System Administrator's Companion for Windows® Server

Release 4.0.0

9844088-002

March 2006

Notices

This document contains information proprietary to FileNet Corporation (FileNet). Due to continuing product development, product specifications and capabilities are subject to change without notice. You may not disclose or use any proprietary information or reproduce or transmit any part of this document in any form or by any means, electronic or mechanical, for any purpose, without written permission from FileNet.

FileNet has made every effort to keep the information in this document current and accurate as of the date of publication or revision. However, FileNet does not guarantee or imply that this document is error free or accurate with regard to any particular specification. In no event will FileNet be liable for direct, indirect, special incidental, or consequential damages resulting from any defect in the documentation, even if advised of the possibility of such damages. No FileNet agent, dealer, or employee is authorized to make any modification, extension, or addition to the above statements.

FileNet may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Furnishing this document does not provide any license to these patents, trademarks, copyrights, or other intellectual property.

Please take a few moments to read the ***End User License Agreement*** on the Image Services 4.0.0 documentation CD. By installing the Image Services 4.0.0 software, the customer agrees to be bound by the terms of this agreement.

FileNet, ValueNet, Visual WorkFlo, and OSAR are registered trademarks of FileNet Corporation.

Document Warehouse and UserNet are trademarks of FileNet Corporation.

All other product and brand names are trademarks or registered trademarks of their respective companies.

FileNet Corporation
3565 Harbor Boulevard
Costa Mesa, California 92626
800.FILENET (345.3638)
Outside the U.S., call:
1.714.327.3400
www.filenet.com

Contents

About This Manual

The *Image Services System Administrator's Companion for Windows Server* is written for the system administrator and describes duties specific to the Image Services for Windows Server Release 4.0.0. This manual is a companion to the ***Image Services System Administrator's Handbook*** for release 4.0.0.

This manual contains chapters describing the Windows Server operating system environment, supported tape drives, and Image Services system backup operations.

We assume that you are familiar with basic computer terminology and have some familiarity with Windows Server.

Related Documents

You should have the following Image Services documents, supplied by FileNet, available to you:

System Administrator's Handbook

Installation and Configuration Procedures for Windows Server

Update Procedure for Windows Server

Guidelines for Installing/Updating Site-Controlled RDBMS Software for Windows Server

The following manuals contain information on PC workstations and PC-based servers and can be ordered from FileNet:

Desktop User's Guide *(WorkGroup/Worker)*
Desktop Coordinator's Handbook *(WorkGroup)*

For reference, you may also wish to obtain manuals or online documentation from your relational database management system (RDBMS) vendor.

What to Read First

We assume that you are familiar with your operating system, workstation operations, and the operator's view of the system. If you are not familiar with Windows Server system concepts, we suggest that you familiarize yourself with the operating system and its procedures and commands.

WorkGroup users can refer to the *Desktop User's Guide* and *Desktop Coordinator's Handbook* for information on the PC workstation.

Conventions Used in this Manual

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

Flags

Flags indicate that the text applies to a particular type of server, such as multiple servers or combined server, or a type of platform, such as UNIX or Windows Server. An example is the MultSv flag to the left of this paragraph. The MultSv flag indicates information for users with more than one server. WorkGroup users and other users with single-server configurations need not read the sections with this flag.

Typing Instructions

To indicate commands, values, or other information you enter at your keyboard, we use the following indentation and typeface:

help [CSM_exim]

Console Displays

Information you see displayed at your console is shown in this document in the following manner:

```
Surface ‘3176’ : 1 document processed
Local doc_id = ‘2235007’ Original doc_id = ‘2235007’
Original ssn = ‘8502’
Primary copy. No tranlog copy exists.
* document successfully deleted from databases. *
* Purging pages from disk... *
* This document has been successfully purged. *
```

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 be sure to read.
Tip	Introduces an idea that might make your work easier.

Command Syntax

Command syntax definitions are indented:

```
ddexim –e > <filename>
```

Optional Parameters

Optional parameters and keywords are within square brackets:

```
ddexim [–e] > <filename>
```

Required Parameters

Parameters that require you to provide information are shown within angle brackets (< >).

For example, for the following command:

ddexim –e > <filename>

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

ddexim –e > myfile

FileNet Education

FileNet provides various forms of instruction. Please visit Global Learning Services on FileNet's Web site at: **www.filenet.com**.

Comments and Suggestions

FileNet invites all customers to communicate with the Documentation group on any question or comment related to FileNet manuals and online help. Send email to **docs@filenet.com**. We will make every effort to respond within one week. Your suggestions help us prove the products we deliver.

1
Operating System

This chapter presents guidelines for Windows Server operating system navigation and, where applicable, describes how FileNet software interacts with the operating system. The principal topics in this chapter are the following:

- Image ServicesSources of information on Windows Server
- Running Image Services software as a Windows Server service
- Power on and power off procedures for your system
- Service and user mode processes
- Logging on and logging off the operating system and Image Services with a unified logon approach
- User account creation, Windows Server groups, and security guidelines
- Disabling NCH broadcasts
- Viewing Image Services text files
- Description of the Windows Server file system, FileNet directories, and RDBMS directories
- Description of FileNet monitoring tools, such as Task Manager, Performance Monitor, and Event Viewer

Windows Server Facts and Resources

This chapter refers to the Windows Server 2000 Starndard and Enterprise Edition operating systems.

Books on Windows Server

This chapter does not replace reference materials provided in the Windows 2000 Server/Enterprise Edition documentation. Before reading this chapter, you may want to read the *Windows Server Roadmap* and the *Windows Server System Guide*, along with the other manuals that came with your operating system. If you are a new Windows Server user, you may also want to visit your local bookstore for publications written for new users.

Learning with Microsoft Videos

In addition to the above documentation, you may order the following from Microsoft, both with video tapes:

- Windows Server Resource Kit
- Windows Server Tutorial

Dial the following to order:

1.800.MSPRESS

Microsoft Online Documentation and Help

Windows Server provides the following online documentation:

- Information stored on CD-ROM.
- A tutorial program, Introducing Windows 2000, is contained in the Main window.

Your operating system provides online help for all functions and applications.

Getting Started

The topics described in this section explain how the FileNet Image Services software interacts with the Windows Server operating system.

Overview

To access the Windows Server operating system, log on at a console. After logging on to the operating system, your Windows Server desktop presents the Windows Server and FileNet Image Services applications available to you. You can enter operating system commands, read online documentation, and start Windows Server applications. You can click on FileNet Image Services Applications from Programs to start the following: Application Executive, Background Job Control, Cache Backup, COLD programs, the Task Manager to start and stop FileNet software, and system administration programs such as Database Maintenance, Security Administration, Systems Monitor, and Storage Library Control.

On an Image Services system, FileNet IS software, Relational Database Management System (RDBMS), such as Oracle or the Microsoft® SQL Server™, and the Windows Server operating system

run on one or more Windows servers. When the Image Services system is configured as a combined server, the operating system, the RDBMS software, and the IS software (including root, index, and storage library services) are all on the single combined server. The WorkGroup systems run on a single combined server.

MultSv

When the Image Services system is configured as a dual server, IS software services are distributed across two servers, referred to as the root/index server and the Storage Library server. The root/index server has root and index services and the RDBMS software. The Storage Library server has storage library services. A dual server configuration may also include application servers. A typical example is a separate application server for WorkFlo Queue services.

Root functions refer to the services that maintain the network service directory (the network clearinghouse database) and the security database. Index functions refer to the services that maintain the RDBMS database. Storage library functions refer to servicing of storage media libraries.

All FileNet system administration tasks are run from the console of one of your servers or, in a combined server system, from the server console. For example, use **Storage Library Control** to monitor optical storage library activity, Security Administration to set up FileNet security, and Database Maintenance to define and manage your document classes.

Running Image Services Software as a Service

The FileNet TM_daemon program is written to run as a Windows Server service process, called the IMS ControlService. The TM_ daemon program starts and stops the IS software, based on com-

mands received from the FileNet Task Manager. The terms, TM_daemon and IMS ControlService, may be used interchangeably, although IMS ControlService is the term used in this manual when TM_daemon is discussed in the context of a service process.

TM_daemon is installed as an automatic service during IS software installation.

Automatic Service Process

TM_daemon only runs as a service process. Service processes run independently of a user login session. You cannot start TM_daemon from a user login session as a user-owned process because you cannot start TM_daemon unless TM_daemon is running as a service.

Once TM_daemon is installed as the IMS ControlService during IS software installation, IMS ControlService appears in the Services applet of the Windows Server Control Panel. Click on the Services applet to display the Services dialog box. One of the services listed is IMS ControlService. The IMS ControlService Status column reads “Started” to indicate TM_daemon has been started. The Startup column reads “Automatic” to indicate that Image Services as a service will automatically start when the Windows Server is rebooted.

With Windows Server system administrator privileges, you are able to set the IMS ControlService to manually start or to even disable the IMS ControlService. In the Services dialog box, select IMS ControlService by clicking on it. Then click on the Startup button to open another dialog box where you can change the startup type to “Manual” or “Disabled.”

If you change the startup type to manual, IMS ControlService runs as a service, but only starts manually on demand. You may want to tempo-

rarily set the IMS ControlService to manual if you are frequently rebooting the Windows server for troubleshooting purposes. Otherwise, we recommend you maintain the IMS ControlService as an automatic service to take advantage of Windows Server's capability to automatically start TM_daemon when the server is rebooted.

If you change startup type to disabled, the IMS ControlService no longer runs as a service process and TM_daemon cannot be started.

When TM_daemon does not run as a service you will not be able to start TM_daemon as a user-owned process through any of the FileNet utilities, such as the Task Manager, the initfnsw start command, or the whatsup command.

Note In Image Services release **3.3.1 and earlier**, you were able to restart TM_daemon by typing the initfnsw start or whatsup command or through the Task Manager. In Image Services release **3.4.0 and later**, you can only restart TM_daemon through the Services applet in the Windows Server Control Panel or by rebooting the Windows server. Also the initfnsw start command in Image Services release 3.4.0 and later only starts Image Services software, once TM_daemon is running as a service, and does not start TM_daemon.

Invoking FileNet's Task Manager while TM_daemon is not running displays a dialog box with the following error message:

> Xtaskman.EXE: connect() failed
> with error 'connection refused'!
> Check to ensure that the IMS

ControlService and TM_daemon
are running

Invoking the initfnsw start command or whatsup command while TM_daemon is not running displays the following error message:

Check to ensure that the IMS ControlService
and TM_daemon are running

Automatic Image Services Startup

During Image Services installation, we recommend you enable the IMS ControlService process to immediately start the IS software once the IMS ControlService is started. When enabled in this way, the Image Services software starts when the Windows Server is rebooted. The Edit Installation Parameters dialog box displays automatically during the Image Services installation. Check the “AUTOSTART IMS PROCESSES” box to enable automatic Image Services startup. If the autostart IMS processes is not enabled, Image Services software does not automatically start up when the IMS ControlService is started (when the Windows Server is rebooted).

To enable the IMS ControlService to automatically start Image Services software, you need to be logged on as a member of the Windows Server Administrators group and fnadmin group. Use Task Manager to determine whether the IS software has started.

Not only at Image Services installation but at any time, you can enable or disable the IMS ControlService process from automatically starting up the Image Services software. Click on Setup from the FileNet Image Services Configuration folder. Select FileNet Image Services Installation Maintenance and choose Edit Installation Parameters. In the Edit Installation Parameters dialog box, you may check or not

check the “AUTOSTART IMS PROCESSES” box. You may want to disable autostart of Image Services processes if you are running Image Services as a part-time application on the Windows server. You may temporarily disable autostart of Image Services to avoid the overhead of bringing IS software up whenever the system is rebooted, such as when you are troubleshooting or have hardware problems.

Note If you have configured your system to have a site-controlled RDBMS, you can maintain the IMS ControlService as an automatic service, but the IMS ControlService process cannot be configured to immediately start Image Services software. Make sure the “AUTOSTART IMS PROCESSES” box is not checked. In a site-controlled configuration, one advantage to maintaining the IMS ControlService as an automatic service is that once the Image Services software is started, Image Services will run as a service process. The Windows Server user who started Image Services can log off and IS software will still remain up.

Advantages of Automatic Service and Autostart IMS

When you run the IMS ControlService as an automatic service and enable automatic startup of IMS, you gain the following advantages:

- The advantage of an automatic service is that Windows Server starts all its services, including TM_daemon, automatically when the Windows Server is booted or rebooted.
- If automatic startup of Image Services is enabled, IS software will start up when TM_daemon starts upon reboot.
- For example, when power is restored after a power outage, Image Services software will restart when the Windows Server reboots, without requiring a system administrator to physically log on and restart Image Services at a console.

- Image Services software does not shut down when the user who started the IS software logs off an individual Windows Server session because Windows, not the user, owns the IS service.

Starting and Stopping a Service Process

The Windows Server operating system places time restrictions on starting and stopping service processes.

If a part of the Image Services software does not start up in the normal amount of time expected by the operating system, the IMS ControlService will fail to start up as a service process. You need to investigate the problem by examining information in the Services dialog box, the FileNet Task Manager processes, the FileNet error log, and Windows Server event logs.

If a part of the Image Services software does not shut down in the normal amount of time expected by the operating system, your FileNet system will **not shut down gracefully**. We recommend you shut down the Image Services software through the Task Manager **before** you shut down the Windows Server (through the shut down or restart buttons in the Shut Down Windows dialog box).

Note The killfnsw command does not terminate TM_daemon in Image Services release 3.4.0 and later. You can only terminate TM_daemon by selecting “Stopped” in the IMS ControlService Status column through the Services applet in the Windows Server Control Panel. For example, if you attempt to run the killfnsw –D –y command, the following error message displays:

```
killfnsw: cannot kill tm_daemon when it is running as a service process.
Use Services applet in Control Panel to stop ‘IMS ControlService’
```

Logging off as a Windows Server User

You may want to log off to terminate your Windows Server session or to shut down the Windows Server or to log on as a different user. Normally you click on the Shut Down icon and click the “Close all programs and log on as a different user?” button in the Windows Server Shut Down Windows dialog box.

CAUTION You must close any FileNet Image Services applications you started before logging off as a Windows Server user because Windows Server may not close user-initiated applications gracefully and completely. The result is that you are not able to log off Windows Server and the Image Services software state may be uncertain.

Before logging off Windows Server, first close all user-initiated Image Services server applications, especially Database Maintenance, Security Administration, and COLD, because these applications are not being closed completely by Windows Server.

Powering On Your System

Combined Server System

Power on a combined server system as follows:

1. Power on all peripherals (for example, local printers).
2. Power on the Image Services combined server.
3. Power on any application servers one at a time, in any order.

Dual Server System or Multiple Storage Library System

MultSv

Power on a system with a root/index server and one or more storage library servers as follows:

1. Power on all peripherals.
2. Power on the root/index server.

Note If you are running Image Services software as an Windows Server service and have enabled the automatic startup of IS processes, FileNet software will start up each time after you power on the root/index or storage library or application server.

3. Power on the (main) storage library server and then any other storage library servers in any order.
4. Power on any application servers one at a time, in any order.

Note On a multiple server system, the FileNet software on the root/index server must be completely up before you power on the storage library or application server.

