

Novell Native File Access Pack for NetWare® 5.1

1.0

www.novell.com

INSTALLATION AND ADMINISTRATION GUIDE



N

Novell®

Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

This product may require export authorization from the U.S. Department of Commerce prior to exporting from the U.S. or Canada.

Copyright © 1993-2002 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

U.S. Patent No. 5,157,663; 5,349,642; 5,455,932; 5,553,139; 5,553,143; 5,572,528; 5,594,863; 5,608,903; 5,633,931; 5,652,859; 5,671,414; 5,677,851; 5,692,129; 5,701,459; 5,717,912; 5,758,069; 5,758,344; 5,781,724; 5,781,724; 5,781,733; 5,784,560; 5,787,439; 5,818,936; 5,828,882; 5,832,274; 5,832,275; 5,832,483; 5,832,487; 5,850,565; 5,859,978; 5,870,561; 5,870,739; 5,873,079; 5,878,415; 5,878,434; 5,884,304; 5,893,116; 5,893,118; 5,903,650; 5,903,720; 5,905,860; 5,910,803; 5,913,025; 5,913,209; 5,915,253; 5,925,108; 5,933,503; 5,933,826; 5,946,002; 5,946,467; 5,950,198; 5,956,718; 5,956,745; 5,964,872; 5,974,474; 5,983,223; 5,983,234; 5,987,471; 5,991,771; 5,991,810; 6,002,398; 6,014,667; 6,015,132; 6,016,499; 6,029,247; 6,047,289; 6,052,724; 6,061,743; 6,065,017; 6,094,672; 6,098,090; 6,105,062; 6,105,132; 6,115,039; 6,119,122; 6,144,959; 6,151,688; 6,157,925; 6,167,393; 6,173,289; 6,192,365; 6,216,123; 6,219,652; 6,229,809. Patents Pending.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.

www.novell.com

Novell Native File Access Pack for NetWare 5.1 Installation and Administration Guide
April 2002
100-004513-001 A

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

BorderManager is a registered trademark of Novell, Inc., in the United States and other countries.

ConsoleOne is a registered trademark of Novell, Inc., in the United States and other countries.

eDirectory is a trademark of Novell, Inc.

NetWare is a registered trademark of Novell, Inc., in the United States and other countries.

NetWare Loadable Module and NLM are trademarks of Novell, Inc.

NMAS is a trademark of Novell, Inc.

Novell is a registered trademark of Novell, Inc., in the United States and other countries.

Novell Client is a trademark of Novell, Inc.

Novell Cluster Services is a trademark of Novell, Inc.

Novell Directory Services and NDS are registered trademarks of Novell, Inc., in the United States and other countries.

Third-Party Trademarks

All third-party trademarks are the property of their respective owners.

Contents

Preface	7
Documentation Conventions	8
1 Overview	9
Getting Started	10
2 Installing Novell Native File Access Pack for NetWare 5.1	11
NetWare Server Prerequisites	12
Administrator Workstation Prerequisites	13
Client Computer Prerequisites	14
Installing the Software	14
Accessing and Starting the Installation Program	14
Installing the Native File Access for Windows Component	16
Starting and Stopping AFP and CIFS Protocols Service	20
What's Next?	20
3 Working with Macintosh Computers	21
Administrator Tasks for Native File Access for Macintosh Services	21
Creating Simple Passwords for Several Macintosh Users	21
Editing the Context Search File.	22
Creating a Guest User Account	23
Renaming Volumes.	23
Macintosh End User Tasks.	24
Accessing Network Files	24
Logging In to the Network as Guest	25
Changing Passwords from a Macintosh Computer.	25
Assigning Rights and Sharing Files from a Macintosh Computer	26
4 Working with Windows Computers	29
Administrator Tasks for Native File Access for Windows Services	29
Creating Simple Passwords for Windows Users	30
Two Methods for Creating Simple Passwords for Windows Users.	32
Enabling Users to Change Their Simple Passwords with the NetWare Management Portal	36
Understanding Synchronization of NetWare Passwords and Simple Passwords	37
Specifying Contexts in the Context Search File	37
Managing Network Access with ConsoleOne	38

Providing Network Access to Windows Domain Users	39
Customizing the Network Environment Using a Configuration File	39
Viewing Configuration Details	43
Windows End User Tasks	44
Accessing Files from a Windows Computer	44
Mapping Drives from a Windows Computer	44
Changing Passwords from a Windows Computer	45
5 Setting Up Novell Native File Access Pack with Novell Cluster Services	47
Prerequisites	47
Setting Up for Macintosh	48
Setting Up for Windows	48
What's Next?	54

6 Installation and Administration Guide

Preface

This book contains information on installing, configuring, and managing Novell® Native File Access Pack software specific to the Windows* and Macintosh* native protocols—CIFS and AFP, respectively.

For detailed information on using Native File Access for UNIX and managing workstations that access the network with the native UNIX NFS protocol, see the *Novell Native File Access for UNIX Installation and Administration Guide*.

This book is divided into the following chapters:

- ♦ **Chapter 1, “Overview,” on page 9** describes the benefits of Novell Native File Access Pack software.
- ♦ **Chapter 2, “Installing Novell Native File Access Pack for NetWare 5.1,” on page 11** describes how to install the software on a NetWare server.
- ♦ **Chapter 3, “Working with Macintosh Computers,” on page 21** describes how to set up and manage Macintosh workstations and how to access files on the network.
- ♦ **Chapter 4, “Working with Windows Computers,” on page 29** describes Windows authentication methods and passwords, how to set up and manage Windows workstations, and how to access files on the network.
- ♦ **Chapter 5, “Setting Up Novell Native File Access Pack with Novell Cluster Services,” on page 47** explains Novell Cluster Services™ and how to configure the Novell Native File Access Pack software for Macintosh and Windows computers in a clustered environment.

Documentation Conventions

In this documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

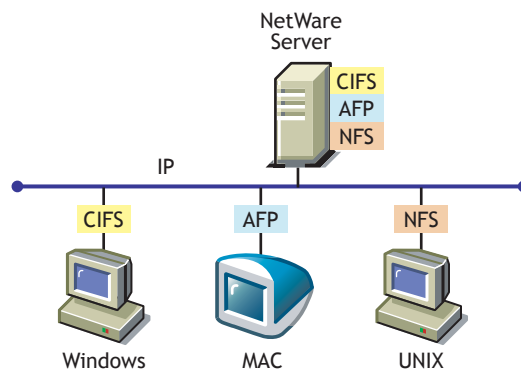
Also, a trademark symbol (® , ™ , etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

8 Installation and Administration Guide

1 Overview

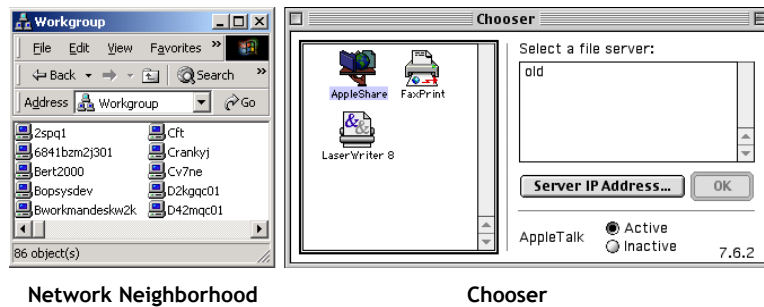
Novell® Native File Access Pack lets Macintosh, Windows, and UNIX workstations access and store files on NetWare® servers without having to install any additional software—such as the Novell Client™. The software is installed only on the NetWare server and provides "out of the box" network access. Just connect the network cable, start the computer, and you have access to servers on your network. No client software installation. No client configuration. No problem.

Novell Native File Access Pack software enables the NetWare server to use the same protocol (referred to as *native*) as the client workstation to copy, delete, move, save, and open files. Windows workstations perform these tasks using the native Common Internet File System (CIFS) protocol, Macintosh workstations use the native Apple* Filing Protocol (AFP), and UNIX computers use the Network File System (NFS) protocol.



Enabling native protocols on a NetWare server means that users can access files on the network, map network drives, and create shortcuts to NetWare servers using the native methods available in their specific operating system.

Windows users can use their familiar Network Neighborhood (or My Network Places). Macintosh users can use Chooser or the Go menu to access network files and even create aliases. Because the NetWare server is running native protocols, users can copy, delete, move, save, and open network files—just like they would if they were working locally.



Network Neighborhood

Chooser

By consolidating user management through Novell Directory Services[®] (NDS[®]), Native File Access Pack simplifies overall network administration. All users who need access to the network are represented in NDS through User objects, which enables you to easily and effectively assign trustee rights and access control and manage all User objects from a single location on the network.

NOTE: Windows users can also be managed through a Windows Domain Controller and UNIX users can be managed through Network Information Service (NIS).

Getting Started

Novell Native File Access Pack is easy to install. To get started, continue with [Chapter 2, “Installing Novell Native File Access Pack for NetWare 5.1,” on page 11.](#)

2

Installing Novell Native File Access Pack for NetWare 5.1

To install the Novell® Native File Access Pack for NetWare® 5.1, complete the following procedure:

1. Prepare the NetWare 5.1 server.
See [“NetWare Server Prerequisites” on page 12.](#)
2. Set up an Administrator Workstation.
See [“Administrator Workstation Prerequisites” on page 13.](#)
3. Ensure all of the client computers (Windows, Mac, and UNIX) that will use the Novell Native File Access Pack software to access network resources are running a supported version of their respective operating system.
See [“Client Computer Prerequisites” on page 14.](#)
4. Install the Native File Access Pack software.
See [“Installing the Software” on page 14.](#)

NetWare Server Prerequisites

The NetWare 5.1 server must meet the following configuration requirements in order to run the Novell Native File Access Pack software.

