Introducing SCO VisionFS™

Document Code: VISUR/07/3.1 AU35200P004 February 2000

Copyright

Software License Notice

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of The Santa Cruz Operation.

Restricted Rights Legend

Any software that accompanies this publication is commercial computer software and, together with any related documentation, is subject to the restrictions on US Government use as set forth below.

If this procurement is for a DOD agency, the following DFAR Restricted Rights Legend applies:

RESTRICTED RIGHTS LEGEND: Use, duplication or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of Rights in Technical Data and Computer Software Clause at DFARS 252.227-7013. Contractor/Manufacturer is The Santa Cruz Operation, Inc., 400 Encinal Street, Santa Cruz, CA 95060.

If this procurement is for a civilian government agency, the following FAR Restricted Rights Legend applies:

RESTRICTED RIGHTS LEGEND: This computer software is submitted with restricted rights under Government Contract No. _____ (and Subcontract No. ____, if appropriate). It may not be used, reproduced or disclosed by the Government except as provided in paragraph (g)(3)(i) of FAR Clause 52.227-14 alt III or as otherwise expressly stated in the contract. Contractor/Manufacturer is The Santa Cruz Operation, Inc., 400 Encinal Street, Santa Cruz, CA 95060.

Trademarks

SCO, The Santa Cruz Operation, the SCO logos, SCO Vision2K, SCO VisionFS, SCO TermLite and SCO CIFS Bridge are trademarks or registered trademarks of The Santa Cruz Operation in the USA and other countries. UNIX is a registered trademark of The Open Group in the United States and other countries. All other brand and product names are or may be trademarks of, and are used to identify products or services of, their respective owners.

Document History

First published, June 1996
Second edition, March 1997
Third edition, August 1997
Fourth edition, November 1998
Fifth edition, February 2000

Corporate Headquarters & US Regional Sales Office

SCO
425 Encinal Street
Santa Cruz, California
95061-1900
United States of America
Tel: +1 831 425 7222
Fax: +1 831 458 4227
Sales and Information:
Tel: (800) 726-8649

Canada, Latin America and Australia Regional Sales Office

SCO
425 Encinal Street
Santa Cruz, California
95061-1900
United States of America
Tel: +1 831 427 7811
Fax: +1 831 427 5418

Europe, Middle East, India and Africa Regional Sales Office

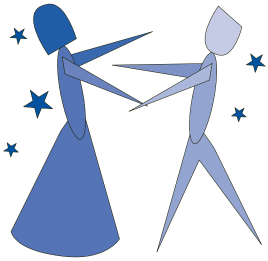
SCO United Kingdom
Croxley Business Park
Hatters Lane
Watford WD1 8YN
United Kingdom
Tel: +44 (0)1923 816344
Fax: +44 (0)1923 813808

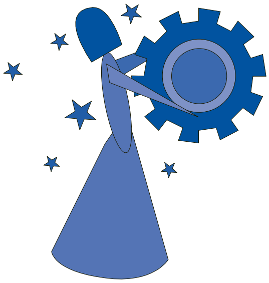
Asia Pacific Regional Sales Office

SCO Singapore
171 Chin Swee Road
#03-05/06 San Centre
Singapore 169877
Tel: +65 536 6606
Fax: +65 536 6619

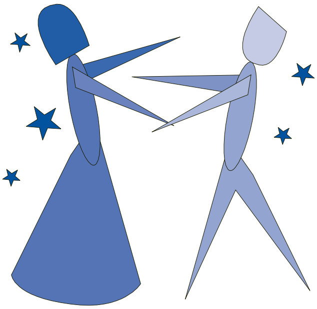
Email:info@sco.com **http://www.sco.com**

Contents





Welcome



Welcome to SCO VisionFS™, part of the SCO Vision2K™ suite of products.

This book introduces you to VisionFS and gets you up and running quickly. You should read it if you're a VisionFS Administrator or an advanced user.

In this book you'll discover why VisionFS is the easiest way to let PC users access UNIX files and printers, and how to tailor your VisionFS configuration using the VisionFS Profile Editor.

What is VisionFS?

VisionFS turns an Administrator's nightmare into a dream come true. It answers the question: PC or UNIX?

Users prefer PCs on their desktops, with good reason: the productivity tools they want to use are PC programs. But Administrators like UNIX systems for their reliability and configurability. UNIX systems are business critical.

VisionFS lets PC users access files on a UNIX host just as if they were on another PC—through network drives or their Network Neighborhood, for example. Not only that, with VisionFS PC users can print to UNIX printers—they're just like any Windows network printer. VisionFS can provide other services for PCs too: WINS, for network-wide naming, and Internet workgroups, for transparent access to computers on other networks.

For Administrators, there's an easy-to-use Windows program to configure VisionFS—no configuration files to edit, and no new file format to remember. More importantly, there's no PC installation. Ten minutes is all it takes to give any number of PCs access to a UNIX host, whatever the size of the network.

VisionFS server

A VisionFS server is a UNIX program with a difference: it speaks the same language as PCs for sharing files and printers across a network. This language is a Windows standard, developed originally by Microsoft and Intel, so it's the only sensible choice for integrating UNIX systems with your Windows users.

VisionFS effectively disguises a UNIX host as a PC. To other PCs and to users, a VisionFS server looks just like any other PC.

In fact, we'll be surprised if anyone notices the difference.

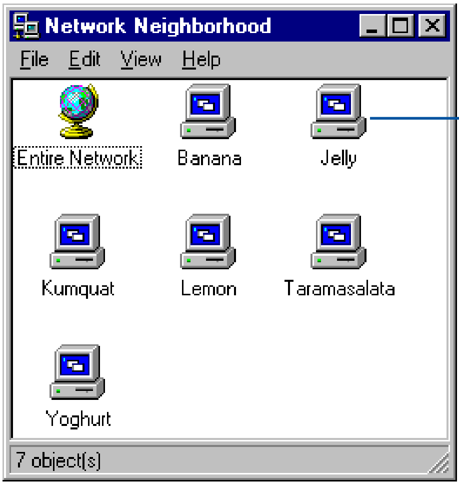
VisionFS Profile Editor

The VisionFS Profile Editor is a Windows program, used to configure the VisionFS server. The Profile Editor, closely integrated with the server, presents an intuitive interface complete with context-sensitive help and step-by-step instructions. It performs as-you-type validation of many settings, giving instant and helpful visual feedback. With multi-level undo and redo, you can change your mind, and change it back again.

Access to the VisionFS Profile Editor is restricted to a set of named *VisionFS Administrators*.

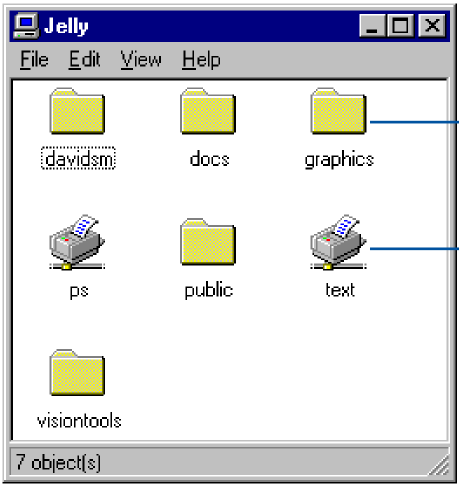
Using a VisionFS server

VisionFS servers appear with other computers in a Windows workgroup. (The only problem might be distinguishing the VisionFS servers from the PCs.)



This one's a UNIX host running VisionFS. Trust us.

VisionFS makes any number of UNIX directories and printers available to use over the network. These network resources are called *shares*.



Double-click a shared folder to view the files in the share.

Double-click a shared printer to view the print queue, or install as a network printer.

VisionFS Administrators name the server, choose which workgroups it appears in, and set up the shares people can access.

The benefits of VisionFS

Here are some compelling reasons why VisionFS gives the best solution for Windows-to-UNIX file and printer sharing and other network services.

Best for PCs

- There's no need to install complex software on PCs, saving a significant amount of time when setting up or upgrading a VisionFS server.
- VisionFS doesn't use any extra valuable memory or disk space on PCs.

Best for UNIX systems

- UNIX systems are ideal for network installations of disk-hungry PC products that can be used by multiple users.
- UNIX systems are robust, reliable and scalable, perfect for coping with the ever-changing, ever-growing world of PCs.

Best for users

- With no special PC software, users don't have to change the way they work or learn confusing new tools.
- If a program works with Windows, it works with VisionFS.

Best for Administrators

- Installed in just ten minutes: a few questions to answer, no fuss, no bother.
- Highly configurable through the Profile Editor, with fine-grained access control and instant feedback.

Part of Vision2K

- VisionFS is an important part of Vision2K, SCO's suite of Windows-to-UNIX integration products.

Setting up VisionFS

It's easy to install and set up VisionFS on your UNIX host. A Setup script, used by all Vision2K products, leads you step-by-step through installation and essential configuration.

Once VisionFS is up and running, you share UNIX files and printers with your PC users using the VisionFS Profile Editor. To make sure users have trouble-free access to VisionFS servers, you should also check out your PC and UNIX network settings.

To get started withVisionFS

‣ 1 Install VisionFS on your UNIX host

As root, run the **setup** script. See the CD insert or the **readme** file for full instructions. See also "What Setup needs to know", later in this chapter.

‣ 2 Import UNIX users (for new installations)

As root, run the VisionFS Password wizard that Setup points you to. This lets you import UNIX users into the VisionFS password database, and configure passwords. See "Importing UNIX users", later in this chapter.

‣ 3 Follow the network checklist

Make sure PCs on your network can access UNIX files and printers through VisionFS, using our simple network checklist. See "Checking out your network", later in this chapter.

‣ 4 Configure VisionFS from your PC

Log into Windows as a VisionFS Administrator, and run the VisionFS Profile Editor. See "VisionFS Administrator privileges", later in this chapter, and "A tour of the Profile Editor", in Chapter 1, "The Basics".

What Setup needs to know

This section gives more information about the settings that Setup uses to get VisionFS up and running.

Important You should read this section whether you accept Setup's suggested settings or choose a custom installation.

This setting…	Is used for…
Vision2K shared directory	Programs and data files, shared between more than one Vision2K product. Defaults to **/usr/local/vision**.
License mode	How the VisionFS server runs. Different license modes provide different levels of functionality, or only let you use VisionFS for an evaluation period.
Authentication method	The method VisionFS uses to authenticate users: using their UNIX password, using another server, or using the VisionFS password database (the default).
VisionFS Administrator	A Windows user allowed to configure the VisionFS server, using the Profile Editor. This user must have a valid UNIX account, but the Windows and UNIX usernames may be different.
Server name	The VisionFS server's network name, which Windows PCs use to access the server.
Start on reboot/Run level	Whether the VisionFS server starts automatically when the UNIX host reboots, and at which point during the reboot process the server starts.
Start now	Whether to start the VisionFS server immediately after Setup finishes.

See Also

"Importing UNIX users" and "VisionFS Administrator privileges", later in this chapter.

"License modes" and "The visionfs command", in Chapter 4, "Issues for Administrators".

All Vision2K products, including VisionFS, use a common licensing mechanism. When you install VisionFS, Vision2K License Services is automatically installed. You can enter license numbers during Setup, or later.

See Also

"License management", in Chapter 4, "Issues for Administrators".

You can configure the server name, and add and remove VisionFS Administrators, using the Profile Editor. To change the Start On Reboot settings later, use the **visionfs setup** UNIX utility.

Note Setup installs a **README.vfs** file in the **docs** subdirectory of the Vision2K shared directory. You should check this file for last-minute information that couldn't make it into this book.

VisionFS and Vision2K

SEE ALSO

"License management", in Chapter 4, "Issues for Administrators".

When you install Vision2K products on your UNIX host, Vision2K Setup lets you choose to make the PC parts of those products, if any, available automatically using a VisionFS shared folder.

If you do so, VisionFS adds a shared folder called **vision2k**. To install the PC parts of these products, users can simply open the **vision2k** shared folder, double-click **setup.exe**, and follow the instructions on the screen.

Importing UNIX users

SEE ALSO

"Passwords and authentication", in Chapter 2, "Beyond the Basics".

VisionFS includes three ways to authenticate users: using UNIX passwords, using another server (for example, a Windows NT or Windows 2000 server) or using its own VisionFS password database.

By default, VisionFS uses its own password database, which stores passwords encrypted in the same way as Windows. This ensures compatibility with current releases of Windows. (Previous releases of VisionFS used UNIX passwords by default, which meant that passwords would be transmitted unencrypted on the network. Current releases of Windows don't allow this by default.)

When VisionFS is first installed, the VisionFS password database is empty. Before you can configure the server using the Profile Editor, you need to add entries to the password database. You can do this easily using the VisionFS Password wizard.

SEE ALSO

"The visionfs command", in Chapter 4, "Issues for Administrators".

