

**DCE 1.2.2 File-Access Administration Guide and  
Reference**

**OSF<sup>®</sup> DCE Product Documentation**

The Open Group

---

Copyright © The Open Group 1997

All Rights Reserved

The information contained within this document is subject to change without notice.

This documentation and the software to which it relates are derived in part from copyrighted materials supplied by Digital Equipment Corporation, Hewlett-Packard Company, Hitachi, Ltd., International Business Machines, Massachusetts Institute of Technology, Siemens Nixdorf Informationssysteme AG, Transarc Corporation, and The Regents of the University of California.

THE OPEN GROUP MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The Open Group shall not be liable for errors contained herein, or for any direct or indirect, incidental, special or consequential damages in connection with the furnishing, performance, or use of this material.

OSF® DCE Product Documentation:

*DCE 1.2.2 File-Access Administration Guide and Reference*

ISBN 1-85912-158-6

Document Number F216

Published in the U.K. by The Open Group, 1997.

Any comments relating to the material contained in this document may be submitted to:

The Open Group  
Apex Plaza  
Forbury Road  
Reading  
Berkshire, RG1 1AX  
United Kingdom

or by Electronic Mail to:  
OGPubs@opengroup.org

## **OTHER NOTICES**

THIS DOCUMENT AND THE SOFTWARE DESCRIBED HEREIN ARE FURNISHED UNDER A LICENSE, AND MAY BE USED AND COPIED ONLY IN ACCORDANCE WITH THE TERMS OF SUCH LICENSE AND WITH THE INCLUSION OF THE ABOVE COPYRIGHT NOTICE. TITLE TO AND OWNERSHIP OF THE DOCUMENT AND SOFTWARE REMAIN WITH THE OPEN GROUP OR ITS LICENSORS.

Security components of DCE may include code from M.I.T.'s Kerberos program. Export of this software from the United States of America is assumed to require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting.

WITHIN THAT CONSTRAINT, permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific written permission. M.I.T. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

### **FOR U.S. GOVERNMENT CUSTOMERS REGARDING THIS DOCUMENTATION AND THE ASSOCIATED SOFTWARE**

These notices shall be marked on any reproduction of this data, in whole or in part.

NOTICE: Notwithstanding any other lease or license that may pertain to, or accompany the delivery of, this computer software, the rights of the Government regarding its use, reproduction and disclosure are as set forth in Section 52.227-19 of the FARS Computer Software-Restricted Rights clause.

RESTRICTED RIGHTS NOTICE: Use, duplication, or disclosure by the Government is subject to the restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 52.227-7013.

RESTRICTED RIGHTS LEGEND: Use, duplication or disclosure by the Government is subject to restrictions as set forth in paragraph (b)(3)(B) of the rights in Technical Data and Computer Software clause in DAR 7-104.9(a). This computer software is submitted with "restricted rights." Use, duplication or disclosure is subject to the restrictions as set forth in NASA FAR SUP 18-52.227-79 (April 1985) "Commercial Computer Software-Restricted Rights (April 1985)." If the contract contains the Clause at 18-52.227-74 "Rights in Data General" then the "Alternate III" clause applies.

US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract.

Unpublished - All rights reserved under the Copyright Laws of the United States.

This notice shall be marked on any reproduction of this data, in whole or in part.



# Contents

---

- Preface . . . . . vii
  - The Open Group . . . . . vii
  - The Development of Product Standards . . . . . viii
  - Open Group Publications . . . . . ix
  - Versions and Issues of Specifications . . . . . xi
  - Corrigenda . . . . . xi
  - Ordering Information . . . . . xi
  - This Book . . . . . xii
  - Audience . . . . . xii
  - Applicability . . . . . xii
  - Purpose . . . . . xii
  - Related Documents . . . . . xii
  - Typographic and Keying Conventions . . . . . xiv
  - Problem Reporting . . . . . xv
  - Pathnames of Directories and Files in DCE
    - Documentation . . . . . xv
  - Trademarks . . . . . xv
- Chapter 1. File-Access Overview . . . . . 1
  - 1.1 What is File-Access? . . . . . 1
  - 1.2 File-Access Configuration . . . . . 4
    - 1.2.1 File-Access Prerequisites . . . . . 4
    - 1.2.2 File-Access Components . . . . . 4
  - 1.3 Basics of File-Access . . . . . 5
    - 1.3.1 Allocating DFS Directories to a Volume . . . . . 6

1.3.2	Accessing DCE from NetWare . . . . .	8
1.3.3	File-Access Users . . . . .	10
1.4	Administrator Tasks . . . . .	11
1.4.1	Tasks Required for the DFS Client . . . . .	11
1.4.2	Tasks Required for the NetWare Server. . . . .	12
Chapter 2.	Starting and Exiting File-Access . . . . .	13
2.1	Starting File-Access . . . . .	13
2.1.1	Starting the Agent Program . . . . .	14
2.1.2	Starting the Gateway Program . . . . .	14
2.2	Exiting File-Access . . . . .	14
2.2.1	Exiting Gateway . . . . .	15
2.2.2	Exiting Agent . . . . .	15
Chapter 3.	Preparations for File-Access Setup . . . . .	17
3.1	Overview of Setup . . . . .	17
3.1.1	Setup Tasks . . . . .	17
3.1.2	Setup Procedures . . . . .	19
3.2	Prerequisites for File-Access Setup . . . . .	22
Chapter 4.	DFS Client Setup . . . . .	23
4.1	DFS Client Setup Procedure . . . . .	23
4.2	Installing Agent and Setting Up the DFS Environment . . . . .	24
4.2.1	Setting Up TCP/IP on the DFS Client . . . . .	25
4.2.2	Setting Up the DCE and DFS Environments . . . . .	25
4.2.3	Setting a Master Key for Gateway Authentication . . . . .	28
Chapter 5.	NetWare Server Setup . . . . .	31
5.1	NetWare Server Setup Procedure . . . . .	31
5.2	Setting Up TCP/IP on the NetWare Server . . . . .	32
5.2.1	File Settings . . . . .	33
5.2.2	Setting TCP/IP Auto-loading . . . . .	33
5.2.3	Important Points . . . . .	33
5.3	Selecting NetWare Users to Use File-Access and Registering Groups . . . . .	33
5.3.1	Selecting Gateway Users . . . . .	34
5.3.2	Registering the NetWare Group . . . . .	34
5.4	Setting Gateway Auto-loading and Exiting . . . . .	34
5.4.1	Gateway Auto-loading and Exiting . . . . .	35

5.4.2	Exiting Gateway . . . . .	35
5.5	Creating a Login Script . . . . .	35
5.5.1	Simultaneous Login . . . . .	35
5.5.2	Creating a Login Script . . . . .	36
5.5.3	Automatic Drive Map Cancellation . . . . .	37
Chapter 6.	Setting up the NetWare Server Environment with Administration Utility . . . . .	39
6.1	Environment Setup Procedure . . . . .	40
6.1.1	Administration Utility Functions . . . . .	40
6.1.2	Setting Up the Environment . . . . .	41
6.2	Administration Utility Startup and Login . . . . .	43
6.2.1	Administration Utility Startup . . . . .	43
6.2.2	Logging into the Administration Utility . . . . .	43
6.3	Administration Utility Operations . . . . .	44
6.4	Environment Setup During Initial Installation . . . . .	46
6.4.1	Registering the Gateway Volume and Setting the Mount Point . . . . .	49
6.4.2	Registering Agent and the Master Key . . . . .	51
6.4.3	Registering Gateway Users and Temporary Passwords . . . . .	52
6.4.4	Registering the Gateway Group . . . . .	55
6.4.5	Setting Options . . . . .	58
6.4.6	Registering Users Who Can Use the Administration Utility . . . . .	60
6.5	Deleting the Gateway Volume . . . . .	61
6.6	Changing the Mount Point . . . . .	61
6.7	Changing the Master Key . . . . .	62
6.7.1	The Master Key Change Procedure . . . . .	62
6.7.2	Important Points . . . . .	62
6.8	Deleting the Gateway User . . . . .	63
6.9	Changing the DCE Username for the Gateway User . . . . .	63
6.10	Changing the DCE Group Associated with a Gateway Group . . . . .	64
Chapter 7.	File-Access Administration and Maintenance . . . . .	65
7.1	Rights . . . . .	65
7.1.1	File-Access Rights . . . . .	66
7.1.2	Users and Groups . . . . .	69

7.1.3	Trustee Rights and Effective Rights . . . . .	69
7.1.4	Rights Mapping . . . . .	73
7.1.5	Restrictions Related to the Use of UFS . . . . .	77
7.2	The Administrator's Tasks When a Failure Occurs . . . . .	78
7.2.1	Collecting Agent Failure Information . . . . .	78
7.2.2	Collecting Gateway Failure Information . . . . .	78
7.2.3	Starting the RAS Utility . . . . .	82
7.3	File-Access Administration . . . . .	83
7.3.1	Impact of File-Access on the System . . . . .	83
7.3.2	File-Access Authentication . . . . .	84
7.3.3	Settings with a Time Limit on the DCE Side . . . . .	85
7.3.4	Directory and Filename Conversion Between DFS and the Gateway Volume . . . . .	85
Appendix A.	File-Access Reference Pages . . . . .	89
A.1	Reference Pages . . . . .	89
	dfaagt . . . . .	90
	setdfakey . . . . .	91



# List of Figures

---

Figure 1-1. How to Access DCE from NetWare via File-Access . . . . .	3
Figure 1-2. Volume Allocation . . . . .	7
Figure 1-3. Process of Accessing DFS Files . . . . .	9
Figure 3-1. Flow of File-Access Environment Setup Tasks . . . . .	21
Figure 6-1. Administration Utility Main Menu . . . . .	44
Figure 6-2. Example of File-Access Environment . . . . .	47
Figure 6-3. Example of Correspondences Between DCE and File-Access Groups and Users . . . . .	48
Figure 7-1. Group and Users . . . . .	71

# List of Tables

---

Table 6-1. Key Assignments for Administration Utility Functions . . . . .	44
Table 6-2. Input Information and Restrictions on Entered Characters . . . . .	45
Table 6-3. Information Set in Administration Utility . . . . .	48
Table 7-1. NetWare Rights . . . . .	66
Table 7-2. Rights Set Through ACLs . . . . .	67
Table 7-3. File-Access Rights . . . . .	68
Table 7-4. Differences in Effective Rights Between File-Access and NetWare . . . . .	72
Table 7-5. Rules for Converting ACL to Trustee Rights . . . . .	73
Table 7-6. Conversion of Trustee Rights to ACL . . . . .	75
Table 7-7. Differences Between Specified Rights and the Rights Actually Set by File-Access . . . . .	76
Table 7-8. Correspondence Between UFS Rights and LFS Rights . . . . .	77

# Preface

---

## The Open Group

The Open Group is the leading vendor-neutral, international consortium for buyers and suppliers of technology. Its mission is to cause the development of a viable global information infrastructure that is ubiquitous, trusted, reliable, and as easy-to-use as the telephone. The essential functionality embedded in this infrastructure is what we term the IT DialTone. The Open Group creates an environment where all elements involved in technology development can cooperate to deliver less costly and more flexible IT solutions.

Formed in 1996 by the merger of the X/Open Company Ltd. (founded in 1984) and the Open Software Foundation (founded in 1988), The Open Group is supported by most of the world's largest user organizations, information systems vendors, and software suppliers. By combining the strengths of open systems specifications and a proven branding scheme with collaborative technology development and advanced research, The Open Group is well positioned to meet its new mission, as well as to assist user organizations, vendors, and suppliers in the development and implementation of products supporting the adoption and proliferation of systems which conform to standard specifications.

With more than 200 member companies, The Open Group helps the IT industry to advance technologically while managing the change caused by innovation. It does this by:

- consolidating, prioritizing, and communicating customer requirements to vendors
- conducting research and development with industry, academia, and government agencies to deliver innovation and economy through projects associated with its Research Institute
- managing cost-effective development efforts that accelerate consistent multi-vendor deployment of technology in response to customer requirements
- adopting, integrating, and publishing industry standard specifications that provide an essential set of blueprints for building open information systems and integrating new technology as it becomes available
- licensing and promoting the Open Brand, represented by the “X” mark, that designates vendor products which conform to Open Group Product Standards
- promoting the benefits of IT DialTone to customers, vendors, and the public.

The Open Group operates in all phases of the open systems technology lifecycle including innovation, market adoption, product development, and proliferation. Presently, it focuses on seven strategic areas: open systems application platform development, architecture, distributed systems management, interoperability, distributed computing environment, security, and the information superhighway. The Open Group is also responsible for the management of the UNIX trademark on behalf of the industry.

## **The Development of Product Standards**

This process includes the identification of requirements for open systems and, now, the IT DialTone, development of CAE and Preliminary Specifications through an industry consensus review and adoption procedure (in parallel with formal standards work), and the development of tests and conformance criteria.

This leads to the preparation of a Product Standard which is the name used for the documentation that records the conformance requirements (and other information) to which a vendor may register a product. There are currently two forms of Product

Standard, namely the Profile Definition and the Component Definition, although these will eventually be merged into one.

The “X” mark is used by vendors to demonstrate that their products conform to the relevant Product Standard. By use of the Open Brand they guarantee, through the X/Open Trade Mark License Agreement (TMLA), to maintain their products in conformance with the Product Standard so that the product works, will continue to work, and that any problems will be fixed by the vendor.

## Open Group Publications

The Open Group publishes a wide range of technical documentation, the main part of which is focused on specification development and product documentation, but which also includes Guides, Snapshots, Technical Studies, Branding and Testing documentation, industry surveys, and business titles.

There are several types of specification:

### CAE Specifications

CAE (Common Applications Environment) Specifications are the stable specifications that form the basis for our Product Standards, which are used to develop X/Open branded systems. These specifications are intended to be used widely within the industry for product development and procurement purposes.

Anyone developing products that implement a CAE Specification can enjoy the benefits of a single, widely supported industry standard. Where appropriate, they can demonstrate product compliance through the Open Brand. CAE Specifications are published as soon as they are developed, so enabling vendors to proceed with development of conformant products without delay.

### Preliminary Specifications

Preliminary Specifications usually address an emerging area of technology and consequently are not yet supported by multiple sources of stable conformant implementations. They are published for the purpose of validation through implementation of products. A Preliminary Specification is not a draft specification; rather, it is as

stable as can be achieved, through applying The Open Group's rigorous development and review procedures.

Preliminary Specifications are analogous to the trial-use standards issued by formal standards organizations, and developers are encouraged to develop products on the basis of them. However, experience through implementation work may result in significant (possibly upwardly incompatible) changes before its progression to becoming a CAE Specification. While the intent is to progress Preliminary Specifications to corresponding CAE Specifications, the ability to do so depends on consensus among Open Group members.

#### Consortium and Technology Specifications

The Open Group publishes specifications on behalf of industry consortia. For example, it publishes the NMF SPIRIT procurement specifications on behalf of the Network Management Forum. It also publishes Technology Specifications relating to OSF/1, DCE, OSF/Motif, and CDE.

Technology Specifications (formerly AES Specifications) are often candidates for consensus review, and may be adopted as CAE Specifications, in which case the relevant Technology Specification is superseded by a CAE Specification.

In addition, The Open Group publishes:

#### Product Documentation

This includes product documentation—programmer's guides, user manuals, and so on—relating to the Prestructured Technology Projects (PSTs), such as DCE and CDE. It also includes the Single UNIX Documentation, designed for use as common product documentation for the whole industry.

#### Guides

These provide information that is useful in the evaluation, procurement, development, or management of open systems, particularly those that relate to the CAE Specifications. The Open Group Guides are advisory, not normative, and should not be referenced for purposes of specifying or claiming conformance to a Product Standard.

#### Technical Studies

Technical Studies present results of analyses performed on subjects of interest in areas relevant to The Open Group's Technical Program. They

are intended to communicate the findings to the outside world so as to stimulate discussion and activity in other bodies and the industry in general.

## Versions and Issues of Specifications

As with all live documents, CAE Specifications require revision to align with new developments and associated international standards. To distinguish between revised specifications which are fully backwards compatible and those which are not:

- A new Version indicates there is no change to the definitive information contained in the previous publication of that title, but additions/extensions are included. As such, it replaces the previous publication.
- A new Issue indicates there is substantive change to the definitive information contained in the previous publication of that title, and there may also be additions/extensions. As such, both previous and new documents are maintained as current publications.