HINT: You can quickly check the server configuration with the NWCONFIG utility. At the server console, enter NWCONFIG and then select Product Options > View/Configure/Remove installed products.

- NetWare 5.1 server with NetWare 5.1 Support Pack 4 or later installed.

[Download the latest NetWare 5.1 Support Pack \(http://support.novell.com/tools/csp/csplist.html\)](http://support.novell.com/tools/csp/csplist.html).

- NDS[®] eDirectory[™] 8.5.12a (or later) for NetWare (DS.NLM internal version 85.00 or later) installed on the server.

IMPORTANT: Do not use an earlier version of eDirectory.

[Download eDirectory \(http://download.novell.com\)](http://download.novell.com).

- The NSS51.EXE patch (TID #2960046) installed on the server.

Download patches from the Novell Support Web site (<http://support.novell.com>).

HINT: From the Novell Support Web site, click Product Updates (patches and files) to search by filename, or click Knowledgebase (text search) to search by TID number.

- Novell Modular Authentication Service (NMAST[™]) version 2 or later installed on the server.

During the Novell Native File Access Pack installation, NMAST 2.0 is automatically installed or earlier versions of NMAST are upgraded to NMAST 2.0.

NMAST Starter Pack 1.0 is automatically upgraded to NMAST Starter Pack 2.0. NMAST Enterprise Edition 1.0 is upgraded to NMAST Enterprise Edition 2.0.

- (For Macintosh/AFP only) Macintosh Name Space loaded on each traditional volume before installing Novell Native File Access Pack.

To load Macintosh Name Space to a volume, enter the following commands at the server console:

```
LOAD MAC.NLM
```

```
ADD NAME SPACE MACINTOSH TO VOLUME volume_name
```

IMPORTANT: On NetWare 5.1, volume SYS: is a traditional volume. If you want Macintosh users to access volume SYS:, you must load Macintosh Name Space on the volume.

- (For Macintosh/AFP only) AFP.NLM and APPLETLK.NLM must be unloaded from the server (if currently running).
- (Conditional) If BorderManager[®] Enterprise Edition version 3.5 or later is running in the same eDirectory tree as the NetWare server where you are installing Novell Native Access Pack software, you must create a Login Policy Object (LPO).
 - 1** Log in to the server running BorderManager.
 - 2** Run the NetWare Administrator utility (NWADMIN.EXE) located in the PUBLIC\WIN32\ directory.
 - 3** From the Object menu, click Create > Login Policy > OK.
 - 4** (Conditional) If the server running BorderManager does not have a local NDS replica, complete the following:
 - 4a** From NetWare Administrator, select the Security container and the LPO.
 - 4b** Click Trustees of This Object > Add Trustee.
 - 4c** Select the Server object of the server running BorderManager.
 - 4d** Deselect all Object rights.
 - 4e** Click Selected Properties > SAS: Policy Credentials.
 - 4f** From Property Rights, click Read/Write > OK.

Administrator Workstation Prerequisites

You will install, configure, and manage Novell Native File Access Pack services from a Windows-based Administrator Workstation. Make sure that the workstation meets the following system requirements.

- Windows workstation running one of the following:
 - ◆ Windows 95/98 with the Novell Client™ for Windows 95/98 version 3.21.0 or later installed.
 - ◆ Windows NT*/2000 with the Novell Client for Windows NT/2000 version 4.80 or later installed.

Download Novell Client software (<http://download.novell.com>).

- Client NCI 1.5.7 (or later) for Windows (Strong Encryption) installed.

Download the NCI Encryption Module software (<http://www.download.novell.com/>).

The NCI client software must be installed on the Administrator Workstation in order to manage passwords using ConsoleOne®. NCI software has to be installed only on the Administrator Workstation, not on any other client computers.

NOTE: NCI (Weak Encryption) works for user authentication but does not support changing passwords from a Windows workstation.

Client Computer Prerequisites

To access NetWare servers running Novell Native File Access Pack, client computers must be connected to the network, properly configured to run TCP/IP, and be running one of the following operating systems:

- Mac OS version 8.1 or later, including Mac OS X
- Windows 95/98/ME, Windows 2000, or Windows NT version 4

Windows computers must be running Client for Microsoft Networks, which is a standard Windows component. The Client for Microsoft Networks can be manually installed by clicking Start > Settings > Control Panel > Network > Add > Client > Microsoft.

- Any NFS platform capable of NFS v2 or NFS v3 such as UNIX, Linux*, or Free BSD

Installing the Software

Novell Native File Access Pack for NetWare 5.1 includes an easy-to-follow installation program that guides you through the required steps.

Accessing and Starting the Installation Program

- 1** Obtain the *Novell Native File Access Pack* CD.
- 2** Ensure your NetWare 5.1 server meets the prerequisites described in “[NetWare Server Prerequisites](#)” on page 12.
- 3** Ensure your Administrator Workstation meets the prerequisites described in “[Administrator Workstation Prerequisites](#)” on page 13.

14 Installation and Administration Guide

- 4** From the Administrator Workstation, log in to the destination NetWare 5.1 server that will run the Novell Native File Access Pack software.
- 5** Create a temporary directory on the NetWare 5.1 server.
- 6** Unzip the Novell Native File Access Pack files to the temporary directory on the NetWare 5.1 server.
- 7** At the NetWare 5.1 server console, enter **STARTX** to launch the graphical server console.
- 8** Click Novell > Install.
- 9** At the Installed Products screen, click Add.
- 10** Enter the path to the temporary directory and select the PRODUCT.NI file.
- 11** Accept the License Agreement.
- 12** At the Components screen, select the Native File Access components you want to install and then click Next.

- ♦ If you choose to install the Native File Access for Macintosh (AFP*) component, the software will be installed transparently during the NetWare installation process. No further interaction is required for the Native File Access for Macintosh software installation.

For information on configuring Native File Access for Macintosh services and managing Mac users, see [Chapter 3, “Working with Macintosh Computers,”](#) on page 21.

- ♦ If you choose to install the Native File Access for Windows (CIFS) component, continue with [“Installing the Native File Access for Windows Component”](#) on page 16.

For information on configuring Native File Access for Windows services and managing Windows users, see [Chapter 4, “Working with Windows Computers,”](#) on page 29.

- ♦ For detailed information on installing and configuring the Native File Access for UNIX component, see the *Novell Native File Access for UNIX Installation and Administration Guide*.

Installing the Native File Access for Windows Component

If you chose to install the Native File Access for Windows component (CIFS protocol), complete the following steps:

- 1 From the Administrator Workstation, log in as a user with the Supervisor right.

IMPORTANT: You must specify the full context for the user.

- 2 At the Server Properties screen, configure the following server settings and then click Next.
 - ♦ **Server Name:** Enter a unique name for the NetWare 5.1 server running CIFS that will appear in Network Neighborhood when users browse the network. The server name cannot be longer than 11 characters and must be different from the actual NetWare server name.

NOTE: The default Server Name is the NetWare server name with an added underscore (_) and a W. For example, a NetWare server named SERVER1 defaults to SERVER1_W.
 - ♦ **(Optional) Server Comment:** Enter a comment for the server. The text in the Server Comment field displays when viewing details of the server from a Windows workstation.
 - ♦ **Enable Unicode:** Specify whether to enable Unicode character support. When checked, this option enables Unicode characters that are used in double-byte languages.

To support Unicode, an additional file named UNINOMAP.TXT must be created and saved in the SYS:\ETC directory. When the UNICODE parameter is set to On, the UNINOMAP.TXT file is used to resolve Unicode-to-ASCII "no-map" problems.

To specify "no-map" cases in the UNINOMAP.TXT file, enter the first Unicode value to watch for and then the second value representing the ASCII replacement code. For example:

0178 98

20AC CC

Save the values in the UNINOMAP.TXT file. If an unmappable character is encountered, the system uses the ASCII substitution character specified in the file.

3 At the Authentication screen, select one of the following authentication methods and then click Next.

- ♦ **Local:** Select if your Windows users will authenticate using NDS.

With Local authentication, the NetWare 5.1 server running Novell Native File Access Pack software performs the user authentication when clients are a member of a workgroup. With local authentication, the username and password on NetWare must match the username and password used to log in to the Windows workstation.

If you select Local as your authentication method, fill in the following fields:

- ♦ **Workgroup Name:** Enter the name of the domain or workgroup that the NetWare server will belong to. In this case, *workgroup* and *domain* are interchangeable terms.
- ♦ **WINS Address:** Enter the IP address of the WINS server to be used to locate the primary domain controller (PDC), if the PDC and server running Novell Native File Access Pack software are on different subnets.

NOTE: Windows Internet Naming Service (WINS), part of the Microsoft Windows NT and 2000 Servers, manages the association of workstation names and locations with Internet Protocol (IP) addresses. WINS automatically creates and maintains a computer name and corresponding IP address mapping entry in a table. When a computer is moved to another geographic location, the subnet part of the IP address is likely to change. Using WINS, the new subnet information will be updated automatically in the WINS table.

