminals. You can turn on terminal security as a system default or in templates and object records and then define terminals to control their use.

You can approach terminal security in one of two ways:

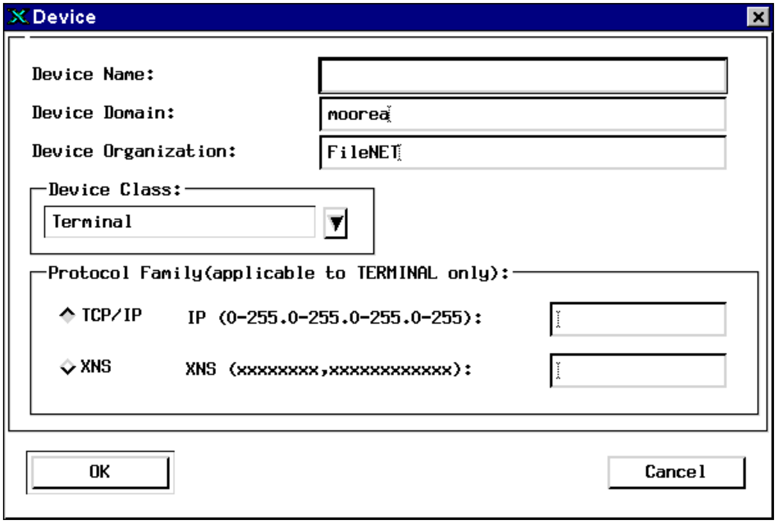
- Turn on terminal security. Each user logon will fail, but the terminal is added to the security database. Administrators can then set appropriate security for each terminal.
- Leave terminal security off. Identify each terminal, set the appropriate terminal security features for each terminal, and then turn on terminal security.

Administrators need the same kinds of administrative attributes to manage devices as described for users and groups. If you have trouble accessing devices, turn off terminal security. (You may have to turn it off for more than one security object.)

CAUTION If you have fax servers, do not use terminal security as a system setting. Instead, use individual terminal security. Do not set terminal security for fax server associated PC terminals, fax user logins, or primary groups associated with those users or terminals. The fax server will experience login failure even if the membership has been defined correctly.

Add Devices

1 Select Add Device from the Devices menu to display the Device dialog box:



Device Name:

Device Domain: moorea

Device Organization: FileNET

Device Class: Terminal

Device
Protocol Family(applicable to TERMINAL only):
TCP/IP
IP (0-255.0-255.0-255.0-255):
XNS
XNS (xxxxxxxx,xxxxxxxxxxxx):
OK
Cancel

2 Enter a device name.

You must use the printer or fax server name configured through the System Configuration Editor. For terminals, you can use any name. “PC” is the device name prefix of a Desktop terminal. “WS” is the prefix for other Image Services client terminals.

3 Select a device class of Terminal, Printer, or Fax.

4. Click the TCP/IP protocol button and enter the terminal’s address in the field to the right (use the format in the dialog box).

5. Click OK.

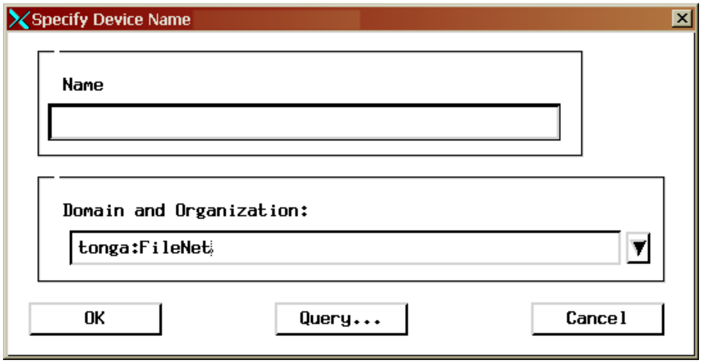
   A new dialog box displays the device name and type. You can now set System attributes and Administrative Group, and make the device a member of the appropriate groups.

6. Click OK in this dialog box to save the device and close the dialog box; click Save and Next to save this device and add another; click Cancel to close the dialog box without saving.

Update Devices

To update an existing device:

1. Select Update Device from the Devices menu. The Specify Device Name dialog box appears.

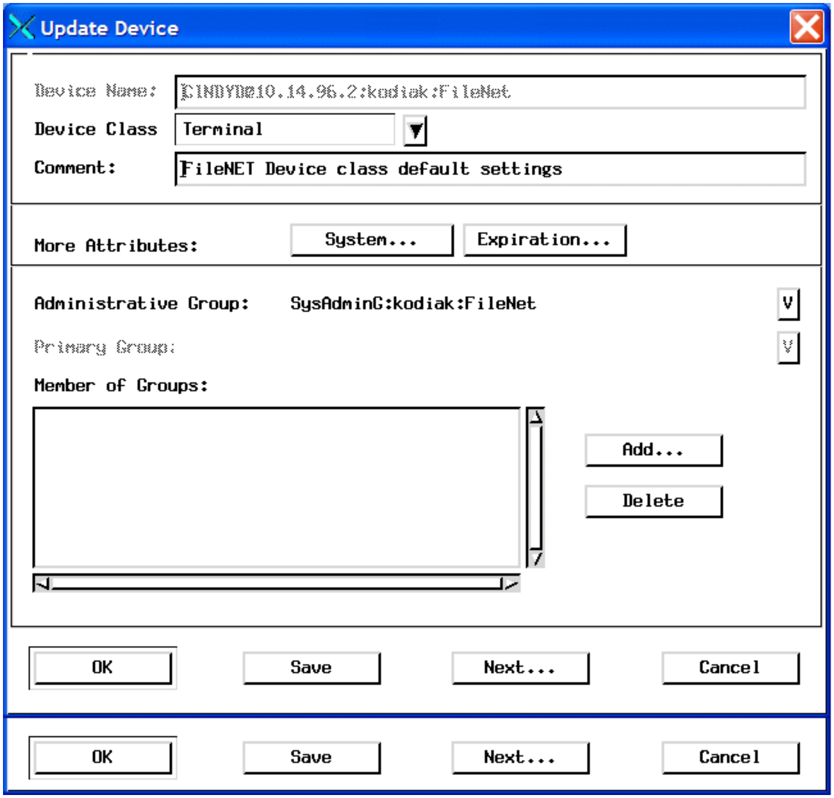


Domain and Organization: tonga:FileNet

2. Enter the device name in the Name field or click Query to search for the device name. See **“Using the Query Feature to Select a Device Name” on page 101**.

Note The Domain and Organization field information you specify will only be utilized if you enter a name and click OK. It is not passed on to the Query function.

3 Click OK. The Update Device dialog box appears.



Device Name: CINDYD@10.14.96.2:kodiak:FileNet
Device Class Terminal
Comment: FileNET Device class default settings
More Attributes:
Administrative Group: SysAdminG:kodiak:FileNet
Primary Group:
Member of Groups:

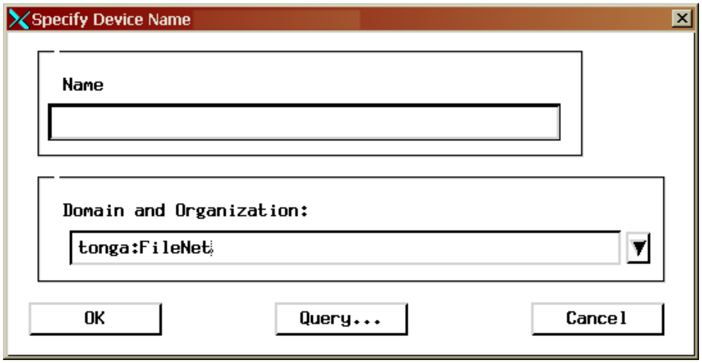
Change the device attributes or group membership as described in **“Add Devices” on page 94** and click OK.

Note You cannot update the device class or address. To change these values, you must delete the device and add it again.

Delete Devices

To delete a device from the security database:

1 Select Delete Device from the Devices menu. The Specify Device Name dialog box appears.



Domain and Organization: tonga:FileNet

2 Enter the device name in the Name field or click Query to search for the device name. See **"Using the Query Feature to Select a Device Name" on page 101**.

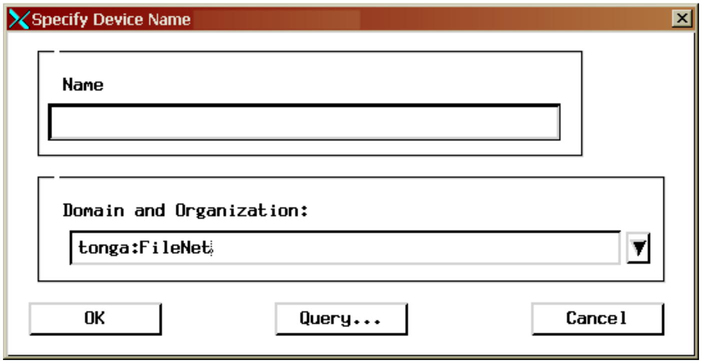
Note The Domain and Organization field information you specify will only be utilized if you enter a name and click OK. It is not passed on to the Query function.

3 Confirm or cancel your selection when prompted.

Update Device Membership

To change the group membership of a device:

1 Select Update Device Membership from the Devices menu. The Specify Device Name dialog box appears.

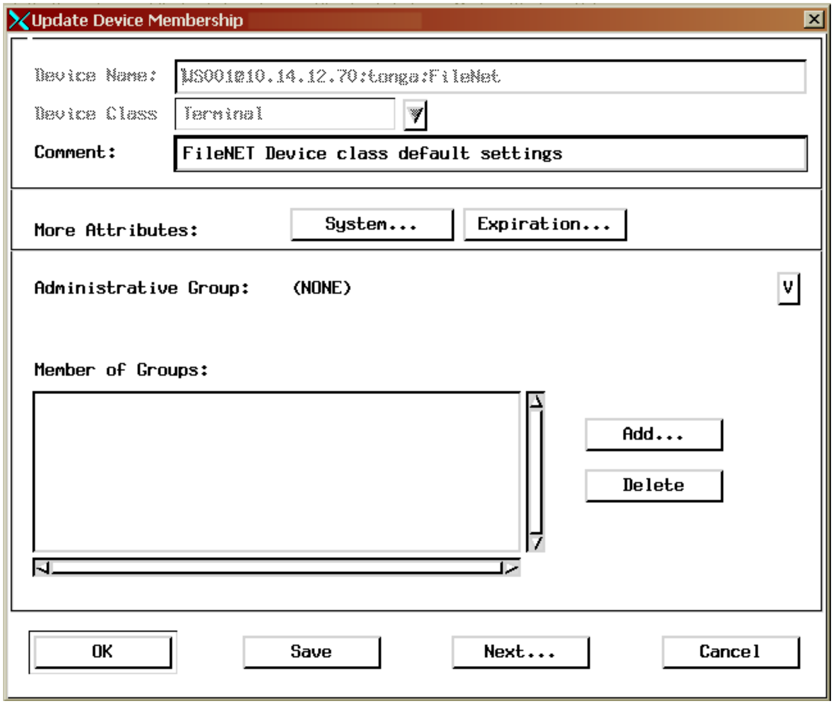


tonga:FileNet

2 Enter the device name in the Name field or click Query to search for the device name. See **“Using the Query Feature to Select a Device Name” on page 101**.

Note The Domain and Organization field information you specify will only be utilized if you enter a name and click OK. It is not passed on to the Query function.

3 Click OK. The Update Device Membership dialog box appears.



Update Device Membership

Device Name: WS001@10.14.12.70:tonga:FileNet

Device Class: Terminal

Comment: FileNET Device class default settings

Administrative Group: (NONE)

Member of Groups:

4 Click Add to add the device to a group.

5 Select one or more groups from the list that displays and click OK.

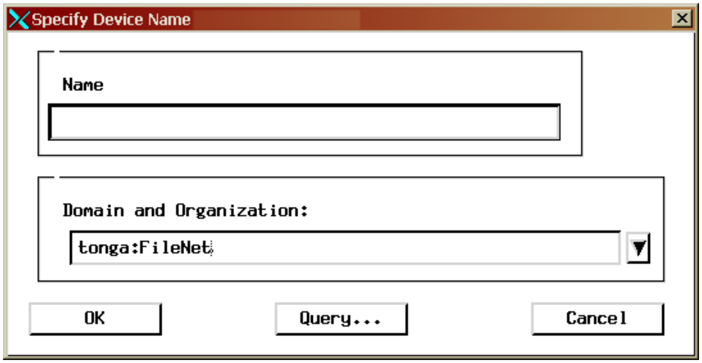
6 To delete the device from a group, select the group and click Delete.

7 Click OK, Save, or Cancel, as appropriate.

Rename Devices

An administrator with the Supervisor attribute can rename devices in his administrative domain.

1 Select Rename Device from the Devices menu. The Specify Device Name dialog box appears.

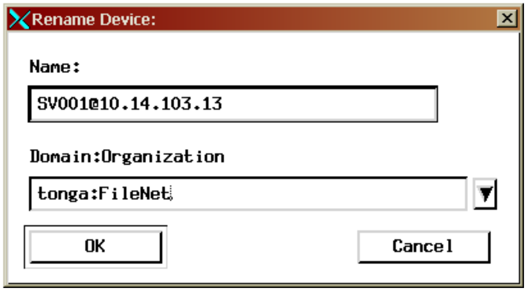


Domain and Organization: tonga:FileNet

2 Enter the device name in the Name field or click Query to search for the device name. See **“Using the Query Feature to Select a Device Name” on page 101**.

Note The Domain and Organization field information you specify will only be utilized if you enter a name and click OK. It is not passed on to the Query function.

3. Click OK. The Rename Device dialog box appears. Enter the new name for the device in the Device dialog box and click OK.



Name:
SV001@10.14.103.13

Domain:Organization
tonga:FileNet

Using the Query Feature to Select a Device Name

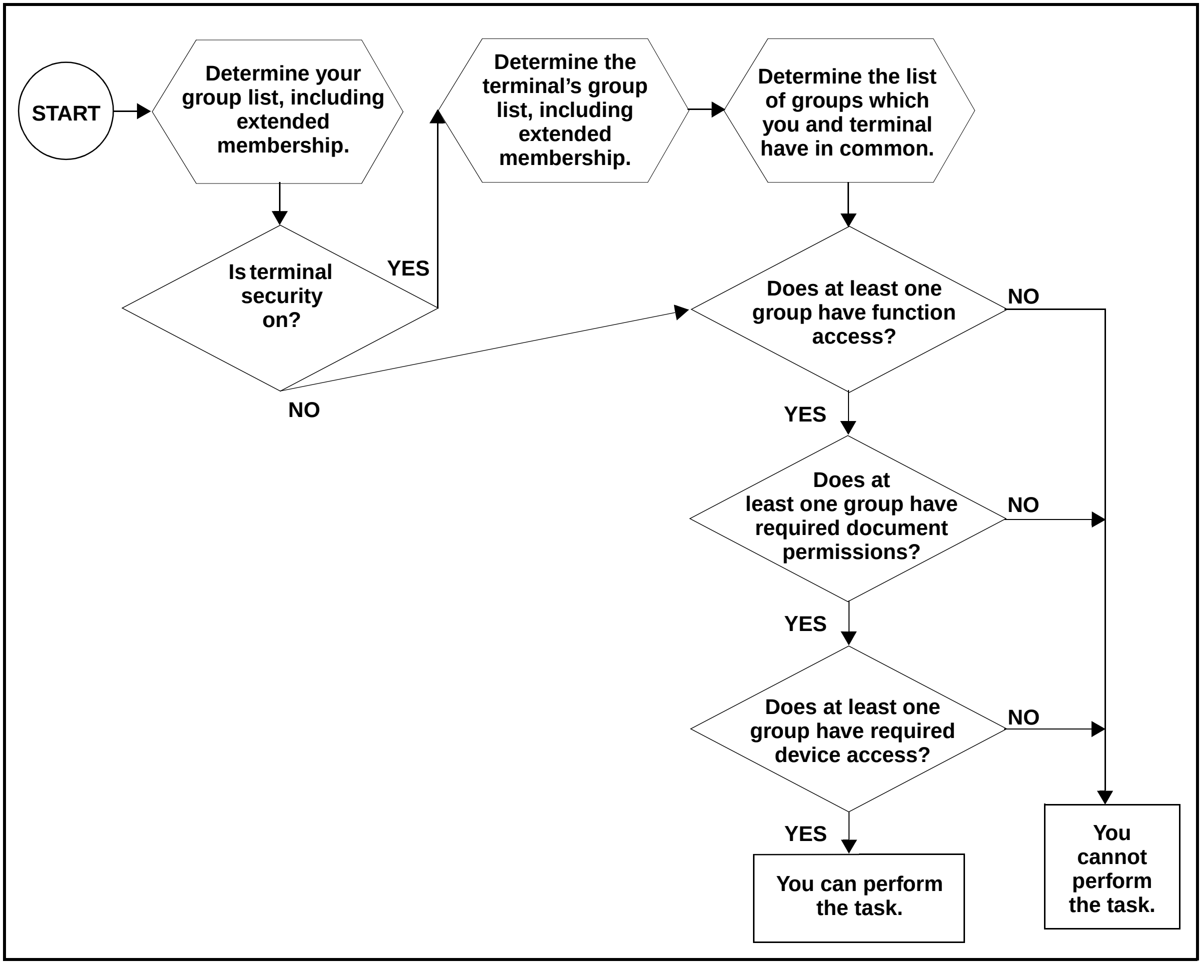
If you aren’t sure of the device name, click Query to search by name. The Query for Device Name dialog box appears. You have two options for searching by name:

- Choose Select All and click Submit. Select a name from the Match List and click OK.

- Choose By Name, enter a number in the Number in Match List field and enter one or more characters in the Name field. These characters should match the name you are searching for. Click Submit. Select a device name from the Match List and click OK.

Task Flowchart

Use the following flowchart to help you determine whether or not the user can perform a task, based on the permissions owned by the user and, if terminal security is on, the terminal.


START
Determine your group list, including extended membership.
Is terminal security on?
YES
NO
Determine the terminal's group list, including extended membership.
Determine the list of groups which you and terminal have in common.
Does at least one group have function access?
NO
YES
Does at least one group have required document permissions?
NO
YES
Does at least one group have required device access?
NO
YES
You can perform the task.
You cannot perform the task.

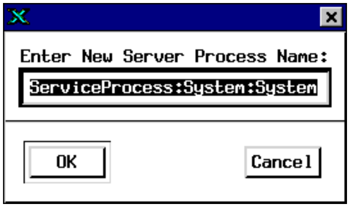
Security for Internetworking

Change Server Process Name

MultSv

If your system is networked to other systems, you can log on as SysAdmin and prevent those systems from using your resources by changing your server process name.

Choosing Change Server Process Name from the System menu displays the following dialog box.



Enter New Server Process Name: ServiceProcess:System:System

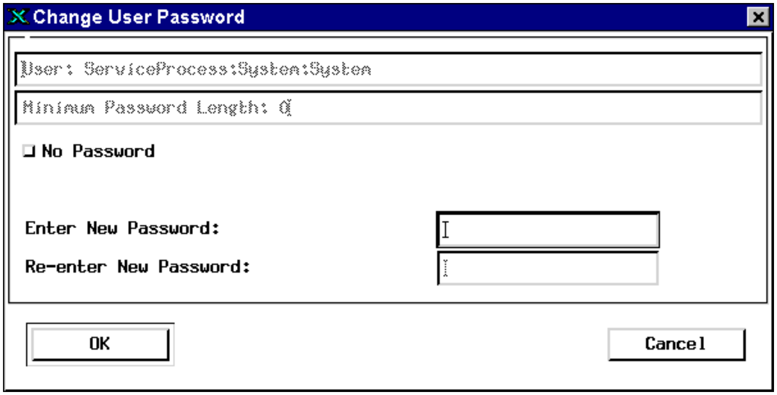
To change the name from the default, shown here, type another name and click OK. Once you save this name, other systems will not be able to access your system’s resources.

To make your system’s resources available to other systems, reset the server process name either to that shown in the illustration or to a name common to the systems that must communicate.