Powering Off Your System

Normally, you can leave the system running. However, you occasionally need to shut down to correct problems or to upgrade the software. In addition, you may want to shut down quickly in an emergency.

To power off a dual server or multiple storage library server system, perform the following steps at each Image Services non-root server and last at the root server.

To power off a single combined server system, perform the following steps at the Image Services server.

1. Notify all users that the system is going down and ask them to log off.
2. Log on as a user who is a member of the fnadmin or fnop group and dba and fnusr groups.
3. Log off or exit from any open applications (for example, all IS application windows must be closed).
4. Shut down the FileNet Image Services software:
   a. Click on Task Manager in the FileNet Image Services Server Applications folder.
   b. Select the Stop button.
5. Click the Start button and select the Shut Down icon.
6. Select “Shut down the computer?” from the Shut Down window and click the Yes button.
7. Turn off the power to the Image Services server, when Windows Server notifies you that it is safe to power off.
8. Power off peripheral devices connected to your server (for example, local printers), if necessary.

Rebooting

Sometimes you must reboot your system, for example, after a hardware maintenance operation.

Before rebooting, shut down the Image Services server. See **“Powering Off Your System” on page 23** before rebooting.

After shutting down, reboot your server in one of two ways:

- Press the Reset button on the front panel of your server

  or

- Turn off the power to your server, wait approximately 30 seconds, then turn the power back on.

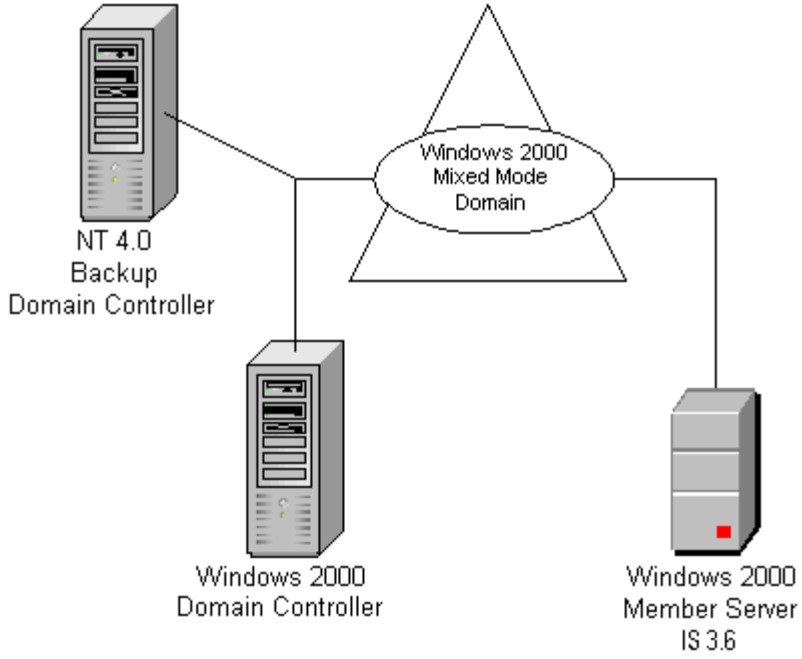
If Windows Server finds a problem, it displays a warning message. Windows Server also adds an entry to the event log. Examine the event log using the **Event Viewer** in the Administrative Tools window.

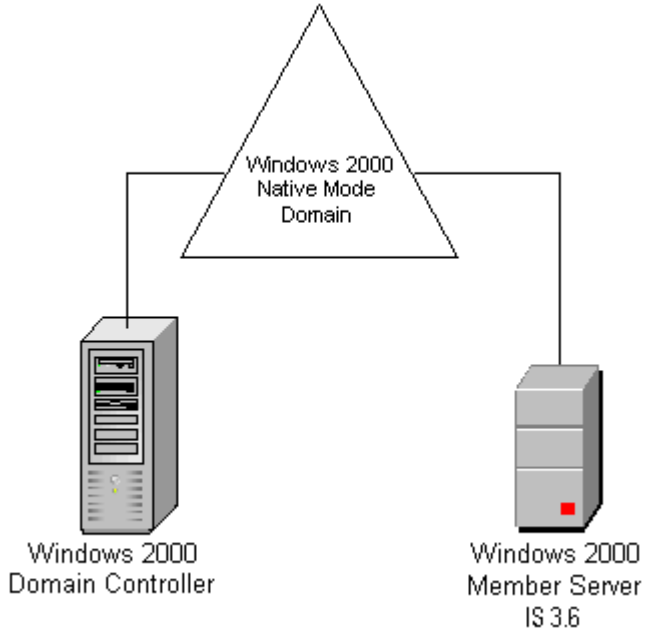
If you have enabled the IMS ControlService process to automatically start up Image Services software, then IS software will start up when the server is rebooted.

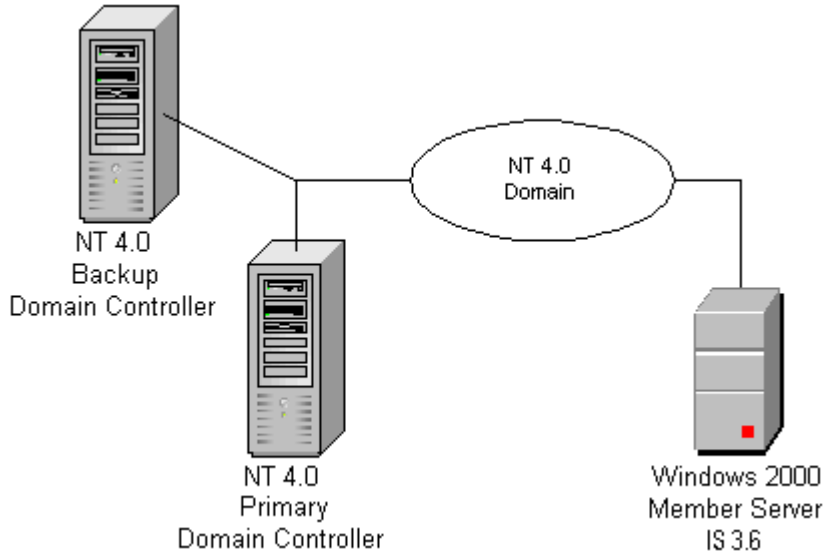
Domain Security and Planning

Although Image Services 4.0.0 can be installed on both Windows 2000 member servers and domain controllers, FileNet strongly recommends that you **DO NOT** install Image Services on domain controllers. Installations on member servers or stand alone servers are preferred. The Windows 2000 domains can be in mixed or native mode.

You can also install IS 4.0.0 on a Windows 2000 member server if you are still using NT 4.0 Primary and Backup domain controllers. Image Services 4.0.0 does not have to be installed on a server in a domain to function properly. Here are a few very basic examples.




Windows 2000
Native Mode
Domain
Windows 2000
Domain Controller
Windows 2000
Member Server
IS 3.6



FileNet Users and Groups

FileNet users and groups must be created on the local machine. To facilitate centralized security, you can create Global Groups on the domain controller and then add the Global Groups to the local FileNet groups.

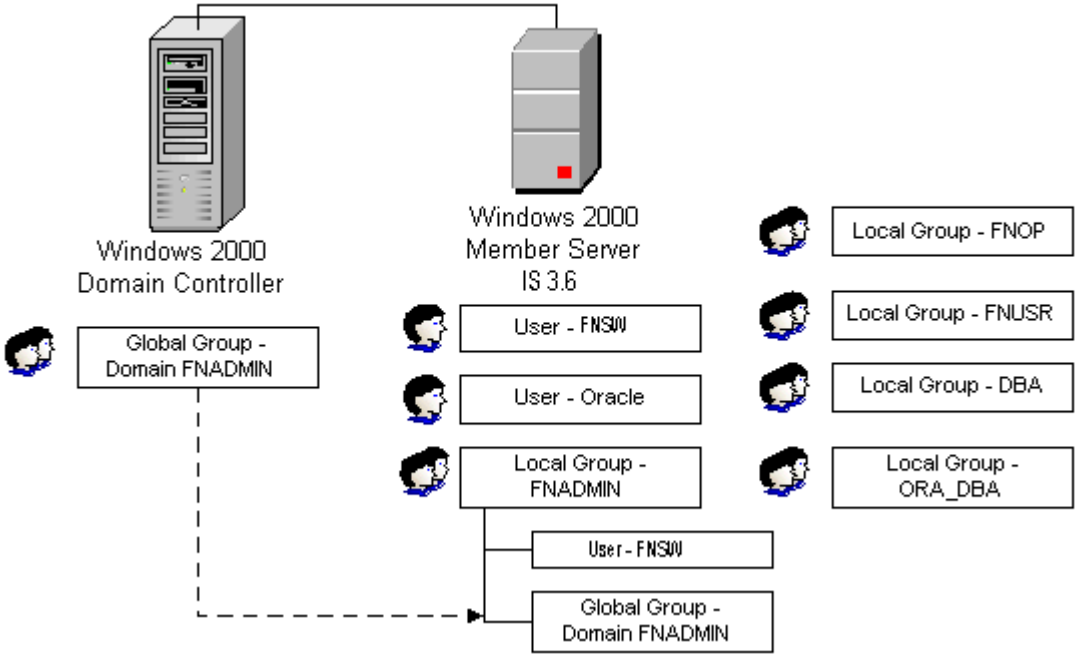
FileNet strongly recommends that **ONLY** local IS users and groups be established on the IS server for the following reasons:

- This configuration reduces security complexity and aids in IS troubleshooting.
- It is NOT necessary to configure Global Groups and users in order to effectively implement the Windows Domain security model.

The following page shows a simple example of how you can configure users and groups.

For more information regarding security, see **“Security” on page 43**.

For information regarding group membership for using IS tools, see the ***IS System Tools Reference Manual***.



Operating System Logins

A user logs on to the operating system with a Windows Server account name and password. To simplify logging on to Image Services server applications, you can enable a unified logon approach that allows

approved users to directly log on to any Image Services server application by just logging on to their Windows Server account. Refer to **"Windows Server Interface" on page 33** for more information.

Administrator Account

As the system administrator, you can log on to the operating system as **Administrator** or as another login that you create. The Administrator is a built-in account, receives superior rights and permissions, and is reserved for the user who manages the configuration for the domain. The Administrator has permission to perform any operating system task. Because the Administrator login is so powerful, safeguard it with a password and change the password frequently. This account should be reserved for high-level, security-related tasks. When the administrator is not performing tasks that require the Administrator login, it is recommended that even the administrator log on with a different account.

The Administrator account can be renamed, but cannot be deleted or removed from its inherent groups (Administrators, Domain Admins, and Guests).

Note Windows Server logins may be associated with FileNet logins such as SysAdmin.

Other User Accounts

Additional user accounts can be created. Administrative accounts can be created for any user who is designated to execute administrative-level tasks. Other user accounts can be created or copies of existing accounts can be made. Each account acquires its privileges according to group memberships. For details, refer to the chapter, "User Manager

for Domains” in the *Windows Server System Guide* and to **“Security” on page 43** in this manual.

Service and User-Owned Processes

When TM_daemon is run as a Windows Server service process, the operating system owns TM_daemon. Because the operating system, not a user owns TM_daemon, you do not experience the problem of Image Services shutting down when the user who starts Image Services logs off. In a user-owned process when a user logs out of a process started by that user, that process automatically terminates.

If you have disabled the IMS ControlService from running by changing the startup type to disabled in the Services applet of the Control Panel, the operating system no longer owns TM_daemon. TM_daemon no longer runs and you cannot start TM_daemon unless you re-enable TM_daemon as a service.

If you are not sure whether TM_daemon is running as a service, you can view FileNet’s Task Manager to determine whether the operating system owns TM_daemon. The following examples are used for illustration only.

Scroll through the “Current Processes” section of FileNet’s Task Manager to look for the following information that verifies that TM_daemon is running as a service process and Image Services software is started automatically. Under “Processes”, look for TM_daemon located in the directory path \FNSW\bin\tm_daemon.exe. The full directory path name indicates that TM_daemon started and is running as a service. The -c and start options indicate that IS software has been automatically started if you have enabled the autostart of Image Services pro-

cesses. Look across under “User.” You should see that SYSTEM, which is the operating system privileged user, owns TM_daemon.

Software State: Software started since Tue Feb 25 16:23:11 1997				
Current Processes:				
User	PID	TID	Start Time	Processes
SYSTEM	0xe0	0xdf	4:23:11 PM	PRI_worker
SYSTEM	0xda	0xd9	4:23:11 PM	rmt_commit
SYSTEM	0x94	0x8e	4:23:11 PM	SEC_daemon
SYSTEM	0x81	0x80	4:23:11 PM	E:\FNSW\bin\tm_daemon.exe -c start

The example below illustrates the information provided by FileNet’s Task Manager when a Windows Server user, fnsw, has logged on and started a user-owned process, Storage Library Control.

CAUTION If you log on as a Windows Server user to start a non-service process to perform tasks such as Storage Library Control or Security Administration, you own that user session. When you log out, whichever user-owned process you started will terminate. However, Image Services software is still up because it was started as a service process and is owned by the operating system privileged user, SYSTEM.

If you are not sure if the process is user-owned or system-owned, look at the information in FileNet’s Task Manager.

Under “Processes”, you should see the path name for Storage Library Control, E:\FNSW\bin\xslc.exec. Under “User” you should see that fnsw is the user and owner of that process. If the fnsw user logs out,

the Storage Library Control session terminates because fnsw owns that session.

Software State: Software started since Tue Feb 25 16:23:11 1997				
Current Processes:				
User	PID	TID	Start Time	Processes
SYSTEM	0xe0	0xdf	04:23:11 PM	PRI_worker
SYSTEM	0xda	0xd9	04:23:11 PM	rmt_commit
SYSTEM	0x94	0x8e	04:23:11 PM	SEC_daemon
SYSTEM	0x81	0x80	04:23:11 PM	E:\FNSW\bin\tm_daemon.exe -c start
fnsw	0xfa	0xf9	05:27:42 PM	E:\FNSW\bin\xslc.exec

Logging on to Your System

This section describes the process of logging on to the operating system and the Image Services software.

Windows Server Interface

On a newly booted system, press the following to display the Windows Server login prompt:

Control + Alt + Del

A login window follows, requesting your Windows Server login name and password. Enter your assigned operating system login name and password.

After successfully logging on to Windows Server, you can then select from the Program folder those applications which have been config-

ured for your user account. You can start an application and, if you wish, reduce it to an icon.

For any application you want to start automatically, place its icon in your Startup group of icons. Applications are started according to the order of the icons in the Startup group. However you do not want a FileNet application to start automatically unless your FileNet software is already started.