- ♦ **Domain:** Select if your Windows users will authenticate using a Microsoft Networking Domain.

With Domain authentication, it is important to remember that a simple password is *not* required when using domain authentication. Because the password is kept on the Windows domain controller, it is not possible to use the Windows native Change Password feature to change the password. Instead, you must use the Windows domain management utilities. To work properly, the username and password on the domain controller must match the username and password used to log in to the Windows workstation.

If you select Domain as your authentication method, fill in the following fields:

- ◆ **PDC Is on the Same Subnet as This Server:** Select this option if the primary domain controller (PDC) is on the same subnet as the NetWare server.
 - ◆ **Specify PDC Using DNS or WINS:** Select this option to use DNS or WINS to specify the primary domain controller (PDC).
 - ◆ **PDC Name:** A PDC server name and static IP address are needed if the PDC is on a different subnet. This field should be used only when there is a valid reason for overriding WINS or DNS.
 - ◆ **PDC Address:** The address of the PDC must be static; otherwise, if the PDC reboots and the address changes, the server running Novell Native File Access Pack software will not be able to contact the PDC.
- 4** At the IP Addresses screen, specify the IP addresses on the server that you want to be attached to the CIFS protocol, or keep the default selection to Enable CIFS on All Addresses (recommended), and then click Next.
 - 5** At the Share Point Setup screen, specify additional NetWare volumes or folders that you want to appear as share points in Network Neighborhood, or keep the default selection to Share all Mounted Volumes, and then click Next.

Any volume or directory on the server can be specified as a shared point and made accessible via the Network Neighborhood. If no share points are specified, then all mounted volumes are displayed in Network Neighborhood.

If you want to specify a share point, click New, fill in the following fields, and click Submit.

- ◆ **Directory:** Enter the path to the server volume or directory which becomes the root of the sharepoint. Beginning at the volume name, the full path must be specified and it must end with a backslash (\). For example:
`VOL1:GRAPHICS\`
- ◆ **Share Name:** Enter the name by which the sharepoint is displayed to Windows computers. For example, if you enter "Lots of Pics" as the share name associated with VOL1\GRAPHICS, then Windows workstations browsing the network will see "Lots of Pics" instead of "VOL1\GRAPHICS."

- ♦ **Connections:** Enter the number of connections allowed to access the sharepoint. Or, check Unlimited to allow an unlimited number of connections.
- ♦ **Comment:** Enter a description for the sharepoint that appears in Network Neighborhood.

- 6** At the Context Setup screen, specify the NDS contexts for your Windows (CIFS) users who need access to this NetWare server and then click Add.

NDS contexts added here are saved in a list in the CIFS context search file (SYS:\ETC\CIFSCCTXS.CFG). When the Windows user enters a username, the Novell Native File Access Pack software searches through each context in the list until it finds the correct User object.

For example, if you had users with full NDS distinguished names such as Robert.sales.acme, Maria.graphics.marketing.acme, Sophia.graphics.marketing, and Ivan.marketing.acme, then you would enter the following contexts:

sales.acme

graphics.marketing.acme

marketing.acme

NOTE: If User objects with the same name exist in different contexts, each user object attempts authentication in order until one succeeds with the corresponding password.

The CIFSCCTXS.CFG context search file can be edited manually after installation. For more information, see [“Specifying Contexts in the Context Search File” on page 37](#).

- 7** Check the Summary screen and then click Finish.

The installation program copies the required files to your server.

- 8** Restart the server by entering the following command at the server console:

RESTART SERVER

Starting and Stopping AFP and CIFS Protocols Service

Each time the server starts, the Novell Native File Access Protocols are loaded from commands that were automatically added to the AUTOEXEC.NCF configuration file by the installation program.

You can also load and unload the Native File Access Protocols service manually at the server console.

Macintosh (AFP) Protocols Service

- 1 At the server console, enter **AFPSTRT** to load the Macintosh (AFP) protocols on the server.

Any changes made in the AFP configuration files since the last time you started the service are applied when the AFP protocols are reloaded.

- 2 At the server console, enter **AFPSTOP** to unload the Macintosh (AFP) protocols on the server.

Windows (CIFS) Protocols

- 1 At the server console, enter **CIFSSTRT** to load the Windows (CIFS) protocols on the server.

Any changes made in the CIFS configuration files since the last time you started the service are applied when the CIFS protocols are reloaded.

- 2 At the server console, enter **CIFSSTOP** to unload the Windows (CIFS) protocols on the server.

What's Next?

After installing the Native File Access Pack software, you must now create simple passwords for Macintosh, Windows, and UNIX users before they can access files on the server using their native protocols.

To set up and manage Macintosh users, see [Chapter 3, "Working with Macintosh Computers,"](#) on page 21.

To set up and manage Windows users, see [Chapter 4, "Working with Windows Computers,"](#) on page 29.

To set up and manage UNIX users, see the [Novell Native File Access for UNIX Installation and Administration Guide](#).

3

Working with Macintosh Computers

This chapter contains the following information:

- ♦ [Administrator Tasks for Native File Access for Macintosh Services \(page 21\)](#)
- ♦ [Macintosh End User Tasks \(page 24\)](#)

Administrator Tasks for Native File Access for Macintosh Services

Native File Access for Macintosh provides several ways to simplify your administration tasks and customize how Macintosh workstations interact with the network:

- ♦ [Creating Simple Passwords for Several Macintosh Users \(page 21\)](#).
- ♦ [Editing the Context Search File \(page 22\)](#).
- ♦ [Creating a Guest User Account \(page 23\)](#).
- ♦ [Renaming Volumes \(page 23\)](#).

Creating Simple Passwords for Several Macintosh Users

You can create simple passwords for users one at a time using ConsoleOne[®]. But if you want to create passwords for several Macintosh users at once, you can add the CLEARTEXT option to the LOAD AFPTCP command at the server console. For example:

```
LOAD AFPTCP CLEARTEXT
```

When the CLEARTEXT option is added to the AFPTCP command, users logging in to the server from a Macintosh workstation are prompted to provide their NDS[®] username and password. Once the NDS password is verified, a

simple password is automatically created and stored in NDS. The simple password is the same as the NDS password.

The CLEARTEXT option is meant to be a temporary way to create simple passwords for many Macintosh users. After Macintosh users have created simple passwords, the AFPTCP NLM™ should be loaded without the CLEARTEXT option.

WARNING: The CLEARTEXT option allows unencrypted passwords to be sent over the network. If you are concerned about someone capturing your password over the network, you should not use this option. Instead, you should manage passwords using ConsoleOne on the Administrator Workstation.

Editing the Context Search File

A context search file allows Macintosh users to log in to the network without specifying their full context. The context search file contains a list of contexts that are searched when no context is provided or the object cannot be found in the provided context. When a Macintosh user enters a username, the server searches through each context in the list until it finds the correct User object.

Macintosh allows only 31 characters for the username. If the full NDS context and username are longer than 31 characters, you must use a search list to provide access.

HINT: Macintosh users do not need to enter a context or have an entry in the context search file if their User objects are placed in the same container as the Server object.

If User objects with the same name exist in different contexts, the first one in the context search list will be used.

To edit the context search file, do the following:

- 1 Using any text editor, edit the CTXS.CFG file stored in the SYS:\ETC directory of the server running Novell® Native File Access Pack.

- 2 On separate lines, enter the contexts to search.

For example, if you had users with full NDS distinguished names such as Robert.sales.acme, Maria.graphics.marketing.acme, Sophia.graphics.marketing, and Ivan.marketing.acme, then you would enter the following contexts to the CTXS.CFG file:

```
sales.acme
graphics.marketing.acme
marketing.acme
```

- 3 Save the file in the SYS:\ETC directory.

The file is read the next time a Macintosh user logs in.

When Macintosh users log in, they enter only a username and the simple password. The system finds the User object in the context specified in the CTXS.CFG file.

Creating a Guest User Account

Novell Native File Access Pack allows you to create a Guest User object. Macintosh users are accustomed to being able to log in as Guest with no password required.

- 1 From the Administrator Workstation, use ConsoleOne to create a User object named Guest.
- 2 Determine and assign the appropriate rights to the Guest object by double-clicking the Guest object and then clicking Rights to Files and Folders.
- 3 Remove the ability for the user to change the password by clicking Restrictions and then unchecking Allow User to Change Password.
- 4 Enable the Guest account by adding the full NDS context of the Guest object to the context search file as described in [“Editing the Context Search File” on page 22](#).
- 5 Unload and reload the AFPTCP.NLM program with the GUEST option to make the Guest button available on the login screen.

Any Macintosh user can now log in as Guest with no password and receive the access rights assigned to the Guest object.

Renaming Volumes

Volumes can be renamed so that they appear in Chooser under a different name.

- 1 Using any text editor, create a file named AFPVOL.CFG.
- 2 On separate lines, enter the current name of the volume and, in quotes, the new name of the volume. For example:

```
server1.sys "System Volume"  
server1.img "Graphics"  
#The above volume contains image files.
```

NOTE: The pound sign (#) marks a line as a comment.

- 3 Save the file in the SYS:\ETC directory of the server running Novell Native File Access Pack.