Change Server Process Password

MultSv

Just as you can change your server process name, you can log on as SysAdmin and prevent other systems from using your resources by changing your server process password. Select Change Server Process Password from the System pulldown menu to display the following dialog box.



Change User Password

User: ServiceProcess:System:System

Minimum Password Length: 0

□ No Password

Enter New Password:

Re-enter New Password:

The following table describes each element of the dialog box.

Field	Description
User	Contains the current server process name whose password you want to change. You cannot edit this field.
Minimum Password Length	The default reflects the value set in Default Security Settings (in the System menu). You cannot edit this field.
No Password checkbox	If you check this checkbox, the system disables the Enter New Password and Re-enter New Password fields.
Enter New Password	Enter the new password for your system.
Re-enter New Password	Re-enter your new password to confirm correct input.

Security Reports and Logs

Security Administration provides reports that summarize and detail your security configuration. You can print these reports, save them to a file, or append selections to a file. In addition, the FileNet system logs security events. You can determine what information to log and then read the event logs through the Security Administration application.

Security Reports

The Users, Groups, and Devices menus include the following reports that you can view, save to a file, or print:

Report Type	Description
Summary	A list of three-part security object names
Detail	A complete record showing all attributes of the security object
Extended Membership	The extended membership list of the security object

As an administrator, you can view information about all users, groups, and devices. Once you have selected a view, you can change the view by selecting a different one from the View menu.

You cannot print reports if your primary group is (NONE).

Logon Reports

Selecting View Logons from the Users menu displays users currently logged on to the system. You can save all or portions of the report to a file or print the report. In addition, you can sort the information by user, by location (endpoint), and by time. To terminate a logon, select it and choose Kill Logons from the Logons menu. You will see no confirmation prompt, so be sure you're selecting the appropriate logon names.

Event Logs

You can view Security event logs on the server. For more information see the *Image Services System Administrator’s Handbook*. To download this handbook from the IBM support page, see **“Accessing IBM FileNet documentation” on page 17**.

3

Database Maintenance

Overview

Remote Admin Console allows you to:

- Create and maintain media families, indexes, and document classes
- Change indexes from primary to informational, or from informational to primary
- Delete documents and folders
- View reports on indexes, document classes, and media families

You can select from the most frequently used options in Database Maintenance by clicking the function button or by using the menus. The options tied to these function buttons are:

- Define/Update Index
- Define/Update Family
- Define/Update Class
- Report on defined Indexes
- Report on defined Families
- Report on defined Classes

For detailed information on Database Maintenance concepts, refer to the *Image Services System Administrator’s Handbook*. To download this handbook from the IBM support page, see **"Accessing IBM FileNet documentation" on page 17**.

Start Database Maintenance

Choose Database Maintenance from the Remote Admin Console's Applications menu. The Database Maintenance main window appears.

Available menu options are described in the following table (see also **"Online Help" on page 24**). Use this table as a quick reference when you need to find a particular Database Maintenance function.

Available Menu Options

Miscellaneous	Indexes	Classes	Families
Delete Doc./Folder Exit	Define/Update Index Rename Build Retrieval Key Drop Retrieval Key Define/Update Cluster Report	Define/Update Class Report	Define/Update Family Report

CAUTION It is highly recommended that the Define/Update options under both the Indexes and Classes menus be executed during non-production hours. These tools will issue locks on the relational database that may cause long delays in system processing. This primarily affects systems with very large databases, but is the recommended procedure for all systems.

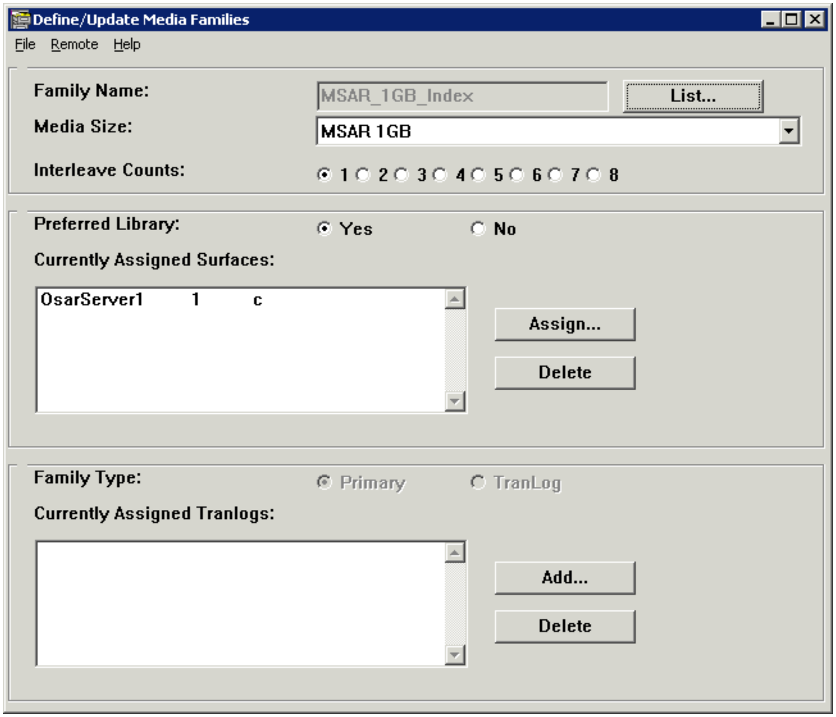
The Report function under both the Indexes and Classes menus provides a method to list these definitions and should be used in place of the Define/Update option whenever possible.

Note Any modifications made to the Index fields, Document Classes and Disk Families will not take effect until the FileNet software is recycled.

Define a Media Family

You must define a media family before you can create document classes, even if you keep all your documents in magnetic disk cache.

1 Choose Define/Update Family from the main window's Families menu to display the following window.



Family Name: MSAR_1GB_Index

Media Size: MSAR 1GB

Interleave Counts: ● 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7 ○ 8

Preferred Library: ● Yes ○ No

Currently Assigned Surfaces:

```
OsarServer1      1        c
```

Family Type: ● Primary ○ TranLog

Currently Assigned Tranlogs:

2 Click the List button beside the Family Name field to see a list of existing family names.

3 Select a name for updating, or enter a new name and click OK.

To enter a new name, type only alphanumeric characters and underscores (up to 18 characters) in the blank field beneath the list.

A media family name consists of 1-18 alphanumeric characters in any case (upper, lower, or mixed), without spaces or any other special characters, such as the Euro € character, except for an underscore.

4 Select the disk size (if you are creating a new family).

For a system without storage media, you can select any disk size. If you later add storage media, you can change the disk size to match the media (see **“Change Disk Size” on page 117**).

Click the arrow to display the list of media types. For any media family name (whether primary or transaction log), you must choose one type of media. However, the transaction log types can be different from the primary type.

Note If you enter a size that is not configured, an error message does not appear until you attempt to save the family.

5 Select the interleave count.

To set up interleaving, click the appropriate button to the left of the number. You can change this number after creating the family.

6 Click the Yes radio button in the Preferred Library field to assign more than one current write surface to speed up committals or to specify writing to a particular server or library. The system will then only look at the storage library before performing a write.

This displays the Currently Assigned Surfaces list box along with the Assign and Delete buttons.

Note Always ensure that the preferred library setting for the family is still correct after adding or deleting storage libraries.

Important In a multi-Storage Library server environment, if you do not choose to migrate documents from cache immediately after committal, you must assign a preferred storage library for the media family before migrating documents.

Important When the Image Services system is put into production, the system administrator should monitor cache resources frequently to prevent the cache on a particular server from becoming full. If the cache on a Storage Library server nears capacity, the system administrator can re-assign the Preferred Library of a media family to prevent it from filling up completely.

If you make no assignments, the system attempts to balance the writing load. The system assigns one current write surface to the next eligible library server (a server with the proper media type for the family).

For example, if you have a multiple storage library configuration where the primary family and an associated tranlog is write compatible on one server but not on the others, then the writes will go to the servers with the primary/tranlog setup. However, if your multiple Storage Library server configuration is such that the primary family and an associated tranlog are write compatible on all servers, the system will automatically balance the writes among all servers. Please note that Image Services requires that the primary and its associated tranlog surfaces reside on the same Storage Library server. Also, be aware that the system will look at all storage libraries before determining which one(s) to write to. Be aware of the following rules:

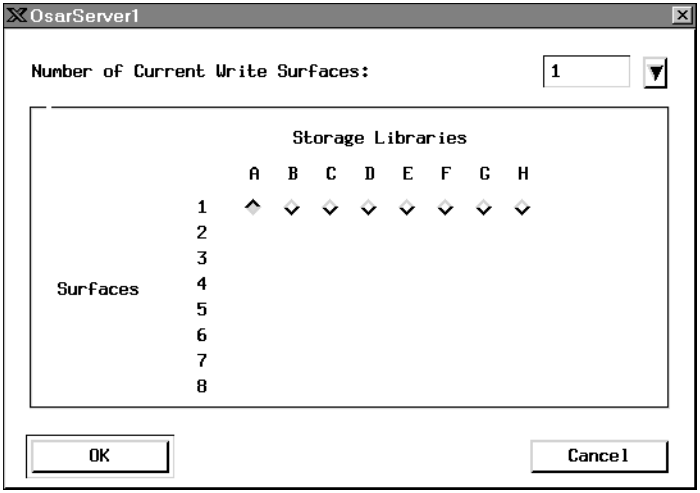
- If a primary family does not have a preferred library and it has an associated tranlog family, then the primary family and tranlog family must be write compatible on the same Storage Library server.
- If a primary family has a preferred library and it has an associated tranlog family, then all tranlogs must be write compatible on the same preferred server.

For a system without storage media, this selection is ignored.

Note If you have a multiple storage library server configuration, click the Yes option in the Preferred Library area and assign a preferred storage library. If the storage library has an associated tranlog family then it must be attached to the same Storage Library server.

7 Click the Assign button to display a list of library servers.

8 Select a storage library server and click the Assign button to display the following dialog box (in the illustration, one write surface is already selected).



Number of Current Write Surfaces: 1

a Click the down arrow to display a list (1–8) and select the number of write surfaces you want to be active at one time.

b Click the appropriate button in the grid to assign a surface to a particular storage library. For example, to assign surface 1 to library A, click the upper left button (1 A). To assign surface 2 to library B, click the second button on the second line (2 B).

c Click the OK button when you are finished, then close the Storage Library Server dialog box by clicking Cancel. The list box on the main window displays your assignments.

Note If you assign a surface to a non-existent library, the system displays this message when you try to save the family:

> Cannot assign current surface to a storage library which does not exist or does not match the family media type.

9 Select the family type.

- If you are defining a primary media family, click the Primary radio button and skip to step 12.
- If you are defining a transaction log media family, select the TranLog radio button and go to step 10.

10 Assign a transaction log family to the primary family.

- To assign a transaction log family to a primary family:

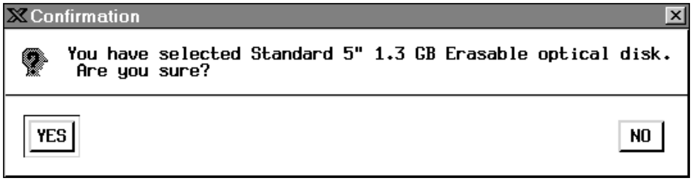
  a Click the Add button, which displays a list of transaction log families.

  b Select one or more names from the list and click OK. The names appear in the list on the main window.

- To write to several transaction log media, choose one family whose addresses you want to retain in your permanent database and be sure that name is the last one on the list.
- To add a tranlog family later:
  - temporarily delete the name of the tranlog family from Step a
  - add the new tranlog family
  - add back the tranlog family you deleted

11 When you finish all definitions, choose Save from the File menu.

12 Confirm your choice of media at the prompt.



You have selected Standard 5" 1.3 GB Erasable optical disk.
Are you sure?

13 Click OK to dismiss the popup window that confirms you created the family.

Validate the Media Family

Whenever a change in storage library configuration occurs, especially when a storage library is deleted, you must validate the media families by resaving the media families manually and resolving any errors.

Follow these steps to resave a media family:

1 Choose Define/Update Family from the main window's Families menu.

2 Click the List button beside the Family Name field to see a list of existing family names.

3 Select the name of the media family you wish to save and click OK.

4 Choose Save from the File menu.

If the system saves the media families successfully, you're done.

If the system does not save the media families, you will see an error message indicating the library number that is incorrect. Some reasons for save errors include:

- deleting a library

- reassigning a library number
- configuring a new library type over (with the same letter as the old one.)
- adding a new Storage Library server and more.

Correct the warnings and errors that appear by adding or changing the preferred library to match the current storage library configuration.

Add Disk Size

In an existing system with a storage library, you can add a new drive that supports a different disk size. When you do this, you must create new media families for this new disk size.

CAUTION Do not modify MKF database tables to change the disk size.

To add a new disk size to an existing system:

1. Commit all outstanding batches.
2. Create new media families for both primary and secondary surfaces.
3. Add the new families to a document class.

All future batches for this document class go to the new disk type.

Change Disk Size

After you create a media family, you can change the disk size if the surfaces are not assigned. This is usually done if you add a storage library to a cache-only system (all committed documents are stored on magnetic disk) so you can migrate documents to the storage library.

CAUTION Do not modify MKF database tables to change the disk size.

To add storage media to a cache-only system:

1. Commit all outstanding batches.
2. Change the disk size for your media families for both primary and secondary surfaces.
3. At the Storage Library server, use Background Job Control to migrate already committed documents from magnetic disk to storage media. For more information, see the *Image Services System Administrator’s Handbook*. To download this handbook from the IBM support page, see **“Accessing IBM FileNet documentation” on page 17**.

Commit to a Remote System

MultSv

Before you can commit to a remote system, your system must be configured correctly (with a remote domain) and that system must be available. You must also be logged on with a user name that is valid on both your local system and the remote system.

1. Choose Define/Update Media Families from the Database Maintenance window’s Families menu.

2. Select the primary family whose documents you want to commit to a remote family.

3. Choose Families from the Remote menu to display the Remote Media Families dialog box.

4. Click the down arrow beside the Domain text field and select the system to which you want to commit the documents.

Note When you select the target domain, you will see a pop-up window prompting you to enter an account password for the user common to both systems.

5. Click the down arrow beside the Families text field and select the family on the remote system that will receive the documents.

Note When you save the family you just added, you will see a pop-up window prompting you to enter an account password for the user common to both systems.

6. Each family you choose on the remote system appears at the top of the screen when you click the Add button. When you finish assigning families at one site, you can select another site and add families.

Note If the remote family uses transaction logging and the remote site does not want to make additional copies of the documents, the remote site must delete the transaction log families from that primary family.

7 When you are finished with all assignments, click OK.

Define an Index

Indexes must exist before you can create document classes.

Note In a FileNet P8 Content Federation Services environment, a document class may or may not have index values associated with it. If you want the documents associated with the document class to be retrievable only from the Content Engine system, indexes are not required. However, if you want the documents to be retrievable from both the Content Engine system and the Image Services system, you need to specify indexes in the Document Class. For information on mapping the index values between the IS and the CE systems, see the *FileNet P8 Content Federation Services for Image Services Guidelines*. To download the guidelines from the IBM support page, see **“Accessing IBM FileNet documentation” on page 17**.

CAUTION Do not define unnecessary indexes. The maximum number of indexes you can define is 224. You cannot delete an index or change its type. For restrictions on changing an index, see **“Modify an Index” on page 146**.

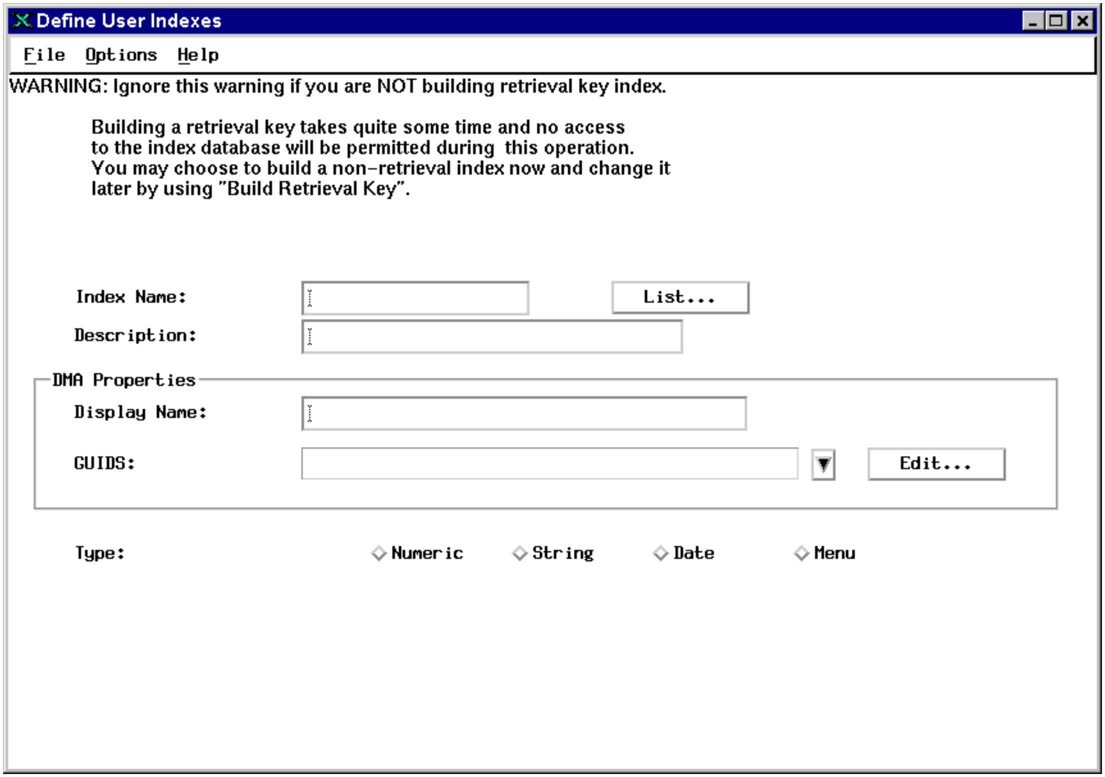
Before you can define a new index, you must make sure that no one else accesses the database. While other users are on the system, you can modify and get information about existing indexes without disturbing normal system operation.

However, you may lose any data you enter for a new index. If any index database activity (committal, retrieval, filing documents in folders) occurs before you save the new index, the system cannot write the data and an error message appears.

Tip To prevent users from logging on while you're defining new indexes, put all the users in a session group and expire the session.

To define an index, follow these steps:

1 Choose Define/Update Index from the Database Maintenance window's Indexes menu, which displays the following window.



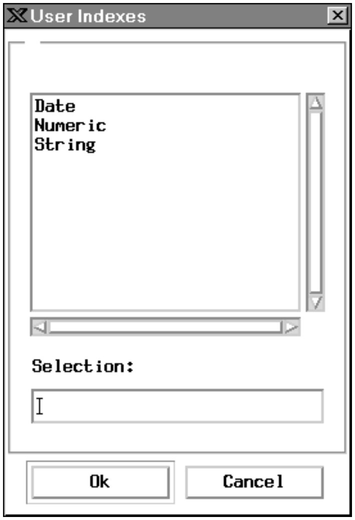
WARNING: Ignore this warning if you are NOT building retrieval key index.

Building a retrieval key takes quite some time and no access to the index database will be permitted during this operation. You may choose to build a non-retrieval index now and change it later by using "Build Retrieval Key".

The Define User Indexes window displays a warning about the time required to create a retrieval key. To change an index to a retrieval key later, see **“Change Retrieval Key Status” on page 143**.

2 Define the index name.

a Click the List button to enter a new name. This displays the User Indexes dialog box listing all current indexes.



To view information about an index, select its name and click the Ok button. Check the list to see if the index name you want to use already exists.

b Enter a new name in the Selection field at the bottom of the dialog box. This name appears on the default indexing forms of document classes that use the index. See Indexes in the *Image Services System Administrator's Handbook* for naming conventions. To download this handbook from the IBM support page, see **"Accessing IBM FileNet documentation" on page 17**.