Image Services Interface

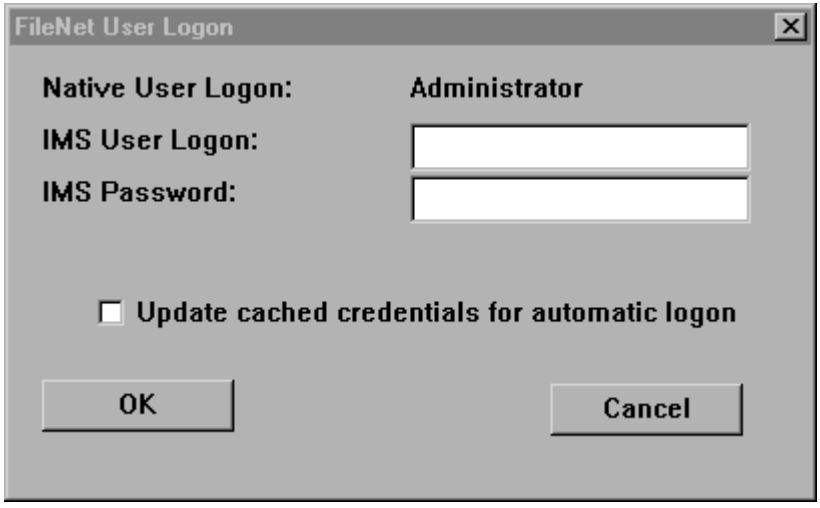
After logging on to the operating system with your Windows Server login, you can choose to enable automatic IS server application authorization. Automatic authentication allows approved users to directly log on to any Image Services application by just logging on to their Windows Server account. Automatic authentication simplifies usability by allowing for a unified logon approach with just a Windows Server user login. You no longer need to authenticate yourself through the Application Executive each time before using any IS application.

Enabling Automatic Authentication

1 Initially log on to the Application Executive in the FileNet Image Services Applications folder.

Click the Logon button in the Application Executive window.

2 The FileNet User Logon dialog box automatically displays the first time you log on to the Application Executive. A sample display is shown below.



a Enter your user logon and password.

b Check the “Update cached credentials for automatic logon” box if you elect to enable automatic authentication.

c Click OK.

Your new IS user login is now associated with the Windows Server user login and, if elected, automatic authentication is enabled for the new IS user login. You must check the “Update cached credentials for automatic logon” box to use the automatic authentication feature because it is not the default.

The initial logon to Application Executive is required to authenticate your FileNet user ID the first time and to allow you to enable automatic authentication. Afterwards, you may use any of the IS server applications, such as Task Manager, Database Maintenance, Security Admin-

istration, and Storage Library Control without having to log on to the Application Executive again.

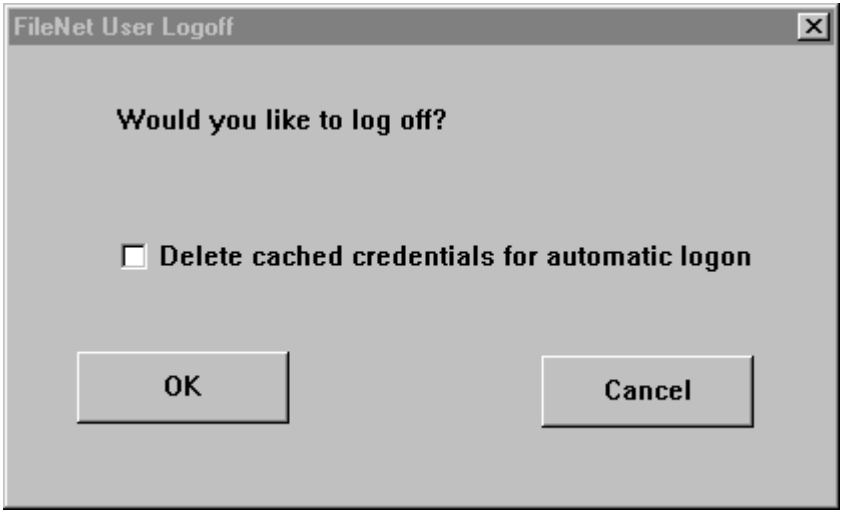
Once automatic authentication is enabled, the Windows Server account or user login is associated with a specific IS user login. The automatic authentication feature is enabled whenever you log on to Windows Server until you choose to disable it.

Logging On as a New Image Services User

You can associate any Windows Server user login with any IS user login. Therefore you can easily log on as a new IS user when you want to perform tasks that require other account privileges, as long as you have the password. For example, you may be logged on as a member of the fnop group to do backup operations. You find you need to run a system administration task and need to be logged on as a member of the fnadmin group.

To log on as a new IS user:

1. Close or exit any running IS server applications.
2. Log off the Application Executive by clicking the Logoff button in the Application Executive window.
3. The FileNet User Logoff dialog box displays. A sample display is shown below:



a If you had enabled cached credentials at login time, you may leave the “Delete cached credentials for automatic logon” box unchecked and the new user name and password will be automatically cached. Checking the box disables whichever user name and password had been cached for automatic authentication.

b Click OK.

4 Click the Logon button in the Application Executive window.

5 The FileNet User Logon dialog box displays.

a Enter the new IS user login and password.

b If needed, enable automatic authentication for the new user and password by checking the “Update cached credentials for automatic logon” box.

c Click OK.

Your new IS user login is now associated with the Windows Server user login and, if elected, automatic authentication is enabled for the new IS user login.

Using the Task Manager

After your user credentials have been authenticated or entered, you can start up FileNet Image Services software by selecting the Start button in the Task Manager application in the FileNet IS Server Applications folder. You can also use Task Manager to stop or restart IS software and to put IS software in Backup Mode or Restore Mode.

- Start is used to start the MKF databases (permanent, security, and transient) and IS software. The RDBMS database is also started if the database is FileNet-controlled.
- Stop is used to shut down the MKF databases (permanent, security, and transient) and the IS software. The RDBMS database is also shut down if the database is FileNet-controlled.
- Restart is used to terminate and start the IS software in one step. It is primarily used during configuration procedures which require the software to be re-cycled or restarted.
- Backup Mode initiates a minimal environment for backup operations. You must select Stop first to shut down FileNet software before selecting the Backup mode.
- Restore Mode terminates FileNet processes and places the IS software in a state appropriate for performing restores of the Image Services datasets and databases. After the restore, select Restart.

Using Windows Server

You can run multiple applications simultaneously in separate windows. Use the mouse to click and activate the window of your choice, or use the following task-switching capabilities of the Windows Server operating system.

- Press Control + Esc to display the Task List and then highlight the task you wish to switch to.
- Press the Alt + Esc keys to rotate active tasks.

Close any window you are not using with one of the following procedures:

- Point the mouse cursor at the upper left corner of the window and click on the Close option.
- Select Exit from the File menu bar item.
- Double click on the system menu button.

Most programs have an Exit option from the application's File menu bar and/or a Close button. Exit programs by using either the Exit option or Close button, instead of using the Close item on the system menu. See the *Microsoft Windows Server System Guide* for more help in using the Windows Server desktop.

Command Line Interface

Occasionally, you may run a tool or command from the command line interface. Click on the MS DOS prompt icon to open a command prompt window. The window appears with your default directory and system prompt. Enter your command at the prompt.

Logging Out from Your System

We recommend that you log out whenever you leave the console. If you walk away from the console while logged on, especially if you are an administrator, you leave the system vulnerable.

If you do not wish to log off when leaving the Windows server, then secure the console before leaving by pressing Control + Alt + Delete to initiate a dialog box for that purpose. Console security does, however, require your password to regain access.

You may also use a password-protected screen saver program to further secure the console. To configure a screen saver, click the Start button and select, in sequence, the Settings icon, the Control Panel folder, the Display icon, and the Screen Saver folder.

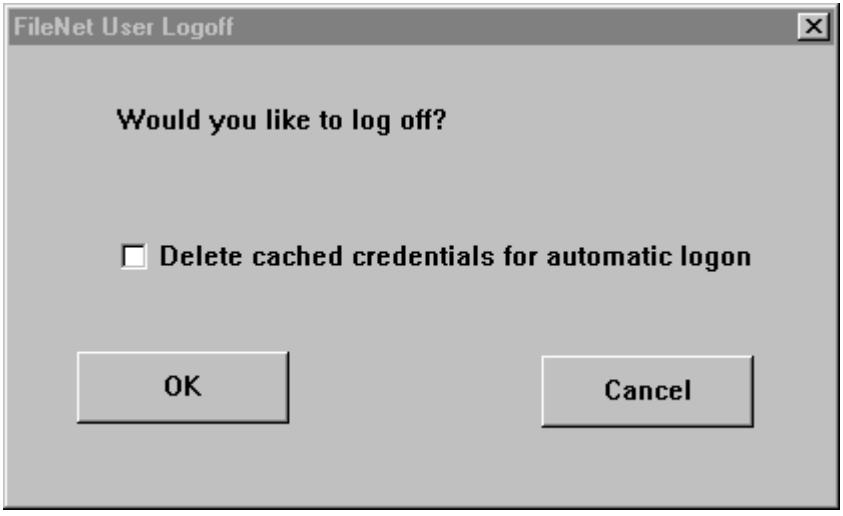
To exit from Image Services software and the operating system:

1. Close or exit any running IS server applications.

CAUTION You must close any FileNet Image Services applications you started before logging off as a Windows Server user because Windows Server may not close user-initiated applications gracefully. Without a graceful logoff, you are not able to log off Windows Server and the IS software state may be uncertain.

2. Log out of the Application Executive by clicking the Logoff button in the Application Executive.

The FileNet User Logoff dialog box displays, as shown below:



3 To disable automatic authentication, check the “Delete cached credentials for automatic logon” box, then click OK.

Deleting cached credentials unmaps your Windows Server login from your FileNet IS login. Your Windows Server login will no longer be associated to log on to Image Services software.

4 Close all open Windows Server applications with the Exit option or the Close button.

5 Click the Start button and select the Shutdown icon.

6 Select “Shut down the computer?” from the Shut Down window.

7 Click the Yes button on the confirmation dialog to log out of the operating system.

Creating a User Account

To create a new user account, choose User Domain Management from the System Application folder. Choose Add/Update User from the Users menu. If you have questions about the meaning of any field, use the online help. You can also read about security and login recommendations in the Windows Server documentation prior to creating new users.

You should create the users you want and assign them to appropriate groups, based on the tasks the user must perform.

After setting up your user accounts, you can create a profile for one user or save it as a system default. Click on the Programs icon from the Start button. Select the User Manager from the User Manager for Domains icon of the Administrative Tools folder.

For additional information, refer to the *Windows Server System Guide*.

Assigning and Changing Passwords

You can create or change an operating system password for a login. Click on the Programs icon from the Start button. Select the User Manager from the User Manager for Domains icon of the Administrative Tools folder.

Refer to the *Windows Server System Guide* and the online help text for details.

Security

The FileNet system provides security for folders, documents, and other data objects.

Viewing and Changing Permissions

The Windows Server operating system provides its own form of security at the operating system level. Permissions are set on objects, such as files, directories, or printers. Permissions specify the users who may have access to objects and their level of use. The creator of an object is the owner, who usually sets permissions.

Follow these guidelines to set up security for data objects:

1. Create groups that represent common operating system functions that must be performed by various groups of users.
2. Create user accounts for all of your users.

   Assign each user to groups that represent the type of operating system functions that the user needs to perform.
3. Use the Permissions item on the File Manager Security menu to assign users or groups various permissions on your files and directories.

   The FileNet Setup program assigns appropriate permissions to the files and directories used by the IS software, based on the appropriate groups.

   For more information on permissions, refer to your *Windows Server Concepts and Planning Guide* and the *Windows Server System Guide*.

Looking at Windows Server Groups

In addition to the built-in Windows Server groups, four operating system groups that you created during FileNet software installation are used to control FileNet software and for specific FileNet purposes. The following chart is a brief overview of both built-in and created groups:

Group Name	Group Type
Administrators	Windows Server admin group
Server Operators	Windows Server operator group
Account Operators	Windows Server operator group
Print Operators	Windows Server operator group
Backup Operators	Windows Server operator group
Everyone	Windows Server— Applies to all users
Users	Windows Server user group
Guests	Windows Server temporary user
fnadmin	Administrative group used by FileNet
fnop	Operator group used by FileNet
fnusr	Server application group used by FileNet
dba	RDBMS group used by FileNet

Members of the group **fnadmin** have full rights to all the applications and tools in the FileNet software. The fnadmin group is usually reserved for system administrators. Members of fnadmin can make system configuration changes and perform restores. They may also run tools (without running Application Executive) that require FileNet security. However to start and stop FileNet software, you must also be a member of the fnusr group. We **require** that members of fnadmin be members of the Windows Server Administrators group as they need

Windows Server administrator privileges to configure the operating system.

Members of the **fnop** group have privileges for starting and stopping the FileNet software, performing backups, and performing daily operator duties. However to start and stop FileNet software, you must also be a member of the fnusr group. Members of fnop can run certain system tools with hard-coded passwords, such as MKF_tool or CSM_tool. The fnop group is usually reserved for FileNet operators. For example, users who need to use the Task Manager to start and stop FileNet software may be a member of fnop (or fnadmin).

Members of the **fnusr** group have privileges for running the FileNet server applications, such as Cache Backup, COLD, Database Maintenance, and Storage Library Control. A user with only fnusr membership cannot execute the Application Executive. If that user were a member of not only the fnusr group, but also the fnadmin and dba groups, then that user can execute the Application Executive.

Members of the **dba** group are granted privileges for starting and stopping the RDBMS and configuring an Oracle or Microsoft SQL Server database.

The following are examples of how a system administrator can grant privileges based on tasks a user performs:

- If a member of the Windows Server **Administrators** group needs to run COLD, add that member to the fnadmin group and fnusr group.
- If a member of the Windows Server **Server Operators group** needs to back up FileNet software, add that member to the fnop group and fnusr group.

- If a member of the Everyone or Users group needs to retrieve and print a document, add that member to the fnusr group.

Since the Image Services software is installed by a member of the Administrators group, the Administrator is the owner; the owner can always change permissions.

Later, if files, not owned by the Administrator, are created by the IMS, the Administrator can first take ownership (an Administrators group right), and then change the permissions.

Making a user a member of the fnadmin group grants that user full access to FileNet applications and tools. This access should be used very carefully—a user could delete or modify critical data. If a user does need full access to FileNet applications and tools, that user should be added to fnadmin. Do not change permissions of IS files and directories.

Using Server Manager for Your Domain and Other Domains

Through the Server Manager, you can perform functions on the displayed domain or use the Select Domain menu item from Computer to display and perform functions on a different domain.

To use the Server Manager for another domain, you must be logged on to a user account that is a member of the Administrators, Domain Admins, or Server Operators group for that domain. Certain functions require that you are a member of the first two groups only.

If using Server Manager to perform functions on a Windows Server workstation, you must be logged on to a user account that is a member of the Administrators or Power Users group for that workstation.

Additional Security References

For more information on Windows Server security, see

- *Windows Server Concepts and Planning Guide*
- *Windows Server System Guide*
- Online documentation
- Online help text

Setting Date and Time

FileNet software uses the system date and the system time for scheduling and timestamping events. For example, a deferred print job executes at the scheduled system date and time according to the clock on the server. While waiting in the print queue, the job shows the submission time according to the clock on the workstation from which it was submitted. If the server clock and the workstation clock are not synchronized, the print job may print sooner or later than you expect.

As the system administrator, you are responsible for setting the clocks on all FileNet servers to the same date and time. (The PC coordinator is responsible for setting workstation clocks.)

Refer to your *Windows Server System Guide* for details.