To start theVisionFS Password wizard

- As root on the UNIX host, type the following, replacing ***vision_dir*** with the name of the Vision2K shared directory, by default **/usr/local/vision**:

  ***vision_dir*/bin/visionfs password --wizard**

  Follow the instructions on your screen.

  Note The option is prefixed by two dashes, "--", not one.

Using the VisionFS Password wizard, you can:

- Import as many users as you want from the UNIX user database.
- Use a blank, random or fixed password for each user, or their username.
- Change passwords on a per-user basis.
- Send email to everyone whose password is affected, telling them their password.
- Use your own email message.

Note It's not possible to import passwords as well as users. This is because the encryption mechanisms used by Windows and UNIX are incompatible. Users can change their VisionFS password later, if they want.

If you don't want to use the VisionFS Password wizard, you can run the **visionfs password** command with other options. Use **visionfs password --help** to see what you can do.

VisionFS Administrator privileges

A user with *VisionFS Administrator privileges* (also known as a *VisionFS Administrator*) is a Windows user who's allowed to run the VisionFS Profile Editor. The Profile Editor is restricted because it lets you grant access to any UNIX directory, even as root.

There must always be at least one VisionFS Administrator, and all VisionFS Administrators must have valid UNIX accounts. When you install VisionFS, you name a VisionFS Administrator.

SEE ALSO

"Username mappings" and "Adding and removing VisionFS Administrators", in Chapter 2, "Beyond the Basics".

The VisionFS Username Mappings database lets users—including VisionFS Administrators—have different usernames on Windows and UNIX. To run the Profile Editor, you log into Windows using the Windows username.

Using the Profile Editor, VisionFS Administrators can give other users VisionFS Administrator privileges, or remove them. *Only let users you trust have Administrator privileges—a VisionFS Administrator is as powerful as root on the UNIX host.*

In summary:

- VisionFS Administrators are Windows users who can run the Profile Editor to configure a VisionFS server.
- VisionFS Administrators are as powerful as the UNIX superuser.
- There must always be at least one VisionFS Administrator.
- All VisionFS Administrators must have valid UNIX accounts.
- Username mappings let VisionFS Administrators (and everyone else) have different Windows and UNIX usernames.

Checking out your network

Follow this simple checklist to be sure your PCs and UNIX hosts are suitably configured for VisionFS.

See Also

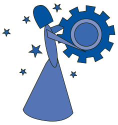
"Troubleshooting", in the Help index.

"Troubleshooting", in Chapter 4, "Issues for Administrators".

To make sure PCs can accessVisionFS

- Check your Windows 95, Windows 98 and Windows 2000 PCs have Client for Microsoft Networks installed
- Check your Windows NT 4 PCs have Workstation and NetBIOS Interface services installed
- Check your PCs are using TCP/IP as one of their network protocols
- Check your PC and UNIX broadcast addresses are identical

What's in this book



In Chapter 1, "The Basics", you'll take a tour of the Profile Editor and its extensive Help. You'll be introduced to some Windows and VisionFS terms, create a share, and discover how to change the VisionFS server's name.

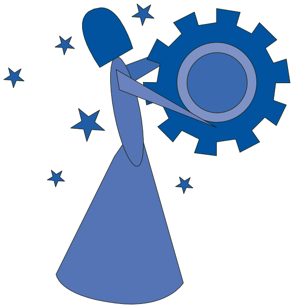
In Chapter 2, "Beyond the Basics", you'll discover some of the more sophisticated features of the VisionFS Profile Editor and server, including automatic shares, access rights, username mappings, and encrypted passwords.

In Chapter 3, "The Possibilities", you'll discover just a few of the ways in which you can take advantage of the flexibility of the Profile Editor and server, such as WINS, Internet workgroups, overriding automatic shares, and placeholders.

In Chapter 4, "Issues for Administrators", you'll learn how to control the VisionFS server from the UNIX host, and find information about things that matter to you, such as security, licensing and troubleshooting.

The Basics

1



Look in this chapter to find out how to get started with VisionFS and the Profile Editor.

You'll take a tour of the Profile Editor and its extensive Help. You'll be introduced to some Windows and VisionFS terms, create a share, and discover how to change the VisionFS server's name.

Contents

A tour of the Profile Editor

In this section, we'll point out the important parts of the VisionFS Profile Editor: what you see, and how you use it. We'll show you how the Profile Editor's instant validation and feedback stops you making mistakes, and how to get Help.

Finding and starting the Profile Editor

SEE ALSO

"Using more than one VisionFS server", in Chapter 3, "The Possibilities".

"License management", in Chapter 4, "Issues for Administrators".

For Help on TermLite and License Manager, use the Help menu in each program.

You use the VisionFS Profile Editor to configure the VisionFS server. A complete VisionFS configuration is called a server *profile*.

The VisionFS Profile Editor is stored on the UNIX host, and isn't installed on any PC. Every VisionFS server has its own Profile Editor, but you can use a Profile Editor to configure more than one server, as long as they're all the same version of VisionFS.

You access a VisionFS server's Profile Editor through a share on the server. This share, called **visiontools**, is created automatically by Setup. The **visiontools** share holds the Profile Editor and other useful tools, such as the License Manager and SCO TermLite.

How you access the **visiontools** share depends on your version of Windows:

- Windows 95, Windows 98 and Windows NT 4 users can open Network Neighborhood (or Windows Explorer).
- Windows 2000 users can open My Network Places.

SEE ALSO

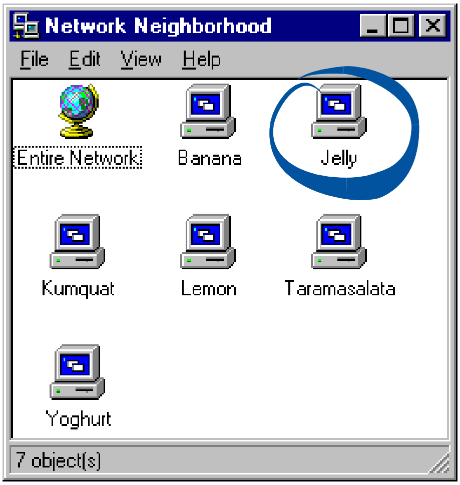
"Adding and removing VisionFS Administrators", in Chapter 2, "Beyond the Basics".

Note Only users with VisionFS Administrator privileges can run the Profile Editor. A VisionFS Administrator is named during Setup; this user can add and remove other VisionFS Administrators using the Profile Editor.

To find and start the Profile Editor

1 Log into Windows as a user with VisionFS Administrator privileges.

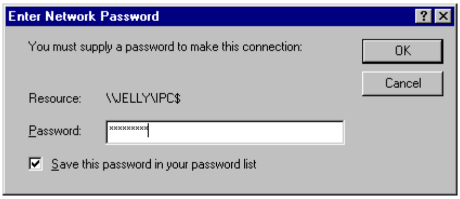
2 Open Network Neighborhood (or in Windows 2000, My Network Places) and locate the VisionFS server. You may need to open Entire Network and look for the workgroup it's in.



3 Double-click the VisionFS server.

See Also

"Passwords and authentication", in Chapter 2, "Beyond the Basics".


Enter Network Password

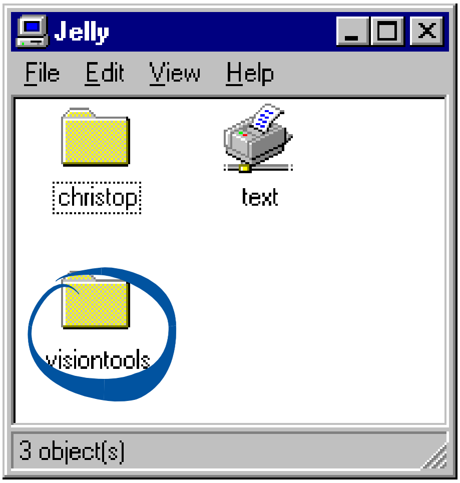
You must supply a password to make this connection:

Resource: \\JELLY\IPC$

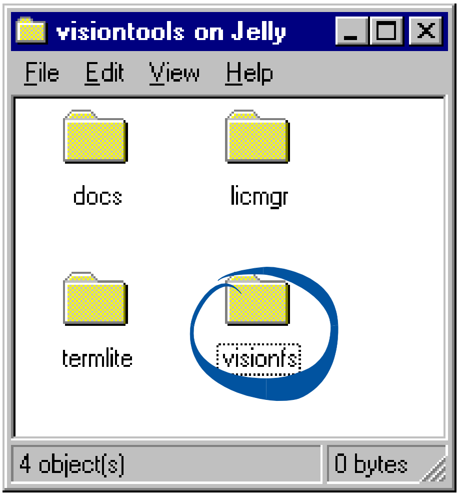
Password: *********

☑ Save this password in your password list

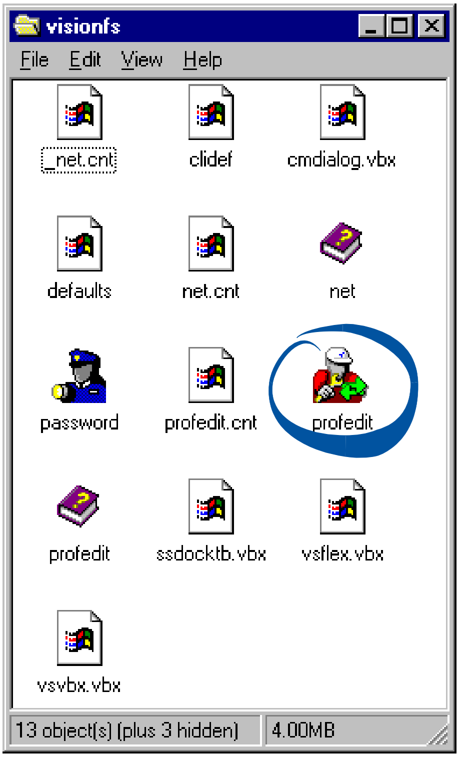
4 If prompted, type the VisionFS Administrator's password for this server.



5 Double-click the **visiontools** share.



6 Double-click the **visionfs** folder.



7 Double-click the Profile Editor.

Tip

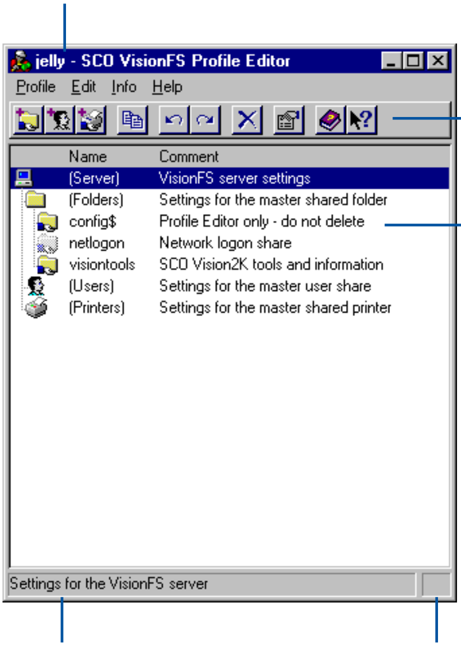
Create a shortcut to the Profile Editor on your desktop.

You can also click the Start button, click Run, then type \server\visiontools\visionfs\profedit.exe (replacing*server* with the name of your VisionFS server) to start the Profile Editor without browsing the network.

The Profile Editor window

The first time you run the VisionFS Profile Editor, you'll see a window like this:

The title bar shows the name used to access the server you're configuring.



Name	Comment
(Server)	VisionFS server settings
(Folders)	Settings for the master shared folder
config$	Profile Editor only - do not delete
netlogon	Network logon share
visiontools	SCO Vision2K tools and information
(Users)	Settings for the master user share
(Printers)	Settings for the master shared printer

Settings for the VisionFS server

The toolbar provides quick and easy access to useful menu commands.

The Profile tree shows the server, all the shares available, and the master shares.

The status bar gives information about buttons on the toolbar and entries in the Profile tree…

…and shows whether you've modified the profile.

SEE ALSO

"Main window", in the Help index.

Toolbar

To see a brief description of each button in the toolbar, rest the pointer over the button.

Profile tree

The Profile tree gives an overview of your server's configuration. Some parts of the tree are always shown: the entries with names in parentheses ( ). Other parts depend on the shares you have on your particular server.

At the top of the tree is the server you're configuring. Below that are three groups: *shared folders*, *user shares* and *shared printers*. Each group has a *master share*, handy for more advanced use. We'll explain more about the different types of share later in this book.

SEE ALSO

"Master shares" and "Automatic shares", in Chapter 2, "Beyond the Basics".

The first time you run the Profile Editor, you'll see two shared folders in the Profile tree: **config$** and **visiontools**. You've already used the **visiontools** share to access the Profile Editor. The **config$** share is a special share used by the Profile Editor (Windows doesn't show this share). Both shares are created by Setup.

When you add and remove shares, entries appear and disappear in the Profile tree.

Changing settings

The Profile tree is the starting point for configuring your VisionFS server. From the Profile tree you can access all settings for your shares and the server.