An index name typically consists of 1-18 alphanumeric characters in any case (upper, lower, or mixed), without spaces or any other special characters, such as the Euro € character, except for an underscore. You cannot start a document class name with a numeral or with the characters F_ (capital F, underscore).

c Click the Ok button to save the index name. The list box closes and the cursor moves to the description field of the Define User Indexes window.

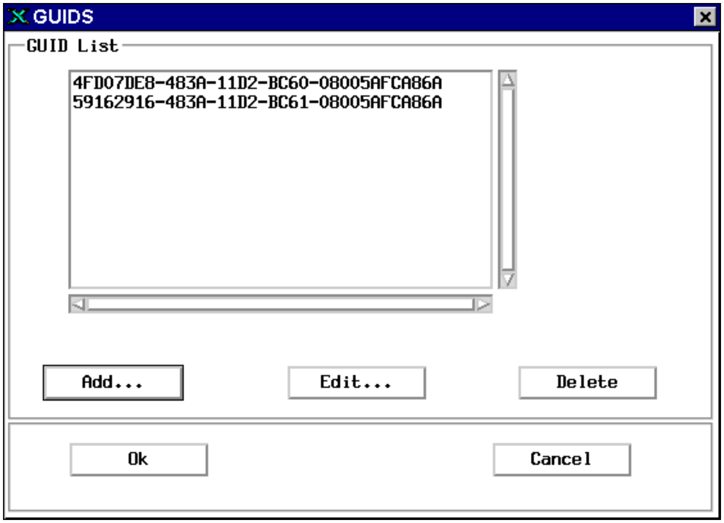
d Enter a description for the index that clarifies its purpose. You see the description in this window and in the User Indexes Report. It does not appear in list boxes. A description can have from 1 to 30 characters, including spaces and special characters, in any case (upper, lower, or mixed).

3 Define the DMA properties. The DMA Properties enable you to specify a DMA display name and up to 10 GUIDs (Globally Unique IDentifiers) for each defined user index.

a Specify the Display Name. When you first enter a name in the Index Name field, the system automatically duplicates that name in the DMA Properties Display Name field. You can change this name by selecting all or part of the text and typing the desired name.

This field accepts up to 30 alphanumeric characters, including spaces and special characters.

b Click the Edit button to open the GUIDS dialog box, which enables you to add, delete, or modify GUIDs for the currently defined user index. You must assign at least one GUID to the index and may assign up to 10 GUIDs for each user index.



4FD07DE8-483A-11D2-BC60-08005AFCA86A
59162916-483A-11D2-BC61-08005AFCA86A

c Select the GUID you want associated with the user index. For details on adding, editing, and deleting GUIDs, see **“GUIDs Assigned to User Index” on page 126**.

d Click Ok. The selected GUID displays in the GUIDS field on the Define User Indexes dialog box. Each additional GUID defined on the GUID list may serve as an alias for the user index.

4 Define the index type.

a Choose an index type. An index is one of four types: numeric, string, date, or menu. Additional parameters appear at the bottom of the window as appropriate for the index type.

b Indicate if the index is a retrieval key by selecting either the Yes or No radio button.

- Select Yes if you want to use the index as a primary key (instead of only using it as a secondary filter) in a query. You may use only a retrieval key as a primary key in a query.

- Select No if you never want to use the index as a primary key. Secondary filters always use a sequential search.

c Complete additional parameters for the type of index. See **“String Index” on page 131**, **“Date Index” on page 136**, **“Numeric Index” on page 133**, or **“Menu Index” on page 138**.

Note Once you have created an index, you cannot delete it or change its type.

5 Save the index.

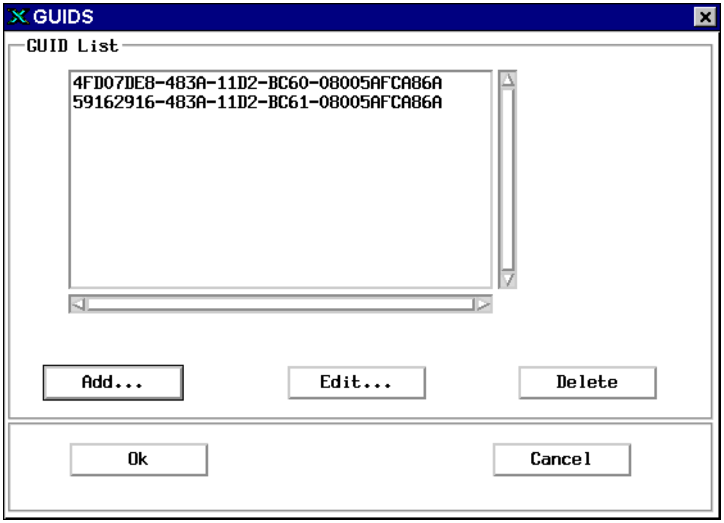
When you complete all fields for each index, choose Save from the File menu. If no other database activity or input errors occur, the system saves the index successfully. Otherwise, it displays an error message. If this happens, you’ll need to try later or change the appropriate fields.

GUIDs Assigned to User Index

GUIDs (Globally Unique IDentifiers) are DMA-compliant, 16-byte integers used to uniquely identify each element transported over a network. The system ensures unique GUID assignments by automatically generating this integer using an algorithm based on the system's network card MAC address and a format that complies with the specifications provided for the system's platform.

Each GUID must have a unique name that conforms to the format specified for your Image Services system platform. For platform specifications, see the GUID naming conventions described in the documentation that came with your operating system.

To add, delete, or rename GUIDs for the current user index, click the Edit button in the DMA Properties box of the Define User Indexes dialog box. The GUIDs dialog box opens, displaying a list of currently defined GUIDs.



GUIDS

GUID List

4FD07DE8-483A-11D2-BC60-08005AFCA86A
59162916-483A-11D2-BC61-08005AFCA86A

As you add or rename GUIDs, the system validates the assigned name, making sure it meets the following requirements:

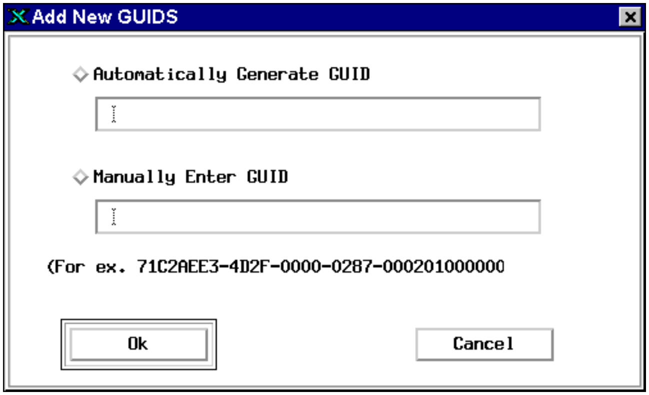
- Unique name assignment
- No duplication of name in the Image Services database
- At least one and no more than 10 GUIDs assigned to each user index

You may modify the currently defined list as follows:

- To delete an existing GUID, select it from the list and click the Delete button. A message box opens, asking you to verify deletion. Click Yes to delete the selected GUID or No to cancel deletion.
- To add a new GUID to this user index, click the Add button. The Add New GUIDS dialog box opens. For details, see **"Add New GUIDs" on page 128**.
- To rename an existing GUID, select it from the list and click the Edit button. The Edit GUID dialog box opens, displaying the exiting name of the selected GUID. For details, see **"Rename GUID" on page 129**.

Add New GUIDs

The Add New GUIDS dialog box opens after you click the Add button on the GUIDS dialog box when defining the DMA properties of a user index.



(For ex. 71C2AEE3-4D2F-0000-0287-000201000000

Automatically Generate GUID

Click this radio button to have the system automatically generate a GUID. The system displays the GUID in grayed-out, uneditable text.

To save the automatically generated GUID, click the OK button. The system closes the Add New GUIDS dialog box and displays the newly assigned GUID in the GUIDS list.

Manually Enter GUID

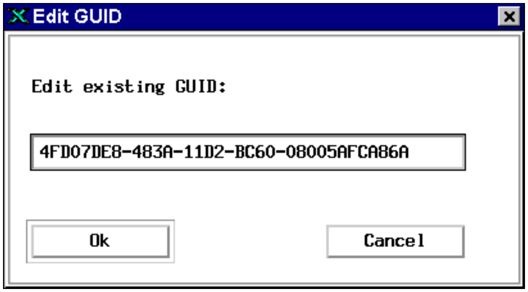
Click this radio button if you want to manually assign a GUID. Type a 16-byte character set into the field, using the format shown in the sample displayed below the entry field.

To save the manually defined GUID, click the OK button.

- If you entered a GUID that already exists in the Image Services database or does not use the correct format, a message box opens, alerting you to the problem. When this happens, you must enter an acceptable GUID and click OK again.
- If you entered a unique GUID using the correct format, the system closes the Add New GUIDS dialog box and displays the newly defined GUID on the GUIDS list.

Rename GUID

The Edit GUID dialog box opens after you select an existing GUID from the GUIDS list and click the Edit button on the GUIDS dialog box when defining the DMA properties of a user index.



Edit existing GUID:

4FD07DE8-483A-11D2-BC60-08005AFCA86A

Edit existing GUID field

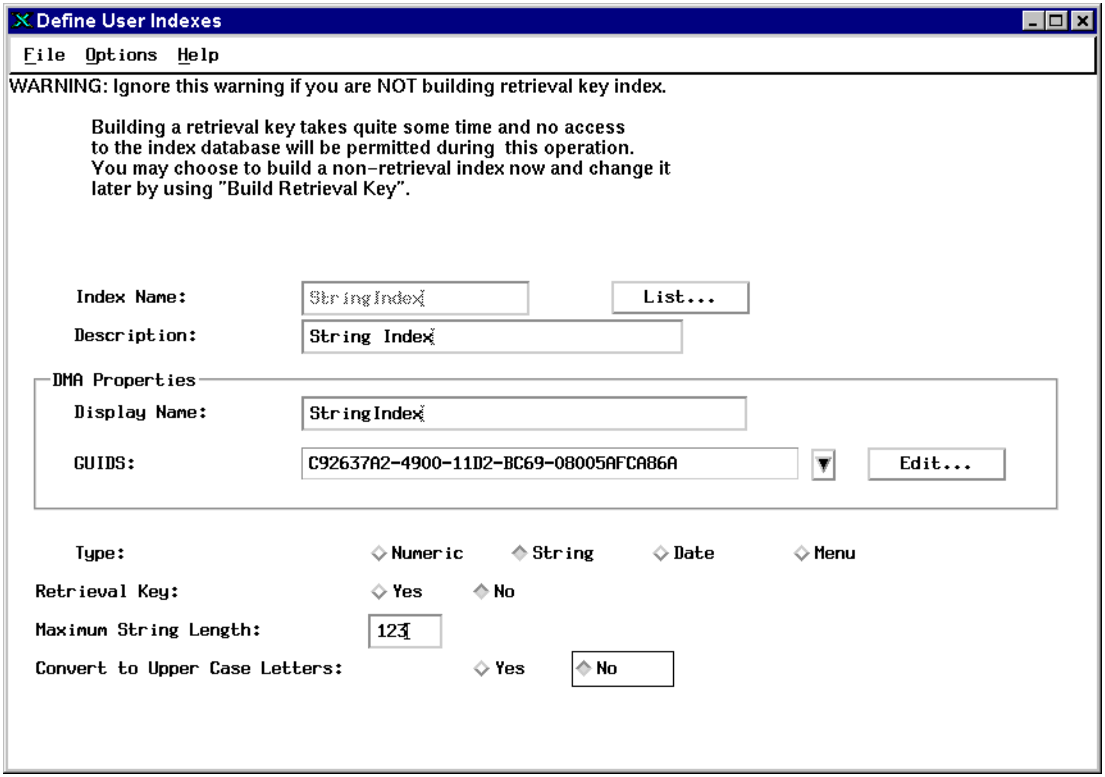
This field displays the currently selected GUID and allows you to rename it.

To change the current name, select all or any part of the displayed text, type in the desired text, and click Ok.

- If you entered a GUID that already exists in the Image Services database or does not use the correct format, a message box opens, alerting you to the problem. When this happens, you must enter an acceptable GUID and click Ok again.
- If you entered a unique GUID using the correct format, the system closes the Edit GUID dialog box and displays the renamed GUID on the GUIDS list.

String Index

Selecting the String index type displays the following entry fields and buttons in the Define User Indexes window:



Define User Indexes

WARNING: Ignore this warning if you are NOT building retrieval key index.

Building a retrieval key takes quite some time and no access to the index database will be permitted during this operation. You may choose to build a non-retrieval index now and change it later by using "Build Retrieval Key".

Index Name: StringIndex

Description: String Index

DMA Properties

Display Name: StringIndex

GUIDS: C92637A2-4900-11D2-BC69-08005AFCA86A

Type: ◇ Numeric ◆ String ◇ Date ◇ Menu

Retrieval Key: ◇ Yes ◆ No

Maximum String Length: 123

Convert to Upper Case Letters: ◇ Yes ◆ No

1 Enter the maximum number of characters you want the indexing operator to enter (the system maximum is 239; the default length is one character).

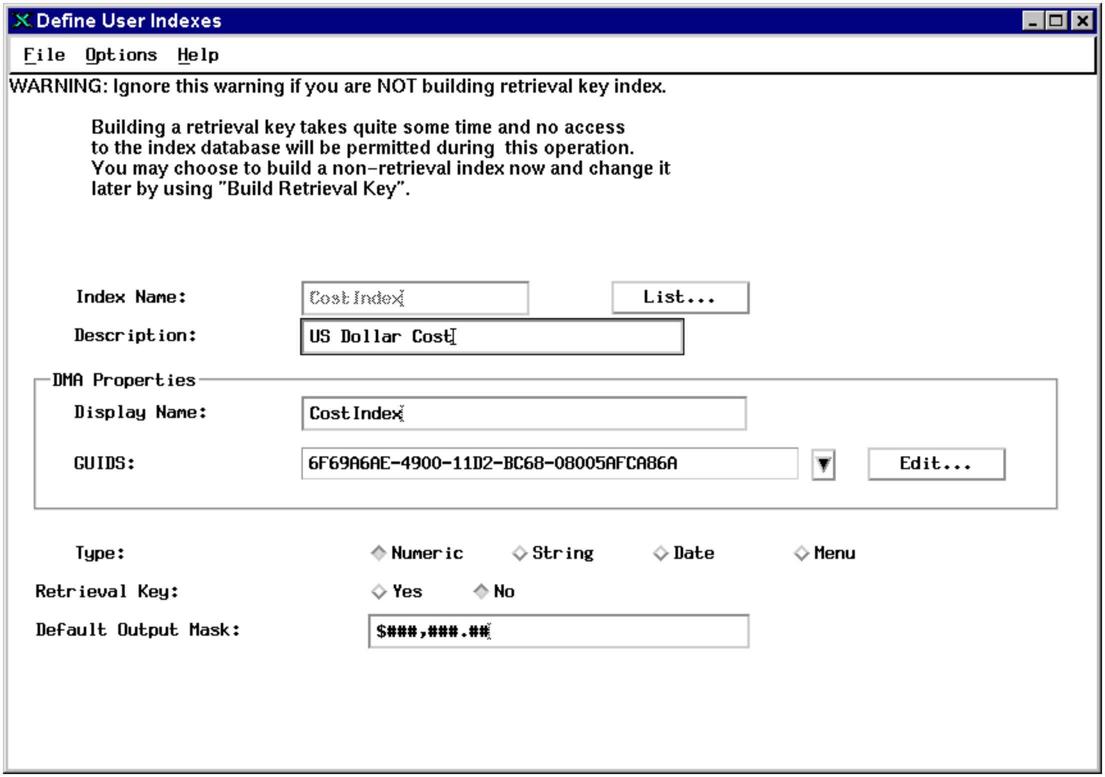
2 Select Yes if you want the index value automatically converted to uppercase before the system stores its values. (You cannot change this selection once you have created a string index.)

Note Once you have created an index, you cannot delete it or change its type.

3 If you select No, the index value becomes case-sensitive (each character in the query must match the case of the stored value to qualify for the report).

Numeric Index

Selecting the Numeric index type displays the following entry fields and buttons in the Define User Indexes window:



WARNING: Ignore this warning if you are NOT building retrieval key index.

Building a retrieval key takes quite some time and no access to the index database will be permitted during this operation. You may choose to build a non-retrieval index now and change it later by using "Build Retrieval Key".

Index Name: Cost Index

Description: US Dollar Cost

DMA Properties

Display Name: Cost Index

GUIDS: 6F69A6AE-4900-11D2-BC68-08005AFCA86A

Type: ◆ Numeric ◇ String ◇ Date ◇ Menu

Retrieval Key: ◇ Yes ◆ No

Default Output Mask: $###,###.##

As an option, you may assign an output mask to a numeric index type. This specifies how the system displays the value (in the Query Match Report, for example). If you do not specify an output mask, the system uses the numeric mask defined in the Image Services server's operating system parameters.

The system accepts only numerals, a minus sign, and a decimal point in numeric fields. Whether document entry operators need to key the decimal point depends on the value and the mask. The mask also determines the index length.

Note On an Image Services server configured with an Oracle RDBMS, the system does not use the mask size, precision, or scale to validate data entered into the field.

CAUTION On an Windows Server platform with a SQL database, the system checks the numeric input value against the precision and scale values defined for a numeric mask on the MS SQL server. If the input value does not fit into the numeric mask, document committal fails, displaying the error:

> <90,0,104> Precision and scale specified in numeric index mask cause overflow

The precision is the total number of digits, on both the left and right side of the decimal point (excluding the decimal point, commas, and the like). The scale is the number of digits shown on the right side of the decimal point. For details on how to enlarge these values, see the *Image Services System Administrator’s Handbook*. To download this handbook from the IBM support page, see **“Accessing IBM FileNet documentation” on page 17**.

Numeric masks can use these characters:

# Place holder for a numeral. Specify as many as needed for the maximum number of digits. Unused positions are blank and the number is right justified.

0 Position of a numeral with leading zeros. A digit always displays in each position. Any position for which there is no other value displays a zero.

+ Displays the sign (+ or –) of the number. You can place it at the beginning or end of the mask depending on where you want the sign to display.

– Displays the sign of the number only if it is negative. You can place it at the beginning or end of the mask depending on where you want the sign to display.

$ Places a floating dollar sign in front of the number.

. Position of a decimal point. A mask ending in .00 indicates fixed point—two digits are always to the right of the decimal and operators do not need to enter the zeros. A mask ending in .## indicates floating point—**up to** two digits can be to the right of the decimal.

, Position of an embedded comma within the mask to make the value more readable.

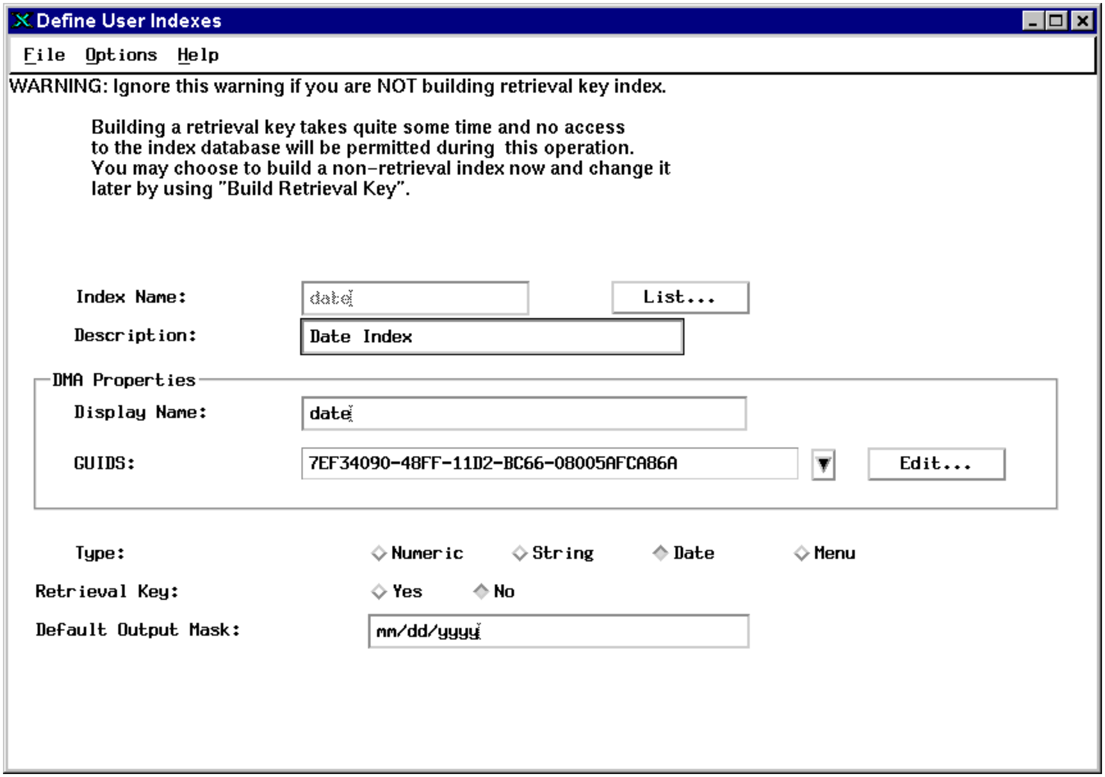
The following table shows several examples of edit masks, stored (keyed) values, and their resultant output.