Note For the year 2000 and above, make sure the date format is set to display yyyy for the year. For example, select the mm/dd/yyyy format in the Date tab from the Regional Settings icon of the Control Panel.

Disabling NCH Broadcasts

MultSv

The Network Clearinghouse (NCH) shared library locates distributed resources in the FileNet system when requested by a client (user or application program). In multiple server configurations, the NCH server software runs on the root server. Non-root IS servers must find the IP address for the NCH server to retrieve location and attribute information for other servers. For example, cache services accesses the NCH database for information about caches configured on a server.

NCH attempts to find the NCH server first by broadcasting on each available server network interface. In making these lookup attempts, servers always generate broadcast packets, even if the NCH server was not reachable using broadcasts. You can disable NCH server location broadcasts to reduce broadcast traffic on the network. You can enable or disable NCH broadcasts without restarting the FileNet software because NCH checks whether broadcasts are enabled or not on each lookup.

You may want to disable NCH broadcasts if:

- You want no broadcast activity on the networks.
- You have routers between servers.
- You want to force a multi-homed server to use a specific IP address configured by the operating system network directory search faclity.

If NCH broadcasting is disabled and NCH needs to locate the NCH server for a requested domain, NCH resorts to a secondary method. NCH converts the domain name to an IP host name (<domain>–<organization>–nch–server) and attempts to get an IP address for that IP host name using the server's name resolution mechanism. You must create an entry (typically an alias entry) for the IP host name.

Converting to IP Host Name

NCH converts domain names to IP host names by making the following changes:

- Eliminating all characters except for ASCII alpha-numeric characters and hyphens
- Converting all characters to lower case
- Inserting a hyphen between the domain and organization names
- Appending the string “–nch–server”

The following is an example of NCH domain to IP host name conversion:

NCH Domain Name	IP Host Name
Accounts_Payable:BigBank	accountspayable–bigbank–nch–server

Creating the Alias Entry

You need to create an alias entry for the IP host name, using your server name resolution mechanism (gethostbyname), which may involve one of the following methods:

- Edit the hosts file on each server.

  In this example, the directory name containing the hosts file is WINNT35\system32\drivers\etc, but it may be set up differently on your system.

- Edit the master hosts file and use Network Information Service (NIS) to distribute this information to each server.

- Provide this information through the Domain Name Service (DNS).

An example of an entry in the hosts file, where ServerName is the name of the server and accountspayable–bigbank–nch–server is the added alias, is as follows:

135.01.02.0 ServerName accountspayable–bigbank–nch–server

You can use the nch_tool, findserver, to locate a server, for example:

findserver domain:organization

Disabling NCH Broadcast Procedures

To disable NCH broadcast packets, use the Registry Editor, REGEDT32, to add a new IS registry key value:

1. Open the Windows Registry Editor window by entering the following command at the DOS prompt:

   REGEDT32

Note You can also enter the above command in the taskbar Run dialog box.

2. Select the IS registry key in:

   HKEY_LOCAL_MACHINE\SOFTWARE\FileNet\IMS\CurrentVersion

3. Add to this IS registry key a new value, NCHBroadcast, of data type, REG_DWORD.

   Select Add Value from the Edit folder.

4 The Add Value dialog box displays.

a In the Value Name field, enter:

NCHBroadcast

b Select the data type, REG_DWORD, from the Data Type pull down menu.

c Click OK.

5 The DWORD Editor dialog box displays.

a In the Data field, enter zero: **0**

b Select Decimal in the Radix field.

c Click OK.

6 Once completed, the new value looks like the following example:

NCHBroadcast:REG_DWORD:0

7 Create the alias entry.

See **“Creating the Alias Entry” on page 49**.

Viewing Image Services Text Files

You may need to read Image Services text files found on the IS software distribution media for installation instructions or you may want to view or edit Enterprise Backup Restore (EBR) ASCII sample text script files. Image Services text files may be in UNIX or MS DOS format and you cannot readily determine which format has been used.

We recommend you use the **WordPad** editor when you want to view or edit any IS text files. WordPad handles IS text files in both MS DOS and UNIX formats. Do not use the Notepad editor because Notepad cannot handle text files in UNIX format. Notepad displays UNIX text files as continuous, run-on text because it cannot interpret UNIX text files that do not contain a Control M character at the end of each line.

Environment Variables

The System dialog box displays your environment variables as well as the current system environment variables. You should not have to set an environment variable. If you installed Image Services software in directories other than the default directories, the FileNet Setup program automatically sets up the required differences.

For specific information, refer to your *Windows Server System Guide*.

Databases

FileNet databases and their associated recovery logs include the MKF databases: transient, permanent, and security. The index database may contain index tables, WorkFlo queues, and VWService tables.

Windows Server maintains a separate database called the **Registry**. The Registry contains system configuration information, third-party configuration information, security information, and user environment profiles.

The Registry eliminates the need for the configuration files CONFIG.SYS, AUTOEXEC.BAT, LANMAN.INI, WIN.INI, and PROTOCOL.INI. Windows Server, however, retains these files to support Windows 3.1 applications that use these files. The FileNet Image Services is a 32-bit Windows Server application that does not use CONFIG.SYS, AUTOEXEC.BAT, or any of the .INI files.

Note The Registry database **must** be backed up daily with the other databases or immediately after security or configuration changes.

Windows Server File Systems

FileNet software resides in the Windows Server File System (NTFS). The Windows Server system contains other file systems, such as File Allocation Table (FAT) and High-Performance File System (HPFS).

The NTFS supports Windows Server security, keeps a log of all magnetic disk activities, supports file and directory names up to 256 characters, and supports extended file attributes. For information on the advantages and characteristics of the NTFS, refer to your *Windows Server System Guide.*

Directories & Files

The next topics explain navigation through the directory structures, file organization, and file naming.

Directories

A directory is a collection of files in a subdivision of your magnetic disk. FileNet software may be installed in any directory.

The directories \fnsw, \fnsw_loc, and \fnsw\dev\1 are the FileNet default directories. FileNet Image Services software is installed in the \fnsw directory. The \fnsw_loc directory contains Oracle control files and site-specific data such as configuration files and log files. Files under the \fnsw\dev\1 directory contain data files residing in cache, the permanent database, the transient database, the security database, and the index database.

Although FileNet software may be installed in the directory of your choice, we recommend that you use the default directories.

Note Examples in this manual use the default directory names: \fnsw, \fnsw_loc, and \fnsw\dev\1.

Root Directory

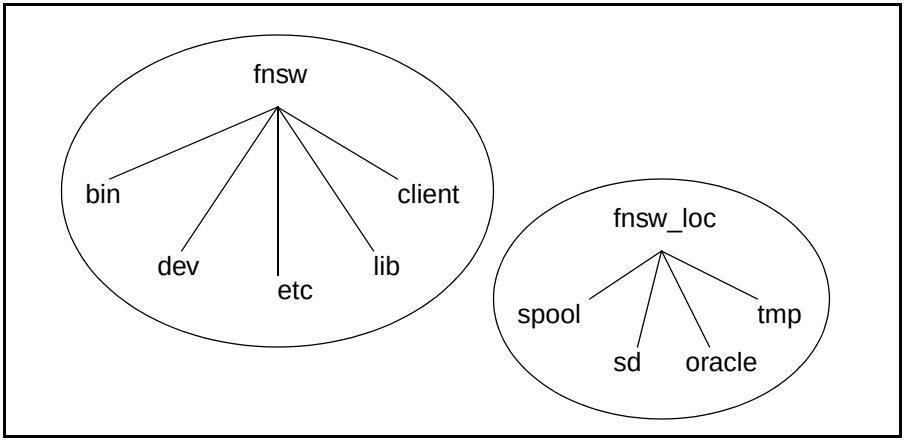
The root directory is the highest level directory on a disk. All subdirectories and files on that disk are below the root directory in the hierarchy. A single backslash (\) designates the root directory.

All paths are relative to a drive letter on your system. The \fnsw tree is located under one drive letter. The \fnsw_loc tree may be located under the same logical drive or a different drive than the drive where \fnsw is located.

Subdirectories

To organize files, the operating system allows you to place directories under root, to further divide those directories into another level of directories, and so on. This subdirectory structure is a top-down hierarchy that resembles a typical organizational chart, with root as the permanent head.

The following diagram shows how a typical FileNet system directory structure is laid out.



FileNet Directory Structure Example

Listing the Contents of a Directory

Use the **File Manager** to list the contents of a directory. See the Windows Server documentation for options and other usage information.

File and Directory Names

One advantage of using the NTFS for FileNet software is file naming conventions. Longer file and directory names and special characters are allowed. A file or directory name can have up to 256 characters.

For files that may be transferred to PC workstations or DOS-based file servers, we recommend that you observe the DOS file-naming conventions.

For details about file and directory naming conventions, refer to your Windows Server documentation.

File Systems

The Image Services Windows server is an integrated set of file systems that appears to you as one large file system. The file systems include:

- Windows Server file systems\WINNT35
  \ (root)
  \tmp
- FileNet file systems\fnsw
  \fnsw_loc
  \fnsw\dev\1
- RDBMS file systems\usr\oracle
  \fnsw_loc\oracle\control0

All of these directory trees may be located on separate logical drives.

File System Locations

Unless designated otherwise, the FileNet software resides in the default directories \fnsw and \fnsw_loc and in subdirectories of \fnsw. At installation time, the operating system recognizes the FileNet file system by its path. We recommend that FileNet software be installed in the default directories.

Accessing File Systems

Use the File Manager to list directory and file information, including file name, file type, file size, and last modification date.

Setting File Permissions

See **“Security” on page 43** for information on setting file permissions. See **“Creating a User Account” on page 42** for information on setting up new user accounts.

Disk Administration

Use the Disk Administrator program to manage disk resources, including creating volume sets to more effectively use available free space on a disk. The Disk Administrator is located in the Administrative Tools folder. You must be a member of the Administrators group to use the Disk Administrator.

Refer to the *Windows Server System Guide* for instructions to:

- Partition your disk
- Create or delete volume sets
- Extend volumes and volume sets
- Create or delete stripe sets
- Create or delete stripe sets with parity
- Establish and break mirrored sets
- Recover data

Problem Solving

Each system has an individual profile. If you check your system frequently, you will become familiar with your system’s workload and average processing times. If the system seems slow or other problems

occur, you may examine the current processes through the Task Manager, Performance Monitor, and the Event Viewer.

Task Manager

The FileNet Task Manager indicates the software state, lists the current processes, monitors Event logs, and reports RPC (Remote Procedure Call) activity.

Performance Monitor

The Windows Server Performance Monitor is a graphical tool that provides detailed information for performance tuning and capacity planning. Functions are represented by icons. When an icon is clicked, the information line at the bottom of the screen displays the function.

The Performance Monitor can measure system responsiveness and track use of system components to aid in determining the cause of performance problems. Functions of this tool include:

- Charting and logging current activity
- Setting alerts on current activity
- Creating reports on current activity

Event Viewer

The Windows Server Event Viewer monitors various types of events in the system, such as errors, warnings, informational events, and successful and unsuccessful security access attempts. Events are recorded in logs and may be generated by the Windows Server system, services, and application, or through audited user activity.

When you start your Windows Server system, event logging starts automatically.

For details on the Performance Monitor and the Event Viewer, refer to the *Windows Server System Guide*.

2
Tape Support

This chapter describes the FileNet-supported tape media and tape drives for use with FileNet applications, such as the Cache Backup Program and CSM_exim, on the Windows server. Other tape-related information needed in preparing and using tape media is also presented. See your server hardware manuals for more information about data compression and tape capacity.

Supported Tape Media

The table on the next page lists the FileNet-supported tape media on the Windows server for FileNet backup and restore using the Cache Backup Program and CSM_exim.

Note If you are using Windows Server Backup or another third-party backup product, check with your software vendor for information on the type of tape media supported by that product.

Supported Tape Media on Image Services for Windows Server

Tape	Used For	Description	Uncompressed Tape Capacity	Compressed Tape Capacity
DAT	Backup/Restore (Cache Backup, CSM_exim)	60 meters, 4mm	1.3 GB	Approximately 2.6 GB
DAT	Backup/Restore (Cache Backup, CSM_exim)	90 meters, 4mm	2 GB	Approximately 4 GB

Supported Tape Media on Image Services for Windows Server, continued

Tape	Used For	Description	Uncompressed Tape Capacity	Compressed Tape Capacity
Exabyte 8mm	Backup/Restore (Cache Backup, CSM_exim)	15 meters, 8mm	650 MB	Approximately 1.3 GB
Exabyte 8mm	Backup/Restore (Cache Backup, CSM_exim)	54 meters, 8mm	2.322 GB	Approximately 4.644 GB
Exabyte 8mm	Backup/Restore (Cache Backup, CSM_exim)	112 meters, 8mm	5 GB (maximum)	Approximately 10 GB
QIC	Backup/Restore (Cache Backup, CSM_exim)	¼-inch cartridge	500 MB	N/A

Supported Tape Drives

This section describes the FileNet-supported tape drives for use with FileNet applications.

8mm Tape Drive

Many FileNet Image Services users purchase an 8mm internal tape drive. The regular capacity 8mm tape drives compress data and can back up nearly 10 GB of compressed data. (FileNet images are already compressed and will not compress further.) The earlier tape drives that do not compress data only write about 5 GB of data. Tape capacity is a function of the tape drive model and whether or not compression is used.

The 8mm tape drives back up approximately 1 GB per hour. The drive initially takes a few seconds to perform diagnostics. However, the diagnostics, including the tape writes and reads, increase confidence in the drive's reliability.

Enabling/Disabling Data Compression

Usually the current model 8mm tape drives can read uncompressed tapes from the older model drives. However, the reverse is not true—the older drives cannot read tapes written by the current drives if the data is compressed (the default). If you have the half-height (1-inch) 8mm tape drive, compression is **on** by default. If you have a mix of new and older tape drives and prefer that tapes be interchangeable, be sure to **disable** compression on the new tape drives.

Recommended Exabyte Tape and Cleaning Cartridge

FileNet recommends **Exabyte** 8mm tapes. If you purchase any other brand, make sure it is data quality. Do not attempt to use the lower-quality tapes intended for video recording.

In addition, we strongly suggest that you purchase and use a cleaning cartridge. Order an Exabyte One 12 Pass Cleaning tape using FileNet part number 2900049-902 or Exabyte part number 727386.

DAT 4mm Tape Drive

The Digital Audio Tape (DAT) drive that uses the Digital Data Storage (DDS) format is supported on Image Services for Windows Server. This tape drive uses a 4mm cartridge and can back up approximately 2 GB (maximum) of data per tape. If compression is enabled, tape capacity ranges from 2 GB to 4 GB.

QIC (¼-Inch Cartridge) Tape Drive

The QIC tape drive is also supported on Image Services for Windows Server. It backs up approximately 500 MB of data per tape.

3
Backup

Introduction

This chapter describes the process to back up Image Services on the Windows Server operating system using one or both of the following:

- Windows Server Backup utility

  Use the Windows Server Backup utility to back up your entire system, including FileNet datasets, the index database, transaction logs, and cache. Windows Server Backup can also be used to restore your system.