## Corrigenda

Readers should note that Corrigenda may apply to any publication. Corrigenda information is published on the World-Wide Web at <http://www.opengroup.org/public/pubs>.

## Ordering Information

Full catalogue and ordering information on all Open Group publications is available on the World-Wide Web at <http://www.opengroup.org/public/pubs>.

## **This Book**

The *DCE 1.2.2 File-Access Administration Guide and Reference* provides concepts and procedures to help you manage the DCE/File-Access software product developed by the Open Software Foundation (OSF).

## **Audience**

This document is written for system and network administrators who are familiar with OSF's Distributed Computing Environment (DCE), with Novell NetWare<sup>™</sup> software, and with the MS-DOS<sup>™</sup> operating system for personal computers.

## **Applicability**

This document applies to the OSF DCE Version 1.2.2 offering and related updates. (See your software license for details.)

## **Purpose**

The purpose of this guide is to help system and network administrators to plan, configure, and manage DCE/File-Access. After reading the guide, you will understand what the system administrator needs to do to plan for DCE/File-Access. Once you have built the DCE/File-Access source code on your system, use this guide to assist you in installing executable files and configuring the File-Access software. The *DCE 1.2.2 Release Notes* contain instructions for installing and building DCE source code.

## **Related Documents**

For additional information about the Distributed Computing Environment, refer to the following documents:



- *DCE 1.2.2 Introduction to OSF DCE*  
Document Number F201, ISBN 1-85912-182-9
- *DCE 1.2.2 Command Reference*  
Document Number F212, ISBN 1-85912-138-1
- *DCE 1.2.2 Application Development Reference*  
Document Number F205A, ISBN 1-85912-103-9 (Volume 1)  
Document Number F205B, ISBN 1-85912-108-X (Volume 2)  
Document Number F205C, ISBN 1-85912-159-4 (Volume 3)
- *DCE 1.2.2 Application Development—Introduction and Style Guide*  
Document Number F202, ISBN 1-85912-187-X
- *DCE 1.2.2 Application Development Guide—Core Components*  
Document Number F203A, ISBN 1-85912-192-6 (Volume 1)  
Document Number F203B, ISBN 1-85912-154-3 (Volume 2)
- *DCE 1.2.2 Application Development Guide—Directory Services*  
Document Number F204, ISBN 1-85912-197-7
- *DCE 1.2.2 DFS Administration Guide and Reference*  
Document Number F209A, ISBN 1-85912-123-3 (Volume 1)  
Document Number F209B, ISBN 1-85912-128-4 (Volume 2)
- *The DCE 1.2.2 Administration Guide—Introduction*  
Document Number F207, ISBN 1-85912-113-6
- *The DCE 1.2.2 Administration Guide—Core Components*  
Document Number F208, ISBN 1-85912-118-7
- *DCE 1.2.2 File-Access User's Guide*  
Document Number F217, ISBN 1-85912-163-3
- *DCE 1.2.2 Problem Determination Guide*  
Document Number F213A, ISBN 1-85912-143-8 (Volume 1)  
Document Number F213B, ISBN 1-85912-148-9 (Volume 2)
- *DCE 1.2.2 Testing Guide*  
Document Number F215, ISBN 1-85912-153-5
- *DCE 1.2.2 File-Access FVT User's Guide*  
Document Number F210, ISBN 1-85912-189-6
- *DCE 1.2.2 Release Notes*  
Document Number F218, ISBN 1-85912-168-3

For a detailed description of OSF DCE documentation, see the *DCE 1.2.2 Introduction to OSF DCE*.

## Typographic and Keying Conventions

This guide uses the following typographic conventions.

**Bold**            **Bold** words or characters represent system elements that you must use literally, such as commands, options, and pathnames.

*Italic*            *Italic* words or characters represent variable values that you must supply. *Italic* type is also used to introduce a new DCE term.

Constant width    Examples and information that the system displays appear in constant width typeface.

[ ]                Brackets enclose optional items in format and syntax descriptions.

{ }                Braces enclose a list from which you must choose an item in format and syntax descriptions.

|                  A vertical bar separates items in a list of choices.

< >               Angle brackets enclose the name of a key on the keyboard.

...                Horizontal ellipsis points indicate that you can repeat the preceding item one or more times.

This guide uses the following keying conventions.

< **Ctrl-x** > or ^ *x*            The notation < **Ctrl-x** > or ^ *x* followed by the name of a key indicates a control character sequence. For example, < **Ctrl-C** > means that you hold down the control key while pressing < **C** >.

< **Return** >    The notation < **Return** > refers to the key on your terminal or workstation that is labeled with the word Return or Enter, or with a left arrow.

## Problem Reporting

If you have any problems with the software or vendor-supplied documentation, contact your software vendor's customer service department. Comments relating to this Open Group document, however, should be sent to the addresses provided on the copyright page.

## Pathnames of Directories and Files in DCE Documentation

For a list of the directories and files referred to in this guide, see the *DCE 1.2.2 Administration Guide—Introduction* and the *DCE 1.2.2 Testing Guide*.

## Trademarks

Motif<sup>®</sup>, OSF/1<sup>®</sup>, and UNIX<sup>®</sup> are registered trademarks and the IT DialTone<sup>™</sup>, The Open Group<sup>™</sup>, and the “X Device”<sup>™</sup> are trademarks of The Open Group.

DEC, DIGITAL, and ULTRIX are registered trademarks of Digital Equipment Corporation.

DECstation 3100 and DECnet are trademarks of Digital Equipment Corporation.

HP, Hewlett-Packard, and LaserJet are trademarks of Hewlett-Packard Company.

Network Computing System and PasswdEtc are registered trademarks of Hewlett-Packard Company.

AFS, Episode, and Transarc are registered trademarks of the Transarc Corporation.

DFS is a trademark of the Transarc Corporation.

Episode is a registered trademark of the Transarc Corporation.

Ethernet is a registered trademark of Xerox Corporation.

AIX and RISC System/6000 are registered trademarks of International Business Machines Corporation.

IBM is a registered trademark of International Business Machines Corporation.

DIR-X is a trademark of Siemens Nixdorf Informationssysteme AG.

MX300i is a trademark of Siemens Nixdorf Informationssysteme AG.

NFS, Network File System, SunOS and Sun Microsystems are trademarks of Sun Microsystems, Inc.

PostScript is a trademark of Adobe Systems Incorporated.

Microsoft, MS-DOS, and Windows are registered trademarks of Microsoft Corp.

NetWare is a registered trademark of Novell, Inc.

# Chapter 1

---

## File-Access Overview

File-Access is a program that allows you to access Distributed File Service (DFS) files resident on a workstation that is part of a Distributed Computing Environment (DCE) cell, from a PC running NetWare<sup>®</sup> and using MS-DOS control operations. This chapter describes the following features of File-Access functions and the programs in File-Access:

- File-Access capabilities
- File-Access configuration
- The basics of File-Access
- Administrator tasks

### 1.1 What is File-Access?

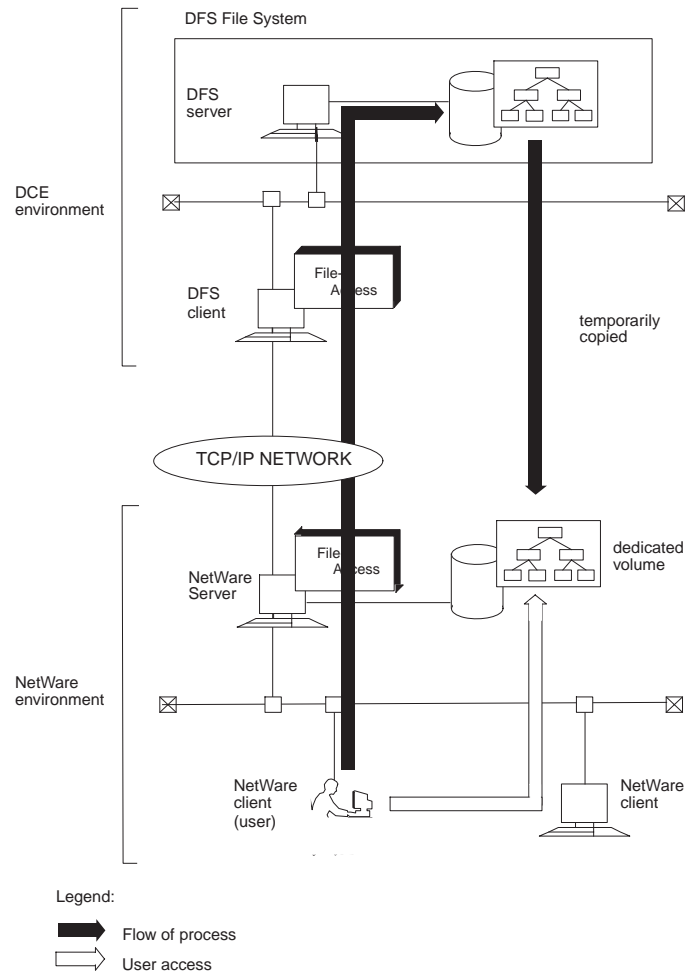
File-Access software allows you to access directories or files on a DCE/DFS workstation from PC-based NetWare via a TCP/IP network. With File-Access, you

can access DFS directories and files in a workstation by using MS-DOS commands and operations on a PC.

With File-Access, NetWare users in multiple NetWare environments can access the same DCE/DFS directories and files. As a result, you can create a file sharing system that uses your PC's NetWare environment and the workstation's DCE environment.

File-Access temporarily copies the DFS/DCE directory structure onto a volume in the NetWare server. This means that you can actually access DFS files by accessing files on the NetWare server through a NetWare client. Figure 1-1 illustrates how to use File-Access to access DCE through NetWare.

Figure 1-1. How to Access DCE from NetWare via File-Access



## 1.2 File-Access Configuration

File-Access consists of three programs: Client utility, Gateway, and Agent. These programs run on the NetWare client, NetWare server, and DFS client, respectively.

### 1.2.1 File-Access Prerequisites

You must have the following software to run File-Access:

Client/Server	System Requirement
NetWare client	MS-DOS 5.0 or newer version, NetWare 3.12J
NetWare server	MS-DOS 5.0 or newer version, NetWare 3.12J
DFS client	OSF DCE V1.1 or newer version, RIOS 3.2.5 or newer DCE compatible version

### 1.2.2 File-Access Components

File-Access consists of the following components:

- Client Utility
- Gateway Program
- Agent program

#### 1.2.2.1 The Client Utility

The Client utility program resides in the NetWare server with Gateway. To open the Client utility, you must first log into the NetWare server from the NetWare client.

The Client utility has the following functions:

- Logging into DCE from NetWare/Logging out of DCE from NetWare



- Setting or changing a DCE password
- Adding and deleting rights to and from files and directories

A user who is accessing DCE from NetWare has a NetWare user account, DCE username, and DCE password. This type of user is called a Gateway user. In this guide, the term user indicates a Gateway user unless otherwise noted.

### 1.2.2.2 The Gateway Program

The Gateway program resides in each NetWare server. This program converts DCE access requests from NetWare to DFS information. After conversion, the information is sent to the Agent program in the DFS client. Each Gateway program sends access requests to only one Agent program; it is not possible to access multiple Agent programs through a single Gateway.

The Gateway program includes an Administration utility, which creates the File-Access environment on the NetWare server. With File-Access, the administrator uses the Administration utility to allocate DFS directories to a Gateway volume on the NetWare server. Once all the DFS directories are allocated to the Gateway volume, it is possible to edit data just as you would in directories and files in other NetWare volumes.

### 1.2.2.3 The Agent Program

The Agent program resides in and runs on the DFS client. This program receives DCE access requests from Gateway, accesses directories and files on the DFS server, and returns the transaction results to Gateway. One Agent program can process access requests from multiple Gateway programs.

## 1.3 Basics of File-Access

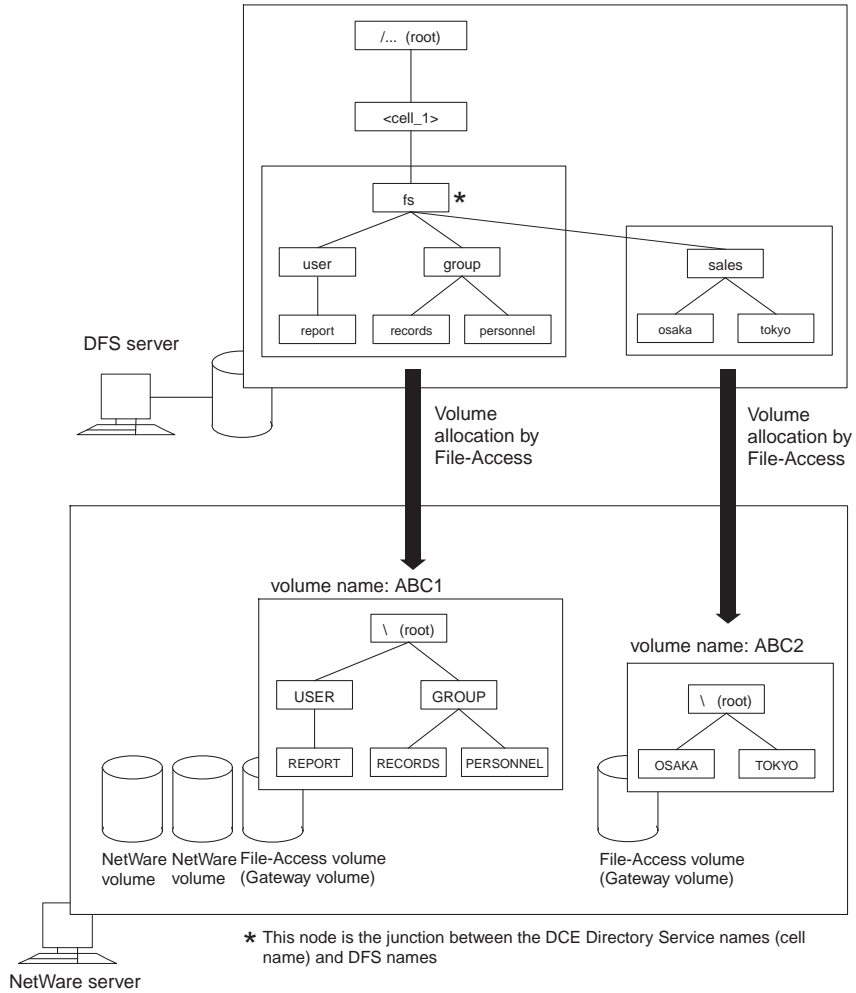
This section explains the basics of File-Access, such as allocating DFS directories to a volume and accessing DCE from Netware. It also describes the type of File-Access users.

### **1.3.1 Allocating DFS Directories to a Volume**

To access DFS directories and files from NetWare in File-Access, you need to create a File-Access-specific (Gateway) volume. This function is used to create the Gateway volume in NetWare. Specified DFS directories (mount points) are allocated to the Gateway volume. You (or a user with rights to use the Administration utility) set up the volume allocations using the Gateway Administration utility.

Figure 1-2 illustrates the basics of volume allocation.