Sample Edit Mask	Stored Value	Sample Display
####	29	29
0000	29	0029
$####	29	$29
$###,###.00	.29	$.29
$###,###.00	29	$29.00

Sample Edit Mask	Stored Value	Sample Display
$###,###.##	29	$29.00
+####	29	+29
+####	–29	–29
–####	29	29
–####	–29	–29
####–	–29	29–
–$###.00	–29	–$29.00
$–###.00	–29	$–29.00
#,###	2929	2,929
##.##	29	29.

Date Index

Selecting the Date index type displays the following entry fields and buttons in the Define User Indexes window:



WARNING: Ignore this warning if you are NOT building retrieval key index.

Building a retrieval key takes quite some time and no access
to the index database will be permitted during this operation.
You may choose to build a non-retrieval index now and change it
later by using "Build Retrieval Key".

Index Name: date

Description: Date Index

DMA Properties

Display Name: date

GUIDS: 7EF34090-48FF-11D2-BC66-08005AFCA86A

Type: ◇ Numeric ◇ String ◆ Date ◇ Menu

Retrieval Key: ◇ Yes ◆ No

Default Output Mask: mm/dd/yyyy

Enter the mask you want the system to use when displaying this date. Date masks use the following codes:

w	Day of the week (0–6, where 0=Sunday and 6=Saturday)
dd	Day of the month (1–31)
ddd	Day of the year (1–366)
day	Abbreviated day name (Sun–Sat)
daynameDay (Sunday–Saturday)	

mm	Number of month (1–12)
mon	Abbreviated month name (Jan–Dec)
month	Month (January–December)
yy	Last two digits of year (00–99)
yyyy	Year (0000–9999)

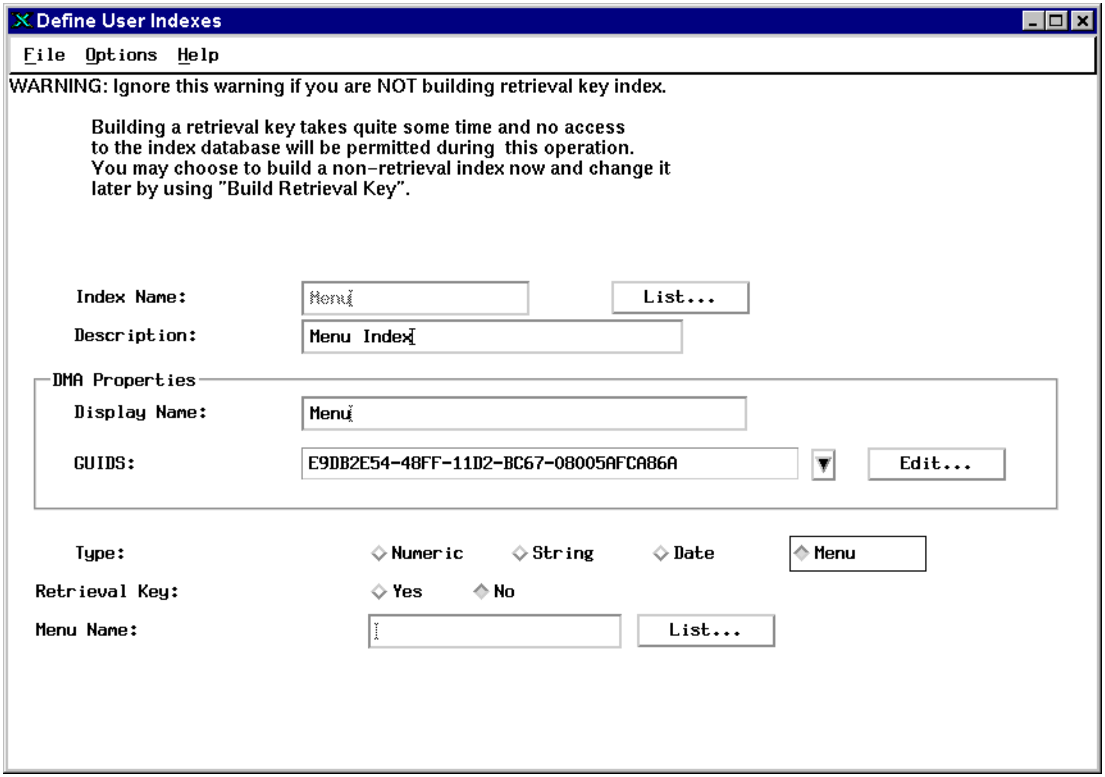
Your mask can include spaces and punctuation characters as separators. Below are some sample date masks and their resulting display.

Date Mask	Display
dayname, month dd, yyyy	Friday, November 10, 1996
dd mon yyyy	10 Nov 1996
mm/dd/yy	11/10/96
ddd	315

For information on how the Image Services system interprets date masks, see the *Image Services System Administrator's Handbook*. To download this handbook from the IBM support page, see **"Accessing IBM FileNet documentation" on page 17**.

Menu Index

Selecting the Menu index type displays the following entry fields and buttons in the Define User Indexes window:



Define User Indexes

File Options Help

WARNING: Ignore this warning if you are NOT building retrieval key index.

Building a retrieval key takes quite some time and no access to the index database will be permitted during this operation. You may choose to build a non-retrieval index now and change it later by using "Build Retrieval Key".

Index Name: Menu List...

Description: Menu Index

DMA Properties

Display Name: Menu

GUIDS: E9DB2E54-48FF-11D2-BC67-08005AFCA86A Edit...

Type: ○ Numeric ○ String ○ Date ● Menu

Retrieval Key: ○ Yes ● No

Menu Name: List...

Click the List button to display a list of existing menus.

If you need to create a new menu, select Build Menu from the Options menu. See **“Create a Menu Index” on page 150**.

Create a Cluster Index

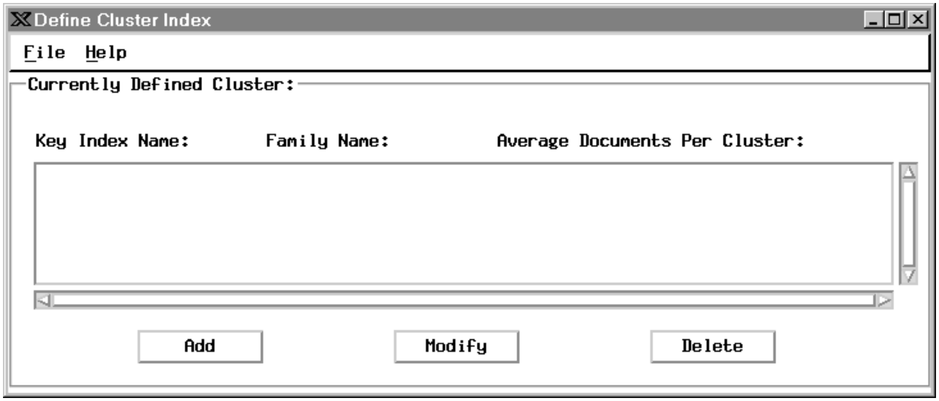
Clustering is associated with a **retrieval key** index. You indicate that all documents with the same value in a specified index should be stored on the same storage media regardless of when you scan and commit them. A selected retrieval key used for clustering must already exist.

You can create as many cluster indexes as you need.

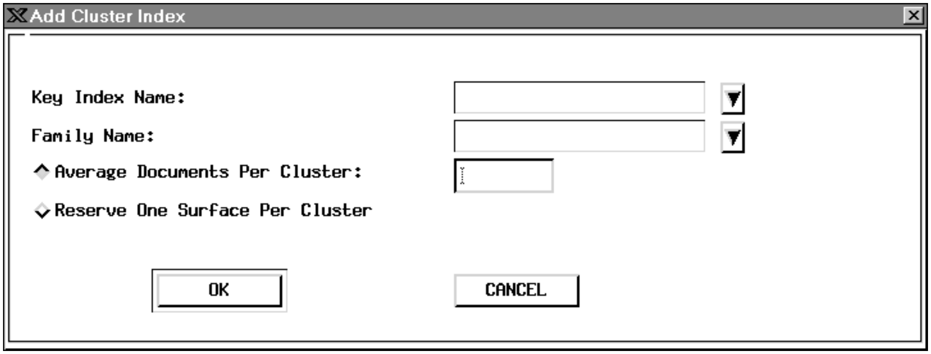
Note You cannot use clustering if your system is configured to use fast batch committal. For more information on fast batch committal, see the *Image Services System Administrator's Handbook.* To download this handbook from the IBM support page, see **"Accessing IBM FileNet documentation" on page 17**.

To create a cluster index:

1 Choose Define/Update Cluster from the Indexes menu to display the Define Cluster Index subwindow.



2 Click the Add button to display the following dialog box.


Add Cluster Index
Key Index Name:
Family Name:
Average Documents Per Cluster:
Reserve One Surface Per Cluster
OK
CANCEL

3 Choose a string or numeric index for clustering from the Key Index Name pull-down list.

4 From the Family Name pulldown list, choose a media family to write to when using this cluster index.

5 Choose one of the two radio buttons to select Average Documents Per Cluster or Reserve One Surface Per Cluster.

- If you choose Average Documents Per Cluster, enter a number in the text field that represents the number of documents you expect to be in one cluster (maximum is 500).

CAUTION Average Documents Per Cluster is critical to your system performance. If you set this value too small, your clusters will eventually split among multiple media surfaces, reducing clustering's effectiveness. If you set the value too large, you can waste a significant portion of each surface.

- If you choose Reserve One Surface Per Cluster, one entire surface of the media is reserved for the cluster.

6. Click OK to accept your settings and return to the Define Cluster Index window; click Cancel to close the Add Cluster Index dialog box without making any changes.
7. Choose Save from the File menu and follow the prompts to save your changes.

Assign a Cluster to a Document Class

Once the cluster index exists, you can set up a document class to use clustering. See **"Create Document Classes" on page 156**. Before you can choose the Cluster Family checkbox in the Define/Update Document Classes window, you must enter the cluster index name at the bottom of the window. Then, when you click the Cluster Family button, the system automatically enters the media family name. Complete the rest of the fields as appropriate and save the document class by choosing Save from the File menu.

Modify a Cluster Index

To modify a cluster index:

1. Choose Define/Update Cluster from the Indexes menu.
2. Select a string or numeric index and click the Modify button.
3. Follow steps 3 through 7 under **"Create a Cluster Index" on page 139**.

Delete a Cluster Index

To remove the clustering attribute from an index:

1. Choose Define/Update Cluster from the Indexes menu.
2. Select a string or numeric index and click the Delete button.
3. Confirm your choice in the dialog box that appears.

Change Retrieval Key Status

You can change a retrieval key index to an informational index and change an informational index to a retrieval key. These functions are on the Database Maintenance window's Indexes menu.

CAUTION It is highly recommended that the Define/Update option under the Indexes menu be executed during non-production hours. This tool will issue locks on the relational database that may cause long delays in system processing. This primarily affects systems with very large databases, but is the recommended procedure for all systems.

The Report function under the Indexes menu provides a method to list these definitions and should be used in place of the Define/Update option whenever possible.

Change a Retrieval Key Index to an Informational Index

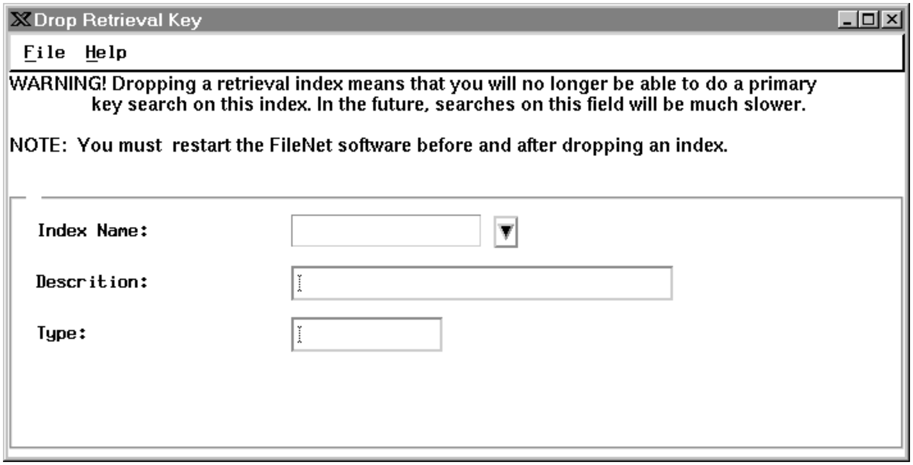
When you change a retrieval key index to an informational index, the system searches sequentially when performing a retrieval based on this index and the index can no longer be used as a primary key.

However, the document entry process is faster for subsequent indexing of documents that use this index because the system is not maintaining a sorted list.

Using this option can save magnetic disk space by eliminating the overhead structure required by retrieval indexes.

1 Restart the FileNet software.

2 Select Drop Retrieval Key from the Indexes menu to display this window.



WARNING! Dropping a retrieval index means that you will no longer be able to do a primary key search on this index. In the future, searches on this field will be much slower.

NOTE: You must restart the FileNet software before and after dropping an index.

Index Name:

Descrition:

Type:

3 Click the down arrow and select the retrieval index from the list.

The description and the index type display.

4 Select Drop from the File menu and answer the prompt.

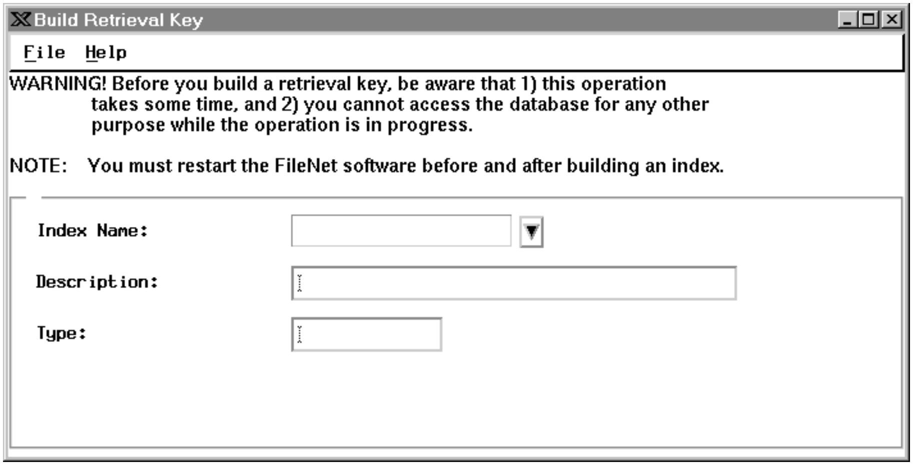
Change an Informational Index to a Retrieval Key Index

You can change an informational index to a retrieval key index.

CAUTION The time it takes to build a retrieval key depends on the number of documents stored in the database. For example, it may take approximately two minutes for every one million documents. You can only build a retrieval key when no one needs to use the database (for example, to commit, retrieve, or print any documents).

1 Restart the FileNet software.

2 Select Build Retrieval Key from the Indexes menu to display this window.



WARNING! Before you build a retrieval key, be aware that 1) this operation takes some time, and 2) you cannot access the database for any other purpose while the operation is in progress.

NOTE: You must restart the FileNet software before and after building an index.

Index Name:

Description:

Type:

3 Click the down arrow and select the index from the list.

4 Select Build from the File menu and answer the prompt in the popup window.

Modify an Index

Before modifying an index, consider the consequences to all document classes that use the index. Changing a description or adding items to menus does not have a significant impact. However, verify that a change that makes sense in one document class does not adversely affect a different document class. Check the Document Class Report (choose Report from the Classes menu) to see which classes use the index.

CAUTION It is highly recommended that the Define/Update option under the Indexes menu be executed during non-production hours. This tool will issue locks on the relational database that may cause long delays in system processing. This primarily affects systems with very large databases, but is the recommended procedure for all systems.

The Report function under the Indexes menu provides a method to list these definitions and should be used in place of the Define/Update option whenever possible.

CAUTION Any modifications made to the Index fields, Document Classes and Disk Families will not take effect until the FileNet software is recycled.

CAUTION Reducing the maximum string index length generates a database error when you query on documents that were committed using the larger maximum.

The following table lists the fields you can modify for each index type.

Index Type	Fields You Can Modify
Numeric	description, mask
String	description, maximum length of string
Date	description, mask
Menu	description, name of menu

Note You cannot delete or change the type of an existing index. You also cannot change the “Convert to Upper Case Letters” setting on a String index.

Although you cannot create new indexes when others are using the system, you can modify them at any time.

To modify an index:

1 Select Define/Update Index from the Indexes menu in the Database Maintenance window.

2 Click the List button to display the list of indexes.

3 Select the index to be updated and make changes as needed.

4 Save the changes by choosing Save from the File menu.

Rename an Index

If you must rename an index, do it very early in the development process and only if you understand the implications for the entire system. For example, if you are not using an index, you can rename and use it instead of creating a new index (if the index is the correct type). If you change the name of an index that is in use, you may need to make other changes, too. Discuss this change with your support representative.

CAUTION It is highly recommended that the Define/Update option under the Indexes menu be executed during non-production hours. This tool will issue locks on the relational database that may cause long delays in system processing. This primarily affects systems with very large databases, but is the recommended procedure for all systems.

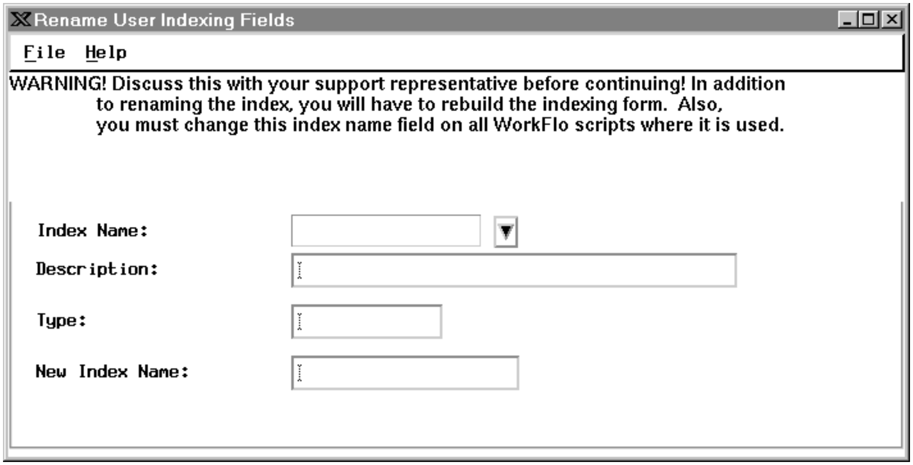
The Report function under the Indexes menu provides a method to list these definitions and should be used in place of the Define/Update option whenever possible.

CAUTION Any modifications made to the Index fields, Document Classes and Disk Families will not take effect until the FileNet software is recycled.