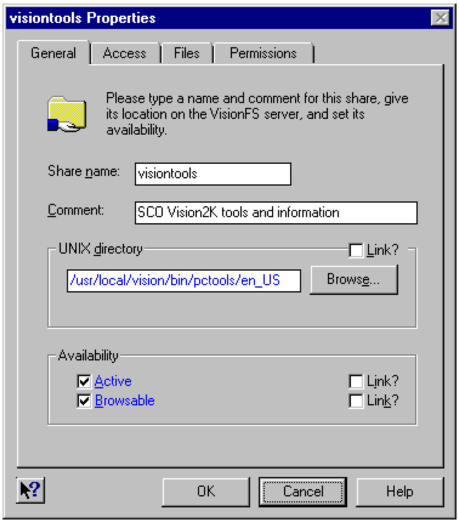
Tip

Double-click an entry in the Profile tree to show its Properties.

To change settings for a share or the server

1 In the Profile tree, click the entry you want to change the settings for.

2 On the Edit menu, click Properties.



Please type a name and comment for this share, give its location on the VisionFS server, and set its availability.

Share name: visiontools

Comment: SCO Vision2K tools and information

UNIX directory □ Link?

/usr/local/vision/bin/pctools/en_US

Availability

☑ Active □ Link?

☑ Browsable □ Link?

3 View or change the settings you want. Click the tabs to show all the options you can set.

Some settings let you include placeholders, like **(share-name)**, to refer to values that aren't constant.

See Also

"Placeholders", in the Help index.

4 When you've finished, click OK to keep any changes you've made. Or click Cancel to close the dialog without making any changes.

When you change a setting in the Profile Editor, it doesn't take effect immediately. An icon in the lower-right corner of the Profile Editor indicates that you've made a change the server doesn't know about yet.

Types of change

There are three types of change you can make:

- A change that affects everybody immediately. For example, creating a new share.
- A change that won't affect people who are already using a share, but will affect new users. For example, changing who can access a share.
- A change that won't affect anybody, unless you restart the server. For example, renaming the server.

SEE ALSO

"Main window", in the Help index.

For this reason, the Profile Modified icon has three forms:

- A transparent background for changes that can take effect immediately.
- A green background if some changes won't affect users who are already connected to the server.
- A red background if you must restart the server for all changes to take effect.

Making changes permanent

When you're happy with the changes you've made, you update the VisionFS server with the new profile. After you've updated the server, the Profile Modified icon disappears.

To update the server with a modified profile

- On the Profile menu, click Update Server.

  Depending on the changes you've made, the Profile Editor may offer to restart the server for you. Restarting the server means the Profile Editor must close.

Undoing and redoing changes

If you change some settings by mistake, you can undo those changes easily as long as you haven't updated the server in the meantime. The Profile Editor remembers your last twenty changes.

SEE ALSO

"Passwords and authentication", in Chapter 2, "Beyond the Basics".

As long as you don't make any new changes, you can also redo changes you've just undone.

Note You can't undo or redo changes to users' VisionFS passwords.

When you update the server or exit the Profile Editor, the undo and redo buffers are cleared.

To undo a change

- On the Edit menu, click Undo. Or click the Undo button ↶ on the toolbar.

TIP

To abandon all your changes, click Reload on the Profile menu.

To redo a change

- On the Edit menu, click Redo. Or click the Redo button ↷ on the toolbar.

Exiting the Profile Editor

You can exit the Profile Editor at any time.

To exit the Profile Editor

- On the Profile menu, click Exit.

  If you've made any changes to the profile, you'll be asked whether you want to update the server. Click Yes to keep the changes, No to forget them, or Cancel to change your mind and stay working in the Profile Editor.

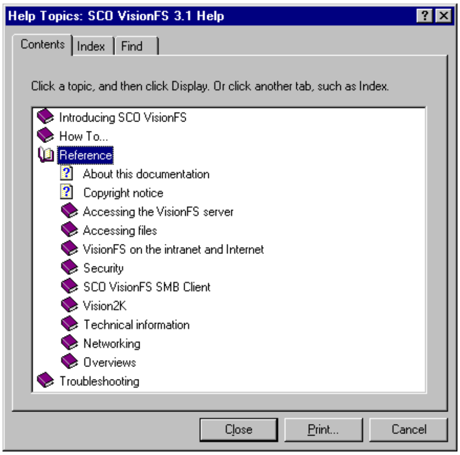
Getting Help

Online Help is the main source of information about VisionFS. All Help is stored with the Profile Editor, in the **visionfs** folder of the **visiontools** share, in Windows Help format. See your Windows manuals for full instructions on using Help.

To get Help

- In the Profile Editor, click Help Topics on the Help menu. Or click the Help button on the toolbar.

  The list of Help topics appears.



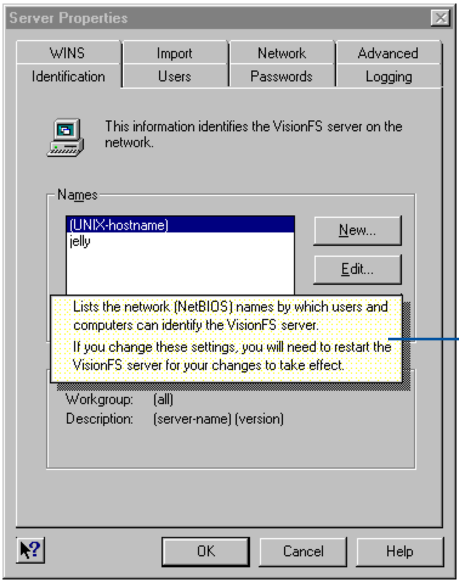
Click a topic, and then click Display. Or click another tab, such as Index.

- Introducing SCO VisionFS
- How To...
- Reference
  - About this documentation
  - Copyright notice
  - Accessing the VisionFS server
  - Accessing files
  - VisionFS on the intranet and Internet
  - Security
  - SCO VisionFS SMB Client
  - Vision2K
  - Technical information
  - Networking
  - Overviews
- Troubleshooting

You can use the tabs in Help to search for information in several ways.

To get Help on a specific item

- For information about an item in the Profile Editor, click ? and then click the item.



This information identifies the VisionFS server on the network.

(UNIX-hostname)
jelly

Lists the network (NetBIOS) names by which users and computers can identify the VisionFS server.

If you change these settings, you will need to restart the VisionFS server for your changes to take effect.

Workgroup: (all)
Description: (server-name) (version)

A pop-up explanation appears. Click it to make it disappear.

Manipulating shared folders

In this section you'll learn the basics of share management: creating, configuring and deleting shares, accessing them, and how to interpret the files you see in a share.

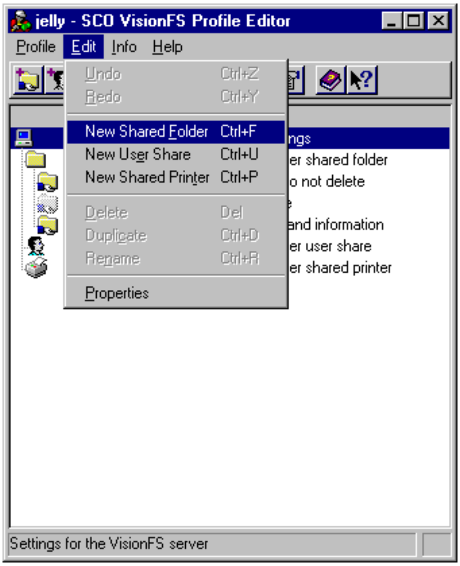
Creating a shared folder

Now you'll use the VisionFS Profile Editor to create your first share: a shared folder, giving access to a UNIX directory. First we'll take you through the process step by step, pointing out how the Profile Editor can help you before you make a mistake. Finally, we'll summarize the procedure.

Starting off

Start the Profile Editor, as described earlier in this chapter.

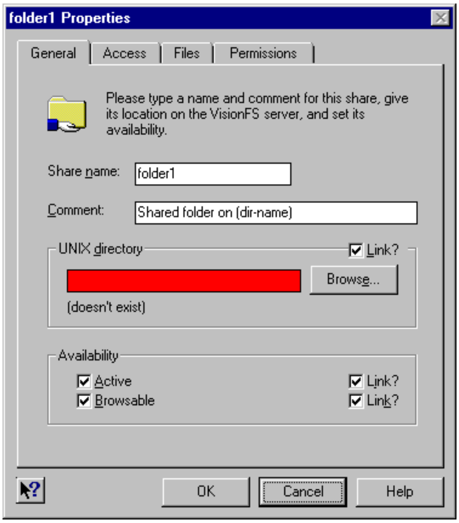
On the Edit menu, click New Shared Folder. Or click the New Shared Folder button on the toolbar.



In the Profile tree, a shared folder called **folder1** appears. The Profile Editor shows properties for the shared folder automatically.

The General tab

Before making any changes, take a look at the General tab.



folder1 Properties

Please type a name and comment for this share, give its location on the VisionFS server, and set its availability.

Share name: folder1

Comment: Shared folder on (dir-name)

UNIX directory ☑ Link?

(doesn't exist)

Availability

☑ Active ☑ Link?

☑ Browsable ☑ Link?

The first thing you might spot is the UNIX Directory box in red. This is the Profile Editor's way of indicating a problem with a setting—in this case, there's no directory in the text box. Before you can add the share, you must fill in a directory name.

Also, below the text box there's a line saying "(doesn't exist)". This is because the current contents of the box don't correspond to a UNIX directory that exists. As you type a directory, the Profile Editor will check silently; the line disappears when you've typed a directory name that exists on the host.

Many different settings give the same helpful indication and feedback:

- If you see a setting turn red and you don't know why, click OK and the Profile Editor will explain how to fix the problem.
- If you see a comment in parentheses beside a setting, or the setting turns yellow, it's the Profile Editor giving instant feedback. It doesn't mean the setting's invalid: just that you might want to think twice before using it.

Filling in the details

First, we'll name the shared folder. Next to Share Name, type **temp**. People use this name to access the share, so you'll probably want to make the name descriptive.

Notice how, as you delete the text **folder1**, the box turns red; this is to remind you that shares must have a name.

SEE ALSO

"Browse lists", in the Help index.

Next to Comment, type **Temporary files**. Windows shows comments in browse lists, and when you use Details view in folders.

Next to UNIX Directory, type **/tmp**. This is the UNIX directory you're giving people access to. As you type the first character, the box stops being red to show the setting's valid.

Also, you'll see that as you type each character, the "(doesn't exist)" line and yellow coloring may appear or disappear. Assuming there's a **/tmp** directory on your UNIX host, the feedback line should disappear when you finish typing.

You can type directories that don't exist, but you'll need to create the directory on the UNIX host before people can see and access the shared folder.

Lastly, notice how the directory you've just typed appears in blue, and the Link box clears. We'll explain blue settings and links later in this book. For now, don't worry—these aren't errors.

SEE ALSO

"Browsing UNIX directories", in the Help index.

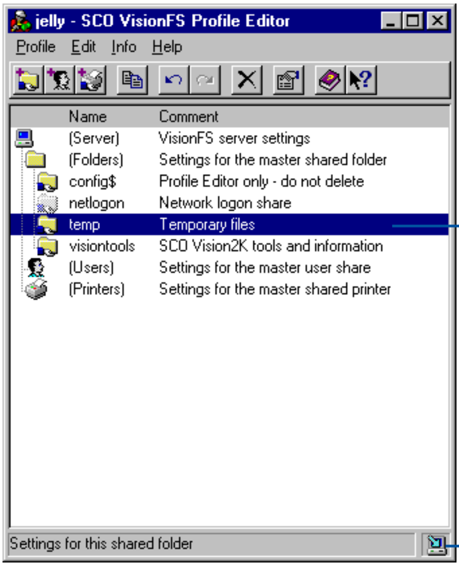
You don't have to remember and type in directory names. If you want, you can click Browse and search for a UNIX directory. Bear in mind that if the UNIX host uses NFS to mount remote UNIX directories in /, it may take a few moments for a directory listing of / to appear.

For normal shared folders, you can leave all the other settings as their defaults. Click OK to use these settings.

SEE ALSO

You can get Help on an item by clicking the question mark button, then clicking the item.

Making the shared folder available



Name	Comment
(Server)	VisionFS server settings
(Folders)	Settings for the master shared folder
config$	Profile Editor only - do not delete
netlogon	Network logon share
temp	Temporary files
visiontools	SCO Vision2K tools and information
(Users)	Settings for the master user share
(Printers)	Settings for the master shared printer

Settings for this shared folder

The Profile tree shows your new shared folder.

The Profile Modified icon indicates a change that can take effect immediately.

At the moment, the server doesn't know about the new shared folder. To let people use it, click Update Server on the Profile menu. The Profile Modified icon will disappear.

Summary

In summary, here's how you create a new shared folder.

To create a new shared folder

1. In the Profile Editor, click New Shared Folder on the Edit menu. Or click the New Shared Folder button on the toolbar.