Once the volume has been renamed, it keeps the name even if you delete the file and restart the server. To return to the previous name, repeat these steps and rename the volume to its original name.

For example:

```
System volume "server1.sys"
```

- 4 Unload and reload the AFPTCP.NLM program.

Macintosh End User Tasks

When Novell Native File Access Pack is properly configured, the Macintosh users on your network will be able to perform the following tasks:

- ♦ [Accessing Network Files \(page 24\)](#).
- ♦ [Logging In to the Network as Guest \(page 25\)](#).
- ♦ [Changing Passwords from a Macintosh Computer \(page 25\)](#).
- ♦ [Assigning Rights and Sharing Files from a Macintosh Computer \(page 26\)](#).

Accessing Network Files

Macintosh users can use Chooser to access files and directories each time they are required or they can create an alias on the desktop that is retained after rebooting.

- 1 In Mac OS 8 or 9, click the Apple menu > Chooser > AppleTalk > Server IP Address.
In Mac OS X, click Go > Connect to Server.
- 2 Enter the IP address or DNS name of the NetWare[®] server and then click Connect.
- 3 Enter the username and password and then click Connect.
- 4 Select a volume to be mounted on the desktop.

Although you now have access to the files, mounting the volume to the desktop does not make it available after rebooting.

- 5 (Optional) Create an alias to the desired volume or directory.
Aliases are retained after rebooting.

24 Installation and Administration Guide

5a Click the NetWare server icon.

5b Click File > Make Alias.

The alias icon appears on the desktop.

Logging In to the Network as Guest

If the network administrator has set up the Guest User object account as described in “[Creating a Guest User Account](#)” on page 23, Macintosh users can log in to the network as Guest with no password required.

1 In Mac OS 8 or 9, click the Apple menu > Chooser > AppleTalk > Server IP Address.

In Mac OS X, click Go > Connect to Server.

2 Enter the IP address or DNS name of the NetWare server, and then click Connect.

3 Click Guest Login > Connect.

The Guest user has rights to access network resources as configured by the network administrator.

Changing Passwords from a Macintosh Computer

Macintosh users can change their passwords. When they change their simple password, their NDS password is automatically synchronized.

1 In Mac OS 8 or 9, click the Apple menu > Chooser > AppleTalk > Server IP Address.

In Mac OS X, click Go > Connect to Server.

2 Enter the IP address or DNS name of the NetWare server, and then click Connect.

3 Enter the username.

4 Click Change Password.

5 Enter the old password and the new password, and then click OK.

Assigning Rights and Sharing Files from a Macintosh Computer

Although using ConsoleOne from the Administrator Workstation is the recommended method for managing rights, Macintosh users have some file sharing and management capability using Chooser.

HINT: For more information on how to use ConsoleOne to set up and manage rights, see the *ConsoleOne Users Guide* (<http://www.novell.com/documentation/lg/consol12d/index.html>) or view the ConsoleOne online Help.

NetWare Rights versus Macintosh Rights

Using Chooser to access network files and folders is fairly consistent with the Macintosh environment, but there are some differences between NetWare and Macintosh file sharing. Macintosh users can view the sharing information about specific folders by clicking Get Info/Sharing.

Inherited Rights and Explicit Rights

The Macintosh file system uses either inherited rights (which use enclosing folder's privileges) *or* explicit rights (which assign rights to a group or user). A folder in the Macintosh file system cannot have both inherited and explicit rights.

NetWare uses both inherited *and* explicit rights to determine the actual rights that a user has. NetWare allows a folder (or directory) to hold file rights for multiple groups and users. Because of these differences, Macintosh users will find that access rights to folders and files might function differently than expected.

NetWare uses inherited rights, so the Macintosh "Use Enclosing Folder's Privileges" option is automatically turned off. When a Macintosh user views the Get Info/Sharing dialog box for a NetWare folder, only the User/Group assignments are visible if there is an explicit assignment on the folder. If the NetWare folder inherits User/Group rights from a parent group or container, those rights are not displayed in the dialog box, nor will there be any indication that the folder is inheriting rights from a group or container.

Owner, User/Group, and Everyone Rights

Because NetWare allows multiple groups and users to have rights to a single folder, users are not able to delete rights assignments using the Apple Macintosh interface. Users can *add* assignments to allow basic file sharing, but more complex rights administration must be done using the NetWare utilities such as ConsoleOne.

When specifying Owners, Users, and Groups, there is no way to select from current groups. You must enter the correct NetWare name and context (fully distinguished NDS name).

HINT: No context is required if the context is specified in the context search file.

Owner Rights

In the Apple File Sharing environment, an *owner* is a user who can change access rights. In the NetWare environment, users can change access rights if they have been granted the Access Control right for the folder. In NetWare, an owner means the one who created the file. A NetWare owner has no rights by virtue of ownership. In the NetWare environment, the owner is the current user if he has access control rights to the folder.

If the user does not have access control rights, the NetWare owner will be shown if the NetWare owner is not the current user. If the current user does not have rights to change access and is also the NetWare owner, a message to "Use NetWare Utility" is displayed in the Owner field.

In Apple File Sharing, there can be more than one owner. If you change the owner, access control rights are added to the new owner, but are not removed from the current owner. In NetWare, there are two ways to have access control rights: (1) have the Access Control right and (2) have the Supervisor right. Adding a new owner only adds the Access Control right, not the Supervisor right. If the current owner already has the Supervisor right through other NetWare utilities, that right will remain. The Supervisor right also gives full file access rights. This means that if you are the current user and have the Supervisor right, you also have read/write access and you cannot change those rights.

Display only allows for one owner. If multiple users have file access rights, only the current user is shown in the Owner field. This means you could change the owner (which in NetWare simply means adding the Access Control right to the new user) and when you open the file sharing dialog box again, you will be listed as the owner, even though you have just given ownership or the Access Control right to someone else.

User / Group

Only one user/group can be displayed for a folder, although NetWare allows multiple users and groups to be assigned file access rights. If both users and groups have access to a NetWare folder, groups are displayed before users. The group with the most access rights is preferred over groups with lesser access rights. Only users or groups with explicit rights (not inherited rights)

are shown in the User/Group field. Users and groups with inherited rights are not shown in the dialog box, nor is there any indication that there are users and groups with inherited rights.

Adding a group or user does not remove the current group or user; it simply adds the rights to the group or user specified. If the user enters the wrong user or group name, the user gets no feedback. If multiple users or groups are assigned to the folder, it is possible that the user is unable to see the user or group that was just assigned. It could be very difficult to know if the rights assignment worked or not.

Rights set through this interface are inherited by the folder's subfolders. It is impossible to manage all inherited rights from the Macintosh interface. (Although not recommended, you could set the inherited rights filters from the NetWare utilities to turn off inherited rights.)

Everyone

Assignment of rights to Everyone acts like the Macintosh user expects, with the exception that Everyone's rights are inherited. In NetWare, the object that represents the rights of any authenticated user is used to set Everyone's rights. Everyone's rights can change from folder to folder, but once they are set, they are inherited by subfolders.

4 Working with Windows Computers

This chapter contains the following information:

- ♦ [Administrator Tasks for Native File Access for Windows Services \(page 29\)](#)
- ♦ [Windows End User Tasks \(page 44\)](#)

Administrator Tasks for Native File Access for Windows Services

Native File Access for Windows provides several ways to simplify your administration tasks and customize how Windows workstations interact with the network:

- ♦ [Creating Simple Passwords for Windows Users \(page 30\)](#)
- ♦ [Enabling Users to Change Their Simple Passwords with the NetWare Management Portal \(page 36\)](#)
- ♦ [Understanding Synchronization of NetWare Passwords and Simple Passwords \(page 37\)](#)
- ♦ [Specifying Contexts in the Context Search File \(page 37\)](#)
- ♦ [Managing Network Access with ConsoleOne \(page 38\)](#)
- ♦ [Providing Network Access to Windows Domain Users \(page 39\)](#)
- ♦ [Customizing the Network Environment Using a Configuration File \(page 39\)](#)
- ♦ [Viewing Configuration Details \(page 43\)](#)

Creating Simple Passwords for Windows Users

In order to take advantage of Novell® Native File Access software, all users must have a NetWare® User object created in eDirectory™.

NOTE: A NetWare User object specifies attributes and information about which network resources the user can access. User objects are created using ConsoleOne®. For more information, see the *ConsoleOne Users Guide* (<http://www.novell.com/documentation/lg/consol12d/index.html>).

In addition, most users must also have a *simple password* created for them before they can access network resources using native protocols. The exception is when Native File Access for Windows software has been configured to use the Domain authentication method.

This section describes the two Windows authentication methods and password requirements and explains how to create simple passwords for Windows users.

NOTE: For information about selecting an authentication method during the installation, see [Step 3](#) of “[Installing the Software](#)” on [page 14](#).

Windows Authentication Methods and Simple Passwords

The method that Windows workstations (using their native Common Internet File System, or CIFS, Protocol) use to authenticate to the CIFS-enabled NetWare server is determined by which authentication method was selected during installation. The two Windows authentication methods are Local and Domain.