CAUTION In a Filenet P8 Content Federation Service for IS environment, do not change the name of any **mapped** index unless absolutely necessary. If you do need to change the index name, you must remap the index on the Content Engine system. Otherwise, index properties exported from IS will be mismatched with Content Engine mapping.

To rename an index:

1 Choose Rename from the Database Maintenance window's Indexes menu to display this window:



WARNING! Discuss this with your support representative before continuing! In addition to renaming the index, you will have to rebuild the indexing form. Also, you must change this index name field on all WorkFlo scripts where it is used.

2 Select the index you want to rename from the pulldown list.

The Description and Type fields display and the cursor moves to the New Index Name text field.

3 Type the new name.

See Indexes in the *Image Services System Administrator's Handbook* for naming conventions. To download this handbook from the IBM support page, see **"Accessing IBM FileNet documentation" on page 17**.

4 Select Save from the File menu. A dialog box asks for confirmation.

5 Click OK to confirm or Cancel to exit without saving.

If anyone used the database between the time you restarted the FileNet software and the time you saved the name change, you see a message asking you to try later.

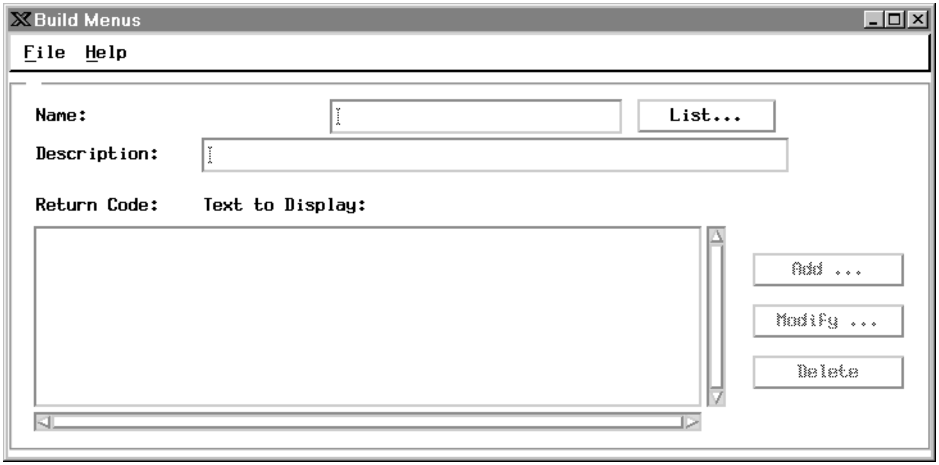
6 Rebuild indexing forms that use this index. (For details, see your FileNet client software documentation.)

Create a Menu Index

To create a menu index:

1 Choose Build Menu from the Options menu of the Define User Indexes dialog box (see also **"Menu Index" on page 138**).

The following window displays.



2 Click the List button to display a list of menus and the blank text field beneath the list.

3 Enter from 1 to 14 alphanumeric characters as a menu name.

Do not imitate batch names (a, b, d, f, q, p, pv, t, w, x, or X followed by a number) or use Visual Workflo reserved words. You cannot start a name with F_ (capital F, underscore) or with a numeral, but you can use an underscore as part of the name.

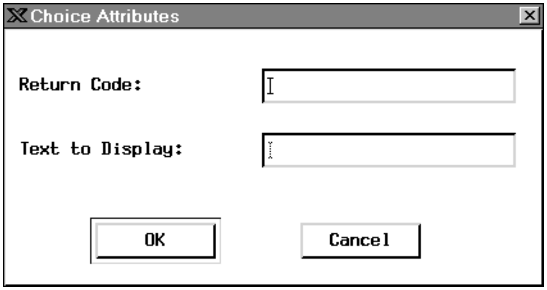
4 Click OK.

The selection box disappears and the menu name appears in the Name field.

5 Enter a description (optional) for the menu.

A description can be up to 177 characters. Only the first 55 characters display without scrolling.

6 Click the Add button and the Choice Attributes dialog box appears:



7 In the Return Code field, enter a character to be used as a return code.

A return code is a single character that tells the system (including a WorkFlo script) which menu option an operator selected. Specify any character, as long as each return code in the menu is different.

Note A return code can be any upper- or lower-case letter in the alphabet, a number (0-9) or a keyboard symbol. 94 different return codes are available.

When the indexing operator selects an item from the menu, the system passes the return code to Visual Workflo. The item does not appear on the display during indexing. If retrieval operators use a menu index as the basis for sorting the Query Match Report, the return code determines the sort order. To avoid confusion, you might want to assign letters of the alphabet to sort the menu items alphabetically.

Note The IDM Desktop Find program cannot locate a document based on a single-digit menu item selection unless its return code matches the text displayed on the menu. If you are defining a single-digit menu item, you must assign it an identical return code. For example, if you create a menu item in the Text to Display field as an upper-case letter A, you must also enter an upper-case letter A in the Return Code field.

8 In the Text to Display field, enter text for a menu item.

After entering the return code, press Tab and enter the text you want to appear on the menu for the indexing operator.

9 Click the OK button.

The new menu item is added. You can continue to add entries, clicking OK after each one.

10 When you finish adding entries, click Cancel to go back to the Build Menus window.

11 Choose Save from the File menu and a dialog box pops up to tell you that the menu was successfully created.

12 Exit the dialog box by choosing Exit from the File menu.

Change a Menu

You can add, modify, or delete items in existing menus, or you can copy, rename, or delete menus.

CAUTION It is highly recommended that the Define/Update option provided for the Document Classes be executed during non-production hours. This tool will issue locks on the relational database that may cause long delays in system processing. This primarily affects systems with very large databases but is the recommended procedure for all systems.

The Report function under the Classes menu provides a method to list these definitions and should be used in place of the Define/Update option whenever possible.

CAUTION Any modifications made to the Index fields, Document Classes and Disk Families will not take effect until the Image Services software is recycled.

Add, Modify, Delete Items in a Menu

1 Choose Define/Update Index from the Indexes menu.

2 Choose Build Menu from the Options menu.

3. Select the menu you want to change by clicking the List button and selecting an item from the list box. Click OK.

   - To add an item to the menu, click the Add button.

   - To modify an item in the menu, select the item and click the Modify button.

   In each case, enter the appropriate text in the resulting dialog box and click OK.

   - To delete an item, select it and click Delete. No confirmation prompt appears.

4. Save your changes by choosing Save from the File menu.

5. Select Exit from the File menu.

Copy, Rename, Delete Menu

1. Choose Define/Update Index from the Indexes menu.
2. Choose Build Menu from the Options menu.
3. Select the menu you want to copy, rename, or delete by clicking the List button and selecting an item from the list box. Click OK.
4. From the File menu, choose the appropriate action:

   - Save As to make a copy of the menu using a different name.
   - Rename to give the menu a different name.
   - Delete to delete the menu entirely.

   Save As and Rename present a prompt for a new name. Enter the new menu name and click OK.

   Delete asks you to confirm that you want to delete the item. To delete the menu, click Yes.

5. Select Exit from the File menu.

Create Document Classes

Before you create a document class, the indexes and media families needed by the class must already exist.

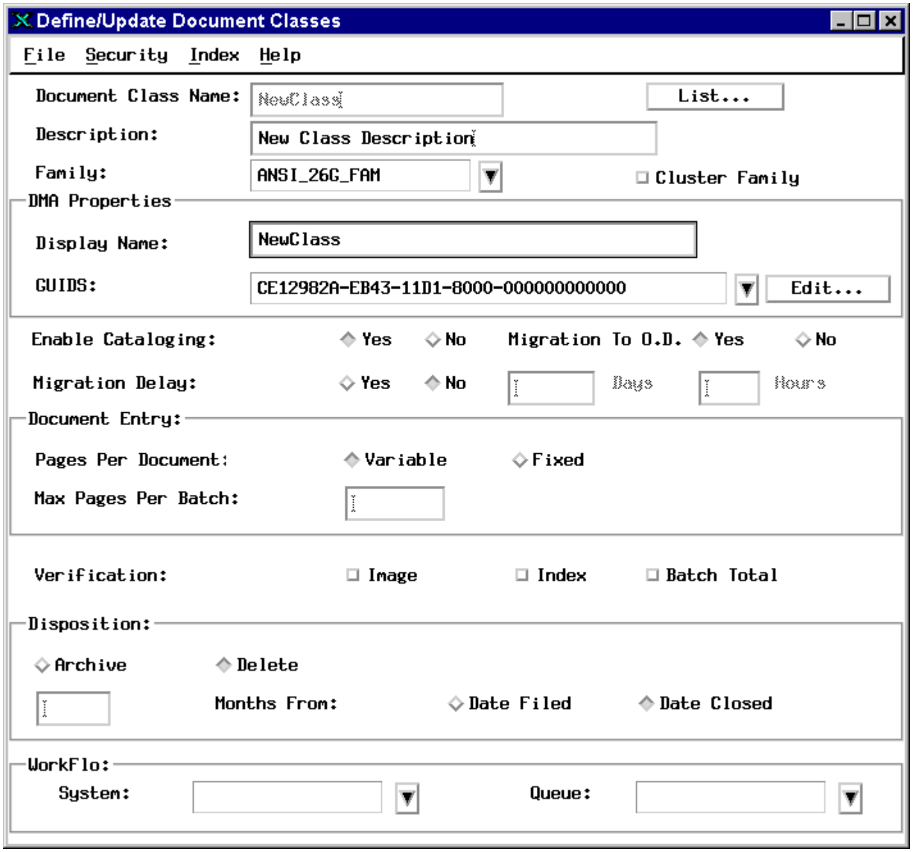
Note In a FileNet P8 Content Federation Services environment, a document class may or may not have index values associated with it.

Define only as many document classes as you need. You **cannot delete** a document class once you define it.

Regardless of whether you are adding or modifying a document class, the change takes about five minutes to be effective at the workstations.

CAUTION Do not modify a document class if any uncommitted batches exist that use that document class. These batches **cannot be committed** if the document class changes.

1 Choose Define/Update Class from the Classes menu to display the following window.



Document Class Name: NewClass

Description: New Class Description

Family: ANSI_26G_FAM ▼ □ Cluster Family

DMA Properties

Display Name: NewClass

GUIDS: CE12982A-EB43-11D1-8000-000000000000 ▼

Enable Cataloging: ◆ Yes ◇ No Migration To O.D. ◆ Yes ◇ No

Migration Delay: ◇ Yes ◆ No Days Hours

Document Entry:

Pages Per Document: ◆ Variable ◇ Fixed

Max Pages Per Batch:

Verification: □ Image □ Index □ Batch Total

Disposition:

◇ Archive ◆ Delete

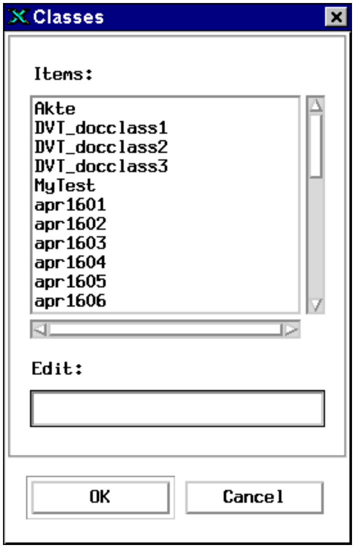
Months From: ◇ Date Filed ◆ Date Closed

WorkFlo:

System: ▼ Queue: ▼

2 Define document class.

a Click the List button to display a dialog box listing document class names you can modify.



Akte
DVT_docclass1
DVT_docclass2
DVT_docclass3
MyTest
apr1601
apr1602
apr1603
apr1604
apr1605
apr1606

- To modify an existing document class, choose the name of the document class you want to modify and click OK.
- To create a new document class, type the new name in the Edit field at the bottom of this list and click OK.

Note In a FileNet P8 Content Federation Services environment, select a name such as CFS_apps or P8_acct, that will be easy to identify when you map it to the Content Engine document class.

b Enter a description.

You can enter up to 30 characters (of any type or case) that describe the purpose of this document class. The description appears on the document class report and is required. If you chose an existing document class to modify, the system automatically enters the description. You can change the description or leave it as is.

c Select the media family name.

If you chose an existing document class to modify, the system automatically enters the media family name. Use the pull-down list to select a primary media family name. If documents in this class will not be stored on storage media, you must still enter a media family name.

Important When you make any configuration change to Image Services through the Application Executive (Xapex) such as reassigning a media family or adding an index, **you must restart** any associated client server that runs IS Toolkit-based applications. This includes CFS-IS servers in a FileNet P8 Content Federation Services environment. For example, If you assign a mapped IS Doc Class to a different media family in a FileNet P8 Content Federation Services environment in New York, you must restart the associated Content Engine server in Chicago. Otherwise, the Chicago server will not recognize the change and may commit documents to the wrong media.

d If you store documents in clusters, check the Cluster box.

You must also enter the currently defined cluster index in your index list (see **“Assign a Cluster to a Document Class” on page 142**). Talk with your support representative before choosing this option. This setting is ignored if your system is configured to use fast batch committal. For more information on fast batch committal, see the *Image Services System Administrator's Handbook*. To download this handbook from the IBM support page, see **"Accessing IBM FileNet documentation" on page 17**.

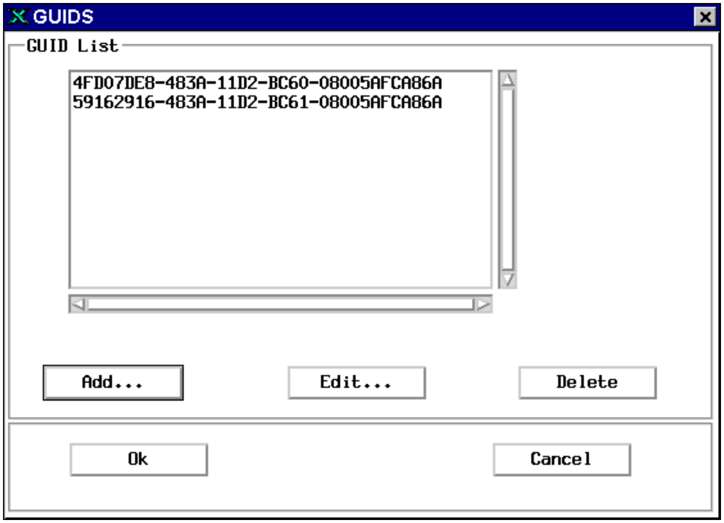
3 Define DMA properties. The DMA Properties enable you to specify a DMA display name and up to 10 GUIDs (Globally Unique IDentifiers) for each defined document class.

a Specify the Display Name. When you first enter a name in the Document Class Name field, the system automatically duplicates that name in the DMA Properties Display Name field. You can change this name by selecting all or part of the text and typing the desired name.

This field accepts up to 30 alphanumeric characters, including special characters. The following display name restrictions apply:

- space, tab, colon (:) and equal sign (=) are not allowed.
- cannot start with a single or double quotation mark.
- cannot end with a backslash (\) character.

b Click the Edit button to open the GUIDS dialog box, which enables you to add, delete, or modify GUIDs for the currently defined document class. You must assign at least one GUID to the document class and may assign up to 10 GUIDs for each document class.



4FD07DE8-483A-11D2-BC60-08005AFCA86A
59162916-483A-11D2-BC61-08005AFCA86A

c Select the GUID you want associated with the document class. For details on adding, editing, and deleting GUIDs, see **“GUIDs Assigned to Document Class” on page 169**.

d Click Ok. The selected GUID displays in the GUIDS field on the Define/Update Document Classes window. Each additional GUID defined on the GUID list may be an alias for the document class.

4 Click the Yes radio button to enable cataloging (the default).

To disable cataloging for a document class, click the No button. To re-enable cataloging, click the Yes button. The system keeps track of when you turn cataloging on and off via a table in the index database.

CAUTION If you turn off cataloging and commit documents to the document class, the index information will not be in the index database, but the address information will still be in the permanent database, causing a discrepancy between the databases. Import the documents from the media to get the index database information (see “Importing Documents” in the *Image Services System Administrator’s Handbook*). T

5 Specify migration options.

a Select a migration option (click Yes or No).

Select Yes to migrate your documents to storage media. This setting is ignored if your system does not use storage media or if you are doing a fast batch committal. For more information on fast batch committal, see the *Image Services System Administrator’s Handbook*. To download this handbook from the IBM support page, see **“Accessing IBM FileNet documentation” on page 17**.

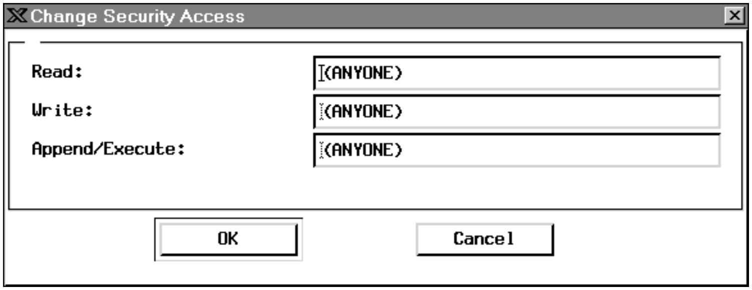
Note If you have a cache-only, multi-server system and you have configured phantom storage libraries, set “Migration to O.D.” to No.

b Set migration delay.

Click Yes to delay migration, then set the number of days and hours until migration starts. At the end of this time, documents migrate to storage media and the space they occupy in page cache can be reused. The maximum delay you can set is 24,855 days and 3 hours.

6 Set security options.

Select Change Access from the Security menu to display this dialog.



Read: (ANYONE)
Write: (ANYONE)
Append/Execute: (ANYONE)

- To restrict any of these functions (read, write, or append/execute) to one user or group, replace the name (ANYONE) with the name of the user or group that should have each kind of access.
- To change access back to anyone, you must type **(ANYONE)**, including the parentheses and using uppercase letters.

7 Set document entry parameters.

a Set pages per document.

- If the number of pages usually varies, leave the Variable button selected.
- If documents in this class usually have the same number of pages, click the Fixed button. A text field appears where you enter the number of pages (up to three digits). This number serves as a default for the operator who defines the batch, but the operator can change the default as required for any one batch.

b Enter maximum pages per batch.

Click in the text field and type the maximum number of pages you expect to scan in one batch.

8 Set verification options.

Click the Image, Index, and Batch Total checkboxes as required. You can select any combination, as long as you use indexes with the appropriate definition.

Verification Options	Description
Image	Check this box to require the operator to verify the scanned image on screen as an extra step between the scanning and indexing steps. Even if you do not select this option, operators can verify images for any batch at any time.
Index	Check this box to set up a verification pass as a default step to be performed for documents in a class. PC workstation operators can verify indexes at any time.
Batch Total	Check this box and the system adds up the values of a numeric index. After the batch is completely indexed, the total for that numeric index should match a predefined batch total entered during the define batch session. Batch total verification also verifies the number of pages and documents expected in the batch. You can enable batch totals as a default, or as an optional step for any particular batch, only if the document class includes a numeric index enabled for batch totals. Document entry operators can perform batch total verification only if you set up the document class to use it.

9 Set disposition parameters.

In this section of the dialog, you indicate how you want to eventually dispose of the information stored in the index database for documents in this class. You also indicate how long to wait before flagging the information and when to start counting the time.

Disposition Parameter	Description
Archive	Choose Archive to move the information to an archive database on storage media. You can then query the archive database and still access documents, even though the index information is no longer in the index database on magnetic disk.
Delete	Choose Delete to remove the information from the index database permanently and never access the documents on storage media again. If you use erasable storage media and plan to reuse the media, you would most likely choose this option.
Months From	In this text field, indicate how many months you want to keep the index information available in the index database. The actual time index information remains in the index database depends on when you start counting the time (committal date or closing date) and when you run the processes that actually archive or delete the information.
Date Filed	Choose Date Filed to start counting time on the day the system writes the document information to the index database.
Date Closed	Choose Date Closed to start counting time when an operator closes the document.

10 Route data about scanned documents to a Visual Workflo queue (optional).

Parameter	Description
System	Click the arrow to the right of the System field and select the name of a workspace from the pulldown list.
Queue	Click the arrow to the right of the Queue field and select the name of a queue from the pulldown list.