   Your new share is shown in the Profile tree, and the shared folder properties dialog is displayed.

2. Type a name, comment and UNIX directory for the share.
3. Change any other properties you want.
4. Click OK.
5. On the Profile menu, click Update Server.

Accessing a shared folder

See Also

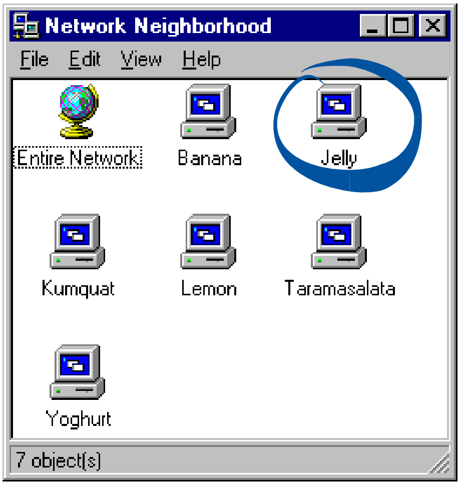
"Finding and starting the Profile Editor", earlier in this chapter.

Now you've created a shared folder, you'll want to make sure you can use it. Accessing a shared folder you've created is very similar to accessing the **visiontools** share, described earlier.

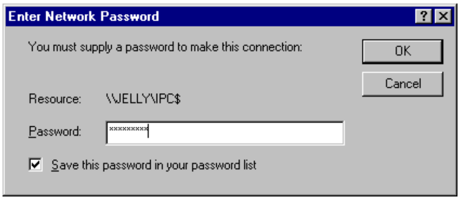
Windows users will recognize the steps: they're exactly the same steps you use to access shares on other Windows PCs. In fact, any method you use to access other Windows PCs can be used to access a VisionFS server.

To access a shared folder using Network Neighborhood

1 Open Network Neighborhood (or in Windows 2000, My Network Places) and locate the VisionFS server. You may need to open Entire Network and look for the workgroup it's in.



2 Double-click the VisionFS server.



You must supply a password to make this connection.

Resource: \\JELLY\IPC$

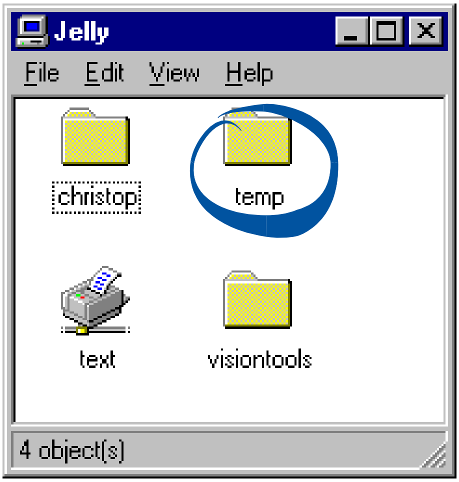
Password: *********

☑ Save this password in your password list

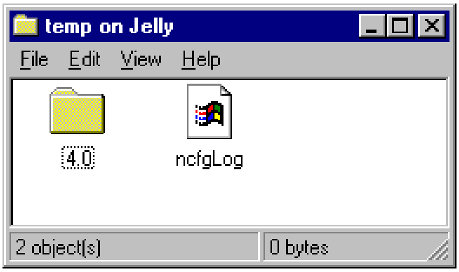
3 If prompted, type your password for this server.

See Also

"Passwords and authentication", in Chapter 2, "Beyond the Basics".



4 Double-click the shared folder.



If you're allowed access to the share, you'll see the files and directories it contains.

Tip

Use shortcuts to give access to frequently used shares, and files within shares.

Windows and UNIX filenames

One important difference between Windows and UNIX systems concerns filenames.

See Also

"PC and UNIX file differences", in Chapter 4, "Issues for Administrators".

- In Windows, filenames are case-insensitive, but case-preserving. For example, Windows treats **foo** and **FOO** as identical names—you can't have files with these names in the same directory—but will remember which characters were upper-case and which were lower-case, and show them appropriately.
- On UNIX systems, filenames are case-sensitive. You can have files called **foo** and **FOO** in the same directory.

Also, Windows for Workgroups filenames are restricted to "8.3" format—up to eight alphanumeric characters, optionally followed by a dot and an extension of up to 3 alphanumeric characters. UNIX systems don't have this restriction.

Windows 95, Windows 98, Windows NT and Windows 2000 allow filenames of any length, but they're still case-insensitive.

VisionFS is designed to work best from a Windows perspective. This means:

- VisionFS can include special characters in the truncated (8.3) form of a filename to distinguish it from other truncated filenames. This lets you access both**myreport1999.doc**and**myreport2000.doc**from all versions of Windows.
- Filenames on UNIX that differ only by case (for example, **foo** and **FOO**) aren't distinguished. Through VisionFS you can access only one of the files.

See Also

"Controlling access", "Username mappings" and "Passwords and authentication", in Chapter 2, "Beyond the Basics".

"How to tell if an action will succeed", in Chapter 4, "Issues for Administrators".

Who's allowed to access a shared folder?

By default, anyone who is authenticated (supplies a valid password for accessing the VisionFS server) is given full access to the files and directories in the shared folder, and all actions are performed using their UNIX username, taking into account any username mappings. Guests (who don't have a password) are denied access.

This means that when an authenticated user tries to manipulate files or directories in any way, for example deleting a file, the result would be the same as if they'd performed the action from the UNIX command prompt. If the UNIX host would deny permission, so will VisionFS.

Deleting a share

Now you'll delete your **temp** share. Deleting a share doesn't delete any UNIX files or directories; it just means people won't be able to access those directories from PCs.

See Also

"Troubleshooting", in Chapter 4, "Issues for Administrators".

Note Don't delete the **config$** or **visiontools** shares, or configure them so that VisionFS Administrators can't access them. If you do so, nobody will be able to run the Profile Editor. If this happens by accident, run the **visionfs setup** UNIX utility to fix your profile.

To delete a share

1. In the Profile tree, click the share you want to delete.
2. On the Edit menu, click Delete. Or click the Delete button ☒ on the toolbar.
3. On the Profile menu, click Update Server.

   If you want to disconnect people using this share at the moment, restart the server when the Profile Editor offers.

Identifying the VisionFS server on the network

A UNIX host has many different types of name, usually (but not limited to) a hostname, an IP address, and a DNS name. It may also have multiple DNS names or multiple IP addresses.

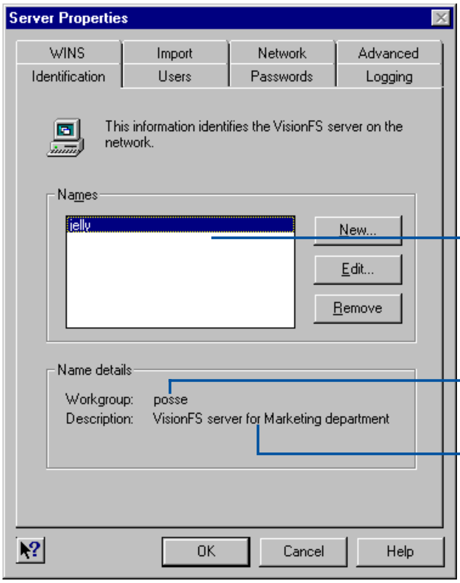
For Windows networking, the VisionFS server uses another name (technically, a NetBIOS name). Other PC users on the network use this name to refer to the server. As well as a name, you can provide a description. Users will see this description when they look at the VisionFS server on the network. Computers are grouped into loose collections called *workgroups*. Workgroups don't have a strict hierarchy, and computers can appear in more than one workgroup.

Your VisionFS server can have as many names as you like. Each name can have its own description, and can appear in any or all workgroups.

To identify the VisionFS server on the network

1 In the Profile tree, click **(Server)**.

2 On the Edit menu, click Properties, then click the Identification tab.



This information identifies the VisionFS server on the network.

Names: jelly

Workgroup: posse

Description: VisionFS server for Marketing department

The names used by this server.

The workgroup the highlighted name appears in.

The description used for this name.

Tip

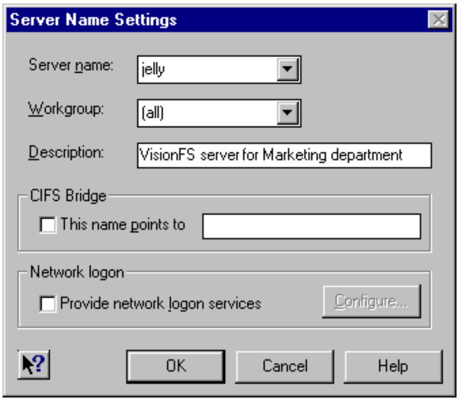
Add the same name repeatedly for each workgroup you want it to appear in.

3 To add a name, click New.

To edit a name, click it in the list, then click Edit.

To remove a name, click it in the list, then click Remove.

4 If you're adding or editing a name, the Server Name Settings dialog appears.



Server Name Settings

Server name: jelly

Workgroup: (all)

Description: VisionFS server for Marketing department

CIFS Bridge

□ This name points to

Network logon

□ Provide network logon services

5 Change the settings you want, then click OK.

See Also

"CIFS Bridge", in the Help index.

"Network logon services", in Chapter 3, "The Possibilities".

To choose one of the server's current names, or one of the workgroups on your network, click it in the appropriate list.

To set up this name as a CIFS Bridge to a computer on another network, check the box and type the DNS name or IP address of the computer.

To use this server name to provide network logon services in its workgroup, check the box.

6 Repeat steps 3 to 5 for all the names you want to use. When you're done, click OK, then click Update Server on the Profile menu. You'll need to restart the server for the new names, workgroups and descriptions to take effect.

CIFS Bridge

CIFS, or the Common Internet File System, is a recent standard for accessing files and printers on remote computers across intranets or the Internet. With a CIFS Bridge, you can include a remote computer in a workgroup as if it were local.

Not all computers understand the CIFS standard. To allow these computers to access remote computers, a VisionFS server can act as a *CIFS Bridge*: any of its server names can point to another computer, anywhere on the intranet or Internet, rather than the VisionFS server itself.

For a CIFS Bridge to a remote PC, make sure the CIFS Bridge name is the same as the remote PC's network name. For a CIFS Bridge to a remote VisionFS server, you can use any CIFS Bridge name.

A CIFS Bridge is "one-way": it points to another computer, but that computer can't use the CIFS Bridge in reverse to access your computer.

Note Although a CIFS Bridge is "one-way", other sites can create a CIFS Bridge to a computer on your site. However, your firewall should prevent any unauthorized access.

For more information on CIFS, point your favorite web browser at **www.cifs.com**.

How are workgroups maintained?

Each workgroup is self-organizing: it automatically elects one of its members to maintain the list of computers in the workgroup. This computer is called the *master browser*.

When you choose to list the computers in your workgroup, your computer contacts the master browser for the details.

If some details change, the master browser may take some time to fully reflect the new information. For example, if you rename your VisionFS server the master browser will show the new name immediately, but the old name may still be displayed for a time.

A VisionFS server will usually become the master browser in a workgroup. It won't become the master browser if the workgroup contains a Windows 2000 or Windows NT PC. Also, a VisionFS server won't try to become a master browser if it's configured to be in *all* workgroups, rather than in specific named workgroups.

See Also
"Master browser", in the Help index.

Beyond the Basics

2

Look in this chapter when you've mastered the basics, and want to know more about how to configure your VisionFS server.

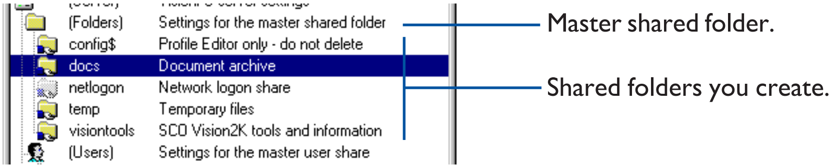
You'll discover some of the more sophisticated features of the VisionFS Profile Editor and server, including automatic shares, access rights, username mappings, and encrypted passwords.

Contents

Master shares

In Chapter 1, “The Basics”, we created and manipulated a shared folder. In this section, we’ll introduce master shares, and explain links.

When you created your shared folder, it appeared in the Profile tree alongside the existing shared folders. Just above these folders is the *master shared folder*.



(Folders)	Settings for the master shared folder
config$	Profile Editor only - do not delete
docs	Document archive
netlogon	Network logon share
temp	Temporary files
visiontools	SCO Vision2K tools and information
(Users)	Settings for the master user share

Master shared folder.

Shared folders you create.

See Also

“Automatic shares”, later in this chapter.

Similarly, there’s a master shared printer and a master user share, just above the other types of share in the Profile tree. You only see these *master shares* in the VisionFS Profile Editor; Windows doesn’t show them.

Master shares contain the master settings for that type of share. The settings from a master share are used:

- As the default settings when you create a new share of that type.
- When you check the Link box next to an option in a share’s properties.
- As the settings for automatically generated user shares and automatically generated shared printers.