If Local authentication is being used, each Windows user must have a simple password associated with their NetWare/NDS® User object in order to access network resources using native protocols. However, if Domain authentication is being used, a simple password is not required. The reason is that Domain authentication uses passthrough authentication to the Windows Domain Controller. As a result, when implementing Domain authentication, Novell Native File Access software does not support the change password feature from the client; the password must be changed using the Domain Controller User Manager tool.

In order to understand how the Novell Native File Access software incorporates the security of NetWare with the native operating system's security (such as Microsoft Networking), it is useful to first know the functionality and interrelation of the following four distinct passwords used in a mixed networking environment.

- ♦ **Windows Local Password**—The Windows operating system requires a username and password to log in to the computer. This password, called the *local password*, is stored on the computer's local hard disk.
- ♦ **Windows Domain Controller Password**—Windows networking uses a domain controller, which is a computer running Windows Server software that manages user access to the Microsoft network. When Windows users log in to the network using a Domain Controller, they are required to enter a username and password for authentication. This password, called the *domain controller password*, is stored on the domain controller computer.
- ♦ **NetWare Password**—To access the NetWare network, each user must have a user account created specifically for him. This account is called a *User object* and is stored in the Novell eDirectory data store. It consists of a NetWare username and a corresponding *NetWare password*.

When the workstation is running Novell Client™ software, users log in by entering their NetWare username (including context) and password. NetWare usernames and passwords are stored securely in the eDirectory structure on NetWare servers.

- ♦ **Simple Password**—The *simple password* is also associated with a corresponding User object and is required to provide network access from workstations which are not installed with Novell Client software. As with the NetWare password, the simple password is stored securely in eDirectory on the network.

IMPORTANT: Remember that if Local authentication has been implemented, Windows users must have a simple password in order to access network resources using their native protocol (CIFS). However, if Domain authentication has been implemented for your server, a simple password is not required.

Two Methods for Creating Simple Passwords for Windows Users

You can create simple passwords either with ConsoleOne or NetWare Management Portal.

Using ConsoleOne

The ConsoleOne management utility lets you create simple passwords for users one at a time by completing the following steps.

- 1** At the Administrator Workstation, log in as a user with the Supervisor right.

Make sure that the Administrator Workstation meets the prerequisites described in “**Administrator Workstation Prerequisites**” on page 13.

- 2** Run CONSOLEONE.EXE (located in the \PUBLIC\MGMT\CONSOLEONE\1.2\BIN directory).
- 3** Right-click the User object and then click Properties.
- 4** Click the Login Methods tab and select Simple Password.
- 5** Create a simple password for the selected user by filling in the following fields:
 - ◆ **Set Simple Password:** Enter a unique password for the user.
 - ◆ **Confirm Simple Password:** Enter the same password for confirmation.

NOTE: If the simple password is different from the NetWare password, users enter the simple password when accessing the network with native protocols and they enter the NetWare password when logging in with Novell Client software.

- 6** Click OK.
- 7** Repeat Step 3 through Step 6 in order to create a simple password for each user that requires network access using Novell Native File Access software.
- 8** (Optional) If you want users to be able to change their own simple passwords after they log in the first time, check the Force Password Change check box.

Using NetWare Management Portal

You can also use NetWare Management Portal (renamed NetWare Remote Manager in later versions) to create simple passwords either for an individual user or for multiple users at once.

Accessing the NetWare Management Portal

- 1 In the Address field of your Web browser, enter the IP address of the server where you installed Novell Native File Access Pack software.

If the NetWare Enterprise Web Server is installed on your server, you will have to add the port number 8008 at the end of the IP address. For example, if your Portal server's IP address were 137.65.123.11, you would enter `http://137.65.123.11:8008` in the Address field of your browser.

- 2 At the login prompt, enter the server administrator username and password.
- 3 In the left frame, click Manage eDirectory > NFAP Security.

The NFAP security page appears.

HINT: For more information about using NetWare Management Portal, see the *NetWare Management Portal Utility Guide* in the NetWare 5.1 documentation (http://www.novell.com/documentation/lg/nw51/docui/index.html#./port_enu/data/a310k9x.html).

Creating Simple Passwords for Multiple Users

- 1 In the NFAP Multi-User Simple Password Set Utility section, select a method for designating which users on your network will receive simple passwords. There are two methods for selecting users:
 - ♦ To select all User objects in that particular context, enter a full context in the NDS Context field.
 - ♦ To select all User objects in the NDS tree, check the Traverse Context Tree for User Objects check box.

NOTE: Searching the entire NDS tree might take several minutes.

- 2 (Optional) If you want an automatic message to be sent to the selected users notifying them of their simple password, check the Send Password to User check box.

IMPORTANT: To use the Send Password to User feature, you must first use the Access Mail Notification Control Page to set up NetWare Management Portal to perform e-mail notification.

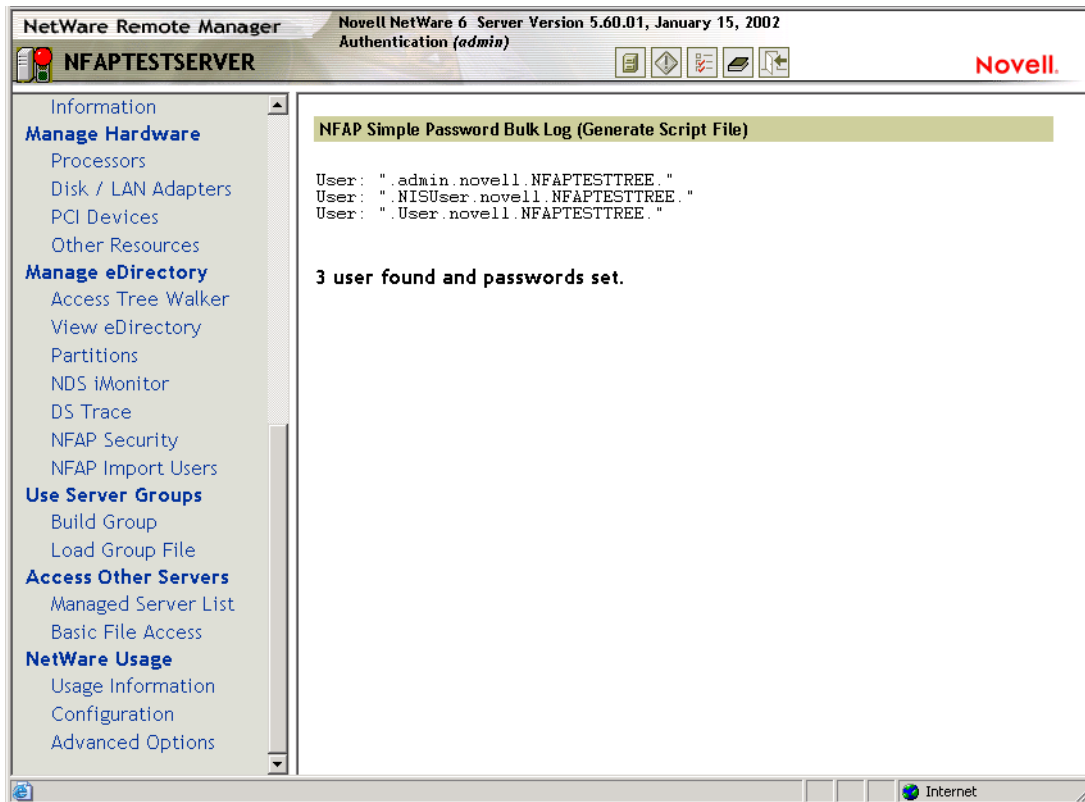
The Access Notification Control Page is available by clicking the configuration icon on the top of the screen. For more information, see the *NetWare Management Portal Utility Guide* in the NetWare 5.1 documentation (http://www.novell.com/documentation/lg/nw51/docui/index.html#./port_enu/data/a3l0k9x.html).

- 3** Specify a common simple password for all users by checking the User Supplied Password check box and entering a password in the field provided.
- 4** Check the Generate Script File check box and enter a filename for the script file.

The generated script file contains a list of users and will be processed by the utility to create the simple passwords for those users. You can choose any name for the script file.

- 5** (Optional) You can verify the contents of a generated script file before actually processing the script file. We recommend that you test the script file until it contains the appropriate list of users.
- 5a** Make sure the Process Script File check box is unchecked and then click Start.

The contents of the script file displays in the right frame.



IMPORTANT: No file will be generated and you will get an error in the browser if you do not fill in a filename for the script file.

- 5b** If the list is what you want, go to the next step and process the script file. If the list is not correct, click the Back button on your browser, change the NDS context settings, and click Start again. Repeat this process until the script file contains the appropriate information.
- 6** When you are ready to process the script file, check the Process Script File check box and enter the name of the script file.
The names in the Generate Script File and Process Script File fields must match exactly.
- 7** Click Start to process the script file.
The utility creates simple passwords for all of the users listed in the script file.

Creating a Simple Password for a Single User

- 1** In the NFAP Single-User Simple Password Set Utility section, enter the username (including the full context) in the Username and Context field.
- 2** Enter the text to be used for the user's simple password in the New Password field.
- 3** Click Set.

IMPORTANT: Remember to notify the user of the password.

Now that you have created simple passwords for User objects in NetWare, those users can use native protocols and familiar access methods (such as Network Neighborhood or My Network Places) to access and manipulate files on the server. When prompted to authenticate, users enter their NetWare username (without context) and their corresponding simple password.