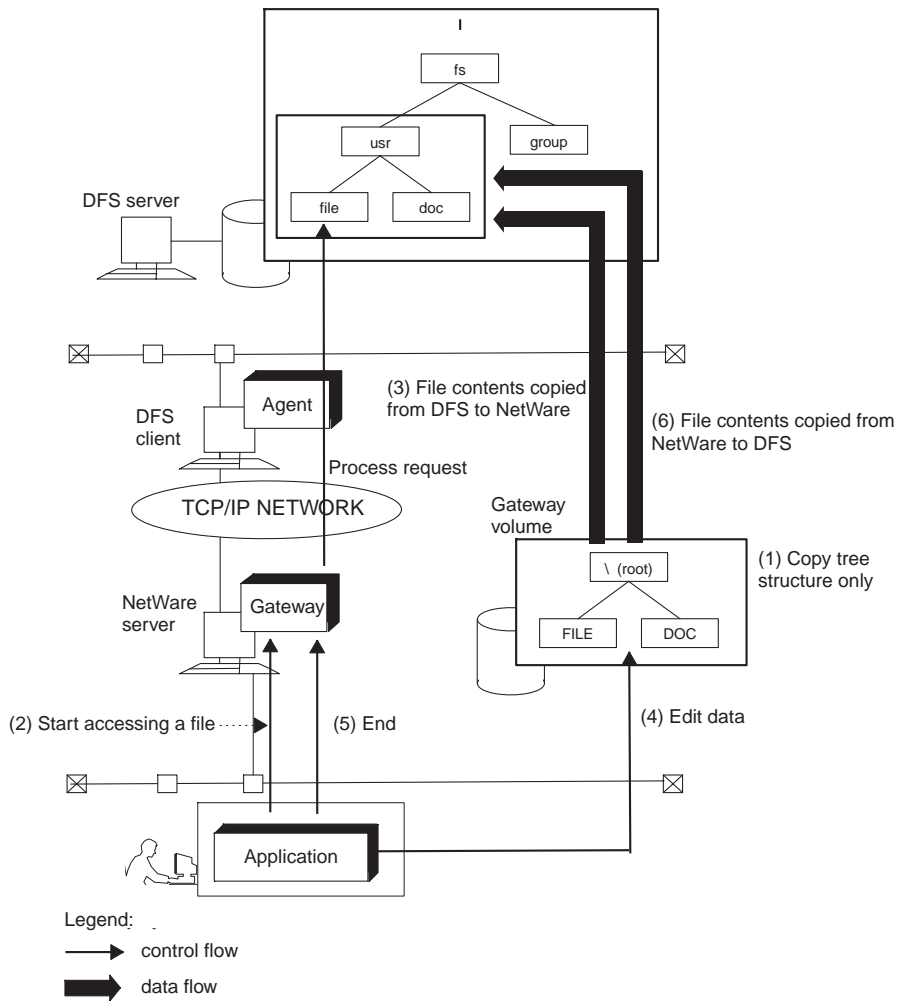
Figure 1-2. Volume Allocation



### **1.3.2 Accessing DCE from NetWare**

Users must log into DCE through the NetWare server before they can access DFS directories and files in the Gateway volume. Figure 1-3 shows the process of accessing DFS files after the logging into DCE from the NetWare client.

Figure 1-3. Process of Accessing DFS Files



**Note:** When you access a file while running an application, Gateway sends a request through the Agent program in the DFS client to the DFS server to perform

the required file process. After a file is opened, it is copied to the Gateway volume on the corresponding NetWare server.

Users who access files in the Gateway volume can perform the following functions:

- Edit data and perform other operations on files copied to the Gateway volume.
- Exit file access process from an application.
- Overwrite the original DFS files with files in the Gateway volume.

### 1.3.3 File-Access Users

The File-Access environment consists of an administrator who creates a File-Access environment and users who access DCE via NetWare. This subsection describes the functions of the administrator and users.

#### 1.3.3.1 Administrator

The File-Access program enables file sharing between NetWare and DCE. To activate file sharing, the administrator first needs to set up a File-Access environment in both NetWare and DCE, as described below.

##### 1.3.3.1.1 Setting Up the File-Access Environment in NetWare

This setup process is handled by the File-Access administrator. The File-Access administrator needs to be a NetWare administrator with NetWare **SUPERVISOR** rights or a user with the equivalent of **SUPERVISOR** rights. When installing File-Access for the first time, the NetWare administrator should also serve as the File-Access administrator because only the **SUPERVISOR** can operate the Gateway Administration utility. As for operation and maintenance after installation, register a user who can use the Administration utility and assign to that user File-Access administration duties. See Chapter 6 for details on registering a user for operating the Administration utility.

### 1.3.3.1.2 Setting Up the File-Access Environment in DCE

This setup process is handled by the DCE system administrator (DCE administrator).

### 1.3.3.2 Users

A File-Access user must have a username and password both in NetWare and DCE in order to use File-Access to access DCE from NetWare. Such users are known as Gateway users.

File-Access registers the usernames and passwords in both NetWare and DCE through the Gateway Administration utility. Thus, it is not necessary to enter your DCE username or password when you log into DCE from NetWare. See Chapter 6 for information on setting up the Administration utility.

## 1.4 Administrator Tasks

To operate File-Access, it is necessary to set up File-Access environments in NetWare and DCE. This section describes the tasks performed by the administrators assigned to the NetWare and DCE machines.

### 1.4.1 Tasks Required for the DFS Client

The environment setup required for the DFS client is usually handled by the DCE administrator. The DCE administrator performs the following setup tasks:

- Installing Agent
- Setting up the TCP/IP environment
- Registering the DCE users who are to use File-Access; setting users' ACLs.
- Registering the administrator group and its ACL
- Registering the master key for Gateway authentication

See Chapter 4 for further details regarding setup.

## **1.4.2 Tasks Required for the NetWare Server**

The environment setup required for the NetWare server is usually handled by the File-Access administrator, who performs the following setup tasks:

- Installing Gateway and the Client utility
- Setting up the TCP/IP environment
- Creating and mounting File-Access volumes
- Setting Gateway auto-loading
- Allocating DFS subdirectories to a Gateway volume
- Registering Gateway users
- Registering Gateway groups

See Chapter 5 and Chapter 6 for further details regarding setup.



## Chapter 2

---

# Starting and Exiting File-Access

To use File-Access, it is necessary to start the Agent program on the DFS client and the Gateway program on the NetWare server. This chapter provides the following sections:

- Starting File-Access
- Exiting File-Access

### 2.1 Starting File-Access

To start File-Access, the DCE administrator must first start the Agent program on the DFS client. After the DFS Agent is started, the File-Access administrator starts Gateway on the NetWare server. Prior to the above actions, DFS and DCE must be running on the DFS client, and the DFS startup process must already be completed. In addition, NetWare must already be running on the NetWare server.

## 2.1.1 Starting the Agent Program

Start Agent by logging in as a superuser to an Agent program installed on a DFS client. Enter the **dfaagt** command as follows:

```
/usr/bin/dfaagt
```

The **dfaagt** command execution file is located in **/opt/dcelocal/bin**, and is linked to **/usr/bin**.

## 2.1.2 Starting the Gateway Program

TCP/IP must be running on the NetWare server before Gateway is started. Before starting Gateway, set **TCPIP.NLM** to be loaded on the NetWare server. See Chapter 5 for details.

To start Gateway, load **DFA.NLM** in the SYS volume as follows:

```
LOAD [SYS:\SYSTEM\]DFA.NLM
```

Gateway can be set to load when the NetWare server is started. See Chapter 5 for details.

## 2.2 Exiting File-Access

To exit File-Access, the File-Access administrator must first exit Gateway and then Agent after all users accessing DCE from the NetWare client have logged out.

## 2.2.1 Exiting Gateway

To exit Gateway, the File-Access administrator enters the **DFASTOP** command from the NetWare server console as follows:

```
DFASTOP
```

If a user is accessing DFS from the NetWare client when the File-Access administrator exits Gateway, file editing results cannot be guaranteed. The File-Access administrator must exit Gateway only after all users accessing DCE have logged out. Since the File-Access administrator cannot directly confirm who is logged into DCE, the administrator must use the NetWare **USERLIST** command to check for users logged into the NetWare server, and then broadcast a message to indicate that Gateway will be exited.

## 2.2.2 Exiting Agent

To exit the Agent program, the File-Access administrator enters the **dfaagt** command through a DFS client, using the **-s** or **-a** option.

### 2.2.2.1 Exiting Agent with the -s Option

If the File-Access administrator selects the **-s** option and enters an exit time (in seconds), the Agent exiting process starts after the specified period has elapsed.

The following example illustrates the command used to exit Agent after a delay of 100 seconds:

```
dfaagt -s 100
```

When the **-s** option is selected, Gateway sends a message to all NetWare clients who are logged into DCE to inform them when Agent is to exit. If an exit time is not

specified, the system uses a default of 60 seconds. However, if no Gateway program is connected to Agent, Agent exits immediately.

### 2.2.2.2 Exiting Agent with the -a Option

If the File-Access administrator selects the **-a** option, Agent exits immediately after the administrator enters the **dfaagt -a** command.

### 2.2.2.3 Important Points on Using the dfaagt Command to Exit Agent

- If Agent exits before Gateway exits, files that have been edited or created in File-Access will not overwrite DFS files.
- Never enter the **dfaagt** command with the **-a** option while Gateway is running.

## Chapter 3

---

# Preparations for File-Access Setup

Before setting up File-Access, you must check the software versions and check the operating conditions of the environment where File-Access will run, since data will be exchanged between DCE and NetWare. This chapter describes the File-Access setup process and prerequisites. Chapters 4, 5, and 6 describe the setup process in detail. Chapter 4 also describes the DFS client setup in detail.

### 3.1 Overview of Setup

Setting up the File-Access environment requires operations in both the DFS client and the NetWare server. The NetWare server setup uses the NetWare utility and the File-Access Administration utility.

#### 3.1.1 Setup Tasks

File-Access setup consists of the following groups of setup tasks:

- DFS client tasks
- Netware tasks
- Environment tasks

### 3.1.1.1 DFS Client Setup

The DCE administrator must perform the following tasks to set up the DFS:

- Install Agent on the DFS client.
- Set up a TCP/IP environment for Gateway-Agent communication.
- Set up DCE user/Gateway user correspondences.
- Create DCE Groups for Gateway users.
- Set an access control list (ACL).
- Set the master key for Gateway authentication.

The DCE administrator can ask the File-Access administrator to set the master key for Gateway authentication.

### 3.1.1.2 NetWare Setup

The NetWare administrator or a Gateway user (File-Access administrator) who operates and maintains the File-Access environment performs the following setup tasks on the NetWare client and the NetWare server. These are described in detail in Chapter 5. Refer to Chapter 6 for more details on setting up the File-Access environment.

#### 3.1.1.2.1 NetWare client tasks

- Install the Gateway and Client utility programs.

#### 3.1.1.2.2 NetWare server tasks

- Select NetWare users who are to be registered as Gateway users.
- Create NetWare group to be used as the Gateway group.
- Create volume to be used as a Gateway volume.
- Set up a TCP/IP environment for communication between Gateway and Agent.
- Set Gateway for auto-loading.

#### 3.1.1.3 Setting Up the Environment by Using the Administration Utility

The File-Access administrator uses the Gateway Administration utility to perform the following tasks to create the File-Access environment:

- Register the Gateway volume and its corresponding DFS subdirectory.
- Register and then delete Gateway users.
- Register the Gateway group.
- Set master key for Agent authentication.
- Set options for the network environment.

When setting up a new File-Access environment, only the NetWare **SUPERVISOR** can initially log into the Administration utility to perform the setup. The **SUPERVISOR** must then register the File-Access administrator as a user who can use the Administration utility. After the **SUPERVISOR** registers a File-Access administrator as a user who can use the Administration utility, the File-Access administrator then registers and deletes Gateway users.

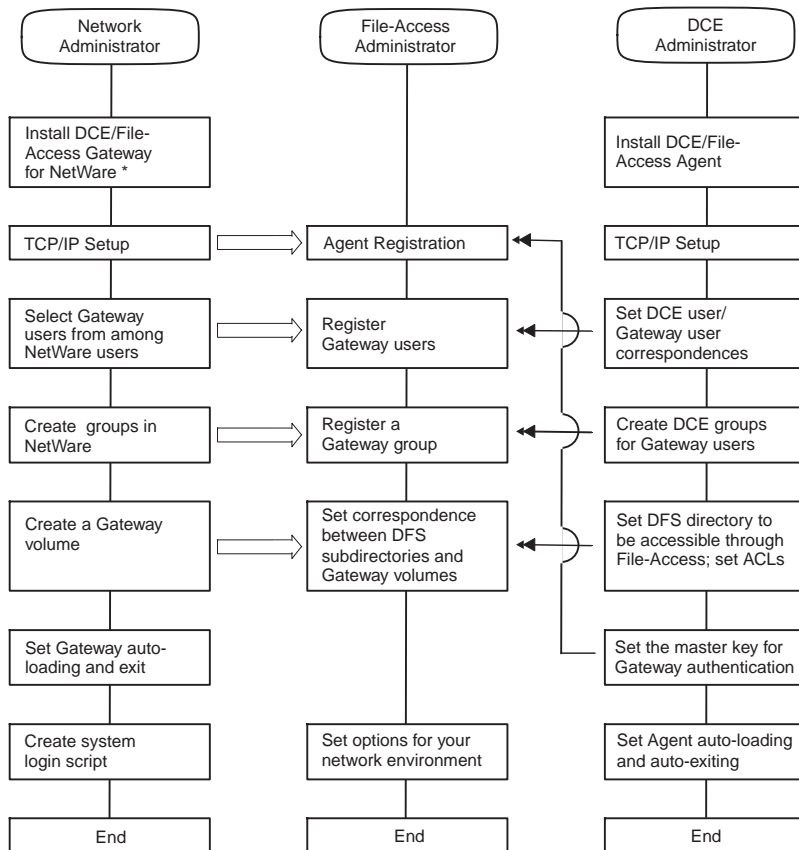
### 3.1.2 Setup Procedures

Figure 3-1 shows the File-Access environment setup task flow for initial installation.

This information is presented in the form of a parallel flow chart to illustrate the relationship between the tasks performed by the different administrators. During actual setup, the File-Access administrator should perform the appropriate tasks after the NetWare administrator and the DCE administrator have completed their tasks.



Figure 3-1. Flow of File-Access Environment Setup Tasks



\* DCE/File-Access Gateway for NetWare should be installed through a NetWare client

Legend:  
 → The File-Access administrator sets this based on the settings made by the NetWare administrator  
 → The File-Access administrator sets this based on the settings made by the DCE administrator

## 3.2 Prerequisites for File-Access Setup

Before you set up File-Access, confirm the following:

- Is the DCE/DFS environment already set up with the proper ACL and Export settings?

If there are errors in these settings, you may not be able to access previously created files or set file access rights for previously created files.

- Is your version of NetWare version 3.12J?

File-Access is only compatible with NetWare 3.12J.

Do not use other versions of NetWare.

- Is TCP/IP running on the NetWare server?

TCP/IP must be running on the NetWare server for Gateway-Agent communication to take place.

- Is the time zone set correctly?

File-Access will not operate if your NetWare server uses **CLIB.NLM** version 3.12g or a previous version. If you replace the **CLIB.NLM** file with a newer version, the NetWare environment time zone will be set to Eastern Standard Time. If Eastern Standard Time is not appropriate for your NetWare server, change the time zone by adding the **SET TIMEZONE** command to **STARTUP.NCF** or **AUTOEXEC.NCF** in the NetWare server. Reboot the NetWare server after replacing the **CLIB.NLM** file to update the time zone. See the *Netware System Administration* manual for details regarding **STARTUP.NCF**, **AUTOEXEC.NCF**, and the **SET TIMEZONE** command.

## Chapter 4

---

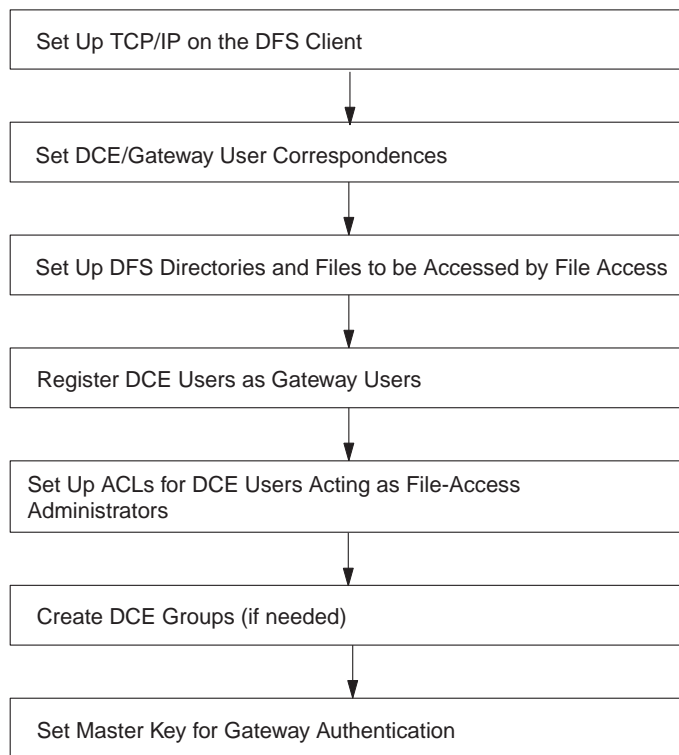
# DFS Client Setup

This chapter describes the tasks required for setting up the DFS Client. It also describes the process of installing Agent, which is a File-Access DCE program in a DFS client.