You configure a master share in exactly the same way as you configure a real share, but you can’t delete the master shares.

Links

In the Profile Editor, Link boxes appear next to some options in a share’s properties. If a Link box is checked, it means the neighboring option is linked to the setting in the master share.

- Linked settings automatically change when you modify the same setting in the master share.
- Settings that aren’t linked appear in blue, so you can easily identify differences from the master share.

When you create a new share, all the settings are automatically linked (except for the name and comment, which don’t have Link boxes), so the share’s effectively a clone of the master share.

If you change a setting in the new share, the Link box automatically clears to remove the link. The setting becomes independent of the master share. You can restore the link by checking the Link box again.

See Also

"Using links effectively", in Chapter 3, "The Possibilities".

You might like to think of a particular share's configuration as a set of differences from the master share; alternatively, that a share inherits settings from its master share.

Using master shares and links effectively can help you minimize the work needed to change a setting in lots of shares simultaneously.

Automatic shares

We've already shown how easy it is to let Windows users access UNIX files and directories just as if they were on another PC on the network.

In this section we'll explain how VisionFS can automatically create shares for your UNIX users and printers, saving you valuable time and effort.

Automatic user shares

See Also

"Generating automatic user shares", in the Help index.

"Accessing a shared folder", in Chapter 1, "The Basics".

"Username mappings", later in this chapter.

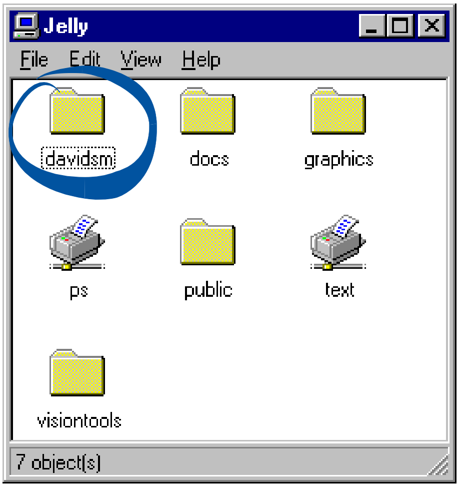
Automatic user shares let Windows users with valid UNIX accounts access their home directories.

In Windows, when you list the shares on a VisionFS server you see a share with your UNIX username, taking into account any username mappings (as long as automatic user shares are enabled, which they are by default). Accessing your home directory through your user share is as simple as accessing any other shared folder.

You'll only ever see one user share in share lists—for yourself.

Tip

To find out who has a user share, click the Info menu, then click UNIX Users.



Your user share, generated automatically.

See Also

"Configuring automatic shares", later in this chapter.

The VisionFS server uses the settings from the master user share for automatic user shares. However, you can override settings for individual user shares, if you want.

As automatic user shares are just "clones" of the master user share, the Profile Editor doesn't show them.

SEE ALSO

"Username mappings", "Controlling access" and "Passwords and authentication", later in this chapter.

"How to tell if an action will succeed", in Chapter 4, "Issues for Administrators".

WHO'S ALLOWED TO ACCESS A USER SHARE?

By default, anyone who is authenticated (supplies a valid password for accessing the VisionFS server) is given full access to the files and directories in their own user share, and all actions are performed using their UNIX username, taking into account any username mappings. All other users are denied access.

This means that when a user tries to manipulate files or directories in any way, for example deleting a file, the result would be the same as if they'd performed the action from the UNIX command prompt. If UNIX would deny permission, so will VisionFS.

Automatic shared printers

SEE ALSO

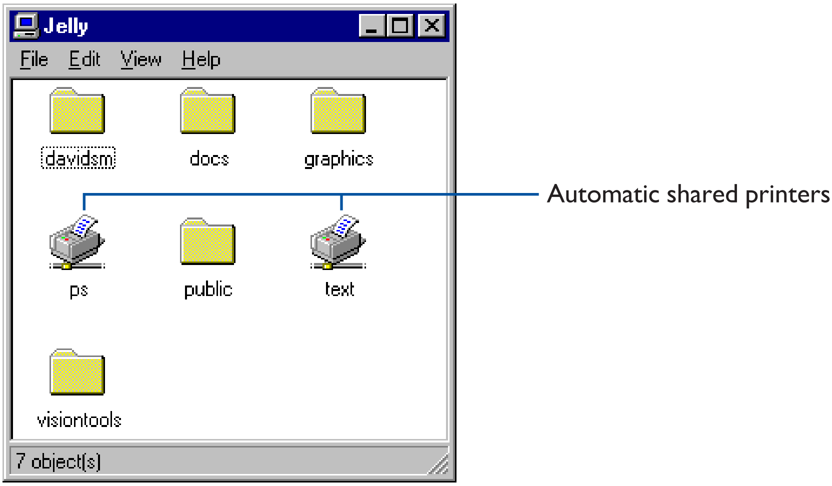
"Restarting the VisionFS server" and "Generating automatic shared printers", in the Help index.

"Using a shared printer", later in this chapter.

When the VisionFS server starts, it scans the UNIX host for printers, and updates your profile with information about each printer.

Note This means if you add a UNIX printer, you'll need to restart the VisionFS server for VisionFS to include the information in your profile.

In Windows, when you list the shares on a VisionFS server you see a shared printer for each UNIX printer (if automatic shared printers are enabled, which they are by default). The share names are the same as the UNIX printer names.



SEE ALSO

"Configuring automatic shares", later in this chapter.

The VisionFS server uses the settings from the master shared printer for automatic shared printers. However, you can override settings for individual shared printers, if you want.

As automatic shared printers are just "clones" of the master shared printer, the Profile Editor doesn't show them.

SEE ALSO

"Username mappings", "Controlling access" and "Passwords and authentication", later in this chapter.

"How to tell if an action will succeed", in Chapter 4, "Issues for Administrators".

WHO'S ALLOWED TO ACCESS A SHARED PRINTER?

By default, anyone who is authenticated (supplies a valid password for accessing the VisionFS server) is allowed to print to the shared printer, and all actions are performed using their UNIX username, taking into account any username mappings.

This means that when a user tries to add, list or remove jobs, the result would be the same as if they'd performed the action from the UNIX command prompt. If UNIX would deny permission, so will VisionFS.

Configuring automatic shares

How you configure automatic shares depends on whether you want to configure all automatic shares of a type, or just override the settings for one particular share.

Here's how the VisionFS server determines what settings to use for an automatic share:

- If there's a share of the appropriate type with that share name, VisionFS uses the settings from that share.
- Otherwise, VisionFS uses the settings from the master share of that type.

Remember that you can check Link next to an option, to link its setting to the master share. This means you can override as many or as few settings in a share as you want.

To configure every automatic share

- Change the appropriate master share's properties.

  In the Profile tree, click **(Printers)** or **(Users)**, click the Edit menu, then click Properties.

SEE ALSO

"Creating a new user share" and "Creating a new shared printer", in the Help index.

"Overriding automatic user shares" and "Using shared printers for custom output", in Chapter 3, "The Possibilities".

To override settings for one automatic share

- Create a new share of that type, and give it the same Share Name as the automatic share you want to configure. Then change any other settings you want, and update the server when you've finished.

Using a shared printer

See Also

Your Windows manual.

"Printing from the UNIX host", later in this chapter.

Before you can print from Windows to a VisionFS shared printer, you need to set up a network printer, just as you would to use a printer on another PC.

Once you've set up a network printer for the VisionFS shared printer, you can print to it from your Windows programs. Follow the particular method for each program.

Tip

To install a shared printer in Windows Explorer, double-click it.

To set up a network printer in Windows

1. Click the Start button, point to Settings, and then click Printers.
2. Double-click Add Printer.
3. Follow the instructions on your screen.

   When you're asked, choose Network Printer, and enter the name of the server and shared printer, in the form **\*server*\*printer*** (or choose to browse, if you prefer). You'll need to know the make and model of the printer.

Controlling access

In this section, you'll learn how to use the Profile Editor to customize exactly who can access a shared folder, shared printer or user share. We'll show you how to allow Guest access, and how to deny access.

Understanding access rights

Each share has an associated list of *access rights*. A particular access right describes:

- A UNIX username and group (after taking username mappings into account), for whom this access right applies.
- Whether this right applies if the user is *authenticated*—supplies a valid password for accessing the VisionFS server, according to the current authentication method.
- Whether this right applies if the user is a *guest*—doesn't have a password for accessing the server, for the current authentication method.
- The actions this user is allowed to perform in the share.
- The UNIX username and group to use when performing the allowed actions.

SEE ALSO

"Username mappings" and "Passwords and authentication", later in this chapter.

You set up the access rights for a share using the Access tab of the share's properties.

The access rights determine whether or not VisionFS tries to perform an action in a share. If a particular action is allowed, it doesn't necessarily mean the action will succeed: the UNIX permissions ultimately determine success or failure.

SEE ALSO

"How to tell if an action will succeed", in Chapter 4, "Issues for Administrators".

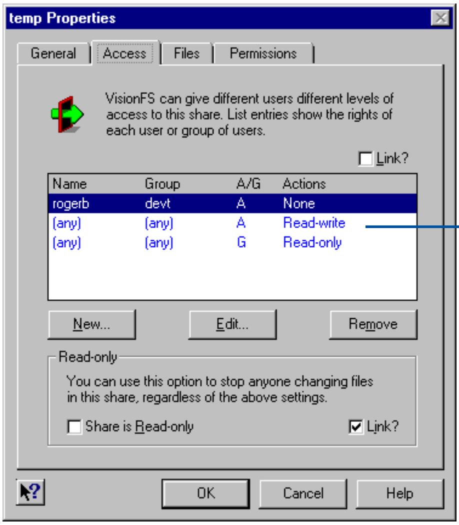
For example, if the access rights for a share grant UNIX user **kevin** full access, performing actions as user **rod**, but the UNIX permissions on the directory only allow read-only access for **rod**, then **kevin** won't be able to write to the directory.

Customizing access

You can customize access to individual shares, or use the master shares to customize access for automatically generated shares, new shares you create, and shares that link the Access settings.

To customize access to a share

1. In the Profile Editor, double-click the share or the master share you want to customize access for.
2. Click the Access tab to see the current access rights.



VisionFS can give different users different levels of access to this share. List entries show the rights of each user or group of users.

□ Link?

Name	Group	A/G	Actions
rogerb	devt	A	None
(any)	(any)	A	Read-write
(any)	(any)	G	Read-only

You can use this option to stop anyone changing files in this share, regardless of the above settings.

□ Share is Read-only ☑ Link?

Entries near the top of the list take precedence over those below. To move an entry, drag it up or down.

3. To add a new access right, click New.

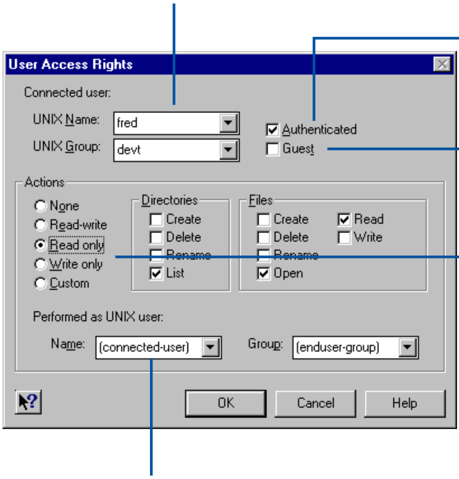
   To edit an existing access right, click it in the list, then click Edit.

   To remove an access right, click it in the list, then click Remove.

4 If you're adding or editing an access right, fill in the details in the User Access Rights dialog.

In the top section, set up the circumstances in which this access right should apply. Then in the bottom section, set up the actions allowed under those circumstances, and who the actions are to be performed as.

Click or type the user's UNIX username and group. Click **(any)** to mean any username or group.



User Access Rights

Connected user:

UNIX Name: fred

UNIX Group: devt

☑ Authenticated

□ Guest

Actions

○ None
○ Read-write
● Read only
○ Write only
○ Custom

Directories: □ Create □ Delete □ Rename ☑ List

Files: □ Create □ Delete □ Rename ☑ Open ☑ Read □ Write

Performed as UNIX user:

Name: (connected-user) Group: (enduser-group)

Check this to mean the right applies if the user has a password for accessing the server.

Check this to mean the right applies if the user doesn't have a password for accessing the server.

Click the type of actions the user will be allowed to perform. You can customize these with the Directories and Files boxes.

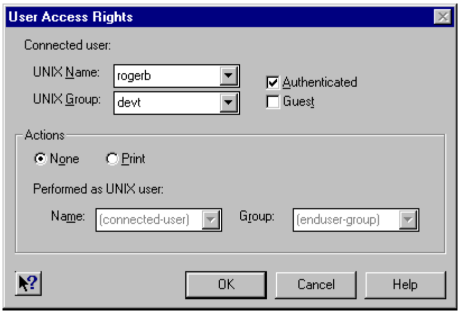
Click or type the UNIX username and group all actions will be performed as. Click **(connected-user)** and **(enduser-group)** to mean the user accessing the share.