Enabling Users to Change Their Simple Passwords with the NetWare Management Portal

You can use ConsoleOne to assign the necessary rights so that users can change simple passwords with the NetWare Management Portal tool.

- 1** At the Administrator Workstation, log in as a user with the Supervisor right.
Make sure that the Administrator Workstation meets the prerequisites described in "[Administrator Workstation Prerequisites](#)" on page 13.
- 2** Run CONSOLEONE.EXE (located in the \PUBLIC\MGMT\CONSOLEONE\1.2\BIN directory).
- 3** Right-click the User object and then click Trustees of This Object.
- 4** Select the User object and click Assigned Rights > Add Property.
- 5** Select the SAS:Login Configuration property from the list and click OK.
- 6** Click Add Property, select SAS:Login Configuration Key, and click OK.
- 7** Enable Compare, Read, and Write rights for both of the properties you just added to the User object.
- 8** Click OK > OK.

Understanding Synchronization of NetWare Passwords and Simple Passwords

Native File Access for Windows (CIFS) software allows users to change their own passwords from a client workstation. Of course, this applies only when Local authentication is being used since the Domain authentication method does not use simple passwords. When users change their simple passwords, their NetWare passwords will be affected differently, as described in the following scenarios:

- ◆ If both the NetWare password and the simple password are already the same when the user changes the simple password, the NetWare password is synchronized and both passwords remain the same.
- ◆ If the NetWare password and the simple password are *not* the same when the user changes the simple password, the NetWare password is not synchronized with the new simple password. The two passwords remain different.
- ◆ Whenever a user changes the NetWare password, the simple password is not synchronized with the new NetWare password. The user must separately change the simple password for the two passwords to match.

NOTE: Password synchronization is simpler for Macintosh users. Native File Access for Macintosh (AFP) software keeps the simple password and the NetWare passwords synchronized. In other words, when a Mac user changes either password using the native client software, password synchronization is automatic and transparent.

Specifying Contexts in the Context Search File

During the installation, you specified the NDS contexts for Windows users who require access to the network. These contexts are saved in the context search file. When Windows users enter a username, the Native File Access component running on the server searches through each context in the list until it finds the correct User object.

NOTE: In Domain mode, if User objects with the same name exist in different contexts, each User object attempts authentication in order until one succeeds with the corresponding password.

You can add or remove contexts by editing the context search file.

- 1 Using any text editor, edit the CIFSCTXS.CFG file stored in the SYS:\ETC directory of the server running Novell Native File Access Pack.

- 2 On separate lines, enter the full contexts to search.

For example, if you had users with full NDS distinguished names such as Robert.sales.acme, Maria.graphics.marketing.acme, Sophia.graphics.marketing, and Ivan.marketing.acme, then you would enter the following contexts to the CIFSCTXS.CFG file:

```
sales.acme
graphics.marketing.acme
marketing.acme
```

- 3 Save the file in the SYS:\ETC directory.
- 4 At the server console, enter **CIFSSTOP** to unload the current context search file.
- 5 Enter **CIFSSTRT** to load the new context search file and apply the changes.

When Windows users log in, they enter only a username and the simple password. The system finds the User object in the context specified in the CIFSCTXS.CFG file.

IMPORTANT: Remember that users must have a simple password before they can access the network.

Managing Network Access with ConsoleOne

ConsoleOne helps you manage Novell Native File Access for each computer platform. You can create users and groups, assign and restrict rights to directories, and view the rights of specific users.

To provide rights to network access, do the following:

- 1 From the Administrator Workstation, log in to the NetWare server running Novell Native File Access Pack software.
You must use a Windows workstation that meets the prerequisites as described in “**Administrator Workstation Prerequisites**” on page 13.
- 2 Run CONSOLEONE.EXE located in
\\PUBLIC\MGMT\CONSOLEONE\1.2\BIN\.
- 3 Set up and manage rights as described in the *ConsoleOne Users Guide* (<http://www.novell.com/documentation/lg/consol12d/index.html>).

Providing Network Access to Windows Domain Users

You can provide access to users from an existing NT domain by importing them into NDS.

- 1** Configure the Novell Native File Access Pack software for Domain authentication.

Importing users from an NT domain is not supported in Local Mode. In Local Mode, the main NetWare Management Portal page is displayed rather than the NFAP Import Users page.

- 2** Run NetWare Management Portal.

The NetWare Management Portal is launched by entering the IP address of the server into the URL field of an Internet browser.

See the *NetWare Management Portal Utility Guide* in the NetWare 5.1 documentation (http://www.novell.com/documentation/lg/nw51/docui/index.html#./port_enu/data/a310k9x.html).

- 3** In the left frame, click Manage eDirectory > NFAP Import Users.

- 4** Browse to the NDS Context that you will import the users into.

Any time you reach a valid context for importing users, a Start button appears.

- 5** Click Start to import users.

The context that you select is automatically written to the CIFSCTXS.TXT file, which contains all the contexts of all users.

Status of the import is given on the interval that you select.

- 6** When the import is complete, click Done to clear the screen.

Customizing the Network Environment Using a Configuration File

- 1** Log in to the server running the Novell Native File Access Pack software.

- 2** Change to the SYS:\ETC\ directory.

- 3** Edit CIFS.CFG using a text editor.

Enter the desired parameters following the rules for syntax.

- 4** Save the CIFS.CFG file to the same directory (SYS:\ETC).

- 5** Restart the server.

Configuration File Parameters

The following parameters can be set in the SYS:\ETC\CIFS.CFG file to customize the user experience for your environment.

HINT: Any parameter can be excluded by placing a # at the beginning of the command line. If the parameter is excluded, the default value is used.

-SERVERNAME

The name of the server running Novell Native File Access Pack. The length can be a maximum of 15 characters. This name is displayed in Network Neighborhood. This server name must be different from the NetWare Server name.

Value: *'Server_Name'*

Default: None

-COMMENT

The comment associated with the server name listed above. This comment is displayed when viewing details.

Value: *'Comments'*

Default: None

-AUTHENT

The method of authentication used by Novell Native File Access Pack software.

- ◆ Domain—Clients are members of a domain. A Windows domain controller performs user authentication. The username and password on the domain controller must match the username and password used to log in to the Windows workstation.
- ◆ Local—Clients are members of a workgroup. The server running Novell Native File Access Pack performs the user authentication. The username and password on NetWare must match the username and password used to log in to the Windows workstation.

Value: Domain | Local

Default: Local

-DOMAIN

The domain or workgroup that the server will belong to.

Value: *'Domain_Name'*

Default: Workgroup

-WORKGROUP

The domain or workgroup that the server will belong to. Workgroup and Domain can be used interchangeably.

Value: *'Workgroup_Name'*

Default: Workgroup

-PDC

The PDC server name and static IP address. This is needed if the PDC is on a different subnet. This option should be used only when there is a valid reason for overriding WINS or DNS.

IMPORTANT: The address of the PDC must be static; otherwise, if the PDC reboots and the address changes, the server running Novell Native File Access Pack will not be able to contact the PDC.

Value: *'PDC_Name' Address*

Default: None

-PDCNAME

The PDC server name. If the PDC and server running Novell Native File Access Pack are on different subnets, clients must use DNS name resolution to find the server. PDCNAME does not include the IP address.

Value: *'PDC_Name'*

Default: None

-WINS

Address of WINS server to be used to locate the PDC, if the PDC and server running Novell Native File Access Pack are on different subnets.

Value: *IP_Address*

Default: None

-ATTACH

Bind the CIFS protocol to the IP address specified. For multiple addresses, repeat the command as needed.

Value: *IP_Address*

Default: Bound to all addresses

-SHARE

Allow any volumes or directories on the server to be specified as shared points and to be accessible via the Network Neighborhood. If no -SHARE line is specified (or is commented out), then all mounted volumes are displayed.

- ◆ *Localpath* is the path to the server volume or directory which becomes the root of the sharepoint. This path must end with a backslash (\).
- ◆ *Sharename* is the name by which the sharepoint is known to the Windows computers.
- ◆ *Connection Limit* is the number of connections allowed to the sharepoint (0 is unlimited).
- ◆ *Comment* is a description for the sharepoint that appears in Network Neighborhood or My Network Places.

Value: '*Localpath*' '*Sharename*' *Connection Limit* '*Comment*'

Default: All mounted volumes are shared

-UNICODE

When On (enabled), this command enables Unicode characters (used in double-byte languages).

Value: On | Off

Default: Off (disabled)

IMPORTANT: To support Unicode, an additional file named UNINOMAP.TXT must be created and saved in the SYS:\ETC directory. When the -UNICODE value is set to On, the UNINOMAP.TXT file is used to resolve Unicode-to-ASCII "no-map" problems.

To specify "no-map" cases in the UNINOMAP.TXT file, enter the first Unicode value to watch for and then the second value representing the ASCII replacement code. For example:

```
0178 98
20AC CC
```

Save the values in the UNINOMAP.TXT file. If an unmappable character is encountered, the system uses the ASCII substitution character specified in the file.