### 4.1 DFS Client Setup Procedure

The DCE administrator installs the File-Access Agent program in the DFS client to set up the required File-Access environment. Doing so makes it possible to exchange DCE/DFS file data with the NetWare machine.

The setup tasks described in this section assume that DCE and DFS have already been set up and are running. The following illustration shows the flow of setup operations required to set up the DFS client.



## 4.2 Installing Agent and Setting Up the DFS Environment

This section describes how to install Agent, which is a File-Access DCE program, in the DFS client. It also describes how to set ACL (which is necessary to use File-Access) and the master key in the DFS client.

## 4.2.1 Setting Up TCP/IP on the DFS Client

File-Access uses TCP/IP for communication between DFS and NetWare. This requires that the DFS administrator make the necessary settings in two files (**/etc/hosts** and **/etc/services**) and connect Agent and Gateway together.

### 4.2.1.1 File Settings

Set up the following files.

- **/etc/hosts**

Register the IP address and hostname of the NetWare server on which Gateway will run. We recommend that you use the NetWare server name as the hostname

- **/etc/services**

Set **dfa** as the File-Access service name. Set the port number for services provided by Agent, and set **tcp** as the protocol. Use a number greater than 5,000 for the port number because 5,000 and numbers up to 5,000 are reserved for the system.

## 4.2.2 Setting Up the DCE and DFS Environments

This subsection describes how to set up the DCE and DFS environments for using File-Access.

### 4.2.2.1 General Environment Settings

Set up the general DFS environment by completing the following four tasks:

1. Set DCE user/Gateway user correspondences. If necessary, create a new DCE user.
2. Set the DFS directories and files to be accessed through File-Access, and check the export settings for the file set in which the directories and files are to be stored.

3. Check the ACL of DCE users (corresponding to File-Access users) who are to have access to files and directories. Make changes if necessary. User access rights are easier to manage if you first create a dedicated DCE group to correspond to a Gateway user, and then assign that group to an ACL. Note that the DCE group names **DFA\_OTHER\_GROUP** or **DFA\_MASK\_OBJ** are reserved by File-Access and cannot be used.
4. Check the initial settings for the container-creating ACLs and the object-creating ACLs for the directories that File-Access will use. Make any necessary changes.

Use the DCE **acl\_edit** command to change an ACL. Use the **rgy\_edit** command to register DCE users and passwords.

#### 4.2.2.2 Setting Up ACLs for DCE Users Corresponding to File-Access Administrators

The following rights must be set for DCE users who are to be registered in NetWare as File-Access administrators. These rights are set in the ACLs corresponding to the root directory of each volume in the DFS file system assigned by File-Access to the NetWare Gateway volume.

- ACL for directory: **[rx]** (read and execute)
- Directory Container Creation ACL initial setting: **[rx]** (read and execute)
- Directory Object Creation ACL initial setting: No access rights are needed.

It is necessary to add these access rights to any existing directories and files that are to be used by File-Access. When registering multiple File-Access administrators as DCE users, it is easier to create a File-Access administration group and set an ACL corresponding to that group than to set each DCE user in an ACL. Use the **rgy\_edit** command to create a group.

If only Gateway users access the directories and files, set all rights to the ACL **mask\_obj** entry. Doing so makes it easier to change directory and file rights through File-Access.

### 4.2.2.3 Setting Up the UNIX File System Environment

If you select UFS (UNIX File System) for File-Access directories and files, it is necessary to set at least **rx** rights (read and execute) in the ACLs of all directories for the DCE user who corresponds to the File-Access administrator.

A UFS ACL has three entries: **owner**, **group**, and **other**. These entries are equivalent to **user\_obj**, **group\_obj**, and **other\_obj**, which are the LFS ACL entries. There is no corresponding entry for **mask\_obj**.

### 4.2.2.4 The dfsd Process Extension

File-Access has a periodic Gateway directory tree-searching process. This process runs in the background and saves search results to a cache. The bigger the Gateway directory tree, the less space available in the cache. When the available cache space decreases, the number of access requests from the DFS client to the DFS server will increase and the processing speed will decrease. To avoid this problem, change the settings for the **dfsd** process status cache entry and name cache entry. The entry settings are described in the **/etc/rc.dfs** file.

The **/etc/rc.dfs** file is described in the following subsections. This description assumes there are 1,000 status cache entries and name cache entries.

#### 4.2.2.4.1 Changing the dfsd Process Setting in the Disk Cache

To change the **dfsd** process setting, change the following text:

```
daemonrunning $DCELOCAL/bin/dfsd
```

to this:

```
daemonrunning $DCELOCAL/bin/dfsd -stat 1000 -namesize 1000
```

#### 4.2.2.4.2 Changing the dfsd Process Setting in the Memory Cache

Change the Before statement to an After statement.

Before Statement:

```
daemonrunning $DCELOCAL/bin/dfsd -memcache -blocks size
```

After Statement:

```
daemonrunning $DCELOCAL/bin/dfsd -memcache -blocks -stat 1000 \  
-namesize 1000"
```

If you increase the number of status cache entries or the name cache entries, use the following memory size per entry:

- Status cache entry: 312 bytes
- Name cache entry: 80 bytes

### 4.2.3 Setting a Master Key for Gateway Authentication

Set the Agent's master key for Gateway authentication. You must set the master key in both Agent and Gateway. The following subsections describe the master key setting procedure for Agent. See "Registering Agent and the Master Key" in Chapter 6 for details regarding the Gateway master key.

#### 4.2.3.1 What is a Master Key?

File-Access encrypts communication data between DFS and Gateway to prevent hacking. You can periodically change the encryption pattern by means of a keyword. This keyword is called a *Master key*. The master key consists of one to eight ASCII characters and is stored in the master key file. The master key changes every time Gateway logs into Agent.



### 4.2.3.2 Setting the Master Key

You set the Agent master key in the `/opt/dcelocal/var/dfa/dfakey` file. To do this, first register an administrator who can create and modify a master key, then register the master key to corresponding Gateway programs.

The registration procedure for the master key is as follows:

1. Log into DFS client host as a superuser.
2. Using the editor, enter the following statement at the beginning of the `/opt/dcelocal/var/dfa/dfakey` file:

```
DfaAdmin=UNIX username_of_user_registered_as_administrator
```

3. Log in again as the user registered in the `/opt/dcelocal/var/dfa/dfakey` file.
4. Set the Gateway hostname by using the `setdfakey` command. Specify the Gateway hostname registered in the `/etc/hosts` file by using the File-Access `setdfakey` command. The `setdfakey` command syntax is as follows:

```
setdfakey [-a Gateway_Host_Name]
```

If you select the `-a` option, the master key for the designated NetWare server will be registered in the `/opt/dcelocal/var/dfa/dfakey` file. If you omit the `-a` option and Gateway hostname, the system displays a message requesting the hostname.

Once you enter the command, the system displays a message requesting the master key.

5. Enter the master key. The master key should be one to eight ASCII characters long. The system displays a master key reenter message for confirmation when you enter the master key.
6. Reenter the master key. If the reentered master key is the same as before, the master key will be registered. If the entries are not the same, the master key registration process fails and the system displays an error message. Enter the `setdfakey` command again if an error message is displayed.

### 4.2.3.3 The **setdfakey** Command Options

The **setdfakey** command has the following options:

- a** Registers the master key for the NetWare server **/etc/dfakey** file.
- l** Displays the names of NetWare servers registered in the **/etc/dfakey** file.
- d** Deletes the specified NetWare server and master key from the file **/opt/dcelocal/var/dfa/dfakey** .

Only one **setdfakey** option can be specified.

### 4.2.3.4 Important Points

- The master key administrator must be a DCE administrator or a File-Access administrator, and the Agent master key and Gateway master key must be the same. Therefore, if the DCE administrator is the master key administrator, the DCE administrator must give the master key to the File-Access administrator.
- Only the master key administrator specified in the **/opt/dcelocal/var/dfa/dfakey** file can change the master key file.
- If the master key needs to be changed, first exit File-Access. Next, change the master key for both Agent and Gateway. Then start File-Access again. If you change either the Agent or Gateway master key without changing the other, Gateway users cannot log into Agent from Gateway.
- The Gateway hostname set in the **setdfakey** command must be registered in advance in the **/etc/hosts** file.

## Chapter 5

---

# NetWare Server Setup

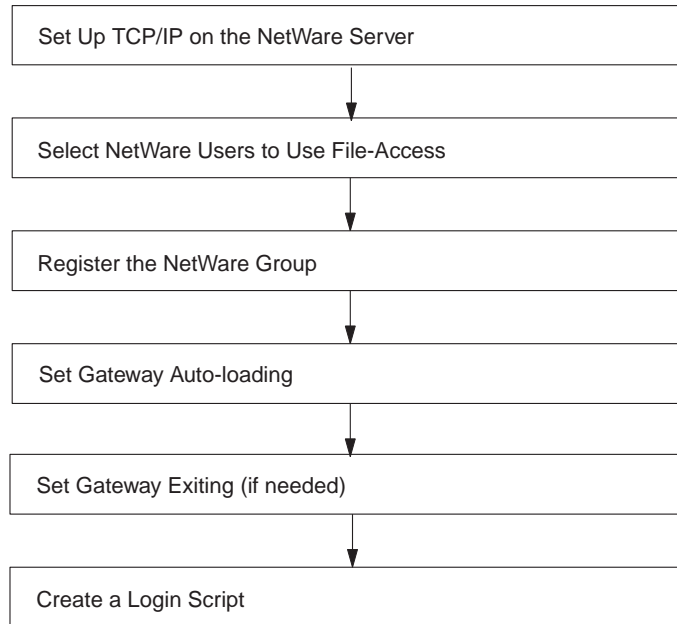
This chapter describes how to perform setup on the NetWare server. It consists of the following sections:

- NetWare Server Setup Procedure
- Setting Up TCP/IP on the NetWare Server
- Selecting NetWare Users to Use File-Access and Registering Groups
- Setting Gateway Auto-loading and Exiting and Exiting
- Creating a Login Script for Simultaneous Login

### 5.1 NetWare Server Setup Procedure

It is necessary to install Gateway and the Client utility on the NetWare server in order to set up the File-Access environment. After these utilities are installed, the NetWare administrator must set TCP/IP and create a Gateway volume dedicated to File-Access (an auto-login procedure for Gateway is optional).

The following are the NetWare server setup tasks and the topics discussed in this section:



## 5.2 Setting Up TCP/IP on the NetWare Server

File-Access uses TCP/IP for communication between DFS and NetWare. To use TCP/IP, the NetWare administrator must connect Agent and Gateway together by using the necessary statements in the **SYS:\ETC\HOSTS** and **SYS:\ETC\SERVICES** files in the NetWare server. It is also necessary to set TCP/IP to load automatically when the NetWare server is booted.

See the *Netware TCP/IP Transport Supervisor's Guide* for details regarding the configuration of the **SYS:\ETC\HOSTS** and **SYS:\ETC\SERVICES** files.

## 5.2.1 File Settings

The following information must be added to **SYS:\ETC\HOSTS** and **SYS:\ETC\SERVICES**:

- **SYS:\ETC\HOSTS**

Register an IP address and hostname for the DFS client on which Agent will be running.

- **SYS:\ETC\SERVICES**

Register DFA as the File-Access service name. In addition, register the port number of the DFS client on which Agent will be running, and set TCP as the protocol.

## 5.2.2 Setting TCP/IP Auto-loading

TCP/IP must be running before File-Access starts. Set TCP/IP auto-loading in the **AUTOEXEC.NCF** file in the NetWare server. See the NetWare manual for details regarding TCP/IP loading and editing the **AUTOEXEC.NCF** file.

## 5.2.3 Important Points

File contents cannot be guaranteed if **TCPIP.NLM** is exited while File-Access is running. When **TCPIP.NLM** is exited, File-Access will be exited because Gateway-Agent communication cannot be continued.

## 5.3 Selecting NetWare Users to Use File-Access and Registering Groups

The NetWare administrator sets the NetWare users (Gateway users) who are to use File-Access, and registers the NetWare groups as Gateway groups.

### 5.3.1 Selecting Gateway Users

The NetWare administrator selects Gateway users or creates new NetWare users who are to be File-Access users. Be sure to include a **SUPERVISOR** among the File-Access users since the system uses the name of the DCE user who is the **SUPERVISOR** when copying the DCE directories to the Gateway volume.

### 5.3.2 Registering the NetWare Group

The DCE access control list (ACL) determines the directory and file access rights on the Gateway volumes. Therefore, you cannot assign NetWare groups any directory and file access rights in Gateway volumes. In Gateway volumes, the NetWare administrator must assign directory and file access rights to Gateway groups that correspond to DCE groups. Each Gateway group has a NetWare group name, allowing it to be checked through a NetWare client. Thus, the NetWare administrator must register NetWare groups that serve only as Gateway group names. DCE has no rights equivalent to NetWare's Inherited Rights Mask, and there are no unspecified user's or group's rights. Unspecified rights for users and groups on DCE are set in the **other\_obj** entry of the ACL. In addition, DCE has a **mask\_obj** entry that limits the rights of specified users or groups that are not owners of DCE directories or files. File-Access treats these ACL entries as Gateway groups. Users can set rights for these groups. See Chapter 7 for details regarding **other\_obj** and **mask\_obj** entries.

The NetWare administrator should register the necessary number of NetWare groups, including those associated with **other\_obj** and **mask\_obj**. Note that it is not necessary to register the members of these groups.

## 5.4 Setting Gateway Auto-loading and Exiting

This section describes the procedure for setting Gateway auto-loading. Load the **DFA.NLM** file to start Gateway.

If you have created your own NetWare exit script, you can add Gateway exiting procedures to it.

## 5.4.1 Gateway Auto-loading and Exiting

To load Gateway automatically, **DFA.NLM** must be added to the **AUTOEXEC.NCF** file on the NetWare server. The following is the Gateway auto-loading setting procedure:

1. Load the NetWare installation utility and select **Edit AUTOEXEC.NCF file**. See the NetWare manual for details regarding the installation utility.
2. Add the following statement to the **AUTOEXEC.NCF** file: **LOAD DFA.NLM**
3. Save the **AUTO/EXEC.NCF** file and exit the NetWare installation utility.

## 5.4.2 Exiting Gateway

If you have your own NetWare exit script, add a **DFASTOP** command before the **DOWN** command as follows:

```
...  
...  
...  
DFASTOP  
DOWN
```

## 5.5 Creating a Login Script

This section describes how to create a login script for Gateway users to log into both DCE and NetWare simultaneously. It also describes how to create a batch file to delete drive mapping automatically when Gateway users log out of DCE.

### 5.5.1 Simultaneous Login

Gateway users must log into DCE to access DFS files from MS-DOS. DCE login must be performed after NetWare login. After DCE login, the Gateway volume must

be mapped to the drive. These operations can be simplified and shortened by creating a NetWare system login script or user login script.

Create a system login script in cases where all user-mapping settings are the same. If the mapping settings vary from user to user, the File-Access administrator should instruct users to create their own user login script or batch file for login. See the *DCE 1.2.2 File-Access User's Guide* for details regarding user login scripts and creating batch files.

## 5.5.2 Creating a Login Script

Use the NetWare **SYSCON** utility to create the login script file for simultaneous login to NetWare and DCE. See the NetWare manual for details regarding **SYSCON**. The following commands are added to the login script:

- **DLOGIN** to log into DCE
- **MAP** to map a Gateway volume to a NetWare drive

Below is an example of a login script. This login script is used to log into DCE and map the Gateway volume to a NetWare drive automatically. Do the following before executing the **DLOGIN** command:

1. Map the NetWare **SYS** volume to a network drive.
2. Set a search path to **SYS:\PUBLIC**.

```
#DLOGIN NetWare server name
if ERROR_LEVEL = "0" THEN
MAP <Network_Drive_Number> = <NetWare_server_name> \
<Gateway_volume_name> :
MAP <Network_Drive_Number> = <NetWare_server_name> \
<Gateway_volume_name directory_name>
...
...
...
END
```



### 5.5.3 Automatic Drive Map Cancellation

When you log out from DCE after accessing a DFS directory or file, the Gateway volume mapping process is not canceled. If you continue NetWare operations without canceling the mapping process, you can see the directory structure in the Gateway volume, but you cannot access the directories or files. Cancel the Gateway volume mapping process every time you log out of DCE. If you want to log out of DCE and cancel the mapping process at the same time, create a batch file to cancel the mapping during DCE logout.