TIPS

Check both Authenticated and Guest if you want the access right to apply whether or not the user has a password for the server.

In UNIX Name, click **(admin-user)** to mean any VisionFS Administrator.

The picture above shows the User Access Rights dialog for shared folders and user shares. For shared printers, the dialog looks like this:



User Access Rights

Connected user:

UNIX Name: rogerb

UNIX Group: devt

☑ Authenticated

□ Guest

Actions

● None ○ Print

Performed as UNIX user:

Name: (connected-user) Group: (enduser-group)

Ordering the access rights

The order of access rights in the list on the Access tab is important. When someone tries to use a share, the VisionFS server checks the details against the list. The first entry that matches determines the actions that user is allowed to perform. If no entry matches, the user is not allowed to access the server.

When you add or edit access rights, make sure the entry appears in the correct place in the list: entries for specific users should appear *before* entries for any user.

If an access right for any user appears before one for a specific user, the specific one will be ignored.

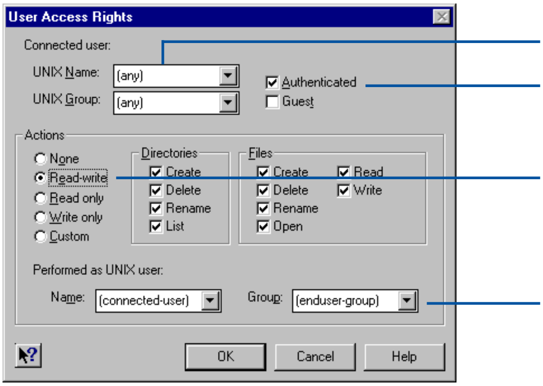
To move an access right

- Drag the entry up or down in the list.

Common types of access

The following sections give examples of common types of access you're likely to want to use.

Granting full access for authenticated users



User Access Rights

Connected user:

UNIX Name: (any)

UNIX Group: (any)

☑ Authenticated

☐ Guest

Actions

○ None
● Read-write
○ Read only
○ Write only
○ Custom

Directories: ☑ Create ☑ Delete ☑ Rename ☑ List

Files: ☑ Create ☑ Delete ☑ Rename ☑ Open ☑ Read ☑ Write

Performed as UNIX user:

Name: (connected-user) Group: (enduser-group)

Allow all users…

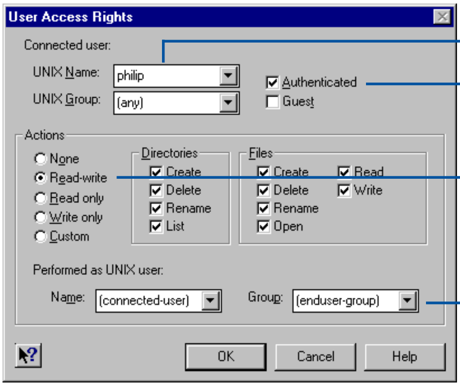
…who have a password…

…full access…

…as themselves.

Remember to put this access right below any access rights for particular named users.

Granting full access for one user



Connected user:

UNIX Name: philip

UNIX Group: (any)

☑ Authenticated
☐ Guest

Actions

○ None
● Read-write
○ Read only
○ Write only
○ Custom

Directories: ☑ Create ☑ Delete ☑ Rename ☑ List

Files: ☑ Create ☑ Delete ☑ Rename ☑ Open ☑ Read ☑ Write

Performed as UNIX user:

Name: (connected-user) Group: (enduser-group)

Allow this user…

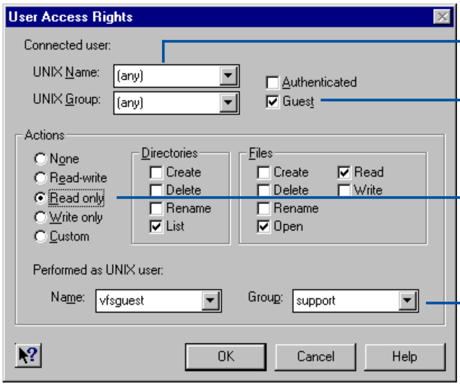
…who has a password…

…full access…

…as that user.

Remember to put this access right above any access rights for multiple users.

Allowing guest access



Connected user:

UNIX Name: (any)

UNIX Group: (any)

☐ Authenticated
☑ Guest

Actions

○ None
○ Read-write
● Read only
○ Write only
○ Custom

Directories: ☐ Create ☐ Delete ☐ Rename ☑ List

Files: ☐ Create ☐ Delete ☐ Rename ☑ Open ☑ Read ☐ Write

Performed as UNIX user:

Name: vfsguest Group: support

Allow all users…

…who don’t have a password…

…read-only access…

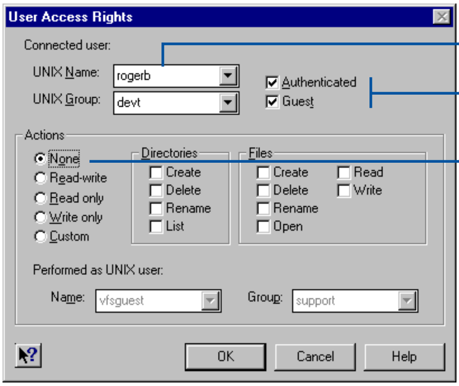
…as user “vfsguest”.

Actions on the UNIX host must always be performed by a valid UNIX user. For guest users—users without a password for accessing the VisionFS server—you must name a UNIX user to use for these actions.

You may want to set up a special UNIX account, called for example “vfsguest”, to use for guest users.

Remember to put this access right below any access rights for particular named users.

Denying access by one user



User Access Rights

Connected user:

UNIX Name: rogerb

UNIX Group: devt

☑ Authenticated

☑ Guest

Actions

● None
○ Read-write
○ Read only
○ Write only
○ Custom

Directories

□ Create
□ Delete
□ Rename
□ List

Files

□ Create
□ Delete
□ Rename
□ Open
□ Read
□ Write

Performed as UNIX user:

Name: vfsguest

Group: support

Allow this user…

…who might or might not have a password…

…no access.

In this case, you don’t need to decide who to perform actions as, as no actions are allowed.

Remember to put this access right above any access rights for multiple users.

Other share settings

You can configure many other settings for shared folders, user shares and shared printers. For full information, look in Help. For example, you can:

- Disable shares without deleting them, to take them out of action temporarily.
- Hide shares, so that users must know and type their names to access them.
- Show or hide UNIX symbolic links, to allow or restrict access to directories outside a share.
- Specify the UNIX file permissions for new files and directories.
- Make shares read-only, whatever the access rights for the share.
- Use Windows-style file locking to manage concurrent file access.
- Automatically convert between Windows and UNIX line endings.
- Make some files appear to have MS-DOS file attributes like “hidden” or “archive”.

See Also

You can get Help on an item by clicking the question mark button, then clicking the item.

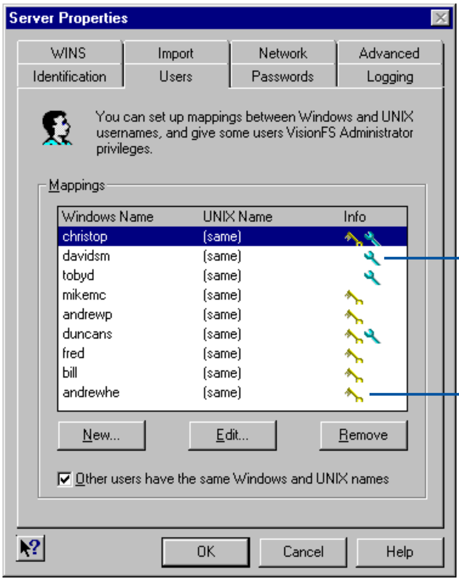
Username mappings

Users can have different usernames for Windows and the UNIX host. For example, your Windows username might be your full name, including spaces, while your UNIX username might be your initials. Alternatively, some or all users might have the same usernames on Windows and UNIX.

Username mappings let you use whichever username you want for Windows, while still allowing access to the UNIX host using your UNIX username.

To add a username mapping

1 In the Profile Editor, open Server properties and then click the Users tab.



You can set up mappings between Windows and UNIX usernames, and give some users VisionFS Administrator privileges.

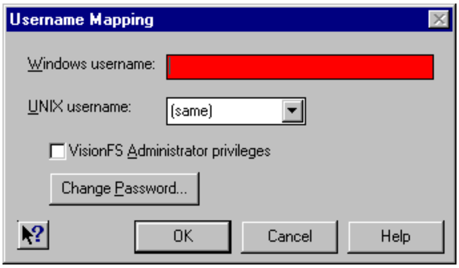
Windows Name	UNIX Name	Info
christop	(same)	🔑🔧
davidsm	(same)	🔧
tobyd	(same)	🔧
mikemc	(same)	🔑
andrewp	(same)	🔑
duncans	(same)	🔑🔧
fred	(same)	🔑
bill	(same)	🔑
andrewhe	(same)	🔑

☑ Other users have the same Windows and UNIX names

Means this user has VisionFS Administrator privileges on this server.

Means a VisionFS password is stored for this user on this server.

2 Click New. The Username Mapping dialog appears.



Windows username:

UNIX username: (same)

☐ VisionFS Administrator privileges

3 Type the Windows and UNIX usernames for this user.

4 Click OK.

5 Repeat steps 2 to 4 for each username mapping you want to add. When you've finished adding mappings, click OK, then click Update Server on the Profile menu. You'll need to restart the server for the new mappings to take effect.

SEE ALSO

"Controlling access", earlier in this chapter.

"Adding and removing VisionFS Administrators" and "Passwords and authentication", later in this chapter.

To allow users with identical Windows and UNIX usernames to access the VisionFS server if they don't have username mappings, make sure Other Users Have the Same Windows and UNIX Names is checked.

Users without username mappings or identical Windows and UNIX usernames (if the box is checked) are treated as users without passwords for accessing the VisionFS server: they will only be granted Guest access.

Mixed-case usernames

UNIX usernames are case-sensitive: they can include both upper-case and lower-case characters. However, Windows sends usernames to the VisionFS server in a case-insensitive way. VisionFS converts these to lower-case before trying to match a UNIX username.

This means if you have users with upper-case or mixed-case UNIX usernames, you must create mappings between the lower-case Windows usernames and the UNIX usernames.

Adding and removing VisionFS Administrators

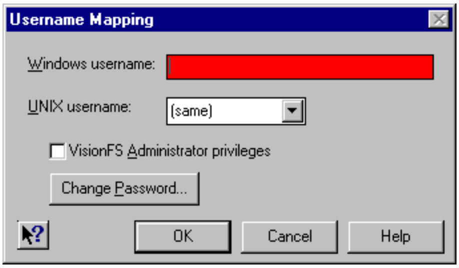
The Profile Editor lets you grant complete access to any files and directories on the UNIX host. For this reason, only a restricted set of users—those with VisionFS Administrator privileges—are allowed to run the Profile Editor. VisionFS Administrators are as powerful as the UNIX superuser.

SEE ALSO

"Username mappings", earlier in this chapter.

Remember that you need to log in to Windows with a VisionFS Administrator's username to run the Profile Editor, and all VisionFS Administrators must have valid UNIX accounts. Every VisionFS Administrator must have a username mapping, but the usernames on Windows and UNIX can be the same.

To add or remove a VisionFS Administrator


Username Mapping

Windows username:

UNIX username: (same)

□ VisionFS Administrator privileges

In the Username Mapping dialog for that user, check or clear the VisionFS Administrator Privileges box.

You'll need to restart the server for the change to take effect.

SEE ALSO

"License management", in Chapter 4, "Issues for Administrators".

A VisionFS server must have *at least* one VisionFS Administrator. If the server is in "Read-only" license mode, *only* one VisionFS Administrator is allowed; otherwise, there are no restrictions.

The Profile Editor will not let you remove the last VisionFS Administrator; in this case, the VisionFS Administrator Privileges box will gray out.

Passwords and authentication

Earlier in this chapter, we explained access rights: how to control which users can access a share. In particular, you can give different rights to users *with* passwords and users *without* passwords. Those without passwords are Guest users; those who supply valid passwords are Authenticated.

SEE ALSO

“Security and authentication”, in Chapter 4, “Issues for Administrators”.

VisionFS has three authentication methods, allowing for encrypted and unencrypted transmission of passwords (and using separate password databases), or the use of another server—which may be another VisionFS server, a Windows 2000 server, or a Windows NT server—to authenticate users.

The authentication methods are independent: a VisionFS server can use either its own VisionFS password database, the UNIX host’s password database, or use another server for authentication—but not any combination of these.

VisionFS (encrypted) passwords

To allow password encryption on the network, VisionFS can maintain a separate password database that uses the Windows encryption method. In VisionFS password mode, only users with entries in the VisionFS password database can be authenticated: all others have guest access only.