Sample Configuration File

```
#This name will display in Network Neighborhood with the
#following comment.

-SERVERNAME 'NW51-NNFAP'

-COMMENT 'NetWare 5.1 running Novell Native File Access Pack'

#Novell Native File Access Pack is configured to use Local
#authentication.

-AUTHENT LOCAL

#The workgroup name is ONENET.

-WORKGROUP 'ONENET'

#When this volume is mounted, the local path CIFSVOL:\ will
appear as a sharepoint named Graphics Volume with unlimited
connections (0) and its corresponding comment.

-SHARE 'CIFSVOL:\' 'Graphics Volume' 0 'Lots of image files'
```

Configuration File Shortcuts

You can enter the following commands at the server console to modify the configuration file.

CIFS SHARE ADD *'localpath'* *'sharename'*
connectionlimit *'comment'* adds a new sharepoint and also adds
the command to the CIFS.CFG file.

CIFS SHARE REMOVE *'sharename'* removes the sharepoint and
comments it out of the CIFS.CFG file.

Viewing Configuration Details

You can view details about how Novell Native File Access Pack is configured by entering the following commands at the server console.

CIFS INFO displays operational information.

CIFS SHARE displays all active sharepoints.

CIFS SHARE *sharename* displays information about a specific
sharepoint.

Windows End User Tasks

When Novell Native File Access Pack is properly configured, the Windows users on your network will be able to perform the following tasks:

- ♦ “Accessing Files from a Windows Computer” on page 44
- ♦ “Mapping Drives from a Windows Computer” on page 44
- ♦ “Changing Passwords from a Windows Computer” on page 45

Accessing Files from a Windows Computer

From a Windows computer, you can access a file and folder each time it is required or you can map drives and create shortcuts that are retained after rebooting.

1 Enter your username (no context) and local password to log in to the computer.

2 Access the network by clicking the network icon.

In Windows 2000 or Windows ME, click My Network Places > Computer Near Me. In Windows 95/98, click Network Neighborhood.

3 Browse to the workgroup or domain specified during the Novell Native File Access software installation.

4 Select the server running Novell Native File Access Pack software.

Although it is the same computer, the Novell Native File Access server name is *not* the same as the NetWare server name. For more information, ask your network administrator.

HINT: You can enter the server name or the server IP address in Find Computer to quickly access the server running Novell Native File Access software.

5 Browse to the desired folder or file.

Mapping Drives from a Windows Computer

1 Enter your username and local password for Microsoft Networking.

2 Click Map Network Drive.

There are several ways to access Map Network Drive. For example, you can use the Tools menu in Windows Explorer or you can right-click Network Neighborhood.

- 3 Browse to or enter the following path:

`\\server_running_Novell_Native_File_Access_software\sharepoint | volume | directory\`

- 4 Select the server running Novell Native File Access Pack software.

Although it is the same computer, the Novell Native File Access server name is *not* the same as the NetWare server name. For more information, contact your network administrator.

- 5 Complete the on-screen instructions for mapping the drive.

Changing Passwords from a Windows Computer

Windows users can change and synchronize their local password and their simple password.

From a Windows 2000/NT Computer

- 1 Press Ctrl+Alt+Delete.
- 2 Click Change Password.
- 3 In the Domain field (or the Log On To field in Windows 2000), enter the name of the server running Novell Native File Access Pack software.
If your Windows computer is running Novell Client software, click Show All Resources and select the appropriate server.
- 4 Enter the username, old password, and new password as prompted.

The NetWare password and the simple password will be synchronized only if the old simple password matches the NetWare password. If they are different, the NetWare password will not be changed and access to the network will be denied. To change and synchronize the NetWare password, you must use the Administrator Workstation running Novell Client software.

From a Windows 95/98/ME Computer

- 1 Change the local password.
 - 1a Click Start > Control Panel > Passwords.
 - 1b Click Change Passwords > Change Windows Password.
 - 1c Enter the username, old password, and new password as prompted.
- 2 Change the simple password.

2a Click Start > Run.

2b Enter

```
NET PASSWORD server_running_NFAP_software
```

For example:

```
NET PASSWORD NetWare1
```

WARNING: The Windows NET PASSWORD utility sends unencrypted text (called *clear text*) over the network. If you are concerned about someone capturing your password over the network, you should manage passwords using ConsoleOne from the Administrator Workstation. For more information on why this issue exists, contact Microsoft Corporation.

2c Enter the same username, old password, and new password when prompted.

The NetWare password and the simple password will be synchronized only if the old simple password matches the NetWare password. If they are different, the NetWare password will not be changed and access to the network will be denied. To change and synchronize the NetWare password, you must use the Administrator Workstation running Novell Client software.

For more information on simple passwords, see [“Creating Simple Passwords for Windows Users” on page 30](#). For information on synchronization between simple passwords and NetWare (NDS) passwords, see [“Understanding Synchronization of NetWare Passwords and Simple Passwords” on page 37](#).

For Computers Using Domain Authentication

If the computer is configured to use domain authentication, then the password checking is done by the domain controller. The password can be changed using the Windows administration tools for a domain controller. For more information, contact your network administrator.

5

Setting Up Novell Native File Access Pack with Novell Cluster Services

Novell® Cluster Services™ software combined with Novell Native File Access Pack for NetWare® 5.1 provides high availability, scalability, and security to your network while reducing administrative costs associated with managing client workstations.

This chapter describes how to set up a NetWare 5.1 clustered environment so that Macintosh and Windows computers can use Novell Native File Access Pack software to access files on the network.

NOTE: For information on setting up UNIX computers to use Novell Native File Access Pack in a clustered NetWare 5.1 environment, see the *Novell Native File Access for UNIX Installation and Administration Guide*.

Prerequisites

Before installing Novell Native File Access Pack in a clustered environment, make sure that you have met the following prerequisites:

- Novell Cluster Services 1.01 installed on NetWare 5.1 servers
For information on configuring Novell Cluster Services, see <http://www.novell.com/documentation/lg/ncs/index.html>.
- NetWare 5.1 configured as described in “[NetWare Server Prerequisites](#)” on page 12
- Administrator workstation configured as described in “[Administrator Workstation Prerequisites](#)” on page 13
- Novell Native File Access Pack software installed on each server in the cluster following the instructions in “[Installing the Software](#)” on page 14

Setting Up for Macintosh

To set up the Macintosh portion of Novell Native File Access Pack in an environment running Novell Cluster Services, complete the following:

- 1** Load AFPTCP.NLM on all servers in the cluster by entering **LOAD AFPTCP** at the server system console.
HINT: You can add this command to the AUTOEXEC.NCF file of each server.
- 2** Cluster-enable the shared-disk volumes by following the procedures described in the [Cluster Services documentation](http://www.novell.com/documentation/lg/ncs/index.html). (<http://www.novell.com/documentation/lg/ncs/index.html>)
- 3** (Optional) Rename cluster-enabled volumes so Macintosh users will see the same volume name regardless of what server has the volume mounted.

For instructions, see “[Renaming Volumes](#)” on page 23.

Volumes are displayed as "ServerName.VolumeName." If the server fails over, the user sees the next failover server with the same volume name. For example, Server1.VOL1 becomes Server2.VOL1. Renaming each ServerName.VolumeName to a common name displays the common name regardless which server is providing the volume. For example, renaming Server1.VOL1 to Graphics, Server2.VOL1 to Graphics, and Server3.VOL1 to Graphics displays Graphics regardless which server is providing VOL1.

Macintosh clients should now be able to access files on the server cluster by entering the IP address or server name of the cluster-enabled volume.

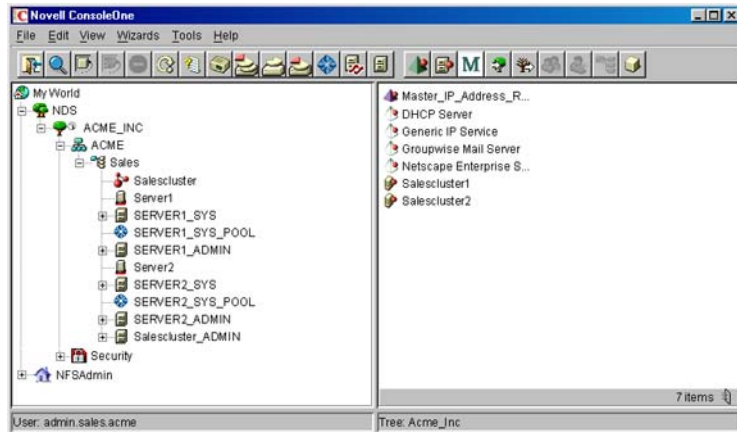
NOTE: Novell Native File Access does not support automatic reconnect for Macintosh computers. If the network connection between a Mac computer and one of the servers in the cluster fails, the user must reconnect using the same IP address for the cluster-enabled volume.

Setting Up for Windows

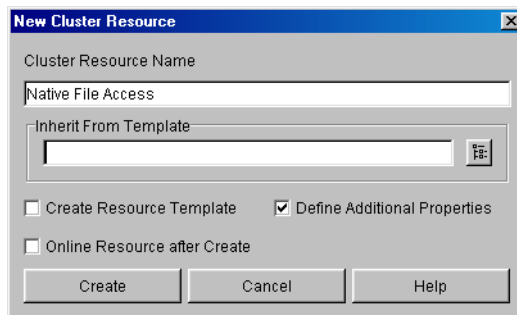
To set up the Windows portion of Novell Native File Access Pack in an environment running Novell Cluster Services, complete the following steps:

- 1** Remove the CIFSSTRT.NCF command from each server's AUTOEXEC.NCF file.
- 2** Create a Cluster Resource object that corresponds with the Novell Native File Access Pack support for Windows.