If you log out of DCE and then log out of NetWare, the mapping to the NetWare server volume is canceled automatically and you will not need to create a batch file.

Use the following commands in the batch file to log out of DCE and cancel the mapping process at the same time:

- **MAP del** to cancel the Gateway volume mapping
- **DLOGOUT** to log out of DCE

The following is an example of a batch file:

```
MAP del *Network drive number
...
...
...
DLOGOUT NetWare server name
```



## Chapter 6

---

# Setting up the NetWare Server Environment with Administration Utility

The settings described in Chapters 4 and 5 are not sufficient to run File-Access. The proper NetWare server environment must also be set up with the Gateway Administration utility. This chapter describes how to log into the Administration utility as well as how to set up the NetWare server environment. It includes the following topics:

- Environment Setup Procedure
- Administration Utility Startup and Login
- Environment Setup During Initial Installation
- Deleting the Gateway Volume
- Changing the Mount Point
- Changing the Master Key
- Deleting the Gateway User

- Changing the DCE Username for the Gateway User
- Changing the DCE Group Associated with a Gateway Group

## 6.1 Environment Setup Procedure

You must set up the NetWare server environment after you set up the NetWare server. Set up the NetWare server environment by using the Gateway Administration utility.

### 6.1.1 Administration Utility Functions

The Administration utility has the following functions available for setting the NetWare server environment:

- Registering and deleting Gateway volumes  
The Gateway Administration utility allows you to register or delete File-Access NetWare volumes as Gateway volumes.
- Setting or changing the mount point  
You can change the DFS directory point registered as the Gateway volume root directory. This directory point is also known as the mount point.
- Registering the Agent machine  
With the Administration utility, you can register the DFS client in which Agent is installed. The DFS client (Agent) cannot be registered while Gateway is running.
- Registering and changing the master key  
You can register or change the master key for data encryption used in communication between Gateway and Agent.
- Registering and deleting Gateway users  
NetWare users can be registered or deleted as Gateway users by setting correspondences between NetWare usernames and DCE usernames. The **SUPERVISOR** must be registered as a Gateway user in all cases.
- Setting a temporary password

The administrator registers temporary passwords for Gateway users. These temporary passwords differ from those that Gateway users use as DCE users (DCE passwords). This difference is why Gateway users logging into DCE from the NetWare client for the first time via File-Access must change their temporary passwords to their DCE passwords.

- Setting and registering Gateway groups

If you need to organize Gateway users into groups and to assign trustee rights to each group, register a File-Access group (Gateway group) that corresponds to a DCE group whose ACLs are set to the NetWare group with the desired trustee rights. You must first register the DCE user as a Gateway user in the DCE group.

- Setting options

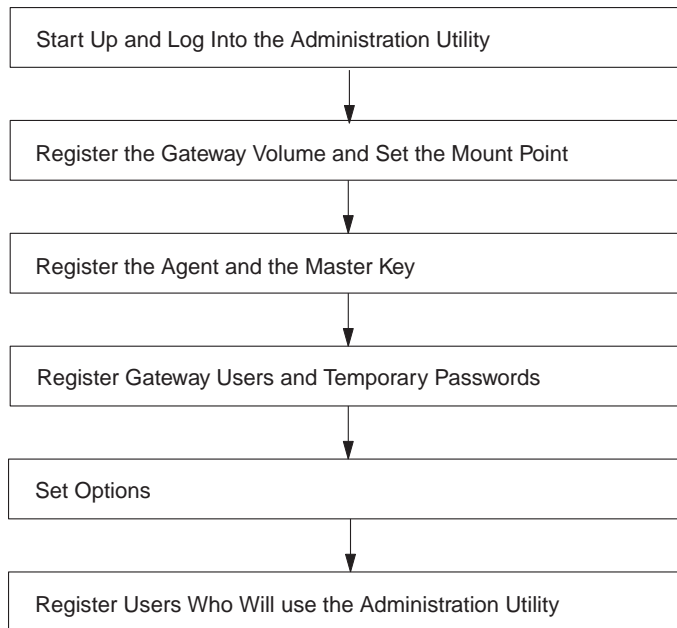
The Administration utility allows you to set various options, such as the time interval at which the configuration of directories and files in the Gateway volume is synchronized with the new DFS directory configuration. You can also set an option to include the Agent-Gateway maximum response time and the maximum time to wait for connection.

- Registering users who can use the Administration utility

You must register the Gateway users who are allowed to use the Administration utility.

### **6.1.2 Setting Up the Environment**

The following diagram shows the initial procedure for setting up the File-Access environment with the functions provided by the Administration utility.



See the following sections for information on changing the File-Access environment once it is set up:

- Deleting the Gateway Volume
- Changing the Mount Point
- Changing the Master Key
- Deleting the Gateway User
- Changing the DCE Username That Corresponds to a Gateway User
- Changing the DCE Group That Corresponds to a Gateway Group

## 6.2 Administration Utility Startup and Login

You can start up the Administration utility from the NetWare server on which Gateway is installed. The Administration utility can be used by the **SUPERVISOR** and by those Gateway users who are registered to use it. See “Registering Users Who Can Use the Administration Utility” for details regarding the registration of users for the Administration utility.

### 6.2.1 Administration Utility Startup

Enter the following command from the NetWare server where Gateway is installed to start the Administration utility:

```
LOAD [SYS:\SYSTEM\] DFAADM [.NLM]
```

### 6.2.2 Logging into the Administration Utility

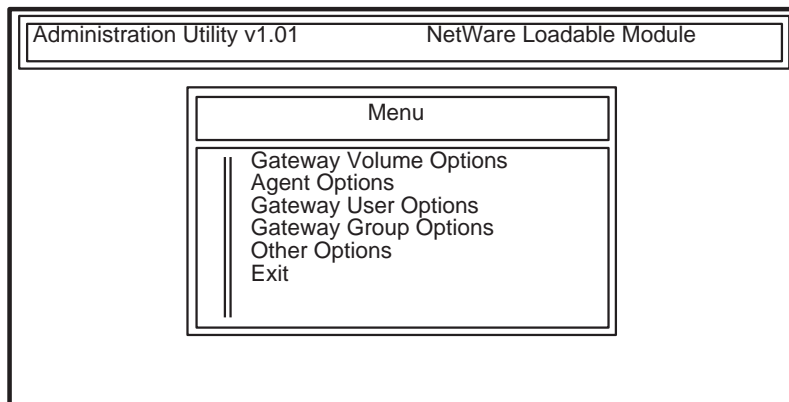
When the Administration utility is started, the following login screen is displayed for entering the Gateway username and password. Initially, only the **SUPERVISOR** can log into the Administration utility.

Username: **SUPERVISOR**

Password:

The Administration utility main menu shown in Figure 6-1 is displayed when you enter the username and NetWare password.

Figure 6–1. Administration Utility Main Menu



### 6.3 Administration Utility Operations

The key actions in the Gateway Administration utility are the same as the NetWare Installation utility. Table 6-1 shows the key assignments for the Administration utility functions.

Table 6–1. Key Assignments for Administration Utility Functions

Key	Functions
< Backspace>	Deletes the character to the left of the cursor.
< Escape>	Returns to the previous box.
< Enter>	Selects a field in the list.
< Insert>	Inserts a new field.
< Delete>	Deletes a field.
Up-arrow key	Moves up one field.
Down-arrow key	Moves down one field.
Left-arrow key	Moves the cursor to the left.



<b>Key</b>	<b>Functions</b>
<b>Right-arrow key</b>	Moves the cursor to the right.
<b>&lt; Page Up&gt;</b>	Scrolls down the list to the previous page.
<b>&lt; Page Down&gt;</b>	Scrolls up the list to the next page.
<b>&lt; Ctrl+Page Up&gt;</b>	Moves the cursor to the beginning of the list.
<b>&lt; Ctrl+ Page Down&gt;</b>	Moves the cursor to the end of the list.
<b>&lt; Home&gt;</b>	Moves the cursor to the beginning of the line.
<b>&lt; End&gt;</b>	Moves the cursor to the end of the line.
<b>Y</b>	Selects <b>Yes</b> in a Yes/No option.
<b>N</b>	Selects <b>No</b> in a Yes/No option.

Be sure to enter the DCE username, temporary password, and other necessary information when you register a Gateway user. Table 6-2 describes the restrictions on those characters you can enter.

Table 6-2. Input Information and Restrictions on Entered Characters

<b>Input Information</b>	<b>Restrictions on Entered Characters</b>
Gateway Username	Spaces and lowercase letters cannot be used.
NetWare Password	Spaces and lowercase letters cannot be used.
DFS Mount Point	No restrictions.
Master Key	No restrictions.
DCE Username	No restrictions.
Temporary Password	No restrictions.
DCE Group Name	No restrictions.

## 6.4 Environment Setup During Initial Installation

The following subsections lead you through a sample setup process for the File-Access environment, using this example:

Create a File-Access environment with the network environment and directory structure shown in Figure 6-2. Set correspondences between File-Access and DCE groups and users as shown in Figure 6-3.

Figure 6-2. Example of File-Access Environment

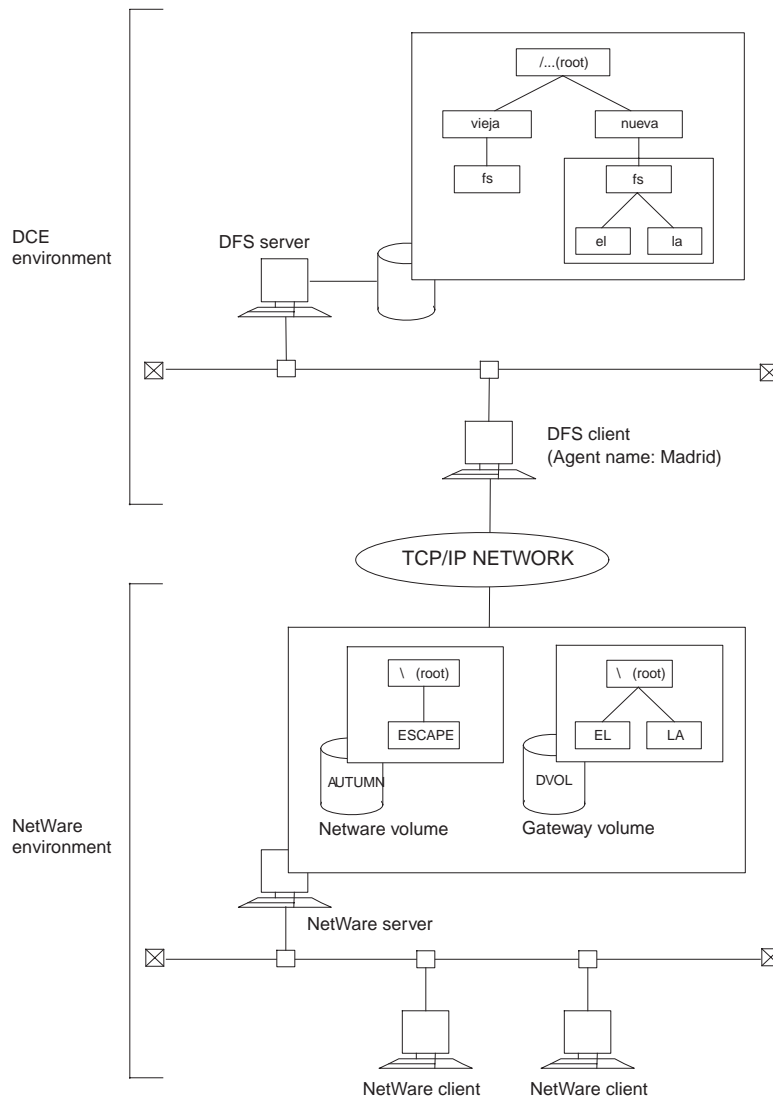


Figure 6–3. Example of Correspondences Between DCE and File-Access Groups and Users

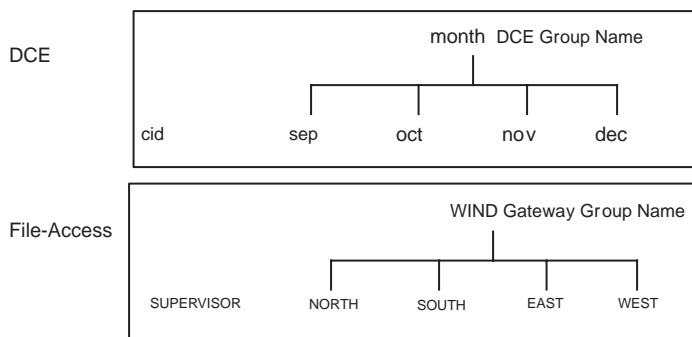


Table 6-3 presents the information set in the Administration utility when you set up the File-Access environment as shown in Figure 6-3.

Table 6–3. Information Set in Administration Utility

Information	Contents
Gateway volume	<b>DVOL</b>
Mount point	<b>.../nueva/fs</b>
Agent name	<b>Madrid</b>
Master key	<b>pyrenees</b>
Gateway username	<b>SUPERVISOR, NORTH, SOUTH, EAST, WEST</b>
DCE username (for Gateway user)	<b>cid, sep, oct, nov, dec</b>
Gateway group name	<b>WIND</b>
DCE group name (for Gateway group name)	<b>month</b>
Gateway group name for ACL <b>other_obj</b> Entry	<b>OTHER</b>

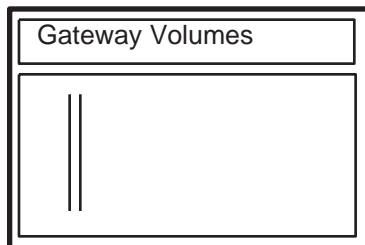
Information	Contents
Gateway group name for ACL <code>mask_obj</code>	<b>MASK</b>
User Permitted to Use Administration Utility	<b>NORTH</b>

## 6.4.1 Registering the Gateway Volume and Setting the Mount Point

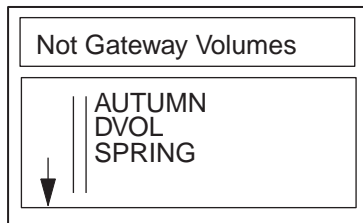
You must register a NetWare volume as a Gateway volume and set the mount point. In this example, **DVOL** is registered as the Gateway volume name and `/.../nueva/fs` is registered as the mount point.

### 6.4.1.1 Operations

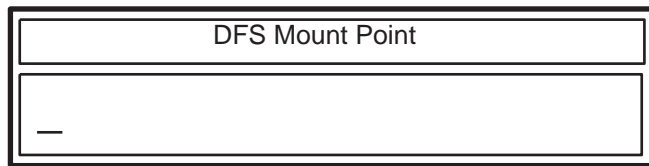
1. Select **Gateway Volume Options** in the main menu to display the Gateway volume list. So far, nothing has been registered.



2. Press `< Insert >`. A list of NetWare volumes not registered as Gateway volumes is displayed in ASCII code, in alphabetical order.



3. Select the NetWare volumes that are to be registered as Gateway volumes. In this example, **DVOL** is selected. The DFS mount point input box is displayed.



4. Enter **/.../nueva/fs** as the DFS mount point corresponding to the Gateway volume. Press < **Enter**>.

The mount point name must include the DFS junction name **/.../cell name/fs**. The maximum length of the mount point name is 1,022 characters; 78 characters can be displayed in the box at one time. When you enter the mount point name by pressing < **Enter**>, the name is registered in the Gateway directory and the corresponding DFS subdirectory. The Gateway volume list display is then restored.

#### 6.4.1.2 Important Points

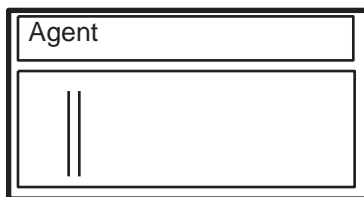
The NetWare volumes registered as Gateway volumes are initialized every time you start File-Access. If you create files on the Gateway volumes through NetWare while File-Access is not running, the files are not saved.