- VisionFS Administrators for a server can set, change and clear VisionFS passwords for any user, using the Profile Editor.
- In VisionFS password mode, users can modify their own VisionFS password using a separate Windows program (**password.exe**, in the same folder as the Profile Editor), or using a UNIX command-line utility on the host.
- The UNIX superuser can change anyone’s password using the command-line utility.

To make moving from unencrypted to encrypted passwords easier, VisionFS can accept UNIX passwords (unencrypted on the network), and automatically store them in the VisionFS password database using Windows-style encryption. This lets you populate the VisionFS password database with UNIX passwords until you’re ready to switch to VisionFS passwords only.

UNIX (unencrypted) passwords

With this authentication method, users type their UNIX password for the UNIX host running VisionFS, as if they are accessing the UNIX host from the console or another UNIX host. UNIX passwords are transmitted in “plain text”—unencrypted—on the network. Although both Windows and UNIX provide facilities for encrypting passwords, the encryption mechanisms used are incompatible.

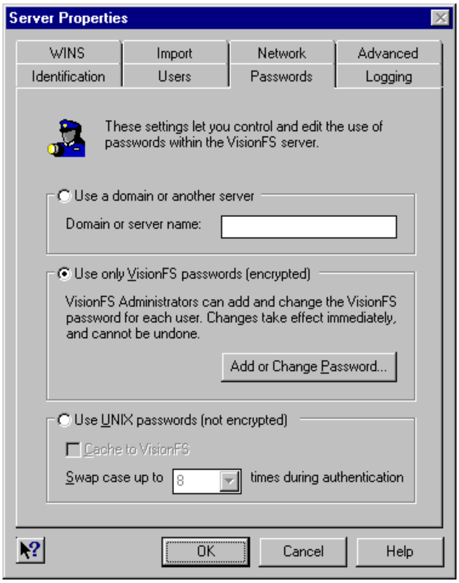
Using another server for authentication

If you specify that users are authenticated on another server, the password databases and username mappings on this VisionFS server are ignored for authentication purposes. The password databases used depend on the authentication server and its configuration:

- Another VisionFS server in UNIX password mode: users are authenticated by their UNIX passwords on that host, using that VisionFS server's username mappings.
- Another VisionFS server in VisionFS password mode: users are authenticated by their VisionFS passwords for that server.
- A Windows 2000 or Windows NT server: users are authenticated by their passwords for that server.

To change how VisionFS authenticates users

1 In the Profile Editor, open Server properties and then click the Passwords tab.



These settings let you control and edit the use of passwords within the VisionFS server.

○ Use a domain or another server

Domain or server name:

● Use only VisionFS passwords (encrypted)

VisionFS Administrators can add and change the VisionFS password for each user. Changes take effect immediately, and cannot be undone.

Add or Change Password...

○ Use UNIX passwords (not encrypted)

□ Cache to VisionFS

Swap case up to 8 times during authentication

TIP

You can get Help on an item by clicking the question mark button, then clicking the item.

2 Click the method you want to use for authenticating users. Use Help to find out more about the settings.

3 Click OK, then click Update Server on the Profile menu. You'll need to restart the server for any changes to take effect.

See Also

"The visionfs command", in Chapter 4, "Issues for Administrators"

To set or change your VisionFS password

- If you're a VisionFS Administrator, you can use the Profile Editor. In Server properties, click the Passwords tab, then click Add Or Change Passwords.
- If the server's using VisionFS passwords, anyone can use the **password.exe** program. In the VisionFS server's **visiontools** share, open the **visionfs** folder, then double-click **password.exe**.
- From the UNIX command line, anyone can change their VisionFS password using the **visionfs password** utility. The UNIX superuser can use this command to change anyone's password.

Printing from the UNIX host

SEE ALSO

"Using a shared printer", earlier in this chapter.

SEE ALSO

"The visionfs command", in Chapter 4, "Issues for Administrators".

A VisionFS shared printer lets Windows users print to a UNIX printer. It's also possible for UNIX users to print to *any* shared printer on the network—not just VisionFS shared printers—using a simple command-line utility. Using this utility you can send, list and cancel print jobs on any printer on the network.

Syntax

visionfs print //*server* [**--verbose**] [*credentials*]

visionfs print //*server*/*printer* [**--verbose**] [*credentials*]

visionfs print //*server*/*printer* **--pause**|**--resume**|**--delete** *job* [*credentials*]

visionfs print //*server*/*printer* *filename* [**--title** *title*] [*credentials*]

Description

In the first form, specifying just a server, this command gives information about the shared printers on that server.

The second form, specifying both server and printer, lets you get information about print jobs on that shared printer.

The third form, specifying a server, printer and print job, lets you manipulate that print job on the shared printer.

The final form lets you send a print job. The command returns the print job number. You can use a dash, "-", instead of a filename to print from standard input.

The available options are:

Option	Description
--delete *job*	Removes a print job from the print queue.
--pause *job*	Pauses printing of a print job.
--resume *job*	Resumes printing of a paused print job.
--title *title*	Specifies a title for a print job.
--verbose	If you specify just a server, displays information about the shared printers on that server, and lists the current print jobs. If you specify a printer, displays information about that shared printer and lists its current print jobs.

Note Each option is prefixed by two dashes, "--", not one.

By default, actions are performed as yourself and you're prompted for a password before the print job is sent. The *credentials* let you specify that actions should be performed as another user, and let you specify a password to prevent prompting. You can use one or both of these *credentials*:

Option	Description
--user*username*	Performs actions as the specified user
--password*pass*	Uses this password for authentication, without prompting

Installing a UNIX printer for Windows printing

Using other options to the **visionfs print** command, the UNIX superuser can set up UNIX printers that print to particular Windows printers. This allows users to print to Windows printers using standard **lp** commands from UNIX.

Syntax

visionfs print --install *unix_printer server share* [*winuser winpasswd*]

visionfs print --remove *unix_printer*

visionfs print --list

Description

The first form of the command installs a UNIX printer that prints to a Windows server. The second form removes one of these printers, and the third form displays complete details for all the printers you have installed.

Argument	Description
unix_printer	The name of a UNIX printer to add or remove.
server	The name of a Windows server sharing a printer on the network.
share	The name of a shared printer on *server* to print to.
winuser	When printing to Windows 2000 or Windows NT servers, the name of a user on the Windows server with printing privileges. If omitted, defaults to "vfsprint".
winpasswd	When printing to Windows 2000 or Windows NT, the password for *winuser* on the Windows server. When printing to other versions of Windows, the password (if any) for the shared printer. If omitted, defaults to "vfsprint".

The **visionfs print --install** command adds a UNIX printer named *unix_printer* that prints to \*server**share* on the network. The printer will convert UNIX-style line endings to DOS-style line-endings, unless the user specifies **-o raw** on the **lp** command line.

When printing to Windows 2000 and Windows NT, *winuser* and *winpasswd* together give the credentials for a Windows user with printing privileges. Users may override these credentials: for example, **lp -o user=rod -o passwd=hull** prints as user “rod”, who has the password “hull”.

When printing to Windows 95 and Windows 98:

- If the shared printer is not password-protected, then you may omit *winuser* and *winpasswd* when installing the printer.
- For password-protected printers, *winpasswd* specifies the password, and we suggest you set *winuser* to “vfsprint”. Users may specify their username with **lp -o user=*username*** if they wish.

In all cases, the Windows print queue window shows the name of the Windows user who’s printing.

Important The *winuser* and *winpasswd* are stored in plain text—not encrypted—in the file ***vision_dir*/etc/vfsprinters**. This file must be world-readable to allow printing to work. For security reasons we strongly recommend that you create a special user account, for example “vfsprint”, on Windows 2000 or Windows NT systems you print to in this way, and ensure this user has printing privileges only.

When you first install a printer using **visionfs print --install**, a printer interface model file **visionfs** is added in your UNIX system’s usual location. The same file is used no matter how many printers you install.

Example

A Windows 2000 server **meringue** shares a printer named **color**. If the UNIX superuser types this:

```
visionfs print --install salesprinter meringue color
```

Then any UNIX user may print the file **report.ps** to **meringue****color** using this command:

```
lp -d salesprinter report.ps
```

The Windows 2000 server **meringue** must have a user account “vfsprint”, with password “vfsprint”, and that account must have printing privileges, for printing to succeed. Alternatively, the user may supply different credentials, for example:

```
lp -d salesprinter -o user=rod -o passwd=hull report.ps
```

The Possibilities 3

Look in this chapter when you're ready to examine the world of possibilities offered by VisionFS.

You'll discover just a few of the ways in which you can take advantage of the flexibility of the Profile Editor and server, such as WINS, Internet workgroups, and overriding automatic shares.

Contents

WINS

In this section we'll describe WINS, which brings the benefits of intranet-wide and Internet-wide naming to your network. We'll also show you some alternatives to WINS, which might be more appropriate for your circumstances.

Overview

When a computer wants to access a remote server or application, the computer must have a way to identify and contact the service. Service identification is commonly referred to as *naming*.

Windows uses NetBIOS names to identify applications and servers on a network. The names you see in workgroups, such as PC and VisionFS server names, are NetBIOS names. These names have a number of limitations:

- They aren't hierarchical—unlike DNS names, which are. Although workgroups let you organize computers in groups, the workgroup name isn't part of the computer's name—you don't need to know which workgroup a computer is in to access it.
- NetBIOS names use broadcasts, which limits them to a single subnet.

For intranets—which typically span several subnets—and the world-wide Internet, a more sophisticated solution is needed for naming. As one way to solve this problem, Microsoft developed WINS: Windows Internet Naming Services.

About WINS

WINS is a set of services for storing and retrieving information about the NetBIOS names and IP addresses of computers on a network.

- A *WINS server* is a computer that provides these services.
- A *WINS client* is a computer that uses the services of a WINS server.

WINS clients register their NetBIOS names and IP addresses with one or more WINS servers. A WINS server looks after this information and keeps it up-to-date. When a WINS client wants to locate a resource on the network, it sends the resource's NetBIOS name to the WINS server. The WINS server returns the IP address of the resource to the WINS client.

See Also

"Installing Microsoft TCP/IP", in Chapter 4, "Issues for Administrators".

A VisionFS server can be both a WINS client and a WINS server. Windows PCs can also be WINS clients, if they use a suitable TCP/IP stack, such as Microsoft TCP/IP. Windows 2000 and Windows NT servers can also be WINS servers.

Using WINS to register VisionFS server names

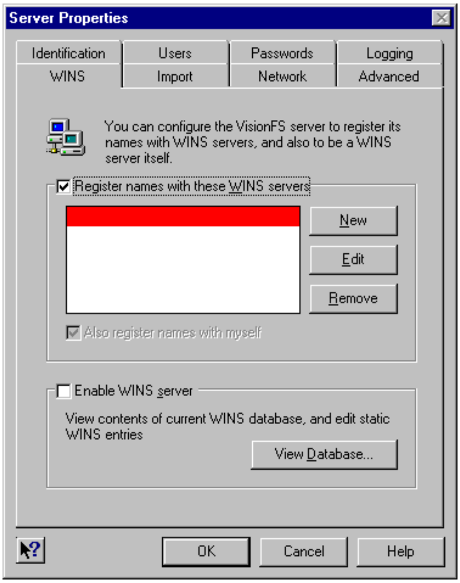
If you don't use WINS, VisionFS servers advertise their names using periodic network broadcasts. Similarly, computers use network broadcasts to locate the VisionFS server.

You can reduce network traffic, and make access to the server more reliable, by setting up VisionFS as a WINS client. When VisionFS registers its names, it sends them to one or more WINS servers; when other computers want to locate the VisionFS server, they can ask one of these WINS servers for its IP address.

VisionFS can register its names with as many WINS servers as you like. The more WINS servers you specify, the more robust your network's WINS operations will be.

To register the VisionFS server's names with a WINS server

1 Open Server properties, and click the WINS tab.



You can configure the VisionFS server to register its names with WINS servers, and also to be a WINS server itself.

☑ Register names with these WINS servers

☑ Also register names with myself

□ Enable WINS server

View contents of current WINS database, and edit static WINS entries

2 Make sure Register Names With These WINS Servers is checked.

3 Click New. In the red box, type the DNS name or IP address of a WINS server you want VisionFS to register its names with.

Using VisionFS as a WINS server

You can set up VisionFS as a WINS server, to enjoy the benefits of WINS on your network even if you don't have any Windows 2000 or Windows NT servers.

However, if you want to use WINS on your network, you should use WINS servers of the same type: either all VisionFS servers, or a mixture of Windows 2000 and Windows NT servers. WINS servers of the same type can share, or *replicate*, their name information for increased redundancy and reliability. If you mix VisionFS and Windows WINS servers, they will not replicate names.