- FileNet Cache Backup program

  Use the FileNet Cache Backup program to back up cache objects that have not been written to storage media (optical disks). This may be desirable if you have a large cache or no storage media. In conjunction with using Cache Backup, you must also use the Windows Server Backup utility to back up FileNet file system datasets, FileNet MKF databases, recovery logs, the index database, and configuration files. You can restore cache with Cache Backup if you backed up cache with Cache Backup.

You can back up Image Services using other third-party tools. However, FileNet recommends, tests, and uses the Windows Server Backup utility as the primary tool to back up the FileNet IS.

Note If you need to restore MKF databases, your index database, or recovery logs, your support representative will help you perform the restore procedure.

We assume that you have some familiarity with the FileNet system and with your RDBMS environment. Procedures in this chapter do not address backup of the Windows Server operating system. Refer to your Windows Server manuals for information on backing up and restoring your operating system.

Backup Methods Available

The Windows Server Backup utility and FileNet's Cache Backup program are the backup methods available on Image Services for Windows Server.

Windows Server Backup Utility

The Windows Server Backup utility is part of the standard Windows Server System Administrator interface and is accessed by choosing the Backup icon in the Administrative Tools folder. Windows Server Backup can also be run from the command line using a script. It can only be run when FileNet software, including the RDBMS database, is **shut down**. Windows Server Backup requires that the file being backed up is not open for writing by another application.

If your databases are not extremely large, we recommend that you back up your entire system daily using the Windows Server Backup

utility. You will have only one backup operation and will not need to use the FileNet Cache Backup program.

Note FileNet recommends that you use the Windows Server disk mirroring capability or the disk striping with parity capability. These capabilities greatly reduce the need for restores. Refer to your *Windows Server System Guide*.

If your databases are extremely large and backing up your entire system at one time is not feasible, you can selectively back up your critical databases with the Windows Server Backup utility. This can be done in one of two ways:

- Select the Backup icon in the Administrative Tools folder and choose only your critical databases to back up.
- Write a backup script that uses a batch file to execute the Windows Server Backup utility from the command line for selected databases. See **"Using the NTBACKUP Program from the Command Line" on page 116** for an example of a backup script.

The Windows Backup user interface displays each volume, both local and remote, as an icon. You may select for backup volumes that have FAT (File Allocation Table) or NTFS (Windows Server File System) file systems.

Use the Windows Backup utility to back up the critical Windows Server Registry. The Registry database contains system configuration information, third-party configuration information, security information, and user environment profiles.

If you are using Windows Backup to back up cache, then you must back up the entire cache file. If more than one cache file is on the system, **all** cache files must be backed up. If one large cache file is on

the system with only a few documents in the cache file, the Windows Backup utility still backs up the entire file.

Note While Windows Server Backup supports incremental backups of your Windows file system, all of your IS database and cache files must be backed up in their entirety each time you back up the Image Services software. For that reason the Windows Server Backup incremental feature is not useful for backing up the IS software.

What to Back Up

Windows Server Backup performs a **full offline** backup of the files and directories that you select. Include the following in your backup:

- \fnsw\dev\1 directory
  - MKF databases
  - MKF recovery logs
  - RDBMS database
  - RDBMS online redo logs or transaction logs
  - Cache
- Oracle control files
- Oracle archived redo logs (if you have Oracle archiving turned on) or Microsoft SQL Server archived/backed up logs
- Registry database
- \fnsw_loc directory

Terminology

An RDBMS refers to its transaction logs and the method of moving the backed up logs to a different location by various names. This manual uses the terms redo logs, archiving redo logs, and archive logs for Oracle transaction logs. This manual uses the terms transaction logs, archiving transaction logs, and archived transaction logs for Microsoft SQL Server transaction logs.

Microsoft SQL Server generally uses the term backing up or dumping (backed up) transaction logs for archiving.

Example Files to Back Up

The following list illustrates examples of files in the default \fnsw\dev\1 directory. Because the location of each database is user-configurable, the path of your directories and files may differ from this list. Also depending on how your caches and index database are configured, you may have additional cache files and RDBMS database files.

\fnsw\dev\1\cache0
\fnsw\dev\1\oracle_db0
\fnsw\dev\1\oracle_sys0
\fnsw\dev\1\oracle_rl0
\fnsw\dev\1\ms_db0.mdf
\fnsw\dev\1\ms_pri0.mdf
\fnsw\dev\1\ms_tl0.ldf
\fnsw\dev\1\ms_tmp0.mdf
\fnsw\dev\1\permanent_db0
\fnsw\dev\1\permanent_rl0
\fnsw\dev\1\sec_db0
\fnsw\dev\1\sec_rl0

\fnsw\dev\1\transient_db0
\fnsw\dev\1\transient_rl0

Oracle archived logs and control files are located in the \fnsw_loc directory:

\fnsw_loc\archivelogs
\fnsw_loc\oracle\control0
\fnsw_loc\oracle\control1

Microsoft SQL Server archived logs are located in:

MSSQL\archivelogs\

For Microsoft SQL Server archived transaction logs, add the location of the dump device so that the transaction logs are archived daily as part of the backup routine. For Oracle archived redo logs, the location is defined in Archive Log Destination in the Configuration Editor.

For a list of Microsoft SQL Server databases to back up, refer to **“Backing Up Microsoft SQL Server Databases” on page 89**.

Execute a full backup of the above files and directories before and after an upgrade. Otherwise, back up as recommended in the table, **“Overview of Databases and Caches” on page 82**.

Finding Location of Files

Use the following method to obtain location information on individual databases and logs. (Be sure to scroll to the right of the screens to view all available information.)

Click the Configuration Editor icon or run the fn_edit tool from the command line.

- Check Read Only on the main screen and click OK.
- Click Datasets to view the location of caches, databases, MKF recovery logs, and Oracle redo logs or Microsoft SQL Server transaction logs.

FileNet Cache Backup Program

The FileNet Cache Backup program enables you to selectively back up only those cache objects that have not been written to storage media. In addition to using Cache Backup, you need to use the Windows Server Backup utility to back up FileNet MKF databases, recovery logs, the index database, Oracle control files, and configuration files.

Note Cache Backup does not allow you to select, for backup purposes, fast batch objects in page_cache. Cache Backup sees fast batch objects, but does not select them for export. So, if you are scheduling to back up some COLD objects only, the “Objects scheduled so far” value will read 0 because COLD always uses fast batch committal. However, all other locked objects in the cache are selectable and backed up. Cache Backup also exports all items in BES cache and imports them, but it skips all fast batch objects in the page_cache.

To get around this issue, enable the Fast Batch Breakup feature on the System Application Services Tab in the System Configuration Editor. When this feature is enabled, all new fast batch objects can be selected by Cache Backup.

For more information on the fast batch feature, see the Fast Batch Committal section in the ***Image Services System Administrator’s Handbook***.

Users who back up their entire system (including caches) daily with the Windows Backup program do not need to use the Cache Backup program.

You may want to use the FileNet Cache Backup program regularly if you use deferred committal or have a system without storage media. In these cases, you may have numerous large objects in your magnetic disk caches that are not protected against disk failure.

You can perform full backups or interval backups with the Cache Backup Program. A full cache backup copies all the cache objects to tape or disk. An interval cache backup copies only the cache objects that have been modified since the date you specify in the **Backup Only Objects Newer Than** field of the Select Caches and Objects list box. The specified date is the date the cache object was created or last updated. You must perform one full cache backup before you can perform the first interval cache backup. Interval cache backups should be done cumulatively so that a restore consists of restoring the last full cache backup followed by the most recent interval cache backup. If you have an extremely large cache, you may want to perform daily interval cache backups along with weekly full cache backups.

Caches are stored in large files in the Windows Server file system. Each cache file may contain multiple caches and each cache contains different cache objects.

Each cache object is usually one page of a document that has been committed to your system. Cache objects may also contain system objects or user-defined objects that are not committed documents.

Each logical cache contains one type of object. A print cache, for example, contains copies of document pages that are queued for printing.

The following factors may indicate a need for using Cache Backup:

- You are using the deferred committal option.
- You are using a system without storage media.
- You have extremely large caches.
- You are **not** using the Windows Server Disk Mirroring capability to mirror your cache.

If FileNet Cache Backup is suitable for your system, you must back up daily using both FileNet Cache Backup and the Windows Server Backup utility. Your backup operation consists of the following two types of backups:

- Selective back up of your cache objects with the FileNet Cache Backup program.
- Back up databases, recovery logs, Oracle control files, redo/transaction logs, and configuration files with the Windows Server Backup utility.

Cache Backup Operation

To access Cache Backup, you no longer need to log on first through the Application Executive if you have authenticated and cached your IS user logon with your Windows Server logon. See **“Logging on to Your System” on page 33** for more information on caching logon credentials. Select the Cache Backup icon from the FileNet Image Services Applications folder.

CAUTION To restore successfully, the transient database backup must be **synchronized** with the cache backup. This means that the transient database must be backed up immediately before or after cache backup is performed.

If you use both Cache Backup and Windows Server Backup, you will have two tapes (one tape for each backup operation). You cannot append the Cache Backup tape to the Windows Server Backup on one tape or vice versa because the internal tape format used by the Cache Backup program is not compatible with the internal tape format used by the Windows Backup utility. If you want to combine both Cache Backup and Windows Server Backup on one tape, see **"Including a Cache Backup on the Windows Server Backup Tape" on page 76**.

The Cache Backup program creates backup directory files, backup data files, and backup log files as described in the table below. Cache Backup also creates corresponding restore files that are described in the following table.

Files Created by the Cache Backup Program

Type of File	Description of File	Default File Name
Backup directory file	One directory file per cache backup or restore that lists all caches and all cache objects contained on the backup or restore. You may choose a unique prefix for the directory file instead of using the default.	\fnsw_loc\tmp\cbmmddyyyy_nn.dir
Restore directory file		\fnsw_loc\tmp\crmmddyyyy_nn.dir

Files Created by the Cache Backup Program, continued

Type of File	Description of File	Default File Name
Backup data file Restore data file	One data file per cache backed up or restored to tape or disk. You may choose a unique prefix for the data file instead of using the default.	\fnsw_loc\tmp\cbmmddyyyy_nn.<cache_id> \fnsw_loc\tmp\crmmddyyyy_nn.<cache_id>
Backup log file Restore log file	One log file that lists backup and restore activity. The log file is always written to disk. A new log file is created for each backup or restore. We recommend that log files be manually deleted periodically. Archive log files before deletion if important information is in them.	\fnsw_loc\tmp\cbmmddyyyy_nn.log \fnsw_loc\tmp\ crmmddyyyy_nn.log

Cache Backup assigns default names for the backup and restore directory files, the backup and restore data files, and the backup and restore log files.

The default file naming for these files is as follows:

- cb represents a cache backup directory, data file, or log file.
- cr represents a cache restore directory, data file, or log file.
- mmddyyyy is the date of the backup.
- nn represents the number of backups done on a given day.

  For example, cb05011997_01 is the name of the first backup file done on May 1, 1997. Subsequent backups done on that same day will be differentiated by the nn, for example, 02 for the second

backup of the day, up to 99. If more than 99 backups are done in a single day, the number wraps. If you have not removed any of the backup files corresponding to the first 99 backups, you will not be able to do another backup that day.

After selecting cache, the Cache Backup program locates each cache file, caches within a file, and objects within a cache. One data file is kept for each cache that is backed up. Each backup consists of a backup directory and the cache data files.

Note If you wish to execute a program to back up cache objects from the command line, the **CSM_exim** utility uses the same format and is compatible with the Cache Backup program.

What to Back Up – Cache Backup

Cache Backup performs an offline backup of the cache objects that you select. Once the objects are selected, the Cache Backup program locates each cache object.

Cache can contain the following types of objects:

- Uncommitted batches

  Uncommitted batches reside in batch cache. When a batch is committed, the documents move (logically) from batch cache to page cache (also called retrieval cache). Each document remains locked in page cache until the system writes all copies, both local and remote, to storage media.

  The transient database contains information related to outstanding uncommitted batches. If you have outstanding uncommitted

batches, you must back up the transient database at the same time as the batch cache and page cache.

- Committed documents not yet written to storage media

  These documents remain in page cache due to delayed migration or because the system has no storage media.

  The transient database contains information related to outstanding write requests. If you have outstanding write requests, you must back up the transient database at the same time as the page cache.

Select for backup those cache objects that are locked and have not been written to storage media because these objects are not protected from disk failure. In general, back up all locked objects.

You do not need to back up either system print cache or application print cache because print caches contain documents that have already been written to storage media.

FileNet recommends you back up the following cache objects daily:

- All objects in batch cache
- All locked objects in page cache (retrieval cache)
- All locked objects in fillin cache

Including a Cache Backup on the Windows Server Backup Tape

If you use both Windows Server Backup and Cache Backup and want only one resulting backup tape, do the following:

1 Run Cache Backup and place all selected cache objects in a file.

2 Run Windows Server Backup and include these files in the backup:

- File containing the cache objects backed up with Cache Backup
- \fnsw_loc\tmp\<directory_file>
- \fnsw_loc\tmp\<data_file>
- \fnsw_loc\tmp\<log_file>

See **“Cache Backup Operation” on page 72** for a description of these files.

While this strategy results in only one backup tape, additional disk space is required to hold the file containing cache objects. After being included in the Windows Server Backup, the file containing the cache objects should be removed.

Recommended Backup Schedule

Backing up Image Services for Windows Server system consists of the following tasks:

- Daily backup of the Multi-Keyed File (MKF) databases and MKF recovery logs using Windows Server Backup.

  With multiple servers, you can run a backup script on each server and write to each tape drive at the same time. You can also back up both local and remote databases from one server.

- Daily backup of the RDBMS database and the associated online redo logs or transaction logs using Windows Server Backup or a script that you run from the Windows command line.

- Daily backups of the archived redo/transaction logs. Include the location of the archived logs in your Windows Server backup.

- Daily backup of the Windows Server Registry (or Configuration Registry database) using Windows Server Backup or a script that you run from the Windows command line.

- Daily backup of new, uncommitted cache objects using one of the following methods:

  - Windows Server Backup

  - Windows Server Backup using a script executed from the command line

  - FileNet Cache Backup program

  - CSM_exim executed from the command line

- Daily backup of the directory \fnsw_loc, which contains site-specific data (configuration database files and log files), using the Windows Server Backup program. Back up \fnsw_loc after you make a change to the FileNet Configuration Database (CDB) file.
- As-necessary backup of the data dictionary using ddexim.

The \fnsw subdirectories contain crucial data files, such as \fnsw\dev\1. The \fnsw\dev\1 directory contains cache, permanent database, transient database, security database, recovery logs, RDBMS database, and redo or transaction log data files that need daily backup.

You do not need to back up the \fnsw\bin directory because it contains FileNet-generated files, which can be restored easily by reinstalling the Image Services software.

Additional References

We suggest you read **“Before You Begin” on page 80** before performing a backup.

For detailed information on recovering a damaged Oracle index database or redo logs, refer to the following Oracle documents:

- *Oracle7(TM) Server Administrator’s Guide*, or
- *Oracle8(TM) Server Backup and Recovery Guide*

For information on Microsoft SQL Server transaction logs, see **“Microsoft SQL Server Transaction Logs” on page 87**. Also refer to the Microsoft SQL Server Books Online documentation.