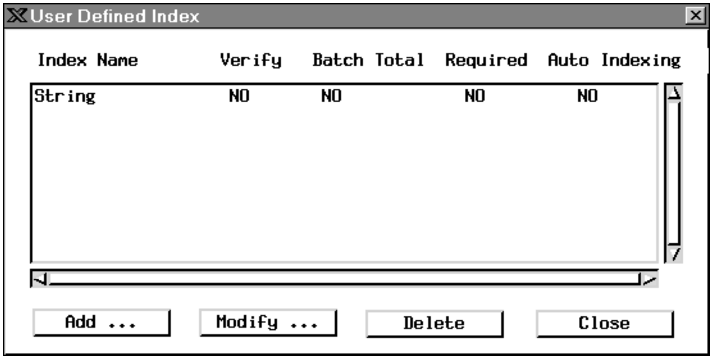
To delete information about scanned documents from a Visual Workflo queue:

- To remove all the queues in a system, double-click on a system name in the list (not in the System field, as this has no effect).
- To remove only one queue in a system, double-click on a queue in the list (not in the Queue field, as this has no effect).

11 Specify the indexes.

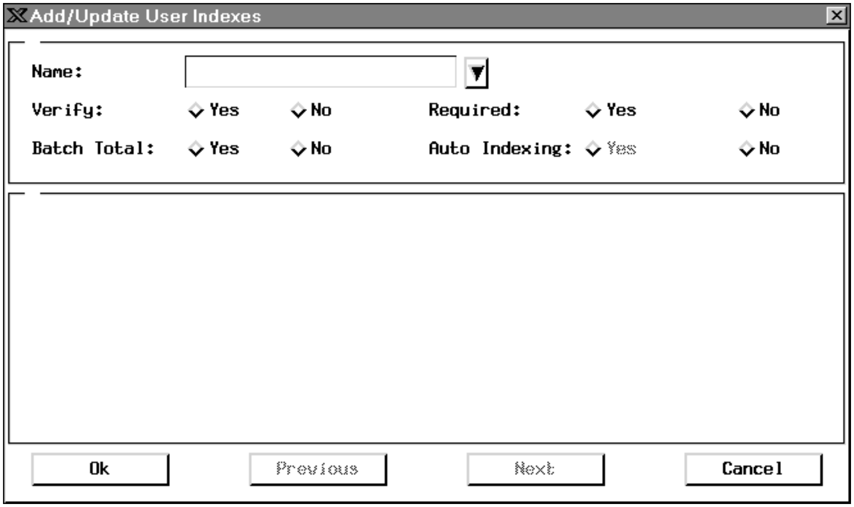
Note In a FileNet P8 Content Federation Services environment, a document class may or may not have index values associated with it.

To assign indexes to the document class, choose Edit from the Index menu. The following dialog displays.



Index Name	Verify	Batch Total	Required	Auto Indexing
String	NO	NO	NO	NO

a Click the Add button to specify the indexes that belong to this document class. The following dialog displays.



Name:

Verify: ◇ Yes ◇ No   Required: ◇ Yes ◇ No

Batch Total: ◇ Yes ◇ No   Auto Indexing: ◇ Yes ◇ No

b Click the arrow to the right of the Name field to display a list of indexes. Click a name to select it.

c Select the document entry options for the index.

Document Entry Option	Description
Verify	Click the Yes button to default to index verification for this index. When indexing accuracy is important, you can require a second entry operator to verify index values. Verification consists of indexing the batch a second time and comparing the results.
Batch Total	For numeric indexes only, click the Yes button to collect totals. The system also keeps track of the number of pages and documents scanned. You must select this option as a default for the class before document entry operators can select it when defining the batch. If the expected totals entered during batch definition do not match the totals calculated by the system during document entry, the entry operator can resolve the inconsistency before committing the batch.
Required	Click the Yes button to require an entry for this index. If the indexing operator can leave the field blank, leave the default of No selected.
Auto Indexing	For string indexes only. The client program used for scanning determines the setting for this value: • WorkFlo/Scan is your scan client. Click Yes if you have some means of acquiring index data automatically (bar codes, patch codes, and so on). WorkFlo/Scan can perform automatic indexing only if you specify Yes in this Auto Indexing field on the Image Services server. • Capture Professional is your scan client. Click No. The Capture settings collection contains the automatic indexing configuration. Capture ignores the Auto Indexing setting on the Image Services server.

d When you are satisfied with the specifications for an index, click the OK button at the bottom of the dialog box. The information is transferred to the User Defined Index dialog box (though it may be hidden behind the currently displayed dialog box).

e To define another index, select another name. To finish selecting indexes for the document class, click the Cancel button.

f Click Close on the User Defined Index dialog box.

12 Save the document class.

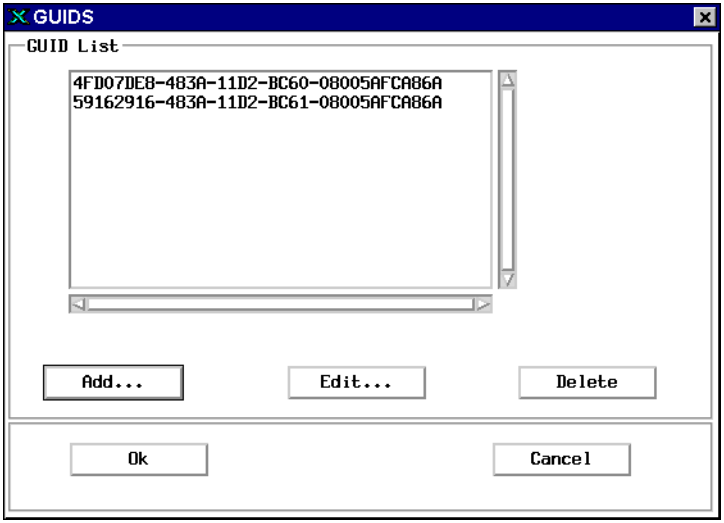
Select Save from the Define/Update Document Classes window's File menu. A message box appears, telling you when the document class is successfully created. You must acknowledge the message by clicking the OK button.

GUIDs Assigned to Document Class

GUIDs (Globally Unique IDentifiers) are DMA-compliant, 16-byte integers used to uniquely identify each element transported over a network. The system ensures unique GUID assignments by automatically generating this integer using an algorithm based on the system's network card MAC address and a format that complies with the specifications provided for the system's platform.

Each GUID must have a unique name that conforms to the format specified for your Image Services system platform. For platform specifications, see the GUID naming conventions described in the documentation that came with your operating system.

To add, delete, or rename GUIDs for the current document class, click the Edit button in the DMA Properties box of the Define/Update Document Classes window. The GUIDs dialog box opens, displaying a list of currently defined GUIDs.



4FD07DE8-483A-11D2-BC60-08005AFCA86A
59162916-483A-11D2-BC61-08005AFCA86A

As you add or rename GUIDs, the system validates the assigned name, making sure it meets the following requirements:

- Unique name assignment
- No duplication of name in the Image Services database
- At least one and no more than 10 GUIDs assigned to each document class

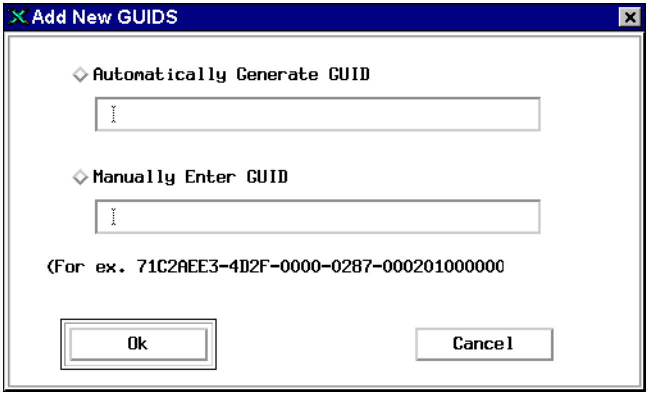
You may modify the currently defined list as follows:

- To delete an existing GUID, select it from the list and click the Delete button. A message box opens, asking you to verify deletion. Click Yes to delete the selected GUID or No to cancel deletion.

- To add a new GUID to this user index, click the Add button. The Add New GUIDS dialog box opens. For details, see **"Add New GUIDs" on page 171**.
- To rename an existing GUID, select it from the list and click the Edit button. The Edit GUID dialog box opens, displaying the exiting name of the selected GUID. For details, see **"Rename GUID" on page 172**.

Add New GUIDs

The Add New GUIDS dialog box opens after you click the Add button on the GUIDS dialog box when defining the DMA properties of a document class.



(For ex. 71C2AEE3-4D2F-0000-0287-000201000000

Automatically Generate GUID

Click this radio button to have the system automatically generate a GUID. The system displays the GUID in grayed-out, uneditable text.

To save the automatically generated GUID, click the Ok button. The system closes the Add New GUIDS dialog box and displays the newly assigned GUID in the GUIDS list.

Manually Enter GUID

Click this radio button if you want to manually assign a GUID. Type a 16-byte character set into the field, using the format shown in the sample displayed below the entry field.

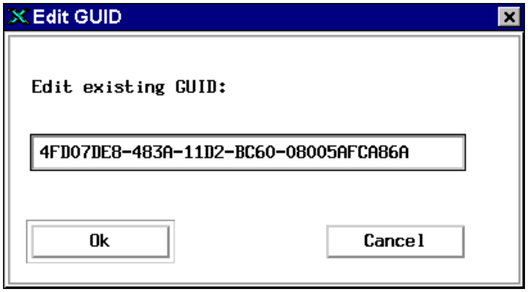
To save the manually defined GUID, click the Ok button.

- If you entered a GUID that already exists in the Image Services database or does not use the correct format, a message box opens, alerting you to the problem. When this happens, you must enter an acceptable GUID and click Ok again.

- If you entered a unique GUID using the correct format, the system closes the Add New GUIDS dialog box and displays the newly defined GUID on the GUIDS list.

Rename GUID

The Edit GUID dialog box opens after you select an existing GUID from the GUIDS list and click the Edit button on the GUIDS dialog box when defining the DMA properties of a document class.



Edit existing GUID: 4FD07DE8-483A-11D2-BC60-08005AFCA86A

Edit existing GUID

This field displays the currently selected GUID and allows you to rename it.

To change the current name, select all or any part of the displayed text, type in the desired text, and click Ok.

- If you entered a GUID that already exists in the Image Services database or does not use the correct format, a message box opens, alerting you to the problem. When this happens, you must enter an acceptable GUID and click Ok again.
- If you entered a unique GUID using the correct format, the system closes the Edit GUID dialog box and displays the renamed GUID on the GUIDS list.

Modify a Document Class

You can modify a document class. Most changes are straightforward. You simply enter different information in the same manner as creating a new document class.

CAUTION It is highly recommended that the Define/Update option provided for the Document Classes be executed during non-production hours. This tool will issue locks on the relational database that may cause long delays in system processing. This primarily affects systems with very large databases but is the recommended procedure for all systems.

The Report function under the Classes menu provides a method to list these definitions and should be used in place of the Define/Update option whenever possible.

CAUTION Any modifications made to the Index fields, Document Classes and Disk Families will not take effect until the Image Services software is recycled.

Be aware of how changing a document class affects your system. You might need to complete several steps, including updating custom indexing forms on PC workstations if you add or delete an index. If you do not complete these steps, indexing cannot function correctly.

If you add an index to a document class, you can only use the index to retrieve documents committed after the addition. If you delete an index from a document class, you cannot retrieve any documents based on that index. You should plan carefully and test your document classes thoroughly.

CAUTION Be sure that **no uncommitted batches** use the document class you are modifying. Otherwise, operators must **repeat the work** for the batch to commit successfully.

Change Indexes

To change an index:

1. Choose Define/Update Document Class from the Database Maintenance Classes menu.
2. Select the document class from the List menu.
3. Choose Edit from the Index menu.
   - To modify an index, select it from the User Defined Index list and click Modify. In the resulting dialog box, change items by clicking the Yes or No button. If changing autoindexing information, you can directly alter the text in the grid.

- To delete an index, select the index and click the Delete button. You must rebuild the custom indexing forms used at PC workstations if you delete an index.

- To add an index, click the Add button and define the index using the procedures described under **“Define an Index” on page 119**. You must rebuild the indexing forms if you add an index.

4 Click the OK button.

5 When you finish modifying all indexes, click Close to return to the User Defined Index dialog box.

Change Security

To change security for a document class:

1 Select Change Access from the Security menu.

2 Enter the new names of groups you want to authorize to read, write, or perform other operations on documents in this class.

When you change security for the document class, **only new documents** scanned into the class acquire these settings. To change all documents previously scanned into the class, see the *Image Services System Administrator’s Handbook*. To download this handbook from the IBM support page, see **“Accessing IBM FileNet documentation” on page 17**.

Save Changes

Select Save from the File menu to save any changes.

Update an Indexing Form

If you change the indexes associated with a document class, you must also update the indexing forms in AutoForm on the PC for any custom indexing forms used by PC workstation users. For the PC only, the **default** indexing form is automatically updated by any changes.

Delete Expired Documents and Folders

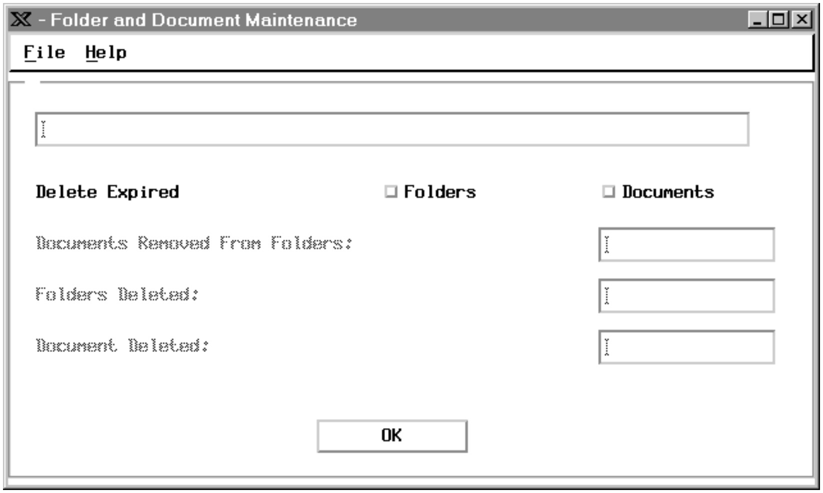
You must be logged on as SysAdmin or as a user with full administrative rights (Admin Group, Session Group, Primary Group and Member of Group are all set to SysAdminG) to delete documents or folders.

CAUTION Before you use this process, be absolutely sure you will never want to access the documents again.

Note You will not be allowed to delete documents or folders on or before the deletion date assigned to them. You can only delete documents or folders **after** their assigned deletion date.

To delete documents or folders:

1. Select Delete Doc/Folder from the Miscellaneous menu to display the Folder and Document Maintenance window.



2 Click Folders, Documents, or both, then click OK.

During the deletion, you can see progress messages in the large field at the top of the window. The three small fields show the number of documents removed from folders and how many folders and documents were deleted.

3 To terminate the deletion, choose Exit from the File menu.

The system deletes all documents and folders eligible for deletion. The next time you delete expired documents and folders, the system deletes any additional documents or folders that are now obsolete, as well as those it missed when you terminated the process.

Note You will not be allowed to delete documents or folders on or before the deletion date assigned to them. You can only delete documents or folders **after** their assigned deletion date.

Get Database Reports

The Indexes, Classes, and Families menus each include a Report option. Select the report for the kind of information you are interested in: user indexes, document classes, or media families.

Save Reports to a File

To save all or part of the report information in a file, you must first select one or more entries. Either double-click the items you want to include or use the Edit menu's Select All option to select all entries at once. After selecting the appropriate entries, choose Save As from the File menu and follow your operating system's procedure for saving files.

Find an Index, Document Class, or Media Family

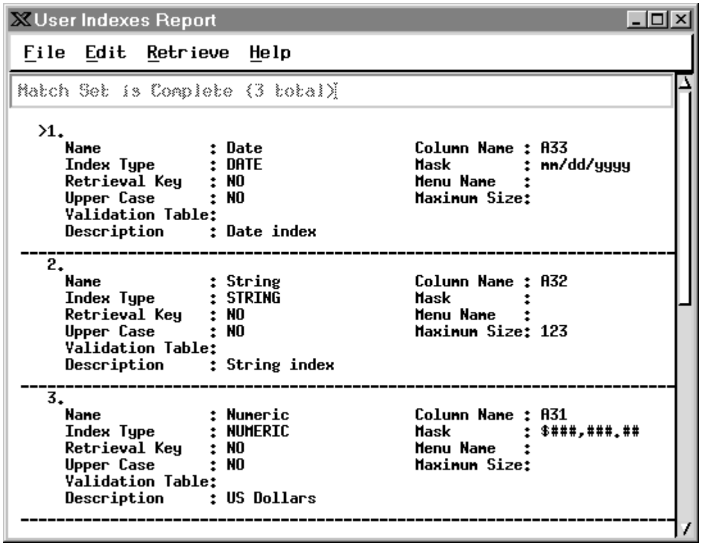
If a large number of indexes, document classes, or media families exist in a report, you can use the report window’s Retrieve menu to go to a particular name or number.

Select **Go to Name** to display a text popup where you can enter the name of the index, document class, or media family. That item then appears at the top of the report window. If the names of two or more items start with the same characters, you must type enough characters to distinguish between the names (the names are case sensitive).

Select **Go to Number** to find the index, document class, or media family by the number in the upper left corner of each row in the report. Indexes, document classes, and media families are numbered in the order they were created.

User Indexes Report

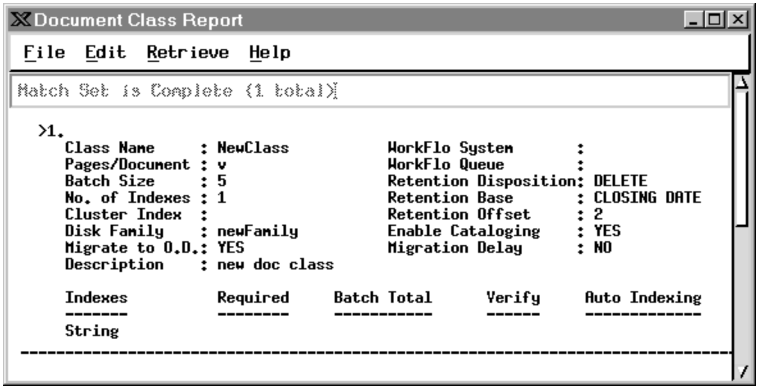
The User Indexes Report shows parameters for each index. The information varies based on the type of index. The display shows as many indexes as fit in the dialog box. Click in the gray area of the scroll bar to scroll to the next page of indexes.



```
Match Set is Complete (3 total)

 >1.
    Name            : Date                 Column Name : A33
    Index Type      : DATE                 Mask        : mm/dd/yyyy
    Retrieval Key   : NO                   Menu Name   :
    Upper Case      : NO                   Maximum Size:
    Validation Table:
    Description     : Date index
--------------------------------------------------------------------------
  2.
    Name            : String               Column Name : A32
    Index Type      : STRING               Mask        :
    Retrieval Key   : NO                   Menu Name   :
    Upper Case      : NO                   Maximum Size: 123
    Validation Table:
    Description     : String index
--------------------------------------------------------------------------
  3.
    Name            : Numeric              Column Name : A31
    Index Type      : NUMERIC              Mask        : $###,###.##
    Retrieval Key   : NO                   Menu Name   :
    Upper Case      : NO                   Maximum Size:
    Validation Table:
    Description     : US Dollars
--------------------------------------------------------------------------
```

Document Class Report

The Document Class Report lists all document classes on the system, one at a time. The amount of information shown depends on the size of the window.