## 6.4.2 Registering Agent and the Master Key

Register the Agent-installed DFS client and a master key for data encryption in Gateway. In this example, the Agent hostname is **Madrid** and the master key is **pyrenees**.

### 6.4.2.1 Operations

1. Select **Agent Options** from the main menu. An empty **Agent Name** box is displayed.



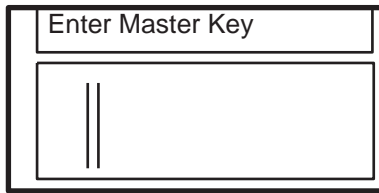
A screenshot of a terminal window showing a text input field labeled "Agent". The field is empty, with two vertical cursor lines on the left side.

2. Press < **Insert**>. The Agent hostname list recorded in the **SYS:\ETC\HOSTS** file is displayed in ASCII code, in alphabetical order.



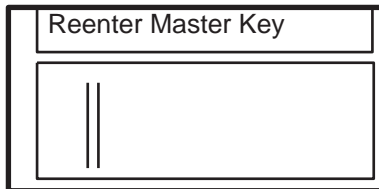
A screenshot of a terminal window showing a list of hostnames. The title bar reads "Not Agents". The list contains the following entries: Berlin, London, Madrid, and Rome. A vertical cursor line is on the left, and a downward-pointing arrow is positioned at the bottom of the list.

3. Select **Madrid** and press < **Enter**>. The **Master Key** box is displayed.



4. Enter **pyrenees** as the master key. Enter the master key registered in Agent. If the master key is different from the master key in Agent, Gateway users cannot log into DCE. The master key is not displayed in the box for security reasons.

After entering the master key, press < **Enter**> and the **Reenter master key** box is displayed.



5. Reenter the master key. If the master key is identical to the previously entered master key, the Agent machine and the master key are registered and the screen displays the **Agent Name** box.

### 6.4.2.2 Important Points

- Confirm that the hostname has been registered in the **SYS:\ETC\HOSTS** file before registering Agent.
- Agent and the master key cannot be changed when Gateway is running. Exit Gateway in order to change Agent or the master key.

## 6.4.3 Registering Gateway Users and Temporary Passwords

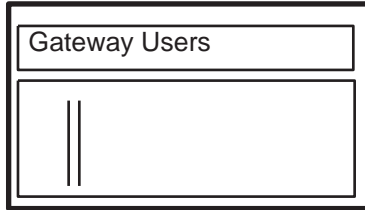
Set DCE users registered in DCE to correspond to Gateway users. Next, register in Gateway a temporary password that is used only for the Gateway user's first login. (Gateway users change their temporary password to their DCE password during the



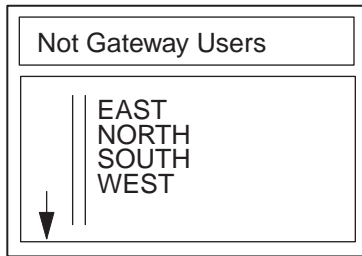
first login.) In this example, the Gateway username is **NORTH** and the DCE username is **sep**.

### 6.4.3.1 Operations

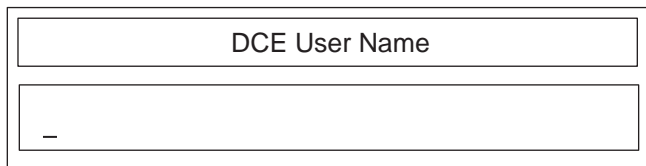
1. Select **Gateway User Options** from the main menu. The **Gateway Users** box is displayed. No one is currently registered.



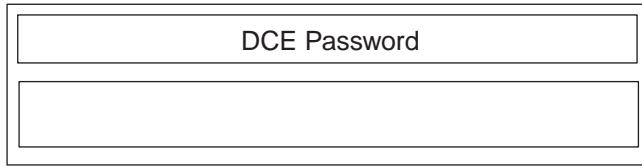
2. Press < **Insert**>. A **NetWare Users** list box showing NetWare users who are not registered in Gateway is displayed in ASCII code, in alphabetical order.



3. Select **NORTH** and press < **Enter**>. The **DCE Username** box is displayed.



4. Enter **sep**, which is the DCE username, and press < **Enter**>. Note: For the DCE username (a maximum of 1,024 characters can be entered, and 78 characters can be displayed at a time). The **DCE Password** box is displayed.

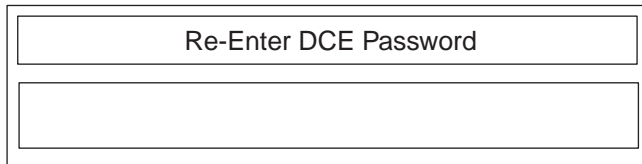


The image shows a rectangular dialog box with a double border. Inside, there are two horizontal input fields. The top field is labeled "DCE Password" in the center. The bottom field is empty.

5. Enter the temporary password for the Gateway user **NORTH**. You should inform the user what password to use when logging in for the first time.

After setup is completed, user **NORTH** will change this temporary password to the DCE password for the DCE user **sep** before logging into DCE from the NetWare client for the first time. This temporary password is not displayed on the screen.

The **Reenter DCE Password** box is displayed upon entering the temporary password and pressing < **Enter**>.



The image shows a rectangular dialog box with a double border. Inside, there are two horizontal input fields. The top field is labeled "Re-Enter DCE Password" in the center. The bottom field is empty.

6. Reenter the temporary password. If the reentered password is the same as the previously entered password, the Gateway user and DCE password are registered and the **Gateway Users** box screen display is restored.

Register **SUPERVISOR**, **EAST**, **SOUTH**, and **WEST** in the same manner.

### 6.4.3.2 Important Points

- A **SUPERVISOR** must be registered as a Gateway user because Gateway uses the name of the DCE user who is the **SUPERVISOR** to log into DCE to copy the DCE tree structure to the Gateway volume.
- Gateway users cannot log into DCE if their DCE passwords do not match the passwords set in File-Access. File-Access administrators have to inform the Gateway users of their temporary passwords so that the Gateway users can change them to their DCE passwords.

### 6.4.4 Registering the Gateway Group

Access rights for Gateway users to a Gateway volume depend on the DCE ACL. Thus, Gateway users or groups must correspond to ACL entries. To assign rights group by group, set a DCE group with an ACL setting to correspond to a trustee that is set as the desired NetWare group. The system then registers the group as a File-Access group (Gateway group). It is not necessary to register members for a NetWare group that is registered as a Gateway group as long as a name is registered.

A Gateway volume does not have NetWare's Inherited Rights Mask (IRM), and no rights are assigned automatically to unspecified users and groups. Rights for unspecified Gateway users and groups are determined by rights in the ACL **other\_obj** entry. DFS has a **mask\_obj** entry that sets restrictions on the rights of specific users and groups that are not owners of directories and files.

File-Access treats **other\_obj** and **mask\_obj** entries as the DCE group's **DFA\_OTHER\_GROUP** and **DFA\_MASK\_OBJ** entries, respectively. The corresponding NetWare groups are given trustee rights. **DFA\_MASK\_OBJ** entry mapping is not necessary if UFS (UNIX File System), which does not have a **mask\_obj** entry, is used. See Chapter 7 for details regarding **other\_obj** and **mask\_obj** entries.

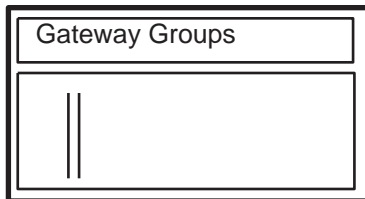
Before Gateway group registration, you have to register the NetWare group and DCE group in NetWare and DCE, respectively. See the NetWare manual for registering the NetWare group. See the *DCE 1.2.2 Administration Guide—Introduction* for details regarding how to create DCE groups.

### 6.4.4.1 Registering Gateway Groups for **other\_obj** and **mask\_obj**

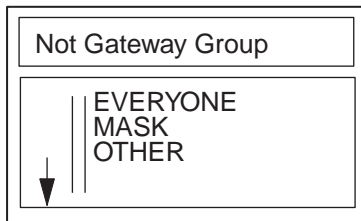
To register a Gateway group, select a NetWare group name and map it to a DCE group. For Gateway groups in which rights for unspecified users or groups are set, map the NetWare group to **DFA\_OTHER\_GROUP** instead of the DCE group name since the group is associated with the ACL **other\_obj** entry. DFS has a **mask\_obj** entry that sets restrictions on the rights of specific users and groups that are not owners of directories and files. Gateway groups that are used for setting rights in the **mask\_obj** entry are mapped to **DFA\_MASK\_OBJ**.

In the following example, the NetWare group **OTHER** and **MASK** are respectively mapped to **other\_obj** and **mask\_obj** as Gateway groups.

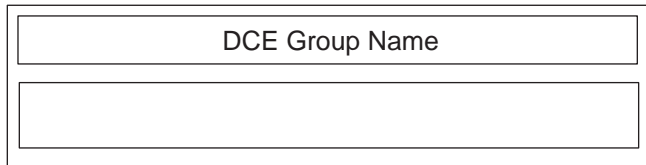
1. Select **Gateway Group Options** from the main menu. The **Gateway Groups** box is displayed. No group is currently registered.



2. Press < **Insert**>. A list of NetWare groups that are not registered as Gateway groups is displayed in ASCII code, in alphabetical order.



3. Select **OTHER**. The **DCE Group Name** box is displayed.



4. Enter **DFA\_OTHER\_GROUP** and press < **Enter**>. The Gateway group **OTHER** is registered and the screen returns to the **Gateway Groups** box. Map the NetWare group **MASK** to **DFA\_MASK\_OBJ** as a Gateway group in the same manner.

#### 6.4.4.2 Group Registration with DCE Group Correspondence

To use access rights corresponding to a DCE group, register the group as a File-Access Gateway group, with the DCE group and NetWare group associated with each other.

In the following example, the Gateway group **WIND** is mapped to the DCE group **month**.

1. Select **Gateway Group Options** in the main menu. The **Gateway Groups** box is displayed.
2. Press < **Insert**>. A list of NetWare groups that are not registered as Gateway groups is displayed.
3. Select **WIND**. The **DCE Group Name** box is displayed.
4. Enter the DCE group name **month**. **WIND** is registered as the Gateway group name and the **Gateway Groups** box screen display is restored.

#### 6.4.4.3 Important Points

Be sure to register the primary DCE group name if it is associated with a Gateway group. If a different name is registered, File-Access treats that name as the primary name. This creates the risk of errors, and the file or directory access rights may not function correctly.

## 6.4.5 Setting Options

The following options can be set in File-Access:

- **Time Synchronization**

Use this option to set the NetWare server local time if it is to be synchronized with Coordinated Universal Time (UTC). UTC is set in the DFS client running Agent when Gateway is started and when a Gateway user logs into DCE. The default setting is **No** (that is, not synchronized).

- **Warning on Mounting a Non-clear Volume**

This feature displays a warning message when the Gateway volume contains a file or directory before Gateway startup. The default setting is **No** (that is, no warning).

- **Copy Back Delay Time**

This is the estimated delay time for copying Gateway files back to DCE. You can set this value from 0 to 10,000 milliseconds. The default delay time is 1,000 milliseconds.

- **Directory Synchronization Interval**

File-Access periodically synchronizes the Gateway volume virtual directory tree structure with the DFS file system directory tree structure. This is called the directory synchronization function, and it is possible to set the interval time of this function. The interval time can be from 0 to 1,440 (minutes). The default interval time is 5 minutes.

- **Agent-Gateway Maximum Response Time**

If the period of time specified for this option passed in the communication between Agent and Gateway, File-Access assumes a time-out has occurred. The time-out interval can be from 1 to 32,767 seconds; the default value is 120 minutes.

- **Maximum Time to Wait for Connection**

The maximum waiting time to establish a connection between Agent and Gateway. The length of time ranges from 1 to 32,767 seconds, and the default value is 45 seconds.

- **Delayed Time for Sparsed File**

This option specifies the delayed time between the file closing and the file sparsing. You can take advantage of this option when the same file is accessed in the delayed

period. The delay time can be from 0 to 10 minutes, and the default value is 0 (which means this option is deactivated).

### 6.4.5.1 Setting the Options

This section leads you through a sample session for setting options, using the following values:

- Time Synchronization: Yes
  - Warning on Mounting a non-clear Volume: Yes
  - Copy Back Delay Time: 1,500 (milliseconds)
  - Directory Synchronization Interval Time: 10 (minutes)
1. Select **Other Options** from the main menu. The **Other Options** box is displayed.

Other Options	
Time Synchronization:	No
Warning on Mounting Non-clear Volume:	No
Copy Back Delay Time:	1000 (milli-seconds)
Directory Synchronization Interval:	5 (minutes)
Agent-Gateway Maximum Response Time:	120 (seconds)
Maximum Time to Wait for Connection:	45 (seconds)
Delayed Time for Sparse File	0 (minutes)

2. Enter the value for each option by moving the cursor to each option and entering its value.
3. Press < **Escape**>. The Other Options information is registered. The menu then returns to the main menu.

### 6.4.5.2 Important Points

You must observe the following requirements when you set options:

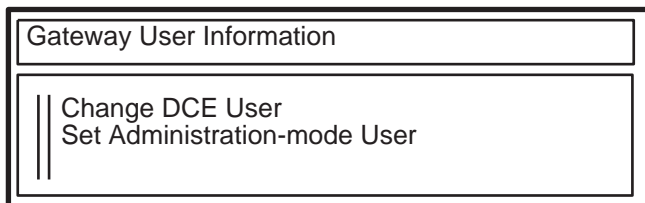
- Gateway Backup Directory  
Specify all optional information according to the characteristics of your network.
- Time synchronization  
Synchronize the system time of the DFS client on which Agent is running to UTC. DCE Distributed Time Service must be running to do this.  
Set the NetWare server Time Zone using the NetWare **SET TIMEZONE** command. (See the NetWare manual for details.)

## 6.4.6 Registering Users Who Can Use the Administration Utility

Only the NetWare **SUPERVISOR** can initially use the Administration utility when a new environment is being set up. A registered Gateway user can use it only after being registered as a user who can use the Administration utility. The following procedure describes how to register a user who can use the Administration utility.

### 6.4.6.1 Operations

1. Select **USER Options** from the main menu. The **Gateway Users** box is displayed.
2. Select the Gateway user you are going to register. The **Gateway User Information** box is displayed.



3. Select **Set Administration-mode User**. The **Administration-mode** box is displayed.



Administration-mode
Administration-mode User : No

4. Select **Yes**. The selected Gateway user is registered as a user who can use the Administration utility.

## 6.5 Deleting the Gateway Volume

Use the following procedure to delete a registered Gateway volume:

1. Select **Gateway Volume Options** from the main menu. The **Gateway Volume** box is displayed.
2. Move the cursor to the Gateway volume you want to delete, then press **Delete**. The **Delete Gateway Volume** confirmation box is displayed.

Delete Gateway Volume
No    Yes

3. Select **Yes**. The selected volume is deleted, and the **Gateway Volume** box is displayed.

## 6.6 Changing the Mount Point

Use the following procedure to change the DFS subdirectory that corresponds to the Gateway volume:

1. Select **Gateway Volume Options** from the main menu. Then select the Gateway volume on which you are going to change the mount point. The **DFS Mount Point** box is displayed.

2. Enter the new mount point. The mount point name must include the DFS junction name `/.../cell name/fs`.
3. Press < **Enter**>. The **Change Mount Point** confirmation box is displayed.
4. Select **Yes**. The new mount point is registered.

## 6.7 Changing the Master Key

You need to change the master key (for data encryption) in the following cases:

- When Agent moves to a different host
- When the security (or integrity) of data is lost

### 6.7.1 The Master Key Change Procedure

Use the following procedure to change the master key.

1. Select **Agent Options** from the main menu. The **Agent** box is displayed.
2. Press < **Enter**>. The **Enter Master Key** box is displayed.
3. Enter the new master key. The **Reenter Master Key** box is displayed after you enter the master key.
4. Reenter the new master key. The master key is registered if the reentered master key is the same as the previously entered master key. The menu then returns to the **Agent** box.