Before You Begin

Read this section to learn about FileNet file systems, databases, information related to backing up an MKF database, an index database, maintaining Oracle redo logs, archiving for Oracle redo logs or Microsoft SQL Server transaction logs, and using Image Services backup scripts.

File Systems

Image Services for Windows Server is an integrated set of file systems that appears as one large file system. See **“Windows Server File Systems” on page 53** for a description of the file systems and directories.

To avoid conflicts with other directories, the FileNet IS usually resides under the \fnsw directory on the drive you selected when you installed the Image Services software.

The files under the \fnsw_loc directory contain site-specific data, such as configuration database files and log files. Files under \fnsw_loc must be backed up daily and after you make a change to the FileNet Configuration Database (CDB) file.

Files under the \fnsw\dev\1 directory contain data files residing in cache, the permanent database, transient database, security database, recovery logs, the index database, and redo logs. Files under \fnsw\dev\1 must be backed up daily with the Windows Server Backup utility.

Note The directories \fnsw, \fnsw_loc, and \fnsw\dev\1 are FileNet default names. We recommend that you retain these names. However, if you did rename these directories during the Image Services installation, verify that correct user environment variables were set up in the system path. Examples in this manual use the default directory names.

Databases

FileNet MKF databases and their associated recovery logs include the transient database, permanent database, and security database.

The index database is managed by your RDBMS. This database stores document attributes for query purposes and contains one row for every document on the system. The index database may contain index tables, WorkFlo queues, and Visual WorkFlo tables.

Windows Server also maintains a separate database called the Registry. The Registry is critical to the system.

Databases are backed up and restored with the Windows Server Backup program.

CAUTION The index database and the permanent database must be synchronized. Back up the index database before or after the permanent database is backed up.

The Windows Server Backup program must be used to back up all databases in the following chart.

Overview of Databases and Caches

Name	Type	Contents	Backup Frequency and Method
(Sec_DBn)	MKF Database	The security database.	Daily using Windows Server Backup.
(Perm_DBn)	MKF Database	Address information for each document.	Daily using Windows Server Backup.
(Trans_DBn)	MKF Database	Information on system work in progress (such as batch status, read/write and print requests), images in cache, and cache space available.	Daily, or concurrently with a backup of cache, using Windows Server Backup.
Oracle database (index database)	RDBMS		Daily using Windows Server Backup. The index database must be backed up immediately after the MKF databases to retain synchronization with the permanent database.
Oracle (online) redo logs Archived redo logs	RDBMS	A redo log is a record of changes made to the Oracle RDBMS since the last backup and is used to reconstruct or recover data lost since the last backup. An archived redo log is a copy of the redo log.	Daily using Windows Server Backup.

Overview of Databases and Caches, continued

Name	Type	Contents	Backup Frequency and Method
Microsoft SQL Server databases (index database)	RDBMS		Daily using Windows Server Backup. The index database must be backed up immediately after the MKF databases to retain synchronization with the permanent database.
Microsoft SQL Server transaction logs Archived transaction logs	RDBMS	A transaction log records all changes made to an SQL Server database. Each database has a transaction log that is used during automatic recovery to recover data lost since the last database backup. An archived transaction log is a copy of the transaction log.	Daily using Windows Server Backup.

Overview of Databases and Caches, continued

Name	Type	Contents	Backup Frequency and Method
Windows Server Registry	Windows System Database	System and third-party configuration information, security information, and user profiles.	Daily or immediately following any configuration change using Windows Server Backup. **Note:** To update the Registry, you must have Windows Server Administrator privileges.
	Cache	Documents waiting to be written to storage media and images retrieved from storage media. Letters *a*, *b*, etc. indicate cache files. If the cache contains uncommitted objects, see column right. **Note:** The cache partition size limit is 16 GB and the number of cache partitions supported is 255 to allow for a maximum cache size of almost 4 terabytes or 4080 GB.	Daily using Windows Server Backup. If caches contain very large objects that have not been written to storage media, use the FileNet Cache Backup program (or CSM_exim from the command line). The transient database must be backed up immediately before or after cache backup to retain synchronization with cache.

Backing Up an MKF Database

Use the Windows Server Backup program to back up the permanent, transient, and security MKF databases to tape.

Each MKF database may have one or more associated MKF recovery logs. MKF recovery logs are not archived when filled. When one log is full, recording continues on the next available log. When the available logs are full, recording wraps to the first log—overwriting the contents of the first log.

To avoid losing data, configure recovery logs large enough to cover **two times** the amount of data normally generated between backups and back up on schedule.

Related Restore Issues

When restoring an MKF backup, the Windows Server Backup program copies the data files to magnetic disk. If you included the MKF database and recovery logs in the backup, you can restore the database to the same point in time as the end of the last backup, plus any “spliced in” recovery log updates.

If the recovery log is available on disk, the recovery log will be applied automatically (“spliced in”) to the MKF database after the MKF database has been restored. It is important that you do **not** restore the recovery logs from tape when you restore the MKF database. You want the recovery logs on disk that contain all the changes up to the moment of the crash, not the changes that correspond to the same point in time as the end of your backup.

Note We recommend that you write recovery logs to a disk other than the disk that contains the related database.

Backing Up the Index Database

Use the Windows Server Backup program to back up the index database to tape with the FileNet software and RDBMS database shut down.

You must also back up the Oracle control files each time the index database is backed up. The control files are located in the \fnsw_loc\oracle directory.

Make a full backup of the index database before and after an upgrade. Then back up as recommended in the table **“Overview of Databases and Caches” on page 82**.

Oracle Redo Logs

Archiving Oracle database redo logs is recommended if you wish to recover data up to the moment of the system failure. We recommend you archive the redo logs to a disk other than the disk that contains the Oracle database.

We recommend you back up archived redo logs with your daily backup. If, however, you choose to back up your archived redo logs individually, refer to **“Maintenance Schedule for Archived Oracle Redo Logs” on page 105**.

CAUTION Always back up the \fnsw_loc\oracle directory simultaneously with the index database to retain Oracle control files that match the index database.

Microsoft SQL Server Transaction Logs

Archiving SQL Server transaction logs (referred to as backing up or dumping by Microsoft SQL Server) is recommended if you wish to recover data up to the moment of the system failure. The Microsoft SQL Server supports one transaction log per database, such as the master, tempdb, model, indexdb, and fnusr database. Each transaction log contains data modification information, similar to Oracle's redo logs. You must archive the transaction log for each database.

CAUTION Once the transaction log is filled up, the Microsoft SQL Server does **not** resume writing data to the beginning of the log until the data is archived or backed up. If you have not archived the transaction log, the Microsoft SQL Server **stops** processing to that database. All processing work stops for the affected database and the server displays an error stating that the transaction log is full, for example, SQL Server error 1105.

Use the SQL Enterprise Manager Backup option or an isql command to archive the transaction logs. We recommend you archive the transaction logs to a dump or backup device or disk other than the disk that contains the Microsoft SQL Server databases.

Archiving the transaction logs to a dump device clears the log and frees the log space for other transactions. See procedures in **"Setting Up SQL Server Transaction Logs for Archiving" on page 91**.

Archive each database to the dump device on a regular basis as part of your system backup procedures. After archiving both database and transaction log, you only need to back up the transaction log for each database until the next scheduled SQL Enterprise Manager database backup. We recommend you archive the logs for 2-3 days, then do a full database and transaction log SQL Enterprise Manager backup.

Additionally, you should back up the archived transaction logs with your daily backup. Each day when you perform the Windows Server Backup, include the database and any transactions logs created during the day. Backed up archived logs are copies of the transaction logs that have been backed up to a dump device.

For more information on transaction logs, see the Books Online documentation for SQL Server provided by Microsoft.

Related Restore Issues

Use the Windows Server Backup program to restore the index database.

If you have an Oracle index database, the Oracle control files must correspond to the state of the database. Determining whether or not to restore an Oracle control file depends on the state of the current control file, the current online redo logs, the archived logs, and the data files. In general, if the current Oracle control file is not damaged, you do **not** need to restore the old version.

Should you need archived Oracle redo logs to bring the database up to date, you can apply the logs written between the last backup and the present.

If you apply Oracle redo logs, be familiar with Oracle database recovery techniques and complete the procedure according to the documentation for your version of Oracle. Refer to the Oracle Server Administrator's Guide or Backup and Recovery Guide.

You must execute Oracle Server Manager and the appropriate RECOVER DATABASE command. Restore the database to a specific time within a redo log by applying archived or current redo logs.

Backing Up Microsoft SQL Server Databases

The following table describes all the FileNet-created and SQL Server databases in a Microsoft® SQL Server™ RDBMS and their backup frequency. Unlike Oracle, the SQL Server has many different databases residing in different locations. You should back up the Microsoft SQLServer databases listed in the physical devices column at the same time you do a full backup.

Microsoft SQL Server Databases to Back Up

Database and Type	Logical Devices	Physical Devices	Contents	Backup Frequency
indexdb SQL Server index database. FileNet-created.	fn_data*n*	ms_db0.mdf	Indexing fields, document classes, document indexing status, folder information, SQL user data and WorkFlo queues. (If you have an Application server that contains SQL or WorkFlo Queue services, the SQL user data and WorkFlo queues reside in a separate database on the Application server.)	Daily
	fn_log*n* (log)	ms_rl0.mdf (log)	Transaction log for indexdb database.	The log is backed up with indexdb.

Microsoft SQL Server Databases to Back Up, continued

Database and Type	Logical Devices	Physical Devices	Contents	Backup Frequency
master SQL Server Master Database. Transaction log for master is located on the same physical/logical device as master. SQL Server-created	master	master.mdf msdb.mdf msdblog.mdf (log)	System tables containing information on all databases, devices, SQL Server logins, space allocation, configuration, remote servers and logins, and server error message language. Do not modify this database—see Caution on next page. Transaction log for the msdb database.	Daily. The log is backed up with the database.
fnusr SQL Server User Database is for *full-use customers only.* FileNet-created.	usr_data*n* usr_log*n* (log)	ms_udb0.mdf ms_url0.mdf (log)	Tables containing user-specific data. Also contains System Tables common to each database. Transaction log for fnusr database.	Daily
tempdb SQL Server Temporary Database; located on the master device. FileNet-modified.	tmp_data*n*	ms_tmp*n.mdf*	Working storage and temporary tables.	Daily
model SQL Server Database; located on the master device.			Defaults for creating user databases.	Daily

CAUTION Do **not** modify the Microsoft SQL Server Master database. The SQL Server Master database is configured automatically during installation. If you manually alter the Master database, you may not be able to successfully restore the database.

Setting Up SQL Server Transaction Logs for Archiving

It is important for the System Administrator to set up sufficient transaction log space for the site. Log space requirement can vary depending on factors, such as amount of data processed, applications used, and type of queries. For a complete explanation of factors causing the transaction log to fill up, refer to the SQL Server Administrator's Companion in SQL Server Books Online.

Each Microsoft SQL Server database has one transaction log. If not enough space is allocated for the transaction log, the log becomes full. Once the transaction log is filled up, Microsoft SQL Server does **not** resume writing data to the beginning of the log until the data is archived or backed up. If you have not archived the transaction log, the Microsoft SQL Server **stops** processing to the affected database. You cannot update, delete, or insert to that database. This situation usually results in SQL Server error 1105.

We recommend you make a decision during the installation phase to set up a method for ensuring that the transaction log for each database does not become full without the log being archived or backed up. Set up the recommended method, described below, for archiving each transaction log for the master, indexdb, and fnusr databases.

Recommended Method

The recommended method is summarized below for archiving Microsoft SQL Server transaction logs that have been backed up daily as part of your regular Windows Server backup. We recommend you add a script to the SQL Performance Monitor, which will automatically archive the log to a dump device when the log reaches an established percentage full value.

Note You must always have the SQL Performance Monitor running in the background and remember to restart the SQL Performance Monitor whenever you reboot.

Step	Procedure for Each SQL Server Database
Step 1	Create the SQL Server dump (backup) device.
Step 2	Add the routine of archiving SQL Server databases and the associated transaction logs to the dump device, as part of your regular backup procedures.
Step 3	Create an SQL Server Agent Alert to execute a backup command whenever the log reaches a specified percentage full.

The following steps describe in more detail the recommended method for archiving SQL Server transaction logs:

1 Create the dump device. This is the destination where the archived transaction logs are put, such as another disk drive or to a tape device.

You can have a different dump device for each transaction log and database.

Create the dump device by using one of the following methods.

- Use the Microsoft SQL Server Enterprise Manager.

  In the Enterprise Manager, expand your server in the Tree panel. In your server's Management folder, right-click the Backup item and select "New Backup Device." Enter the Backup Device name and the location of the disk or tape device. Click OK.

- Use the sp_addumpdevice (system stored procedure) command from isql. Use the Search option in SQL Server Books Online to find the syntax information.

  For example, the following command adds a disk device named MYDISKDUMP, with the physical location name C:\DUMPDEV\DUMP10.DAT:

  sp_addumpdevice 'disk', 'mydiskdump', 'c:\dumpdev\dump10.bak'

Tip If you are not backing up to tape, add the backup device location to your regular backup routine for backing up with Windows Server Backup so that the transaction logs are archived daily during your regular backup routine.

2 Archive each database to the dump device by using one of the following methods. Either method archives the entire database and its associated transaction log.

- Use the Microsoft SQL Server Enterprise Manager.

  In the Enterprise Manager, click the Database Backup/Restore option. Click on the Backup tab. Choose the type of backup device, either a disk backup device or tape backup device. Enter the name of the transaction log and the location of the disk device or tape device.

- Use the isql utility. From a Command Prompt window, run isql. Alternatively, you can run the isqlw GUI utility. At the isql prompt, type:

  backup database <database_name> to <dump_device>

  go

3 Create the SQL Server Agent Alert. Follow these procedures to set up the alert settings for **each** database:

a Make sure that the Microsoft SQL Server is running.

b Start the SQL Server Enterprise Manager.

c Select the correct server.

d Select Management.

e Select the SQL Server Agent.

f Right-click on Alert.

g Select New Alert.

h Enter the name of the Alert.

i For Type, select SQL Server performance condition Alert.

j Specify the following for Performance condition alert definition:

- Object: SQLServer:Databases
- Counter: Percent Log Used
- Instance: Select the appropriate database name—for example, appsdb, indexdb
- Alert if counter: rises above
- Value: 75

k On the Response tab, select New Job from the drop-down list. The New Job Properties window displays.

l On the General tab, specify the following:

- Name: <user-specified>
- Category: Database Maintenance
- Owner: sa
- Description: <optional, user-specified>

m On the Steps tab, click on New. The New Job Step window displays.

n Specify the following General properties for the job step:

- Name: <user-specified>
- Type: Transact-SQL Script (TSQL)
- Database: <select the appropriate database name—for example, appsdb, indexdb>
- Command: backup log <database name> to <backup device name>
- After entering the command, click Parse to verify the syntax.
- Click Apply.

o Specify the desired Advanced properties for the job step.

p Click Apply.

q Click OK in the next three windows.

r Start the SQL Server Agent Service via either the Enterprise Manager or the Windows Server Services tool. The agent must start whenever SQL Server starts for the Alert you created to work correctly.