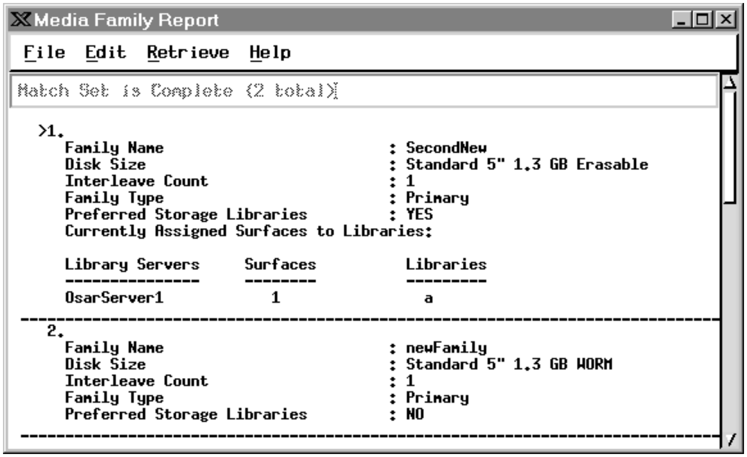


```
Match Set is Complete (1 total)

  >1.
     Class Name     : NewClass          WorkFlo System      :
     Pages/Document : v                 WorkFlo Queue       :
     Batch Size     : 5                 Retention Disposition: DELETE
     No. of Indexes : 1                 Retention Base      : CLOSING DATE
     Cluster Index  :                   Retention Offset    : 2
     Disk Family    : newFamily         Enable Cataloging   : YES
     Migrate to O.D.: YES               Migration Delay     : NO
     Description    : new doc class

     Indexes          Required     Batch Total      Verify     Auto Indexing
     -------          --------     -----------      ------     -------------
     String
-------------------------------------------------------------------------------
```

Use the scroll bar at the right of the window to view all the indexes (scroll up or down).

Media Family Report

The Media Family Report displays the names of all media families on the system and shows how the disks are configured.



```
Match Set is Complete (2 total)

 >1.
    Family Name                           : SecondNew
    Disk Size                             : Standard 5" 1.3 GB Erasable
    Interleave Count                      : 1
    Family Type                           : Primary
    Preferred Storage Libraries           : YES
    Currently Assigned Surfaces to Libraries:

    Library Servers     Surfaces          Libraries
    ---------------     --------          ---------
    OsarServer1            1                 a
--------------------------------------------------------------------------------
  2.
    Family Name                           : newFamily
    Disk Size                             : Standard 5" 1.3 GB WORM
    Interleave Count                      : 1
    Family Type                           : Primary
    Preferred Storage Libraries           : NO
--------------------------------------------------------------------------------
```

Use the scroll bar at the right of the window to view all the media families (scroll up or down).

4

CFS Connector - IS Catalog Export Tool

FileNet P8 Content Federation Services combines the capabilities of Image Services (IS) systems and Content Engine (CE) systems, allowing content stored on the Image Services system to be cataloged and viewed on a Content Engine System.

You can configure the Catalog Export tool so that the index properties of newly captured IS documents, images, or content are automatically exported to the CE system.

For existing IS documents, images, or content, you can configure the Catalog Export tool to export both index properties and annotations to the CE system. If index properties have already been exported, you have the option of exporting only the annotations.

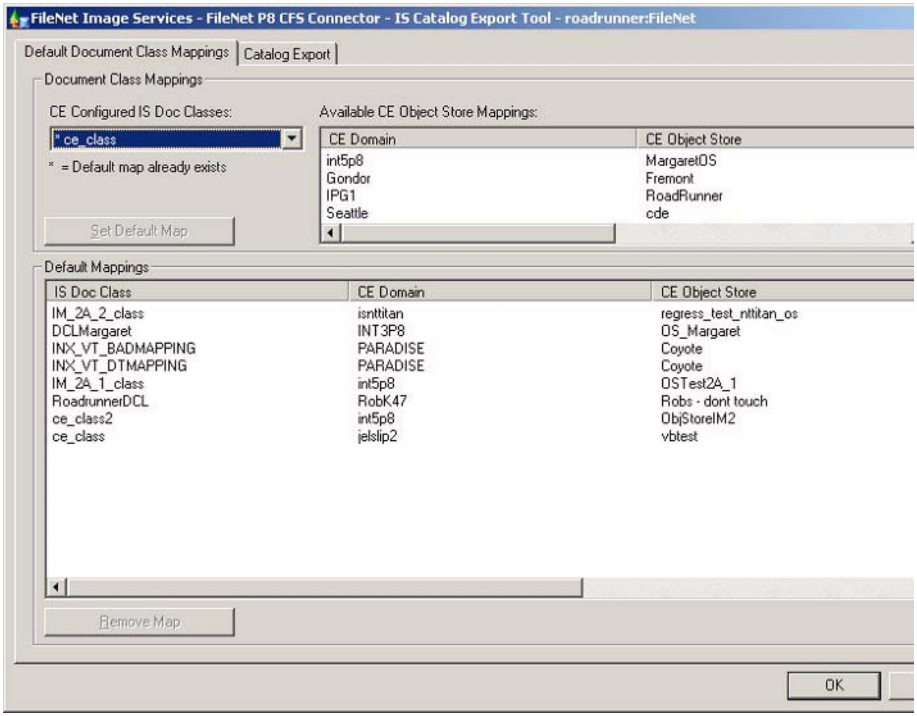
Catalog Export for Newly Captured IS Documents

The index properties for newly captured IS documents can automatically be exported to the CE system.

Configure a Document Class for Export

1 On the main **Remote Admin Console** screen, select **IS Catalog Export Tool** from the Applications pull-down menu.

The **IS Catalog Export Tool** screen displays.



FileNet Image Services - FileNet P8 CFS Connector - IS Catalog Export Tool - roadrunner:FileNet

CE Configured IS Doc Classes: * ce_class

* = Default map already exists

Available CE Object Store Mappings:

CE Domain	CE Object Store
int5p8	MargaretOS
Gondor	Fremont
IPG1	RoadRunner
Seattle	cde

Default Mappings

IS Doc Class	CE Domain	CE Object Store
IM_2A_2_class	isnttitan	regress_test_nttitan_os
DCLMargaret	INT3P8	OS_Margaret
INX_VT_BADMAPPING	PARADISE	Coyote
INX_VT_DTMAPPING	PARADISE	Coyote
IM_2A_1_class	int5p8	OSTest2A_1
RoadrunnerDCL	RobK47	Robs - dont touch
ce_class2	int5p8	ObjStoreIM2
ce_class	jelslip2	vbtest

2 From the **CE Configured IS Doc Classes** pull-down menu, select the IS document class whose index properties you want to export to the Content Engine system.

3 From the **Available CE Object Store Mappings** pane, select the CE domain and object store you want to export to.

The **Default Mappings** between IS document classes and CE domains and object stores appear in the lower pane.

4 Click **OK**. Future IS documents that are committed to the document class you've just selected will automatically have their index properties exported to the CE system.

Catalog Export for Existing Documents and Annotations

Configure a Document Class for Export

1 On the main Remote Admin Console screen, select **IS Catalog Export Tool** from the Applications pull-down menu.

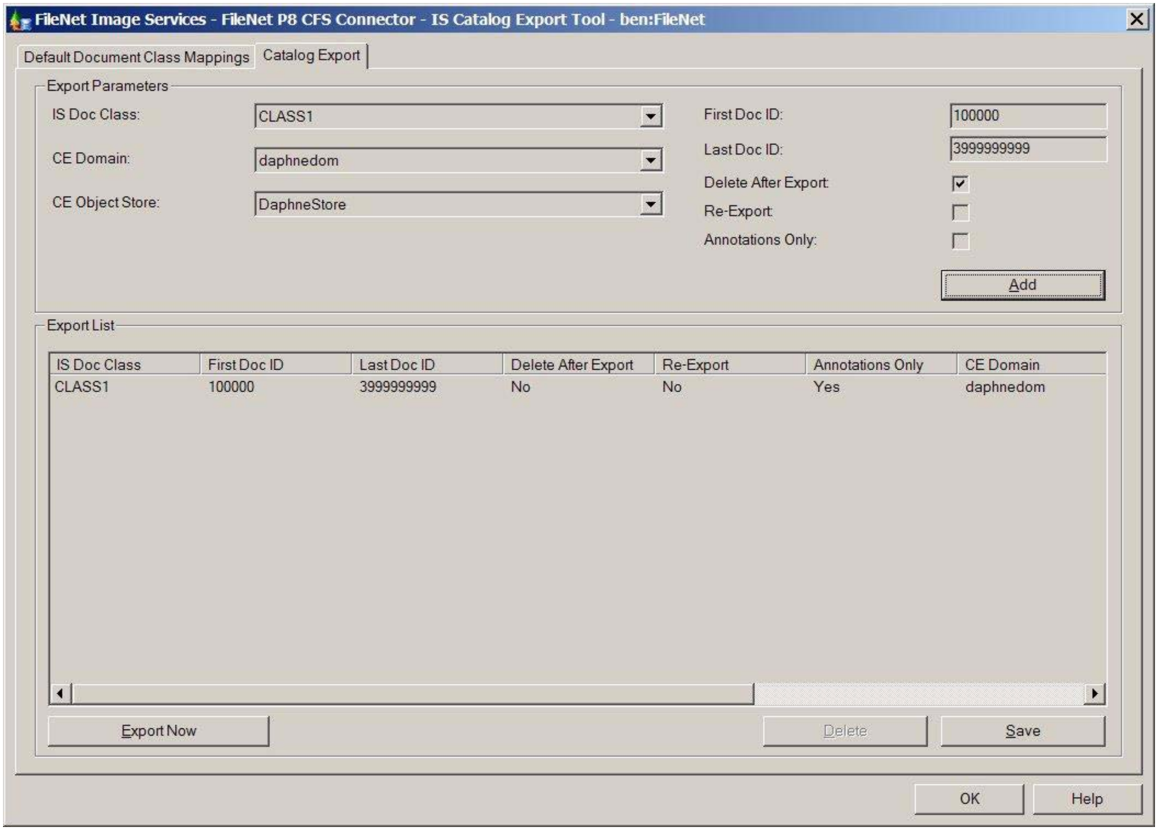
The IS Catalog Export Tool screen displays.

2 On the **Catalog Export** tab, select from the **IS Doc Class** pull-down list for the document class whose index data and annotations you want to export.

3 Select the CE domain and object store you want to export the index data to.

4 Specify values for the fields and check boxes:

- The **FirstDocID** and **LastDocID** are the minimum and maximum document ID numbers. You can accept these default values to export data for the entire IS document class, or you can specify a smaller group of document IDs within this range.


FileNet Image Services - FileNet P8 CFS Connector - IS Catalog Export Tool - ben:FileNet
Default Document Class Mappings
Catalog Export
Export Parameters
Add
Export List
Export Now
Delete
Save
OK
Help

IS Doc Class: CLASS1

CE Domain: daphnedom

CE Object Store: DaphneStore

First Doc ID: 100000

Last Doc ID: 3999999999

Delete After Export: ☑

Re-Export: □

Annotations Only: □

IS Doc Class	First Doc ID	Last Doc ID	Delete After Export	Re-Export	Annotations Only	CE Domain
CLASS1	100000	3999999999	No	No	Yes	daphnedom

- **Delete After Export**: Check this box to remove index data from the index database on the IS server after it has been exported to the CE server.

CAUTION **DO NOT** check this box for documents stored on EMC Centera, NetApp Snaplock, IBM DR550, and so on. These NLS-based devices require entries in the Image Services index database.

The documents associated with the deleted index data will no longer be retrievable by Image Services. Although a locator record still exists in the permanent database, the index information is permanently deleted from the index database.

- **Re-export**: Check this box to export index data that has already been exported, for instance, to a development system.
- **Annotations Only**: Check this box if you want to export only the annotations associated with documents in this class. This option is useful if you've already exported the document properties to CE in an earlier release.

5 Click the **Add** button, the parameters you've just selected display in the Export List pane.

6 To remove a row from the Export List, select the row and click **Delete**.

7 Click **Export Now** to export the index information and annotations immediately. Clicking this button launches the catalog export process on the IS server and a status box displays to indicate that the process was either successfully started or encountered an error.

Note When you export index data, the content always remains in the IS system. All associated annotations are automatically copied to the CE system in their entirety, so the annotations always reside on both systems too.

The only things you can optionally delete from the Image Services system are the index values from the index database.

8 Click **Save** to write the configuration list to the export file on the IS Index server without exporting.

9 Click **OK** to export the index/catalog data to the Content Engine server. If you click the OK button without having clicked the Save button mentioned above, you may be prompted to save, exit without saving, or Cancel.

Export Log

The parameters you specify in the Export List are stored in the Export Log on the Image Services server.

The IS import agents on the Content Engine server monitor the Export Log for catalog information to import.

5

Database Server Connect

Database Server Connect is a utility that you can run through the Application Executive (Xapex) program. It is designed to manage the security issues pertaining to the four required database users (authentication).

These are the four types of relational database users:

- **f_sw:** The Image Services Database and eProcess Primary user.
- **f_maint:** Mainly used by GDB_exim, a generic database export/ import utility. It can also be used by your service representative to gain access to the system's relational database for troubleshooting and investigation.
- **f_sqi:** This legacy user is used by the SQI subsystem of IS Toolkit. If a site has IS Toolkit or IS Process Analyzer installed, the f_sqi user can be used to access some of the features of these products.
- **f_open:** The default database logon user used by the SQI subsystem of IS Toolkit. It is the per user database logon default user.

Overview

It is an industry standard that operating system passwords must change periodically. Changing passwords is just one component of a site’s security policy. Connecting to a relational database requires an operating system account on that server. Supporting a security policy requires the password associated with this operating system account to be periodically changed. The Database Server Connect application is designed to manage this for the relational database user passwords that are set during the initial configuration at the time of installation on the Root/Index and Application server(s).

Image Services integration with the relational database requires the IS system to maintain the connection accounts (operating system accounts) and the associated passwords. These are used to enable IS to connect with the relational database. If the operating system password must change, both the operating system password and the IS maintained password for the specific account must change at the exact same time.

CAUTION Changing one password before the other will result in failed connections between IS and the relational database during the time interval when the passwords are different. In most IS installations, any time interval where this occurs is unacceptable.

To address this, the IS system maintains two passwords for each account, the Primary password and the Secondary password. During typical operation, you will use the Primary password for each account when connecting to the relational database. You use the Secondary password maintained by Image Services only when a connection with the account Primary password fails. In this case, you should try connecting to the relational database with the Secondary password. If the attempt succeeds, this Secondary password replaces the old Primary password and all future database connections use this new Primary password.

With this mechanism, changes in the operating system password will not result in failed connections. To accomplish this, set the IS maintained Secondary password to the new operating system password before any operating system password changes are made. After the Secondary password on the IS system is updated, the operating system password may be changed. The IS system will first attempt to use the old Primary password. This will fail because the operating system password has been changed. Automatically, the IS system will attempt connecting to the relational database using the Secondary password. This will succeed with the Primary password on the IS system being updated with the Secondary password value. It is best that you set a new value for the Secondary password by checking with the Database Administrator for the next Remote database server password and then using the New Password window. See **"Changing the Primary and/or Secondary Password" on page 194**.

Note The relational database passwords (f_sw, f_maint, f_sqi, f_open) must be set up on the Root/Index server, each Application server and the Remote Database server before the software is installed. In addition, when you change or otherwise manage the passwords, the XDB Connect application in Xapex also needs to be run on each IS server, Root/Index server and Application server because the passwords on each of these servers are independent.

Note You must be logged on with System Administrator level privileges in order to use the XDB Server Connect program and change the relational database user passwords.

Database Connect Administration

The Database Connect Administration window allows you to easily change passwords for the f_sw, f_maint, f_sqi and f_open users and keep track of the status of the Primary password with Activation and Expiration date information on each server where the relational database client is installed.

This window contains four tabs, each one corresponding to one of the database users. Each tab has a Primary area and in the case of DB2, a Secondary area.

Primary Area

- **Password:** field and **Change** button. The Primary password always has an assigned value. For instructions on changing the password, see **“Changing the Primary and/or Secondary Password” on page 194**.
- **Activation Date:** Displays the date the Primary password was most recently changed.
- **Expiration Date:** Displays how many days from the current date until the Primary password expires. This field is set to a system default of 60 days.

It is a good idea to periodically check the **Expiration Date** field as part of your password maintenance routine to know when it is time to change these passwords.   For more information on password maintenance, refer to **“Password Maintenance” on page 196**.

Note You will get a reminder message to change your f_sw Primary password. See **"Expiration Notification" on page 194** for more information.

Secondary Area (DB2 Only)

When the Primary password expires and a new connection is attempted, the Secondary password automatically becomes the Primary password, if it is the same as the current password set on the Remote database server. The **Activation Date** field is automatically changed to the current date and there is no value in the **Secondary password** field.

- **Password:** field and **Change** button. If there are asterisks displayed in the field, there is a Secondary password assigned. If the field is blank, there is no password and one should be assigned as soon as possible.

This Secondary password enables you to logon to the system after the Primary password has expired or if the Remote database server password has been changed. If the Secondary password is not assigned and the Primary password expires, you will not be able to log in as that user and the Image Services software may not come up. See **"Password Failure Emergency Procedures" on page 196**.

Note It is key to have the Secondary password set to what will be the next Remote database server password.

Changing the Primary and/or Secondary Password

Regardless of the user, the Primary Password is the current password. For DB2 only, the Secondary Password is the password that will take affect if the Primary Password is allowed to expire.

Change the password(s) by completing the following Steps:

1. From the main Xapex screen, select the **XDB Connect** option from the **Applications** pulldown menu.
2. Select the tab for the user whose password you want to change.
3. Click the **Change** button for either the Primary or Secondary password to display the **New Password** dialog box.
4. In the **New Password** dialog box, enter a new password in the **New Password:** field. This password can be a string of any alpha-numeric characters up to a maximum of 8 characters.
5. In the **Confirm Password:** field, enter the same password that you entered in the previous step.
6. Click **OK**.
7. If you changed the Primary password, verify that the **Activation Date** has been changed to today’s date.

Expiration Notification

All Primary passwords have expiration dates, but you will only be reminded before the f_sw password expires. FileNet Application Executive (Xapex) automatically notifies the System Administrator a certain number of days before the f_sw user’s Primary password expires. The default value is 14 days. The System Administrator will see a pop-up message stating “Your database ‘f_sw’ Account Password will expire in # days”. This notification pop-up will appear each time a new logon to Xapex is made if it is within the value set in fn_edit.

In fn_edit, two values are set for all four database users (f_sw, f_maint, f_sqi and f_open) at the time Image Services is installed: **Password Expiration Policy** and **Notify Administrator**.

The **Password Expiration Policy** is a reminder for the users on the IS system that the password on the Remote database server is going to change soon. This value is set to a default of 60 days, but should be consistent with the site’s IT policy as it relates to the Remote database server. **Notify Administrator** indicates when to start signaling the System Administrator at each logon sometime toward the end of the Password Expiration Policy. This value is set to a default of 14 days (mentioned above). Both of these values can be changed on the Root Index server in fn_edit on the appropriate tab of the **Relational Databases** tab. If you run the same instance of Xapex indefinitely without logging off and logging back on, you may never receive an expiration notification and the f_sw password will expire. If this occurs and there is no set Secondary Password, refer to the **“Password Failure Emergency Procedures” on page 196**. For more information on password maintenance, refer to **“Password Maintenance” on page 196**.

Note When setting **the Password Expiration Policy**, a blank field is not permitted and a value of 0 is equivalent to **Never Expires**. This means that as far as Image Service is concerned the password on the Remote database server is never going to change, so the user will never be prompted that the IS server’s Primary password is going to expire. In this case, the value set in the Notify Administrator field is meaningless.

Password Failure Emergency Procedures

If you are not able to connect to your Remote database server, perform the following steps on each IS server that is unable to connect:

1. Change to the /fnsw/bin directory.
2. Run the **Xdbconnect –r** command.
3. When prompted, logon as System Administrator.
4. In the Xdb Connect window, change the Primary password to match the password set on the Remote database server as described in **“Changing the Primary and/or Secondary Password” on page 194**.
5. For DB2 only, set the Secondary Password to the next Database Administrator issued password for the Remote Database server, if known.
6. Restart the FileNet software to verify that the IS software successfully comes up.

Password Maintenance

It is important that proper database authentication for the IBM Remote server and its associated IS server(s) be maintained for security reasons and potential server accessibility issues.