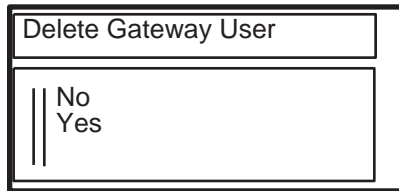
### 6.7.2 Important Points

- Exit File-Access before changing the master key.
- Be sure to change the master key on both Agent and Gateway.

## 6.8 Deleting the Gateway User

Use the following procedure to delete a Gateway user:

1. Select **Gateway User Options** from the main menu. The **Gateway Users** box is displayed.
2. Move the cursor to the Gateway user you want to delete, then press **Delete**. The **Delete Gateway User** confirmation box is displayed.



3. Select **Yes**. The designated Gateway user is deleted.

**Caution:** If you use a Netware command to delete a NetWare user who is registered as a Gateway user, the user's Gateway user registration is deleted as well.

## 6.9 Changing the DCE Username for the Gateway User

If you changed a Gateway user's DCE username, the DCE username registered in the Administration utility must be changed as well. After changing the DCE username, the File-Access administrator must set a temporary password for the Gateway user and then inform that user of the temporary password. The Gateway users should change the temporary passwords to their DCE passwords when they log into DCE the next time.

Use the following procedure to change the DCE username for the Gateway user:

1. From the **Gateway Users** box, select the Gateway user whose associated DCE username is to be changed. The **Gateway User** information box is displayed.
2. Select **Change DCE User**. The **DCE Username** box is displayed.
3. Enter the new DCE username.

4. Enter the temporary password.
5. Reenter the temporary password. The new DCE username and the temporary password are registered if the reentered password is the same as the previously entered password. The **Gateway Users** box is displayed.

## 6.10 Changing the DCE Group Associated with a Gateway Group

You must change the DCE group associated with a Gateway group when the DCE group on DCE is changed. Use the following procedure to accomplish this task:

1. Select **Gateway Group Options** from the main menu. The **DCE Group** box is displayed.
2. Select the Gateway group whose associated DCE group is to be changed. The **DCE Group Name** box is displayed.
3. Enter the new DCE group name and press **Enter**. The new DCE group is matched to the Gateway group, and the screen returns to the **Gateway Group** box.

## Chapter 7

---

# File-Access Administration and Maintenance

DCE and NetWare differ in many ways, such as in directory and file access right settings, and in filename limitations. This chapter describes the basic differences that File-Access administrators should be aware of. This chapter also explains the procedures that the File-Access administrator needs to perform when a failure occurs.

### 7.1 Rights

Gateway users can access DFS directories and files on DCE from NetWare. However, DCE and NetWare differ in terms of the types of rights for accessing directories and files, and the users to whom rights are granted. The following subsections describe how File-Access adjusts for such differences between NetWare and DCE.

## 7.1.1 File-Access Rights

Both NetWare and DCE allow you to set rights for individual directories and files. Rights in NetWare are determined by trustee rights settings and inherited rights mask settings. DCE/DFS rights are determined by ACL settings.

### 7.1.1.1 Differences Between NetWare and DCE Rights

Table 7-1 shows NetWare rights, and Table 7-2 lists the DCE/DFS rights that are set through ACLs. By comparing the tables, you can see many differences.

Table 7-1. NetWare Rights

Type	Directory Rights	File Rights
S (Supervisory)	All rights to the directory.	All rights to the file.
R (Read)	Open files in a directory and read their contents or run the programs.	Open and read the file.
W (Write)	Open and modify files in the directory.	Open and write to the file.
C (Create)	Create files and subdirectories in the directory.	Salvage (recover) a file after it has been deleted.
E (Erase)	Delete a directory, its files, its subdirectories, and its subdirectory files.	Delete the file.
M (Modify)	Change subdirectory and file attributes. Rename the subdirectory and its files.	Change the file's attributes and rename the file.
F (File Scan)	Scan files in a directory.	See the filename when viewing the directory.
A (Access Control)	Modify trustee rights for a directory, file or inherited rights mask.	Modify trustee rights for a file or the inherited rights mask.

Table 7–2. Rights Set Through ACLs

Type	Directory Rights	File Rights
r (read)	See a list of directories and read ACL.	Read the file contents.
w (write)	Write in a directory.	Write to a file.
x (execute)	Same as r.	Execute a file.
c (control)	Modify ACL for a directory.	Modify ACL for a file.
i (insert)	Create subdirectories or files or modify their names in a directory.	Not applicable.
d (delete)	Delete subdirectories or files from a directory.	Not applicable.

### 7.1.1.2 File-Access Rights

File-Access rights and NetWare rights are the same with the following three exceptions:

- **Q** (Qualified) Rights

File-Access provides qualified rights (**Q**) only for Gateway volumes. These rights can be set on directories and files on a Gateway volume. Users or groups who have this right can create directories and files and write to them, but they do not have the right to delete directories or files.

- **E** (Erase) Right for Directory

The **E** right for File-Access directories in the Gateway volume makes it possible to delete subdirectories and files, but the directory itself cannot be deleted. If you need to delete a directory, assign the **E** right to its parent directory. (With NetWare, you can use the **E** right to delete the directory in which it is set.)

- **S** (Supervisory)

The supervisory right is invalid in the Gateway volume.

Table 7-3 illustrates File-Access rights, including the qualified rights.

Table 7-3. File-Access Rights

Type	Directory Rights	File Rights
R (Read)	Open files in a directory and read their contents or run the programs.	Open and read the file.
W (Write)	Open and modify files in the directory.	Open and write to the file.
C (Create)	Create files and subdirectories in a directory.	Not applicable.
E (Erase)	Delete a directory, its files, its subdirectories, and its subdirectory files.	Delete the file.
M (Modify)	Change directory and file attributes. Rename the directory and its files.	Change the file's attributes and rename the file.
F (File Scan)	Scan files in a directory.	See the filename when viewing the directory.
A (Access Control)	Modify trustee rights for directories and files.	Modify trustee rights for files.
Q (Qualified)	Directories can be created and their names can be changed, but they cannot be deleted.	Files can be written to, but they cannot be deleted.

With Netware, you can add or delete all rights other than those assigned to the SUPERVISOR. With File-Access, users who own directories or files, and users with DFS root rights, cannot delete access control rights ( **A**).

### 7.1.1.3 Important Points

Do not set NetWare directory and file attributes to directories and files in the Gateway volume. The contents of DFS directories and files are different from those in the Gateway volume if you set these attributes.



## 7.1.2 Users and Groups

With NetWare, the rights granted to a directory are inherited to the files under that directory. However, with DCE, rights must be granted to both files and directories. This is because the target files and directories to which NetWare trustee rights are granted are different from the target files and directories of the DCE ACL. The users or groups with these rights are called trustees in NetWare and in DCE ACL entries. This subsection describes these differences.

In NetWare directories and files, you can grant rights to the following two entities:

- Users
- Groups

There are 11 rights-holders for ACL entries, and File-Access uses the following 6:

- **user\_obj** (directory or file owner)
- **user** (specified user in the same cell)
- **group\_obj** (group member who possesses the directory or file)
- **group** (specific group in the same cell)
- **other\_obj** (user in the same cell who does not belong to any of the other listed entries)
- **mask\_obj** (limits entry rights to those who are not **user\_obj** and **other\_obj**)

NetWare does not have rights-holders corresponding to ACL **mask\_obj** and **other\_obj**. The File-Access administrator must register a Gateway group for these entries. See Chapter 6 for details on how to register Gateway groups in association with **other\_obj** and **mask\_obj**.

## 7.1.3 Trustee Rights and Effective Rights

Effective rights are the rights that a user can actually exercise in a given directory or file. Gateway users have trustee rights and effective rights for files and directories in a Gateway volume, just as they do in NetWare. File-Access trustee rights are set through command-line settings or menu commands with respect to trustees (users or groups) for directories or files, just as they are in NetWare. The effective rights of a

rights-holder who does not have trustee rights differ depending on whether or not the rights-holder has equivalent security rights.

### 7.1.3.1 NetWare Effective Rights

NetWare effective rights are based upon the following four points:

- If **SUPERVISOR** rights (**S**) are valid for a certain directory, the rights are valid for all subdirectories and files under that directory.
- If trustee rights are set but there is no corresponding security trustee, the effective rights are equivalent to the trustee rights.
- If trustee rights are not set, only the effective rights of the parent directory of the corresponding directory and file and the rights associated with the inherited rights mask of the directory and file are considered effective rights.
- If a corresponding security trustee exists, all of the rights of a certain corresponding security trustee are effective for all other corresponding security trustees.

### 7.1.3.2 File-Access Effective Rights

File-Access shows effective rights on DFS subdirectories and files as if they were NetWare directories and files. However, actual DFS rights and NetWare rights are much different from each other, and there are some differences between File-Access rights and NetWare rights. One of the differences is that File-Access does not have NetWare's Inherited Rights Mask.

Effective rights in File-Access depend on the following two points:

- If the user has trustee rights on the directory or file, the trustee rights are the effective rights.
- If the user does not have trustee rights on the directory or file, the rights for the Gateway group of unspecified users (which the File-Access administrator registered) are the effective rights.

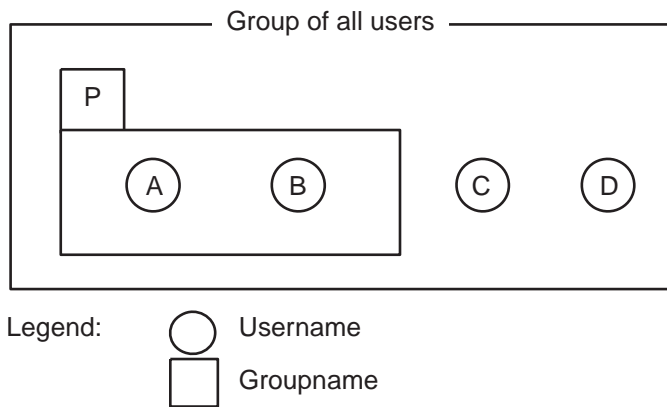
Depending on the DFS ACL **mask\_obj** entry, there is the possibility that the effective rights of trustees (other than the trustees who are not assigned rights for directories and files) will not adhere to these two points. The following subsection explains the situations where the rights do not adhere to these points.

### 7.1.3.3 Important Points About Effective Rights

The DFS ACL **mask\_obj** limits the rights of the DFS user or group entry. This restriction affects Gateway users' rights. Consider the following example:

Assume Gateway group P and Gateway users A, B, C, and D have the relationship shown in Figure 7-1:

Figure 7-1. Group and Users



The following factors determine the effective rights in addition to each trustee's rights:

- File-Access

The Gateway group trustee rights that correspond to the DFS ACL **other\_obj** and **mask\_obj**. (Their group names are **OTHER** and **MASK** in this example.)

- NetWare

The effective rights and inherited rights mask for a parent directory.

Table 7-4 shows the difference in effective rights between File-Access and NetWare, together with the criteria for trustee rights and effective rights for the rights-holders shown in Figure 7-1. Note that this example serves to clarify differences in effective rights, and thus includes some combinations of rights that cannot actually be used.

Table 7-4. Differences in Effective Rights Between File-Access and NetWare

Trustee	Trustee Rights	Effective Rights in NetWare	Effective Rights in File-Access
User A	[ RWCE F ]	[ RWCE FA ]	[ RWC F ]
User B	[ ]	[ RW FA ]	[ RW FA ]
User C	[ RWCE F ]	[ RWCE F ]	[ RWC F ]
User D	[ ]	[ RW F ]	[ R F ]
Group P	[ RW FA ]	—	—
Group OTHER	[ R F ]	—	—
Group MASK	[ RWC MFA ]	—	—
Effective Rights for the Parent Directory	[ RW FA ]	—	—
Right Inheritance Mask	[ RWC F ]	—	—

Legend: — — — No effective rights

It is important to remember that trustee rights always take precedence over effective rights in File-Access. Furthermore, the rights of the ACL **mask\_obj** entry for the Gateway group (in this case, group **MASK**) limit the rights for other Gateway users and Gateway groups.

In this example, NetWare user A belongs to group P. User A’s effective rights in NetWare are [ **RWCE FA** ]because user A has the [**A**] right in group P. But Gateway user A’s effective rights are [ **RWC F** ]and do not include [**A**] . When Gateway users have their trustee rights set both as a user and group, their group rights are ignored. If you want to add [**A**] to user A’s effective rights, you must add the [**A**] right to user A’s trustee rights.

File-Access also does not retain the rights set in the Gateway group that correspond to the **mask\_obj** entry, except for the trustees who do not have trustee rights, and the owners of directories and files. In this example, because the group MASK does not include the erase right [E], users A and C will not hold the erase right [E] under their effective rights even if [E] is set for their trustee rights. For Gateway users A and C to have the [E] right in their trustee rights, the group MASK has to have the [E] right.

If you use UFS for the DFS file system, effective rights are not restricted because UFS does not have a **mask\_obj** entry.

## 7.1.4 Rights Mapping

To control file access rights to directories or files, set the ACL for DCE and establish trustee rights for NetWare. File-Access converts the ACL to trustee rights or trustee rights to an ACL. However, File-Access sets its own trustee rights because it is not possible to convert the entire ACL to trustee rights.

The following subsections describe the ACL-to-trustee right conversion rules.

### 7.1.4.1 ACL-to-Trustee Conversion

Table 7-5 shows the basic rules of converting ACL rights to trustee rights.

Table 7-5. Rules for Converting ACL to Trustee Rights

ACL	NetWare Rights	
	Directory	File
r	F	RF
w	—	WCQ
x	F	RF
c	A	A
wxi	WCFQ	—

ACL	NetWare Rights	
	Directory	File
wxd	EF	—
wxid	WCEMF	—

**Note:** A dash ( — ) indicates that the right will not be effective even if it is set.

The conversion rules for directories and files are different, as follows.

#### 7.1.4.1.1 Directories

- If only **r**, **x**, and **c** rights are combined, the trustee rights are the combination of their converted trustee rights.
- If only **w**, **i**, and **d** rights are combined, no trustee rights are converted.
- If **w**, **i**, and **d** rights are combined with **r** and **c**, then the **w**, **i**, and **d** rights are ignored. Only the **r** and **c** rights are converted.
- If **w**, **i**, and **d** are combined with **x**, only **wxi**, **wxd**, and **wxid** are converted as shown in Table 7-5. Other combinations (**wx**, **ix**, **dx**, **idx**) are ignored and only **x** is converted.

#### 7.1.4.1.2 Files

- The **r**, **x**, **w**, and **c** combination is converted as shown in Table 7-5 above to form trustee rights.
- No trustee rights are set if only **i** and **d** are combined.
- If **i** and **d** are combined with **r**, **x**, **w**, and **c**, the **i** and **d** rights are ignored and the remaining combinations are converted.

#### 7.1.4.2 Trustee-to-ACL Conversion

Table 7-6 shows the basic rules of converting trustee rights to ACL.

Table 7-6. Conversion of Trustee Rights to ACL

Trustee Rights	ACL	
	Directory	File
R	—	r
W	—	w
C	wxi	—
E	wxd	—
M	—	—
F	rx	—
A	c	c
Q	—	—

**Note:** A dash ( — ) indicates that the right will not be effective even if it is set.

The conversion rules for directories and files are different, as follows.

#### 7.1.4.2.1 Directories

- The combination of only **F**, **A**, **C**, and **E** is converted as illustrated in Table 7-6.
- The combination of only **R**, **W**, **M**, and **Q** cannot be set for a directory. Rights conversion does not take place if only **R**, **W**, **M**, or **Q** are set.
- If **F**, **A**, **C**, and **E** are combined with **R**, **W**, **M**, and **Q**, **R**, **W**, **M**, and **Q** are ignored.

#### 7.1.4.2.2 Files

- Only the **R**, **W**, and **A** combination is converted as displayed in Table 7-6.
- Rights cannot be converted for files if only the **C**, **E**, **M**, **F**, and **Q** rights are combined.

- If **R**, **W**, and **A** are mixed with **C**, **E**, **M**, **F**, and **Q**, then R, W, and A are converted as shown in Table 7-6.