Note When defining an Alert, you also have the option of notifying someone of the backup. If you would like to add this optional feature to the Alert you created, see the SQL Server Books Online for information on adding “Operators.”

Alternative Archiving Method

An alternative method may be used to archive Microsoft SQL Server transaction logs if you choose not to use the recommended method. You can use the SQL Server Enterprise Manager to set up a time interval, specific times on a daily or regular basis, for archiving each SQL Server database and its transaction log.

The alternative method works best if the work load in each database is consistent. If the work load is not consistent, you may have the following problems:

- Peak work loads may cause the transaction log to fill up before the time specified for backup.
- Slow work load times may cause too many unnecessary files to be backed up.

Not Archiving SQL Server Transaction Logs

You may choose not to archive Microsoft SQL Server transaction logs if you have a development or test system, where saving the transaction logs is not necessary. Set Truncate Log on Checkpoint, the database configuration option, to ON. Setting the ON option for a database clears all committed transactions from that database's transaction log.

CAUTION We recommend that production systems archive Microsoft SQL Server transaction logs. Otherwise those systems will lose the ability to recover data up to the point of the system failure.

Enabling Oracle Archive Logging

Some backup and restore strategies require that you enable archive log mode for your RDBMS transaction logs. This section provides an overview of these logs and a procedure for enabling archive log mode.

Archive Logs Overview

Archive logs are copies of the RDBMS transaction logs (for example, the Oracle redo logs). During system installation, you can set a FileNet configuration parameter to enable archive logging, or you can set this parameter at any time using the FileNet System Configuration Editor. The procedure to enable archive logging consists of:

- Configuring the FileNet software for archive logging
- Enabling the RDBMS to write archive logs to a selected directory

When you have enabled the FileNet **and** RDBMS archive logging parameters, your RDBMS can write to these archive logs.

If you choose to archive logs in your system, your FileNet support representative can enable archive logging on your system when your FileNet software is installed and configured. You can also use the procedures in this section to enable archive logging at a later time.

CAUTION Do not randomly turn archive log mode off and on. Doing so may prevent a full recovery of RDBMS databases during a restore. Select the archive log mode necessary for your environment and leave the mode at that setting.

Archiving Oracle database redo logs is recommended if you wish to recover data up to the moment of the system failure.

Archiving Oracle redo logs is optional if:

- you perform offline backups and
- recovering the database by restoring to the last backup is an acceptable level of recovery for your system.

However, archiving the Oracle redo logs is required if you choose to perform online backups.

CAUTION Monitor the Oracle index database regularly. The Oracle RDBMS hangs if insufficient space is available to create the archive log. Be absolutely sure you have enough magnetic disk space to hold the archive logs until you copy them to tape. You can create a file system for this purpose alone. The amount of space you allocate to the archive logs is dependent on daily database activity, such as the number of committals, deletions, and updates.

Enabling Archive Logging Procedures

A FileNet support representative or a qualified System Administrator can perform the following procedure to enable automatic archiving.

1 Log in as fnsw or as a user that is a member of the fnadmin and dba groups.

Oracle commands used in this procedure require Database Administrator (DBA) privileges.

2 If FileNet software is running, click on the **Task Manager** icon in the FileNet Image Services Applications folder and select **Stop**.

Note If you have a site-controlled RDBMS database, you must shut down FileNet software first before you shut down the RDBMS software.

3 Use the **File Manager** to create a directory for the Oracle archive logs.

Verify that you selected a drive different from the drive containing your index database.

The following directory is an example of an Oracle archive logs directory:

\fnsw_loc\archivelogs

4 Enable archiving by doing the following:

a Double click on the **Configuration Editor** icon in the FileNet Image Services Configuration folder.

b Select the correct Database Name and Domain name.

c Select the Relational Databases tab.

d Move the right arrow until you see Log Archive Start.

No is displayed. Click on the pane under this heading to change to **Yes.**

e Under the same tab, move the right arrow until you see Archive Log Destination.

f Click on the pane under Archive Log Destination to enter the directory name you created in step 3. Oracle puts the archive logs in this directory.

Oracle creates the archive logs, names the archive logs using its naming convention, and appends a log sequence number to its prefix name. The following is an example of an archive log name:

\fnsw_loc\archivelogs\ARC00028.001

where ARC is the prefix name, 00028 is the log sequence number, and 001 is the thread number.

5 Select Exit from the File pull-down menu.

A dialog box asks you if you want to save changes. Click Yes.

6 From the command prompt, enter the following command to incorporate your changes:

fn_build –a

7 Start Oracle Server Manager in line mode by entering one of the following from the command prompt:

svrmgr23 if running Oracle Version 7.3.x

svrmgrl if running Oracle Version 8.0.x

The prompt changes to SVRMGR>. Issue the SQL commands in the following steps from this prompt.

8 From the SVRMGR> prompt, log in to Oracle as the database administrator and connect to the database:

connect internal

9 Start the database mounted in EXCLUSIVE mode, but not opened, with the following command:

startup pfile=<drive>:\fnsw_loc\oracle\init.ora mount

where <drive> represents the drive, for example c:, where the directory is located.

Oracle Server Manager returns messages similar to the following:

```
Oracle instance started.
Database mounted.
```

10 Verify **Archive destination** and Automatic archival settings.

Archive destination must be set to the path you established in the Configuration Editor and automatic archival must be enabled. Enter the following command to verify this information:

archive log list

Based on the examples used here, Oracle Server Manager returns information similar to the following:

```
Database log mode              Archive Mode
Automatic archival             ENABLED
Archive destination            c:\fnsw_loc\archivelogs\ARC00017.001
Oldest online log sequence     16
Next log sequence to archive   17
Current log sequence           17
```

11 Change the log mode if necessary. Otherwise, skip to **Step 14 on page 104**.

Several log mode setting combinations are possible in the output of the archive log list command. Depending on the settings that exist on your system, different actions are required.

Use the following table of settings and actions to establish the correct environment for archive logging on your system.

Archive Log State	Action
Database log mode = No Archive Mode Automatic archival = DISABLED	With the database mounted EXCLUSIVE and not open, issue the command: **alter database archivelog;** followed by: **alter system archive log start;**
Database log mode = No Archive Mode Automatic archival = ENABLED	With the database mounted EXCLUSIVE and not open, issue the command: **alter database archivelog;**
Database log mode = Archive Mode Automatic archival = DISABLED	At any time, with the database open or closed, mounted or unmounted, issue the command: **alter system archive log start;**

12 Verify the database log mode and automatic archival:

archive log list;

Your settings should be Database log mode = Archive Mode and Automatic archival = ENABLED.

13 Open the database with the following command:

alter database open;

14 Shutdown Oracle and exit Oracle Server Manager:

a From the Oracle Server Manager prompt, enter:

shutdown normal

The following message confirms the shutdown:

Database closed
Database dismounted.
Oracle instance shutdown.

b Exit Oracle Server Manager with one of the following command* at the SVRMGR> prompt:

SVRMGR> **exit,**
or
SVRMGR> **quit**

Note Before you restart Oracle, make sure your Oracle parameter file, init.ora, is set to automatically start archive logging. Restarting Oracle reinitializes the Oracle instance with the settings in init.ora, which may not be set for automatic archiving. To verify the correct setting, change to the directory that contains your Oracle parameter file, init.ora, and enter the following command to display the contents of the file.

type init.ora

You can also use Notepad or a text editor to display file contents.

Check for the setting LOG_ARCHIVE_START=TRUE in the parameter file. If the parameter is set to false, rerun steps 3 through 6. For more information on the Oracle parameter file, see your *Oracle7(TM) Server Administrator's Guide* or *Oracle8(TM) Server Backup and Recovery Guide*.

15 Restart FileNet software by clicking on the Restart button in **Task Manager** (in the FileNet Image Services Applications folder).

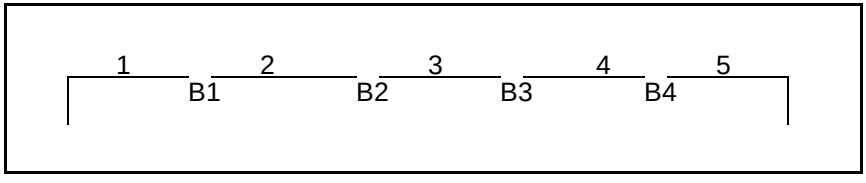
Note Start the RDBMS database first, if you have a site-controlled RDBMS database, **before** starting FileNet software.

16 Perform a backup of the Oracle database for which you have enabled archive log mode.

Maintenance Schedule for Archived Oracle Redo Logs

After you or your support representative sets up automatic archiving with the Configuration Editor, you are ready to set up a maintenance schedule for your Oracle redo logs. Regular maintenance means copying sets of your redo logs to tape and deleting those same logs from your magnetic disk. Strict observance of the maintenance schedule you set up preserves your redo logs safely on tape and frees valuable disk space.

The following describes a suggested maintenance schedule. You can set up a similar schedule, tailored to suit your needs.



Each **number** represents the interval of time between backups of datasets. Each number also represents a set of archived Oracle redo logs occurring within that interval.

Each **B** represents a backup of the datasets. Each B also represents at least one redo log that was automatically closed and archived.

The following table suggests a program to back up redo logs to tape and safely delete the appropriate redo logs from the magnetic disk. Use Windows Server Backup to selectively backup the redo log files.

Schedule to Back Up Archived Oracle Redo Logs

Redo Logs Backed Up	Redo Logs Deleted From Disk	Redo Logs Remaining On Disk
Interval 1, B1		Interval 1, B1
Interval 2, B2		Interval 1, B1 Interval 2, B2
Interval 3, B3		Interval 1, B1 Interval 2, B2 Interval 3, B3
Interval 4, B4	Interval 1, B1	Interval 2, B2 Interval 3, B3 Interval 4, B4
Interval 5, B5	Interval 2, B2	Interval 3, B3 Interval 4, B4 Interval 5, B5

As illustrated in the preceding table:

- Back up (copy to tape) Interval 1 and B1, leaving Interval 1 and B1 on the magnetic disk.
- Back up Interval 2 and B2, leaving Intervals 1, 2, B1, and B2 on the magnetic disk.
- Back up Interval 3 and B3, leaving Intervals 1, 2, 3, B1, B2, and B3 on the magnetic disk.
- Back up Interval 4 and B4. Delete Interval 1 and B1 from the magnetic disk. Intervals 2, 3, 4, B2, B3, and B4 remain on the magnetic disk.
- Back up Interval 5 and B5. Delete Interval 2 and B2 from the magnetic disk. Intervals 3, 4, 5, B3, B4, and B5 remain on the magnetic disk.

If you implement and follow a schedule similar to the example, you always have three previous intervals of redo logs on the magnetic disk as well as a tape backup of those same redo logs.

Using Image Services Backup Scripts

If you use the Windows Server Backup program, you can run a backup script from the command line instead of using the Windows Server interface. Command-line execution requires a batch file to execute the Windows Server Backup. The batch file must specify directories of all FileNet database files, Oracle control files, and specific directories in the FileNet directory structures that contain valuable data files.

For details, refer to **“Using the NTBACKUP Program from the Command Line” on page 116**.

Using CSM_exim

If you use the FileNet Cache Backup program, you may execute CSM_exim (a different but compatible program) from the command line to accomplish the same purpose. CSM_exim backs up your cache objects using the same format as the Cache Backup program. You can perform a cache backup with CSM_exim and restore that backup with Cache Backup, or vice versa.

CSM_exim requires 10 bytes of memory for each object to be backed up. If the number of cache objects to be backed up is very large (for example, millions of objects), CSM_exim may fail with an out-of-memory error during backup attempts. In this case, consider using the Cache Backup program, which does not have this memory constraint.

Other Topics Relating to Backup

The following are other topics relating to Backup.

Authorized Users of Backup Programs

Windows Server provides built-in groups that determine the functions their members may and may not perform. Members of the following three groups can perform backup and restore functions:

- Administrator
- Server Operator
- Backup Operator

Any one of these local groups may contain user accounts and global groups from the same domain and from trusted domains. This means that a user from a different domain, but a member of one of these

groups, can back up and restore the server. Also see **“Looking at Windows Server Groups” on page 44** for more information on groups used for specific FileNet purposes.

Administrator Group

Members of the Administrators local group have more permissions than any group in the domain. Normally this group supervises configuration of the domain and the domain servers.

Server Operator Group

Server Operator group members manage the domain servers. In addition to backing up and restoring server files, a member can lock and unlock servers, format the fixed disk, change system time, create and manage shared printers and shared directories, as well as many other system functions.

Backup Operator Group

In addition to backing up and restoring directories and files from the server, Backup Operator group members may log on and shut down servers. For details on managing groups and users that have backup and restore privileges, refer to the *Windows Server System Guide*.

Data Dictionary

The **data dictionary** refers to the document class, index, storage media, and WorkFlo queue definitions on your FileNet system. These definitions are stored in the index database. Using **ddexim** (data dictionary export/import tool), you can export this information to an ASCII file and store the information in \fnsw_loc as a backup. To be effective,

export the data dictionary every time you create or change a new or existing index and document class.

Under normal circumstances, you could use the data dictionary to initialize another system. However, if a disk failure occurs at a time when you do not have a good backup, you can reinitialize your system, import the data dictionary, then import your storage library. This recovers documents as they were when first committed.

Tape Retention and Storage

If you do full backups daily, retain at least one week (seven generations) of backup tapes. Store backup tapes in an environment protected from extreme heat or cold, magnetic interference, and other factors that would adversely affect them. Consider periodically storing full backups at another site to safeguard your backups in the event you need to recover from a disaster.

Using Windows Server Data Integrity Options

FileNet highly recommends that you use the Windows Server disk mirroring capability or the disk striping with parity capability. If, for example, you are using disk mirroring, you may never need to restore a backup tape unless both disks of a mirrored pair failed simultaneously.

Disk mirroring allows better overall read/write performance than disk striping with parity. Additionally, performance does not decrease when a member of the mirrored set fails. Expense, however, must include the cost of duplicate disks.

Disk striping with parity permits better read performance than disk mirroring. Read performance, however, is degraded if one partition in the

set fails. Write performance is generally reduced. Disk striping with parity is recommended for a majority of read-only applications.

Note Although rare, the potential for simultaneous loss of all mirrored disks suggests a need for performing regular backups in addition to disk mirroring.

Consult the *Windows Server Concepts and Planning Guide* for more information on disk mirroring and disk striping with parity.

Backing Up Your System

This section describes how to use the NTBACKUP program through the Windows interface and from the command line with a batch file.

Using the NTBACKUP Program

The following procedures describe using the NTBACKUP program through the Windows Server interface. You must shut down the FileNet software, including the RDBMS database, before using the NTBACKUP program. The procedures assume you have **FileNet-controlled** databases. Where a procedure differs due to a **site-controlled** RDBMS database, that procedure will be called to your attention.

If you wish to use a backup script, refer to **“Using the NTBACKUP Program from the Command Line” on page 116**.

1. Log on to Windows Server as a member of the Windows Administrators group and as a member of the fnop or fnadmin group and dba and fnusr groups that can control FileNet software.

Note To back up RDBMS files, you must have read and write permissions on these files. You must be a user with dba privileges.

2 Notify PC workstation users that the FileNet software is going to be shut down for backup or publicize backup times to all users.