- 2a** Log in as a user with the Supervisor right to a server in the cluster.
- 2b** Run ConsoleOne™ located in
SYS:\PUBLIC\MGMT\CONSOLEONE\1.2\BIN\.



- 2c** Select the Cluster Resource object.
- 2d** Click File > New > Cluster > Cluster Resource.
- 2e** Name the Cluster Resource (for example, Native_File_Access).



- 2f** Click Create.
- 3** Edit the Cluster Resource Load Script.

HINT: A sample Cluster Resource Load Script is given at the end of this step.

The commands for configuring the Windows portion of Novell Native File Access Pack are controlled by the Cluster Resource Load Script.

- 3a** Click File > Properties.
- 3b** Click Scripts > Cluster Resource Load Script.

- 3c** Add the following commands to the Cluster Resource Load Script replacing *VOL1*, *VOL2*, and *VOL3* with the names of the shared disk volumes:

```
NSS /ACTIVATE=VOL1
NSS /ACTIVATE=VOL2
NSS /ACTIVATE=VOL3
MOUNT VOL1
MOUNT VOL2
MOUNT VOL3
TRUSTMIG VOL1 WATCH
TRUSTMIG VOL2 WATCH
TRUSTMIG VOL3 WATCH
```

- 3d** Assign the IP address that will be used to move the Cluster Resource object during failover and failback by adding the following commands and replacing *A.B.C.D* with the IP address assigned to the Cluster Resource object created in [Step 2 on page 48](#).

```
ADD SECONDARY IPADDRESS A.B.C.D
LOAD SETMD4
LOAD CIFSDNS
```

- 3e** Attach the IP address to the shared volume by entering the following command and substituting the *A.B.C.D* with the proper IP address, *VOL1* with the path you are exporting, *WORK* with the name of the share, *0* with the number of connections, and *Work_Volume* with the name to display.

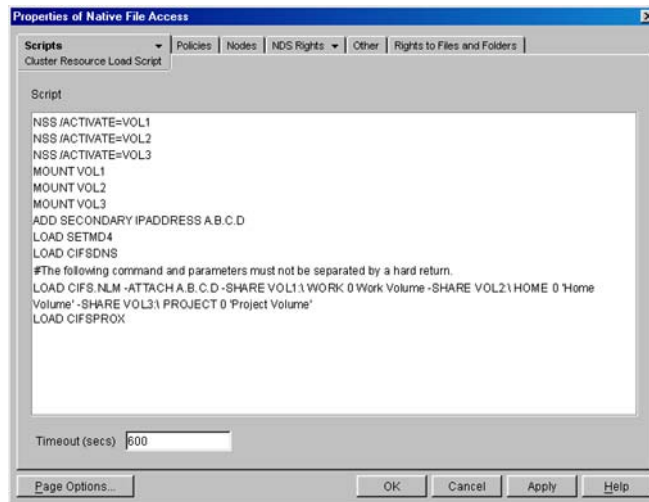
```
LOAD CIFS.NLM -ATTACH A.B.C.D -SHARE VOL1:\
  WORK 0 'Work_Volume'
```

NOTE: Do not separate this command and its parameters by hard returns.

You can specify multiple instances of parameters such as the following:

```
LOAD CIFS.NLM -ATTACH A.B.C.D -SHARE VOL1:\
  WORK 0 'Work_Volume' -SHARE VOL2:\ HOME 0
  'Home_Volume' -SHARE VOL3:\ PROJECT 0
  'Project_Volume'
```

NOTE: All shares to be advertised must reside on the shared-disk system.



- 3f** Make sure that all commands and parameters in the SYS:\ETC\CIFS.CFG file on each server are added to the LOAD CIFS.NLM command.

For example, if the CIFS.CFG file contains the command and parameters LOAD CIFS.NLM -SERVERNAME Server1 -UNICODE Off -AUTHENT Local -WORKGROUP -Workgroup, you would add these parameters to the LOAD command.

Adding to the example in [Step 3e on page 50](#), the command would be updated to

```
LOAD CIFS.NLM -SERVERNAME Server1 -UNICODE Off
-AUTHENT Local -WORKGROUP Workgroup -ATTACH
A.B.C.D -SHARE VOL1:\ WORK 0 'Work Volume' -
SHARE VOL2:\ HOME 0 'Home Volume' -SHARE VOL3:\
PROJECT 0 'Project Volume'.
```

NOTE: Do not separate this command and its parameters by hard returns.

- 3g** Rename each SYS:\ETC\CIFS.CFG file to SYS:\ETC\CIFS.BAK.
- 3h** Add the command **LOAD CIFS PROX**.
- 3i** Add the command **HTTP A.B.C.D /KEYFILE:"SSL CertificateIP"**.
- 3j** Add the command **LOAD NFAP4NRM** to automatically load the NetWare Remote Manager component that lets you set up and manage passwords.

For more information on the NFAP4NRM.NLM program, see
[“Using NetWare Management Portal” on page 33.](#)

Sample Cluster Resource Load Script

```
NSS /ACTIVATE=VOL1
NSS /ACTIVATE=VOL2
NSS /ACTIVATE=VOL3
MOUNT VOL1
MOUNT VOL2
MOUNT VOL3
TRUSTMIG VOL1 WATCH
TRUSTMIG VOL2 WATCH
TRUSTMIG VOL3 WATCH
ADD SECONDARY IPADDRESS A.B.C.D
# Add commands to start Native File Access for CIFS
LOAD SETMD4
LOAD CIFSDNS
LOAD CIFS.NLM -SERVERNAME Server1 -UNICODE Off -AUTHENT
Local -WORKGROUP -Workgroup -ATTACH A.B.C.D -SHARE VOL1:\
WORK 0 'Work Volume' -SHARE VOL2:\ HOME 0 'Home Volume' -
SHARE VOL3:\ PROJECT 0 'Project Volume'
LOAD CIFSprox
HTTPBIND A.B.C.D /KEYFILE:"SSL CertificateIP"
LOAD NFAP4NRM
```

4 Edit the Cluster Resource Unload Script.

4a Open the Cluster Resource Unload Script.

4b Click File > Properties.

4c Click Scripts > Cluster Resource Unload Script.

- 4d** Add the following command replacing *A.B.C.D* with the proper IP address:

```
DEL SECONDARY IPADDRESS A.B.C.D
HTTPUNBIND A.B.C.D
```

- 4e** Add the following commands to stop the Native File Access service:

```
UNLOAD NFAP4NRM
UNLOAD CIFSPROX
UNLOAD CIFS
UNLOAD CIFS DNS
UNLOAD SETMD4
```

- 4f** Add the following commands replacing *VOL1*, *VOL2*, and *VOL3* with the names of the shared disk volumes:

```
TRUSTMIG VOL3 UNWATCH
TRUSTMIG VOL2 UNWATCH
TRUSTMIG VOL1 UNWATCH
DISMOUNT VOL3 /FORCE
DISMOUNT VOL2 /FORCE
DISMOUNT VOL1 /FORCE
NSS /FORCEDEACTIVATE=VOL3
NSS /FORCEDEACTIVATE=VOL2
NSS /FORCEDEACTIVATE=VOL1
```

- 4g** Add any other UNLOAD commands that might exist to the CIFS.CFG file located in the SYS:\ETC\ directory on each server.

Sample Cluster Resource Unload Script

```
DEL SECONDARY IPADDRESS A.B.C.D

HTTPUNBIND A.B.C.D

UNLOAD NFAP4NRM

# Add commands to stop Native File Access for CIFS
UNLOAD CIFSPROX

UNLOAD CIFS

UNLOAD CIFS DNS

UNLOAD SETMD4

# Edit the following lines to match the volume name
```

```
# and IP address chosen.
# Client and server software should be configured with
# the IP address of the service. Use << to pipe
# characters into any command the requires keyboard input.
TRUSTMIG VOL3 UNWATCH
TRUSTMIG VOL2 UNWATCH
TRUSTMIG VOL1 UNWATCH
DISMOUNT VOL3 /FORCE
DISMOUNT VOL2 /FORCE
DISMOUNT VOL1 /FORCE
NSS /FORCEDEACTIVATE=VOL3
NSS /FORCEDEACTIVATE=VOL2
NSS /FORCEDEACTIVATE=VOL1
```

5 Configure the Cluster Resource policies.

For a complete description of policies and modes such as failback, failover, and start mode, see the [NetWare Cluster Services documentation](http://www.novell.com/documentation/lg/ncs/index.html). (<http://www.novell.com/documentation/lg/ncs/index.html>)

6 Assign the cluster resource preferred nodes.

NetWare Cluster Services automatically assigns the Cluster Resource to all nodes in the cluster. The order of assignment is the order that the nodes appear in the resource list.

What's Next?

With the NetWare 5.1 cluster configured with Novell Native File Access, Macintosh and Windows users can receive the benefits of a clustered environment—without needing additional client software.

For an explanation of how Macintosh users access network files and for more information on managing Macintosh workstations, see [Chapter 3, “Working with Macintosh Computers,”](#) on page 21.

For an explanation of how Windows users access network files and for more information on managing Windows workstations, see [Chapter 4, “Working with Windows Computers,”](#) on page 29.

54 Place Book Title Here