We recommend performing the following password maintenance steps:

1. When setting the **Password Expiration Policy** values in fn_edit during software installation, make sure you have an estimate of how often the passwords on the Remote database server will be changed (per your

site's IT policy). Armed with this information, you can set the expiration of the database user passwords on all of the IS servers that will be connecting to the Remote database server to coincide with the changing of the Remote database server's passwords.

2 When you receive the notification message that the f_sw password is going to expire, make sure that Secondary passwords for all four f_* users have been set to what the new passwords on the Remote database server are going to be. This is should be done on all servers that are going to be accessing the Remote database server.

3 Request that the Database Administrator change the four f_* passwords on the Remote database server to match what the Secondary passwords have been set to.

4 **For DB2 only:** After the Database Administrator has changed the four passwords on the Remote database server, the next time those users on the IS server(s) try to access the database server, the Primary password, which is about to expire, will no longer match, the Secondary password will automatically become the Primary password, and the log on will be successful. This also resets the **Activation Date** to the current system date and the **Password Expiration Policy** cycle begins again.

Note You should be aware of what the next password is going to be on the Remote database server so you can set this as the Secondary password on all of the servers where the database client is installed, and that are connecting to the Remote database server.

5 When no passwords succeed, refer to the **"Password Failure Emergency Procedures" on page 196**.

6

Sample Scenarios

In this chapter we present some scenarios that you can use as general guides for using the Remote Admin Console. These scenarios represent only a few of the many ways you can customize your system for your business requirements.

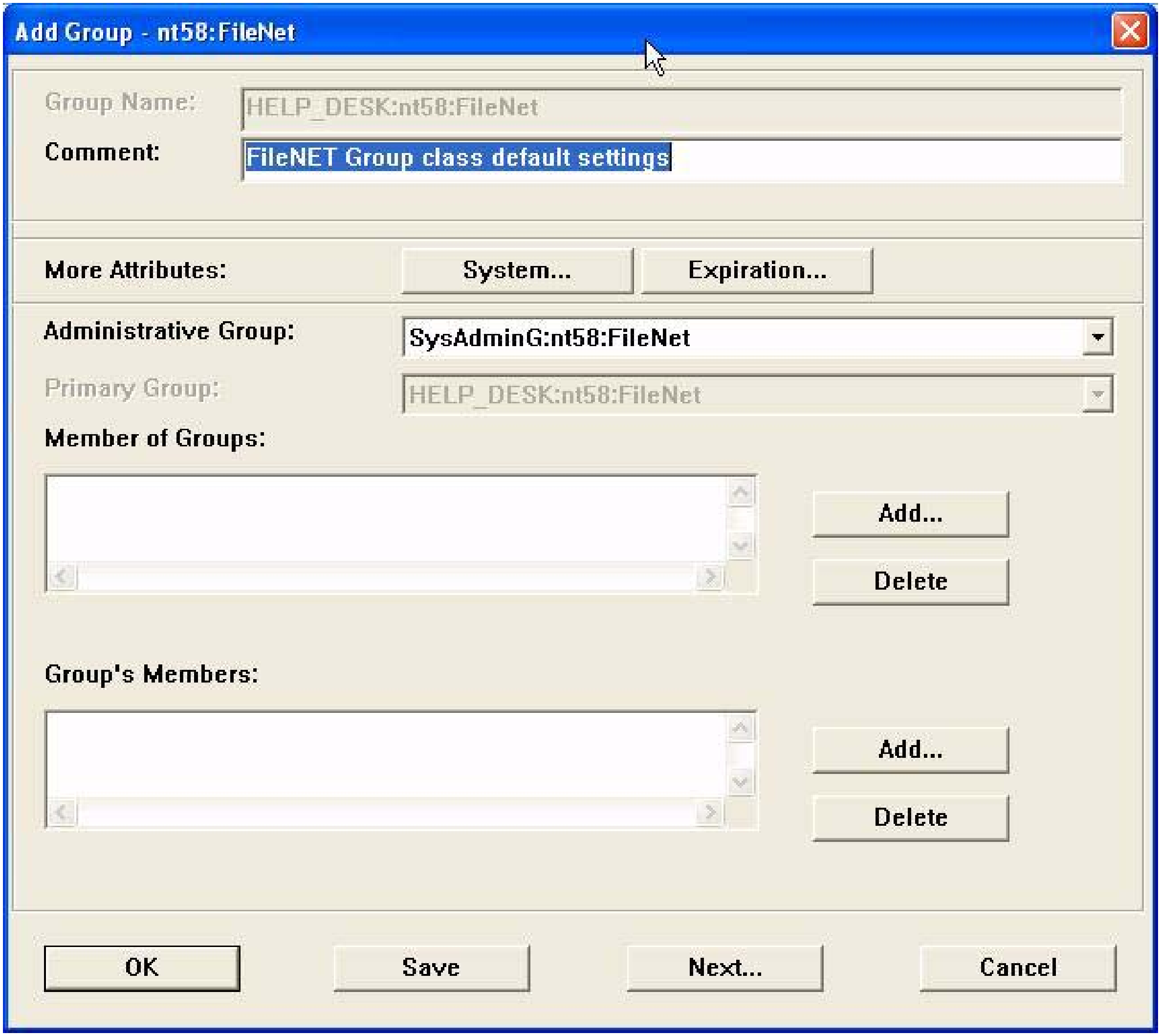
- Scenario 1 describes how to use the Remote Admin Console to set up function security for a help desk group.
- Scenario 2 describes how to use the Remote Admin Console to set up a group of users to perform only a specific function. There are two approaches:
    - Case A describes how to implement the group with **Allow Access to Undefined Functions** turned ON.
    - Case B describes how to implement the group with **Allow Access to Undefined Functions** turned OFF.

Scenario 1: Setting up a Help Desk Group and User

Many large companies have centralized help desks that support a wide variety of business applications and technologies. The front line help desk operators are responsible for taking problem calls. The calls are either escalated to second level support or resolved directly as is the case with changing passwords and resetting accounts. These operators are often required to remain at their desks, and have limited access to the data center and the actual servers. It is most efficient if these incidents can be closed on the first call.

The system can be configured to enable this.

1 **Set up the HELP_DESK group and its user.**
In the Security Administration application, create a group called HELP_DESK.



Add Group - nt58:FileNet

Group Name: HELP_DESK:nt58:FileNet

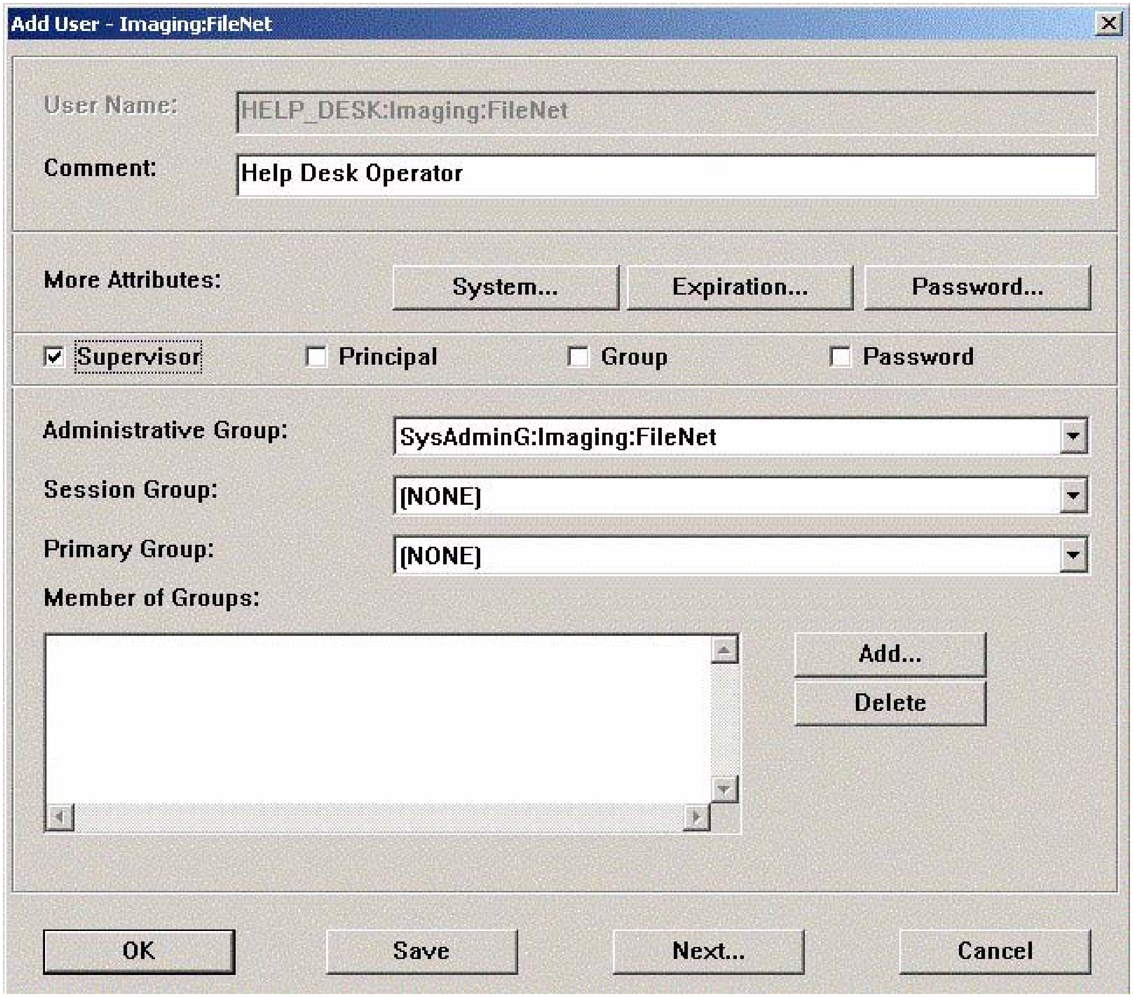
Comment: FileNET Group class default settings

Administrative Group: SysAdminG:nt58:FileNet

Primary Group: HELP_DESK:nt58:FileNet

Next create a user with either of the following:

- To give the user the ability to reset expired passwords only, check the **Password** attribute box.
- To give the user the ability to reset unexpired passwords, as well as the ability to add, remove and modify users and groups, check the **Supervisor** AND **Password** attribute boxes.



Add User - Imaging:FileNet

User Name: HELP_DESK:Imaging:FileNet

Comment: Help Desk Operator

More Attributes:

☑ Supervisor ☐ Principal ☐ Group ☐ Password

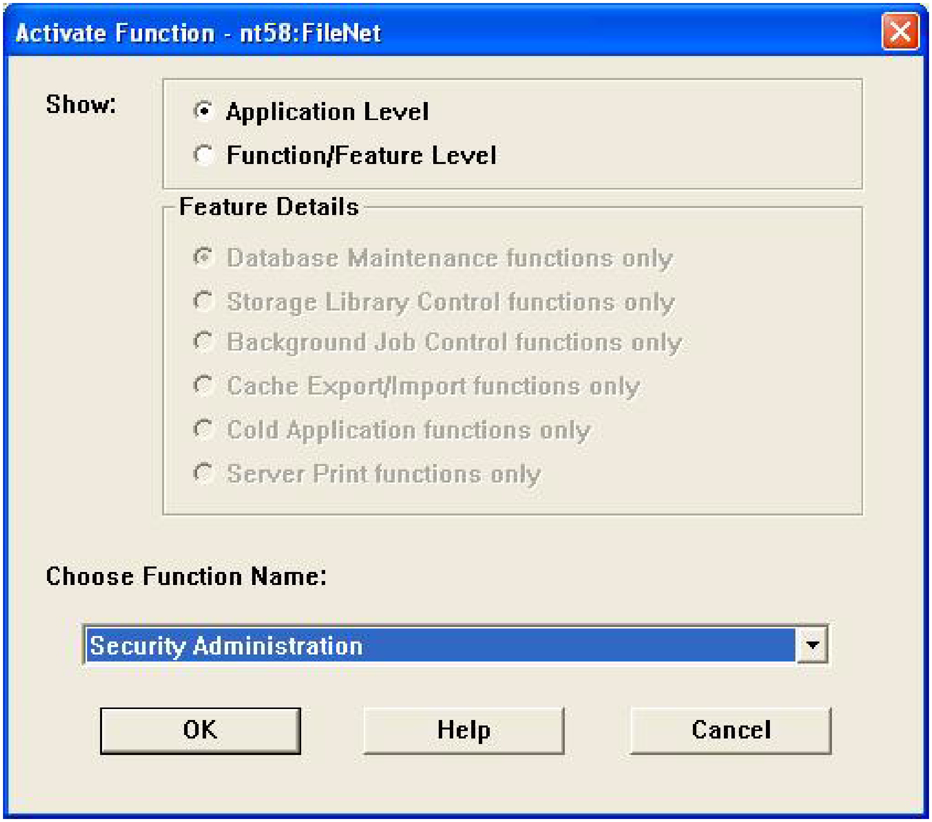
Administrative Group: SysAdminG:Imaging:FileNet

Session Group: [NONE]

Primary Group: [NONE]

Member of Groups:

2 **Activate Security Administration function.**
In the Activate Function window, click the Application Level radio button. From the Choose Function Name pull-down list, select Security Administration. Then click OK. The Add Function Name window displays.



Activate Function - nt58:FileNet

Show:
● Application Level
○ Function/Feature Level

Feature Details
● Database Maintenance functions only
○ Storage Library Control functions only
○ Background Job Control functions only
○ Cache Export/Import functions only
○ Cold Application functions only
○ Server Print functions only

Choose Function Name: Security Administration

3 **Add the HELP_DESK group to Security Administration**.
Click the Add... button to add the HELP_DESK group to the Security Administration function, and click OK.

4 **Disable all other functions.**
In the Activate Function window, click the Application Level radio button. From the Choose Function Name: pulldown list, select one of the following functions:

Database Maintenance
Storage Library Control
Background Job Control
Cache Export/Import
COLD Main Menu

Click OK. When the Add Function Name window displays, click OK **without** adding the HELP_DESK group.

Repeat this step for all the functions **except** Security Administration.

5 **Check the global setting.**
In the main Security Administration window, click the System menu and select Default Security Settings... . The Update Default Security Settings window displays. Make sure that the **Allow Access to Undefined Function** box is checked (**ON**).

At this point, you have successfully configured the system for its HELP_DESK group. Only members in the HELP_DESK group have authority to access the Security Administration application and to modify passwords. This group will not have access to the other application level functions and features.

Scenario 2: Setting up a group whose members can only access one specific application

The SureSafe Insurance company has decided that only data center operators should have access to the Storage Library Control application and all of its related features (and no other admin applications). The data center operator employees work 3-month stints, at which time other employees are rotated into this role. Currently the SureSafe Insurance company has two data center operators, bJones and jSmith. When their stints are over, sWilliams and bJohnson will take over their positions.

Case A and Case B illustrate two ways to implement this scenario.

Case A: The global setting to Allow Access to Undefined Functions is enabled

To allow for an easy change of access privileges, we'll create a special group called the DATA_CENTER group and add the individual users to that group.

With **Allow Access to Undefined Functions** turned ON, we'll activate each of the application level functions, but only add the DATA_ CENTER group to the Storage Library Control function.

When the personnel change takes place, all we'll need to do is remove the two current users from the group and add two new users.

1 **Set up the DATA_CENTER group and its users.**
In the Security Administration application, create a group called the DATA_CENTER group and two users, bJones and jSmith. Assign both users to the DATA_CENTER group.

2 **Activate the Storage Library Control function.**
In the Activate Function window, click the Application Level radio button. From the Choose Function Name: pulldown list, select Storage Library Control and click OK. The Add Function Name window displays.

3 **Add the DATA_CENTER group to Storage Library Control.**
Click the Add... button to add the DATA_CENTER group to the Storage Library Control function and click OK.

4 **Disable all other applications for the DATA_CENTER group.**
In the Activate Function window, click the Application Level radio button. From the Choose Function Name: pull-down list, select one of the following functions:

Database Maintenance
Security Administration
Background Job Control
Cache Export/Import
COLD Main Menu

Click OK. When the Add Function Name window displays, click OK **without** adding the DATA_CENTER group.

Repeat this step for all the functions **except** Storage Library Control.

5 **Check the undefined function global setting.**
In the main Security Administration window, click the System menu and select Default Security Settings... . The Update Default Security Settings window displays. Make sure that the **Allow Access to Undefined Function** box is checked (**ON**).

At this point, the SureSafe Insurance company has successfully configured the system for the data center operators. Only members in the DATA_CENTER group will be allowed to perform tasks in the Storage Library Control application. In addition, no one else will be allowed to access the Storage Library Control application and features. Also, the members of the DATA_CENTER group have no access to other administrative applications.

6 **Make some personnel changes.**
bJones and jSmith are being transferred to another department, and sWilliams and bJohnson will take their positions. Remove bJones and jSmith from the DATA_CENTER group. Add sWilliams and bJohnson to the DATA_CENTER group.

Since they’ve been removed from the DATA_CENTER group, bJones and jSmith no longer have access permission to run Storage Library Control functions, but sWilliams and bJohnson do have access permission because they’re now members of the DATA_CENTER group.

Case B: The global setting to Allow Access to Undefined Functions is disabled

As in Case A, we’ll create a special group called the DATA_CENTER group and add the individual users to that group.

We’ll only add the DATA_CENTER group to the Storage Library Control function. But with **Allow Access to Undefined Functions** turned OFF, we’ll have to add all the Storage Library Control feature roles to the DATA_CENTER group one at a time.

When the personnel change takes place, all we'll need to do is remove the two current users from the group and add two new users, as in Case A.

1 **Set up the DATA_CENTER group and its users.**
In the Security Administration application, create a group called DATA_ CENTER and two users, bJones and jSmith. Assign both users to the DATA_CENTER group.

2 **Activate the Storage Library Control function.**
In the Activate Function window, click the Application Level radio button. From the Choose Function Name pulldown list, select Storage Library Control. Then click OK. The Add Function Name window displays.

3 **Add the DATA_CENTER group to Storage Library Control.**
Click the Add... button to add the DATA_CENTER group to the Storage Library Control function and click OK.

4 **Activate the Storage Library Control features.**

a In the Activate Function Window, click the Function/Feature Level radio button.

b On the Feature Details panel, click the Storage Library Control functions only button.

c From the Choose Function Name: pulldown list select one of the features. Click OK. The Add Function Name window displays.

d Click Add... to add the DATA_CENTER group as a member of the feature you selected. Click OK.

e Repeat these steps for all feature level roles in Storage Library Control.

When this is finished, each feature role of Storage Library Control will contain the DATA_CENTER group as a member.

5 **Check the global setting.**
In the Update Default Security Settings window, make sure that the **Allow Access to Undefined Function** box is **not** checked (**OFF**). Note that all the other applications that have not been activated are no longer launchable (except by SysAdmins).

At this point, the SureSafe Insurance company has successfully configured the system for the data center operators. Only members in the DATA_CENTER group will be allowed to perform tasks in the Storage Library Control application. In addition, no one else will be allowed to access the Storage Library Control application and features. Also, the members of the DATA_CENTER group have no access to other administrative applications.

6 **Make some personnel changes.**
bJones and jSmith have been transferred to another department, and sWilliams and bJohnson will take their positions. Remove bJones and jSmith from the DATA_CENTER group. Add sWilliams and bJohnson to the DATA_CENTER group.

Since they've been removed from the DATA_CENTER group, bJones and jSmith no longer have access permission to run Storage Library Control functions, but sWilliams and bJohnson do have access permission because they're now members of the DATA_CENTER group.

General Recommendations

It is strongly recommended that responsibility-based access control (RBAC) be used with the **Allow Access to Undefined Functions** global setting turned **ON** and that roles be controlled by groups, not individual users. The case examples above demonstrate two different ways of setting up the same RBAC environment. When the global setting is ON, application level roles are very easy to manage (Case A). When the global setting is OFF, all the feature level roles need to be activated, which is more time consuming (Case B).

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**.

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 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.

Index

Program Number: 5724-R95

Printed in USA

SC19-2684-00