3 Shut down the FileNet software using the steps appropriate for your server configuration. All FileNet processes are killed and the MKF databases are shut down. The RDBMS database, if FileNet-controlled, is also shut down.

CAUTION For FileNet-controlled databases, always use the Task Manager to shut down both FileNet software and the RDBMS database. Do **not** use the Microsoft SQL Service Manager to stop the RDBMS. If you do, an error displays because the Microsoft SQL Service is dependent on the IMS ControlService.

Servers must be shut down in a certain order based on server type. Choose one of the procedures in the following table.

Combined Server (Including WorkGroup)	Dual or Multi-Server
1 Click on the Task Manager icon in the FileNet Image Services Applications folder. 2 Select the Task Manager Stop button. 3 Click yes to confirm.	1 On each non-root server in this order: application server, then storage library server. a) Click on the Task Manager icon in the FileNet Image Services Applications folder. b) Select the Stop button. c) Click yes to confirm. 2 On the root/index server: a) Click on the Task Manager icon in the FileNet Image Services Applications folder. b) Select the Stop button. c) Click yes to confirm.

Note If you have a site-controlled RDBMS database, you must shut down the RDBMS software **after** you have shut down the FileNet software.

4 Check file system space and perform the following file maintenance before each backup:

- By default the event logs are in \fnsw_loc\tmp\logs\1. The file name format is elyyyymmdd, where yyyymmdd is the date. For example:

  el19970711

  where:*1997* is the year, *07* is the month, and *11* is the day

- Delete temporary files in \fnsw_loc\tmp\ that you no longer need.

If you need to keep older logs, copy them to tape and then delete them from disk. Older entries are automatically deleted from Oracle logs and the security events logs.

5 Execute Windows Server Backup.

a Select the **Backup** icon in the **Administrative Tools** folder.

b Click the **Drives** icon and select volumes, directories, and files to back up. (For a listing of what to back up, see **"What to Back Up" on page 67**.)

c Insert your tape in the drive with the write-protect off. Wait until the drive light stops flashing.

d Select **Verify After Backup** (optional but recommended) from the Backup Information dialog box.

e Check the **Backup Registry** checkbox. This box is grayed if you are not on the same drive where the Backup Registry is located.

f Specify tape security restrictions (if applicable) by selecting Restrict Access to Owner or Administrator.

g Choose to append or replace existing data on the tape.

h Indicate the type of backup: Normal, Copy, Differential, Incremental, or Daily.

i Specify the log file name and level of log detail.

The default is C:\WINNT\BACKUP.LOG. You may wish to rename (or delete) the log file **before** the backup, so the new log file will not be appended to a lengthy older file.

j Click OK to start the backup.

Refer to the chapter “Backup” in the *Windows Server System Guide* if you need additional information regarding the above steps.

6 When the backup completes, exit Windows Server Backup.

7 Unload the tape and label it with the dataset names, date, and your initials. Write-protect the cartridge and store in a safe place.

CAUTION If the tape drive does not eject the cartridge after a reasonable period of time (15 to 30 seconds after all tape movement has stopped), contact your tape support representative. Do not try to forcibly remove a cartridge. Refer to your tape drive operator’s guide for instructions to load and unload the tapes.

8 Start the FileNet software.

Note Start the RDBMS database first, if you have a site-controlled RDBMS database, **before** starting FileNet software.

Servers must be started in a certain order by server type. Choose one of the procedures in the following table.

Restarting FileNet Software Based on System Configuration

Combined Server (Including WorkGroup)	Dual or Multi-Server
1 Click on the Task Manager icon in the FileNet Image Services Applications folder. 2 Select the Task Manager Start button.	1 On the root server: a) Click on the Task Manager icon in the FileNet Image Services Applications folder. b) Select the Start button. c) Click yes to confirm. 2 On each non-root server in this order: storage library server, then application server. a) Click on the Task Manager icon in the FileNet Image Services Applications folder. b) Select the Start button. c) Click yes to confirm.

In general, application servers are stopped first and restarted last. However, depending on the IS services running on your application server, you may need to change the sequence slightly. For example, if you run index services on an application server, restart that application server immediately after restarting the root/index server.

Using the NTBACKUP Program from the Command Line

Command-line execution requires a batch file to execute the Windows Server Backup program. The batch file is a script that specifies directories of FileNet database files, control files, and specific FileNet directories that contain valuable data files. Use the file \fnsw_loc\sd\ br_ datasets to help you locate critical databases and logs.

Always include the Registry database by using the **/B option** in your backup.

Refer to **“What to Back Up” on page 67**. For details on the NTBACKUP command, refer to the *Windows Server System Guide*. NTBACKUP is the program name of the Windows Server Backup utility.

Usage Notes

Note the following **before executing** the Backup script:

- Verify that NTBACKUP is not active before invoking the program through a script.
- NTBACKUP displays the user interface. The Backup Status dialog box appears, displaying the tape status, the number of directories, files and bytes backed up, recoverable backup errors, skipped files, etc.
- The backup is executed without user input. You may abort the backup at any point by using the Abort button on the dialog box.
- If you do not attach a full path to the log file (as in the examples below), NTBACKUP places the log file in the WINNT\SYSTEM32 directory—not your current directory.
- If the log file you specify already exists, NTBACKUP displays a prompt requiring your acknowledgment.
- If another tape is required, NTBACKUP pauses and prompts you for a new tape.
- Unless you specify the /A option (append to an existing tape), the tape will be overwritten without a confirmation prompt.

Examples

This section presents example backup scripts. The examples assume that:

- \fnsw_loc directory is installed on drive D:
- MKF and index databases are installed on drive E:
- Recovery logs for MKF and redo logs for Oracle are on drive G: in a user-defined directory G:\Recovery\
- Caches are on drive H:

Note Be sure to enter the script as a one-line command with a space between each option, because the script must be executed as one command.

Example 1

This example backs up all Image Services data, including the local Registry and cache. In this example, the directories where the data resides are specified. The command is entered on one line as:

NTBACKUP Backup D:\FNSW_LOC E:\FNSW\DEV\1 G:\RECOVERY H:\FNSW\DEV\ /T NORMAL /L “FN_Log.file” /D “FILENET IMS BACKUP” /B

Note All of the options in the examples can be specified through the Windows Server Backup interface.

Example 2

This example backs up the entire system, including the local registry, if you have the logical hard drives: C:, D:, E:, and F:. If you have tape capacity to back up your entire system, this is the safest procedure.

NTBACKUP Backup C: D: E: F: /T NORMAL /L “Log.out” /B /D “Full Backup”

To verify the backup tape, add the /V option:

NTBACKUP Backup C: D: E: F: /T NORMAL /L “Log.out” /B /V /D “Full Backup”

To create a tape with restricted access, add the /R option:

NTBACKUP Backup C: D: E: F: /T NORMAL /L “Log.out” /B /V /R /D “Full Backup”

To do an incremental backup, change NORMAL to INCREMENTAL:

NTBACKUP Backup C: D: E: F: /T INCREMENTAL /L “Log.out” /B /V /R
/D “Full Backup”

After the backup is complete, check the log file that you designated in the /L option. Verify that NTBACKUP completed without errors.

Using the Cache Backup Program

This section describes using the Cache Backup program through the Windows Server interface. See **“Backing Up Cache from the Command Line” on page 128**, if you wish to use a backup script.

CAUTION To restore successfully, the transient database backup must be synchronized (that is, updated to the same point in time) with the cache backup. You must back up the transient database immediately before or after Cache Backup is performed.

1. Log on to Windows Server as a member of the Administrators group and as a member of the fnop or fnadmin group and dba and fnusr groups that can control FileNet software.
2. Notify PC workstation users that the FileNet software is going to be shut down for backup or publicize backup times to all users.
3. Stop the FileNet software using the steps appropriate for your server configuration.

CAUTION For FileNet-controlled databases, always use the Task Manager to shut down both FileNet software and the RDBMS database. Do **not** use the Microsoft SQL Service Manager to stop the RDBMS. If you do, an error displays because the Microsoft SQL Service is dependent on the IMS ControlService.

Servers must be shut down in a certain order based on server type. Choose one of the procedures in the following table.

Stopping FileNet Software Based on System Configuration

Combined Server (Including WorkGroup)	Dual or Multi-Server
1 Click on the Task Manager icon in the FileNet Image Services Applications folder. 2 Select the Task Manager Stop button. 3 Click yes to confirm.	1 On each non-root server in this order: application server, then storage library server. a) Click on the Task Manager icon in the FileNet Image Services Applications folder. b) Select the Stop button. c) Click yes to confirm. 2 On the root/index server: a) Click on the Task Manager icon in the FileNet Image Services Applications folder. b) Select the Stop button. c) Click yes to confirm.

Note If you have a site-controlled RDBMS database, you must shut down the RDBMS software **after** you have shut down the FileNet software.

4 Put the IS in Backup Mode and start both security and transient databases, on the server(s) where each database is located, using the steps appropriate for your server configuration.

Note The Cache Backup procedure is performed with the Image Services software in Backup Mode. Backup Mode initiates a minimal environment appropriate for running a Cache Backup. The Cache Backup program also requires that both transient and security databases are started up with the fn_util command.

The security and transient databases must be started in a certain order. Choose one of the procedures in the following table.

Selecting Backup Mode and Starting Security and Transient Databases

Combined Server (Including WorkGroup)	Dual or Multi-Server
1 Select the Backup Mode button in Task Manager. 2 Start the security database. At a DOS prompt, enter: **fn_util startsec** 3 Start the transient database. At a DOS prompt, enter: **fn_util starttrans**	1 On the root server: a) Select the Backup Mode button in Task Manager. b) Start up the security database. At a DOS prompt, enter: **fn_util startsec** 2 On all other non-root servers in any order, select the Backup Mode button in Task Manager. 3 On any servers (whether root or non-root) where the transient database is located (where you are backing up cache or where cache services is located): Start the transient database. At a DOS prompt, enter: **fn_util starttrans**

Tip If you wish to leave the Task Manager running, use Alt+Esc or Control+Esc to move between active tasks.

5 If required, log on to the Application Executive from the server where the tape drive is located:

a Log on with an Image Services User Name and Password with System Administrator capabilities.

b Click OK.

6 Select **Cache Backup** from the FileNet Image Services Application folder.

7 Select the cache objects you wish to back up from the **Select Caches and Objects** list box.

The list box displays cache IDs, descriptions, sectors in use and locked, and cache objects in use and locked.

You can select multiple items from the list:

- To select a range of list items, click and hold the mouse button on the first item in the range and click on the last item in the range.
- To select non-contiguous list items, click on the first item. Then hold down the control key and click another list item.

If you need to deselect items, select Refresh from the Options pull-down menu.

You can limit your cache backup by doing the following:

- Select the **Backup Locked Objects Only**.
- Select the **Backup Only Objects Newer Than** and specify a date.

8 If you are backing up to tape, insert your tape in the drive with the write-protect off.

9 Specify the backup destination by selecting the **Tape** or **File** button.

- If you select **Tape**, select the specific tape device in the drop-down list box.
- If you select **File**, use the default name displayed or enter a new file name in the **File** edit box.

10 After verifying that all parameters have been set as you wish on the Cache Backup screen, choose one of the following options:

- Select the **Show Objects** button to preview the list of selected objects to be backed up. **Go to the next step.**

  or

- Click the **Backup** button to start the backup procedure. **Skip to step 12.**

11 If you clicked the **Show Objects button**, Cache Backup displays the number of caches and objects to be backed up in the **Finding Selected Objects** window.

a Click **OK** to display the **Selected Objects Report window** to verify your selections.

The Selected Objects Report displays the following types of information:

- Upper screen: Cache Description, Total Sects., Sel. Sects., Total Objs., Sel. Objs.

- Lower screen: listing of cache objects by SSN, Document, Page, Size, Created/Updated, and Locked fields.

Note You can only display one Selected Objects Report window at a time. Close the window before opening another Selected Objects Report window.

b Click **Close** to exit the Selected Objects Report without backing up and return to the Cache Backup main window.

c Click the **Backup** button in the Cache Backup window to begin the backup procedure.

To return to the Cache Backup main window without reviewing, click **Cancel**.

12 Monitor the backup.

After selecting the **Backup** button, Cache Backup displays the number of caches and objects to be backed up in the **Finding Selected Objects** screen while building temporary catalogs.

Note If your caches are large, more time may be required to build the catalogs. You can cancel the process at any point and return to the Cache Backup main window by clicking Cancel.

a Click **OK** to go to the **Backup Status** screen.

b From the Backup Status screen, select one of the following actions:

- Click **Begin** to start the backup.
- Click **Close** to return to the Cache Backup screen.
- Click **Abort** to terminate a backup in progress.

The Backup Status screen displays completion statistics of the backup in progress in the top section.

The **Summary** section (bottom) indicates the current time and objects being backed up. The final item in the Summary advises “Rewinding and ejecting tape...” However, the tape may have to be ejected manually.

The backup is complete when the **Begin** and **Abort** buttons change to inactive and the Close button changes to active. When the backup completes, you see a completion message in the Summary window:

c When you have viewed the completion results, click **Close**.

d A Cache Backup dialog displays the location of the log. After viewing and recording that information, click **OK**.

13 Eject your tape if you used tape and the tape did not automatically eject. QIC (¼-inch cartridge) tape drives usually do not automatically eject tape.

If tape drive problems occur, Cache Backup presents a dialog defining the problem and requests that you resolve the problem or abort the backup. If tape is in the wrong format, Cache Backup asks you to confirm that you want to reformat and overwrite the tape.

CAUTION If the tape drive does not eject the cartridge after a reasonable period of time (15 to 30 seconds after all tape movement has stopped), contact your tape support representative. Do not try to forcibly remove a cartridge. Refer to your tape drive operator’s guide for instructions to load and unload the tapes.

14 Exit Cache Backup by selecting **Exit** from the **File** pull-down menu.

15 Return to the Task Manager main window.

16 Restart the FileNet software using the steps appropriate for your server configuration**.**

Note Start the RDBMS database first, if you have a site-controlled RDBMS database, **before** starting FileNet software.

Servers must be restarted in a certain order by server type. Choose one of the procedures in the following table.

Restarting FileNet Software Based on System Configuration

Combined Server (Including WorkGroup)	Dual or Multi-Server
1 Click on the Task Manager icon in the FileNet Image Services Applications folder. 2 Select the Task Manager Restart button.	1 On the root server: a) Click on the Task Manager icon in the FileNet Image Services Applications folder. b) Select the Restart button. c) Click yes to confirm. 2 On each non-root server in this order: storage library server, then application server. a) Click on the Task Manager icon in the FileNet Image Services Applications folder. b) Select the Restart button. c) Click yes to confirm.

Restart terminates and starts the Image Services software in a single step.

In general, application servers are stopped first and restarted last. However, depending on the IS services running on your application

server, you may need to change the sequence slightly. For example, if you run index services on an application server, restart that application server immediately after restarting the root/index server.

17 Exit Task Manager by selecting the **File** pull-down menu and choosing **Exit**.

Backing Up Cache from the Command Line

See the cache objects topic in **“Using Image Services Backup Scripts” on page 107** for an overview of CSM_exim, the command line program that is compatible with Cache Backup.

Index