### 7.1.4.3 Differences Between Specified Rights and Rights That Are Actually Set

The trustee rights set through File-Access for directories and files in the Gateway volume are converted to an ACL. When you view the rights in the Gateway volume, File-Access converts ACL rights to trustee rights for you. Because there is a difference in the definition of rights between NetWare and DCE, there are cases where the rights you specify will differ from the rights actually set in the directories and files. For example, if you specify the **[C]** right in a Gateway volume directory, File-Access will set **[WCFQ]** in the directory.

Table 7-7 shows the difference between specified rights and the rights actually set by File-Access.

Table 7-7. Differences Between Specified Rights and the Rights Actually Set by File-Access

Location	Specified Rights	Rights Set by File-Access
Directory	C	WCFQ
	E	EF
	CE*	WCEMF
File	R	RF
	W	WCQ

**Note:** This includes cases where one is already specified and another is added.



## 7.1.5 Restrictions Related to the Use of UFS

File-Access is designed to be used with the Local File System (LFS) for DFS. Thus, there are restrictions if UFS (UNIX File System) is used. The following subsections describe the restrictions imposed and the differences between LSF and UFS.

### 7.1.5.1 Rights

The UFS rights are **r** (read), **w** (write), and **x** (execute).

With File-Access, these rights are recognized and processed as the LFS rights shown in Table 7-8.

Table 7-8. Correspondence Between UFS Rights and LFS Rights

UFS Rights	LFS Rights
r	r
w	Directory : wid
	File : w
x	x

The access control right in UFS ([c] right in LFS) can only be held by a superuser or a file and directory owner.

### 7.1.5.2 ACL Entries

File-Access uses six LFS ACL entries. UFS only has the following three ACL entries:

- Owner (directory/file owner)
- Group (group to which the owner belongs)
- Other (all users who do not belong to a group, excluding superusers)

The UFS ACL entries correspond to LFS **user\_obj**, **group\_obj**, and **other\_obj** entries, respectively.

UFS does not have corresponding entries for the LFS user and group, so rights cannot be set for users and groups that are not owners.

## 7.2 The Administrator's Tasks When a Failure Occurs

If a file access error or communication error occurs in File-Access, the administrator must follow the instructions shown in the message displayed on the NetWare server console or client. If no message is displayed or if the message requires reporting the problem to the system administrator, you may need to obtain failure information from Agent and/or Gateway.

### 7.2.1 Collecting Agent Failure Information

Agent failure information is output to File-Access trace files. The File-Access administrator should save the trace files on a storage medium and report the **/var/adm/syslog** file as well as the message that appears on the client's console to the system administrator. Agent trace information is output to the following file: **/opt/dcelocal/var/dfa/adm/evtraceX (X: 1 or 2)** One or two trace files are created. The maximum file size is 512 kilobytes. Once one file is full, trace information is saved to the other file.

### 7.2.2 Collecting Gateway Failure Information

If a failure occurs in Gateway, save the following files on storage media:

- Trace files
- Dump files
- Error log file and message log file
- Message log files

### 7.2.2.1 Trace Files

To obtain trace information, the File-Access administrator has to create trace files in the root directory of the SYS volume of the NetWare server. There are three kinds of trace files, and each trace file stores different information.

- **MAIN.TRC** for File-Access main program information
- **ADMIN.TRC** for directory synchronization information
- **WATCHDOG.TRC** for Watchdog (Agent's operation status monitoring function) information

Delete trace files from the NetWare server after you have saved them.

### 7.2.2.2 Dump Files

There are two types of Gateway dump files: a dump file that Gateway outputs, and a dump file that the File-Access administrator creates to obtain information.

- Dump file for the Gateway program

The following dump file is created automatically if failure occurs in Gateway:

**SYS:\DFAABND.001**

New dump information overwrites **DFAABND.001** every time new dump information is output. The maximum dump file size is 1.2 megabytes. If the dump information exceeds 1.2 megabytes, a new file (whose extension will be incremented upward starting from **DFAABND.002**) is created.

- Dump file for the File-Access administrator

If the File-Access administrator creates a file named **DFADUMP.001** in the root directory of the SYS volume in the NetWare server, dump information is output when Gateway is exited. The maximum dump file size is 1.2 megabytes. If the dump information exceeds 1.2 megabytes, a new file (whose extension name is incremented upward starting from **DFADUMP.002**) is created. Dump files should be deleted from the NetWare server by the administrator after they have been saved.

### 7.2.2.3 Error Log Files

A File-Access error log is output to the following files:

**SYS:\DFAERL.00X**

where *X* has a value of 1 or 2.

One or two error log files are created depending on the value of *X*. The maximum file size is 64 kilobytes. Once one file is full, the error log is saved on the other file.

### 7.2.2.4 Message Log Files

File-Access has its own message log files with the following name:

**SYS:\DFAERM.00X**

where *X* has a value of 1 or 2.

File-Access outputs all messages to this file, except for the messages output to the NetWare server console. The message format is as follows:

```
MMM dd hh:mm:ss messageID message_text
```

where:

*MMM* month (JAN, FEB, MAR, and so on.)

*dd* day

*hh* hour

*mm* minute

*ss* second

Up to 256 bytes of each message ID and message text are stored. If they are longer than 256 bytes in length, the rest is not stored. One or two message log files are

created. The maximum file size is 64 kilobytes. Once one file is full, the log is saved on the other file.

### 7.2.2.5 Communication Log File

If more detailed information about a communication failure is needed, you can retrieve the data exchanged between Gateway and Agent and stored in the communication log. Please note that File-Access processing speed is reduced if you retrieve the log. Enter the following command before starting Gateway if you do not need to access the communication log:

**LOAD DFADCE /X**

The communications log is output to the following file:

**SYS:\DFADCEX.LOG**

where *X* has a value of 1 or 2.

One or two communication log files are created depending on the value of *X*. The maximum file size is 640 kilobytes. Once one file is full, the log is saved on the other file.

### 7.2.2.6 Conditions of Failure and Information That Must Be Obtained

The failure information that the File-Access administrator needs to obtain depends on the conditions under which the failure occurred. Following are the two failure conditions and the information necessary to solve the problem. The File-Access administrator should retrieve the information and call the system administrator to report the failure.

- An error occurs throughout the File-Access environment.  
Retrieve all Dump files, all trace files, all failure log files, and all message log files.
- There is no response from Agent (communication failure).

Retrieve all trace information related to Watchdog, all failure log files, and all message log files.

## 7.2.3 Starting the RAS Utility

Start the RAS utility from the NetWare server where Gateway is installed.

### 7.2.3.1 How to Start

Type the following command from the NetWare server where Gateway is installed:

**LOAD [SYS:SYSTEM] DFARAS [.NLM] [/M] [E] [/C] [/T] [/D]**

where:

- /M** produces message log file with the RAS filenames **DFAERM.001, DFAERM.002**
- /E** produces error log file with the RAS filenames **DFAERL.001, DFAERL.002**
- /C** produces communication log file with the RAS filename **DFADCE.LOG**
- /T** produces trace file with the RAS filenames **DFAFUNC.TRC, ADMIN.TRC, MAIN.TRC, WATCHDOG.TRC**
- /D** produces dump file with the RAS filename **DFADUMP**

At the starting time, you can designate which RAS file you want to make. You can pick up multiple RAS files. If you do not select any files, no RAS file is made.

When a file is successfully made, a message is issued.

### 7.2.3.2 Conditions and Restrictions

The following conditions and restrictions apply when you are starting the RAS utility:

- **DFANLM** must be running to start **DFARAS.NLM**.

- The Gateway processing stops temporarily when **DFARAS.NLM** is being processed.
- DFA keeps the RAS files as salvage files. Use the NetWare **SALVAGE** command to restore the salvage file.
- You must assign sufficient space for the SYS volume.
- Do not set **purge attribute** on either the root directory of the SYS volume or the RAS file.
- **immediate purge** of deleted files is a NetWare parameter that is set by the set command from the System console. Its default value is **OFF**. Do not change this **OFF** setting to **ON**. If the immediate purge of deleted files parameter is set to **ON**, the target file is immediately purged when the file is deleted, and DFA cannot make a RAS file.

## 7.3 File-Access Administration

This section presents important information for operating File-Access and supervising its use. Refer to this section when setting up the File-Access environment.

### 7.3.1 Impact of File-Access on the System

Keep in mind the following important points when operating File-Access:

- To prevent illegal data access or a loss of power due to sabotage, maintain tight security on the NetWare server and DFS clients where File-Access is used.
- The Gateway volume is initialized and DFS files are copied every time the user starts File-Access. Therefore, the NetWare billing system cannot be used on the Gateway volume.
- If you use File-Access time synchronization, the NetWare server time is changed to DCE time. If the NetWare time is ahead of the DCE time, do not create or update directories or files during the period corresponding to the time difference following File-Access time synchronization. Since NetWare time is moving backward during this process, the time stamps on directories and files are inconsistent if directories or files are created or updated.

- Use MS-DOS commands when you copy or move a directory or file to the Gateway volume. Do not use NetWare commands or utilities.
- Application programs that use the record lock function do not run on the Gateway volume.
- Use the DFS backup function for DFS files when making a Gateway volume file backup. The NetWare backup utility does not work properly.

UNIX and Netware employ file-locking mechanisms that are intrinsically different. Because of this difference, the file access capability of this product does not function when Gateway and DCE simultaneously access a DFS file that is mapped onto the Gateway volume. The file access exclusion control is only operative on files within a single Gateway or multiple Gateways. We strongly recommend that you set up stringent control procedures to prevent such simultaneous access.

### 7.3.2 File-Access Authentication

Gateway users do not need to enter a DCE password when they log into DCE after setting the DCE password in Gateway. DCE authenticates Gateway users based on their DCE usernames and DCE passwords.

Gateway users are authenticated with the following sequence of events:

1. Gateway users log into the NetWare server as a NetWare client.
2. If a Gateway user enters the File-Access **DLOGIN** command and logs into DCE, Gateway searches for the DCE username and DCE password registered in the NetWare server. This information is passed on to Agent along with the login request.
3. Agent logs into the DCE security server by using the DCE username and DCE password received from Gateway.

After File-Access confirms that a Gateway user has logged into DCE, the Gateway user can access the Gateway volume.



### 7.3.3 Settings with a Time Limit on the DCE Side

The DCE user account and DCE password that correspond to the Gateway user have an effective period and expiration date.

The DCE user account becomes invalid after the effective period or expiration date, after which the user will not be able to log into DCE. If a user account becomes invalid, a new account must be recreated. The File-Access administrator should often remind Gateway users to renew the effective period and expiration date of their accounts.

The DCE password is valid even after the effective period or expiration date has passed, provided that notification of expiration is given. You set the effective period or expiration date by using the DCE **rgy\_edit** command.

The login effective period for DCE is set based on the effective period of the ticket granting ticket (TGT). Agent renews the TGT before its effective period expires, allowing Gateway user login to continue. If the TGT renewal fails, an error message is displayed on the NetWare console. After the TGT expires, Gateway users cannot access directories and files and must log out of DCE and then log back in. The TGT effective period is set by using the **rgy\_edit** command.

### 7.3.4 Directory and Filename Conversion Between DFS and the Gateway Volume

The names for NetWare directories and files conform to DOS naming rules. The names for DFS directories and files follow UNIX naming rules. The names of directories and files for NetWare and DFS differ in terms of the number and type of characters allowed. Sometimes the name of a DFS directory or file is invalid in NetWare.

File-Access converts names of DFS directories and files to the NetWare format. The following subsections explain the relationship between the DFS and Gateway volume names.

### 7.3.4.1 Changing Lowercase Letters in a Name to Uppercase Letters

File-Access can be used to capitalize all the lowercase letters of a DFS directory or filename if all of the following conditions are met:

- The name consists of lowercase alphanumeric characters
- The name contains no dot (.) and has eight or fewer characters (1 character = 1 byte)
- The name has a single dot in it, preceded by at least one but no more than eight characters, and followed by at least one but no more than three characters (1 character = 1 byte)
- The name does not include any of the following characters:  
. , + [ ] \* ? : \ / ; = < > | (space)

**Note:** A dot can be used in a name as an extension. However, if a dot is the first or last character in the name, it is not recognized as an extension.

For example:

Name in DFS	Name in Gateway Volume
filelist	FILELIST
file2.txt	FILE2.TXT

### 7.3.4.2 Tildes and Key Numbers as Names

The Gateway volume format is applied to directory names and filenames not described in the subsection, “Changing lowercase letters in a name to uppercase letters.” Some letters are changed to uppercase letters, and tildes or key numbers are assigned to the rest. Key numbers are uniquely assigned numbers that are used to avoid the duplication of the same name in the same directory.

For directory and filenames, the sixth character is converted to a tilde and the seventh and eighth to key numbers. (Some names have a 3-character extension.) If the name has fewer than five characters, tildes are added to increase the length to five characters.

For example:

Name in DFS	Name in Gateway Volume
ABC	ABC ~ ~ ~ nn
Ab.c	AB ~ ~ ~ ~ nn.C
yosandata	YOSAN ~ nn
.login	~ LOGI ~ nn

**Note:** ‘nn’ signifies key numbers.

### 7.3.4.3 DOS Device Names

File-Access recognizes the following character strings as device names in MS-DOS:

**con prn aux nul clock\$ com1 com2 com3 com4 lpt1 lpt2 lpt3**

If these character strings are used as names for DFS directories and files (including cases where the name is on the left side of the extension), File-Access converts them to tildes and keys so that they will not be the same as MS-DOS device names. (If the characters are uppercase letters, they are also converted in the same manner.)

Device names not included in this list are not converted by File-Access. For this reason, directories and files with the same names as MS-DOS devices can be created in the Gateway volume. However, the user should not access these directories and files from the NetWare client.



## Appendix A

---

# File-Access Reference Pages

This appendix contains the reference pages for the DCE-side File-Access commands **dfaagt.8dfa** and **setdfakey.8dfa**.

### A.1 Reference Pages

**dfaagt(system admin)**

## **dfaagt**

---

**Purpose** Starts, terminates, and communicates with File-Access Agent

**Synopsis** **dfaagt** [{-s *Time* | -a }]

### **Options**

**-s** *Time* Stops (terminates) File-Access Agent. The *Time* specifies an interval (in seconds) to wait between the time you invoke **dfaagt** and the time at which the Agent is terminated. The default value is 60 seconds.

**-a** Aborts File-Access Agent immediately, with no waiting time.

**Note:** The **-s** and **-a** options are mutually exclusive.

### **Description**

The **dfaagt** command starts, terminates, or kills a File-Access Agent. If invoked without any options, **dfaagt** starts the File-Access Agent. When used for termination or kill, the **dfaagt** command waits until the Agent is terminated.

### **Related Information**

**dfaagt(8dfa)**

---

## setdfakey

---

**Purpose** Sets, changes, and deletes master key for DCE/File-Access

**Synopsis** `setdfakey` [{**-a** *NetWare\_server\_name* | **-d** *NetWare\_server\_name* | **-l** }]

### Options

**-a** *NetWare\_server\_name*

Sets or modifies the master key of the File-Access Gateway that has the designated NetWare server name.

**-d** *NetWare\_server\_name*

Deletes the master key of the File-Access Gateway that has the designated NetWare server name.

**-l** Displays the NetWare server names stored in the file.

**Note:** The **-a**, **-d**, and **-l** options are mutually exclusive.

### Description

The **setdfakey** command sets, changes, and deletes master keys. If invoked without any options, it sets or modifies the master key, prompting the user interactively for the NetWare server name of the File-Access Gateway.

Before processing the master keys, **setdfakey** checks if the command is entered by a File-Access administrator by comparing the actual UNIX user ID and the File-Access administrator's IDs stored in the master key file. The command terminates if two IDs do not match. You cannot execute the **setdfakey** command if the File-Access Agent is running. In the case of setting and modification, if the desired *NetWare\_server\_name* does not exist in the file, the server name is registered with the file after confirming with the File-Access administrator. When the *NetWare\_server\_name* is settled, the command prompts you to enter an 8-byte character string twice. If the first string and the second one do not match, restart from the first input. If the retry fails, **setdfakey**

## **setdfakey(system admin)**

terminates with a message indicating that setting/modification of the master key is failed. If the first string and the second one match, the string is converted to a master key, and the master key is stored to the file.

### **Privileges Required**

The **setdfakey** command requires that the user be a File-Access administrator.

### **Related Information**

**dfaagt(8dfa)**