See Also

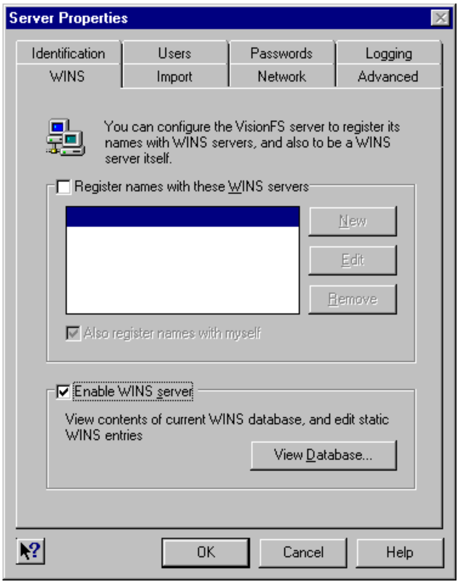
"Internet workgroups", later in this chapter.

We recommend you use VisionFS servers for WINS, to give the extra benefits of Internet workgroups.

Note If your VisionFS server is a WINS server, you should make sure VisionFS registers its server names with itself.

To use VisionFS as a WINS server

1 Open Server properties, and click the WINS tab.



You can configure the VisionFS server to register its names with WINS servers, and also to be a WINS server itself.

□ Register names with these WINS servers

☑ Also register names with myself

☑ Enable WINS server

View contents of current WINS database, and edit static WINS entries

2 Make sure Enable WINS Server is checked.

WINS database

When a WINS client registers its names or requests name information from a WINS server, the server stores or retrieves the appropriate information from the WINS database and sends it to the client.

SEE ALSO

"WINS database" and "Static entry, adding", in the Help index.

You can add static entries to the WINS database to store information about computers that do not register their details with the WINS server, for example computers that can't be WINS clients. When Enable WINS Server is checked, you can click View Database to see the WINS database.

Each entry in the WINS database stores:

- A name, which includes a special code indicating the type of service the owner of the name provides.
- A type, which can be "unique" or "group", for the name.
- A node, indicating how the owner of that name locates computers on the network.
- An IP address for the owner of the name.
- An expiry time, indicating when the owner must re-register the name. Static entries you add to the WINS database don't expire, but you can remove them.

Alternatives to WINS

If you don't want to use WINS, there are a number of solutions for network-wide naming, which are appropriate in different circumstances.

Use DNS for NetBIOS name resolution

The first alternative is to tell Windows to use DNS for NetBIOS name resolution. This option lets you supply a list of suffixes which Windows appends to a NetBIOS name to try to form a DNS name.

For instance, if you're looking for a computer called **jelly**, and you've supplied the suffixes **sales.indigo-insurance.com**, **research.indigo-insurance.com** and **marketing.indigo-insurance.com**, Windows will try to locate computers with the DNS names **jelly.sales.indigo-insurance.com**, **jelly.research.indigo-insurance.com**, and **jelly.marketing.indigo-insurance.com**.

To tell Windows to use DNS for NetBIOS name resolution, and supply a list of DNS name suffixes, follow the instructions for your version of Windows:

On...	Do this...
Windows 95 or 98	Display your TCP/IP protocol settings. On the DNS tab, add your DNS name suffixes. You can check that NetBIOS name resolution uses DNS by running the **winipcfg** program.
Windows NT 4	Display your TCP/IP protocol settings. On the WINS Address tab, make sure Enable DNS for Windows Resolution is checked. On the DNS tab, add your DNS name suffixes.
Windows 2000	Display your Internet Protocol (TCP/IP) settings, and click Advanced. On the DNS tab, choose the appropriate option.

This solution is best if you're using DNS and have unique computer names in the domains in which you are searching.

Use multiple server names

SEE ALSO

"CIFS Bridge", in Chapter 1, "The Basics".

The second alternative to WINS is to use multiple names for each server, and set up some of those names as CIFS Bridges: names which point to another computer anywhere on the intranet or Internet, but which appear in workgroups on your local network.

For example, if you have three VisionFS servers on three separate subnets—in London, New York and Berlin, called **london**, **newyork** and **berlin**—each server would have three names.

The server in London would need a local name for itself, and use two CIFS Bridges for the names **newyork** and **berlin**, pointing to the servers in New York and Berlin respectively. Similarly, the servers in New York and Berlin would each have CIFS Bridges for the other two servers.

This solution is best for sites where there are few remote servers but many clients, since all administration is done on the servers.

Use the LMHOSTS file

The final WINS alternative is to edit the **LMHOSTS** file, which contains instructions about how to map NetBIOS names to remote IP addresses. If the **LMHOSTS** file doesn't exist, copy **LMHOSTS.SAM** to **LMHOSTS**.

In Windows 95 and Windows 98, you'll find both files in the Windows directory. In Windows 2000 and Windows NT, you'll find them in the **system32****drivers****etc** subdirectory of the Windows directory.

Once you've edited the **LMHOSTS** file, you need to instruct Windows to use the file. How you do this depends on your version of Windows:

On…	Do this…
Windows 95 or 98	Nothing. LMHOSTS lookup happens automatically.
Windows 2000 or NT	Display your TCP/IP protocol settings and make sure Enable LMHOSTS Lookup is checked. Click Import LMHOSTS to locate the LMHOSTS file.

This solution is best for sites with few PC clients needing access to few remote servers, because you need to configure all clients.

Internet workgroups

Windows workgroups aren't normally visible between subnets. Although you can see all the computers on your subnet, you can't see any computers on any other subnets.

Internet workgroups let you see and access computers on different subnets, or even on different networks, as if they were local.

To do this, you need at least one VisionFS server on each subnet. On each server, you simply enable Internet workgroups and specify the names of the servers on the other subnets. You can also import WINS information from the other servers, if you want.

Note Information is "pulled" regularly from the other servers. You must configure a VisionFS server on every subnet if you want to exchange information across all subnets.

See Also

"VisionFS and firewalls" and "Filtering unwanted connections", in Chapter 4, "Issues for Administrators".

Internet workgroups don't compromise security: your network's firewall should prevent your workgroups appearing where you don't want them to. In addition, computers which are denied access to the VisionFS server by a filter will be unable to make use of Internet workgroups.

We recommend you use VisionFS servers on each subnet as WINS servers, and import WINS information as well as Internet workgroups. You should also make sure all PCs on each subnet are using the appropriate VisionFS server for WINS. This will increase reliability and robustness.

Tip

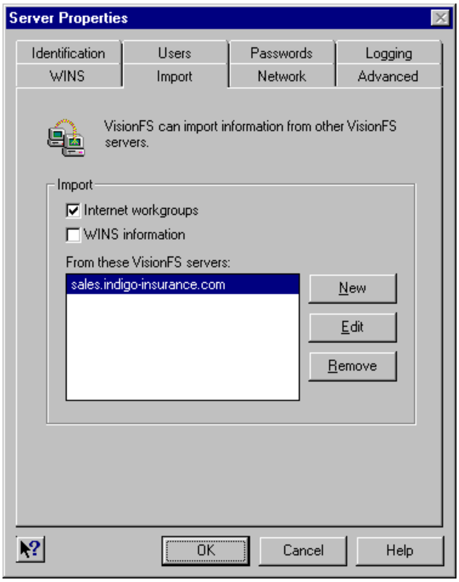
Use more than one VisionFS server on each subnet for increased reliability.

To set up Internet workgroups

- On each subnet, set up a VisionFS server to import workgroups from VisionFS servers on all other subnets you're interested in.

To import workgroups from a VisionFS server on another subnet

1 In the Profile Editor, open Server properties and then click the Import tab.



VisionFS can import information from other VisionFS servers.

Import

☑ Internet workgroups

☐ WINS information

From these VisionFS servers:

sales.indigo-insurance.com

2 Make sure Internet Workgroups is checked.

3 Click New. In the red box, type the DNS name or IP address of the VisionFS server on the other subnet.

TIP

Check WINS Information to replicate WINS information from the servers.

Network logon services

See Also

"Network logon services overview", in the Help index.

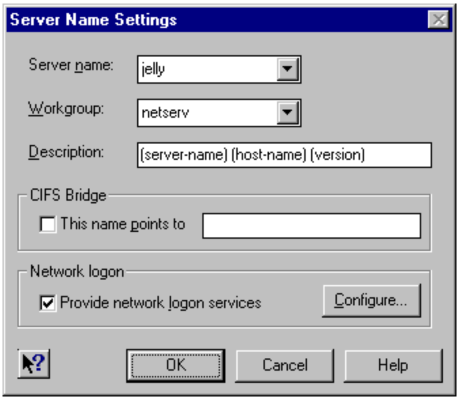
Network logon services let you configure what happens when Windows users log onto the network. When you enable network logon services, users' Windows profiles (personal Windows settings, such as desktop icons and program groups) are stored centrally, on the VisionFS server. A VisionFS server can use one of its server names to provide network logon services to all the Windows PCs in a particular workgroup.

Once you've configured the VisionFS server and users' PCs correctly, then whenever a user logs onto the network from a Windows PC, Windows retrieves their profile and user environment information from the VisionFS server. Retrieving profiles from a central location like this is called *roaming profiles*. Roaming profiles let users log onto different Windows PCs, yet always see the same, consistent Windows environment—the same icons on their desktops, the same applications started, and the same drive letters mapped.

To enable network logon services

1 In the Profile Editor, open Server properties, then click the Identification tab.

2 Click New to add a new server name (or edit an existing server name).



Server name: jelly

Workgroup: netserv

Description: (server-name) (host-name) (version)

CIFS Bridge

☐ This name points to

Network logon

☑ Provide network logon services

3 In Workgroup, type the name of the workgroup the VisionFS server will provide network logon services for.

4 Make sure Provide Network Logon Services is checked.

See Also

"Passwords and authentication", in Chapter 2, "Beyond the basics".

Enabling network logon services means the VisionFS server can provide logon services to users—just like a Windows 2000 or Windows NT server.

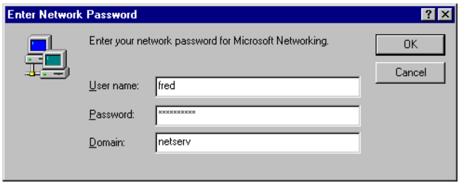
Note Users must be authenticated by encrypted passwords (either on this server or another server) to use network logon services.

Before a user can make use of roaming profiles and network logon services, you’ll need to configure their Windows PCs. You should do so in exactly the same way as if a Windows 2000 or Windows NT server were providing network logon services. Refer to your Windows documentation for more information. You’ll need to do at least the following:

- Place the Windows PCs in the workgroup that the VisionFS server is providing network logon services for (the workgroup **netserv**, in the picture above).
- Configure the Windows PCs to log onto a Windows domain. For the domain to log onto, use the same workgroup name as above (**netserv**).

Note The VisionFS server doesn’t create a real Windows domain for users to log onto—it just emulates one.

Once you’ve enabled network logon services, users can log onto the network using the VisionFS server’s domain name to use network logon services:



Enter your network password for Microsoft Networking.

User name: fred

Password: **********

Domain: netserv

When a user logs onto the network in this way:

1 The VisionFS server runs a UNIX script on the UNIX host.

The default UNIX script, **netlogon.sh**, ensures that the user’s User Profile Path (see below) exists, creating it if necessary.

2 Windows retrieves the user’s Windows profile from the VisionFS server.

When a user logs onto the network for the first time, Windows copies their Windows profile onto the VisionFS server.

3 Windows runs an MS-DOS batch script.

You can use this batch script to map drive letters to commonly used shares, start applications or set environment variables, for example.

4 Windows configures the user’s home directory.

A user’s home directory setting is used as their starting directory when they start an MS-DOS Command Prompt from Windows.

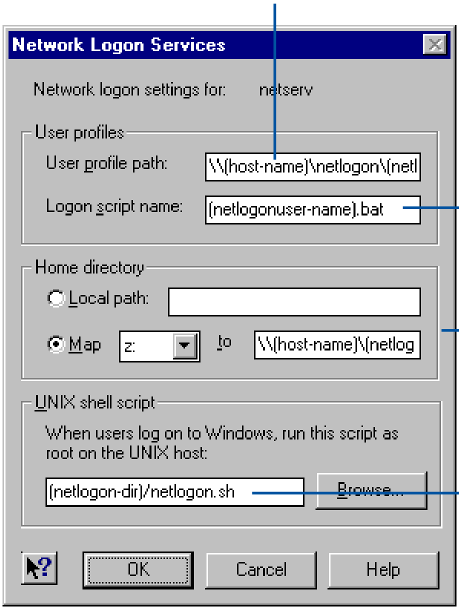
To configure network logon services

- On the Server Name Settings dialog, click Configure. You'll see the Network Logon Services dialog.

SEE ALSO

"Network Logon Services dialog", in the Help index.

Type a UNC pathname which specifies the location of users' Windows profiles on the UNIX host. You probably won't need to change this setting.



Network Logon Services

Network logon settings for: netserv

User profiles

User profile path: \\(host-name)\netlogon\(netl

Logon script name: (netlogonuser-name).bat

Home directory

○ Local path:

● Map z: to \\(host-name)\(netlog

UNIX shell script

When users log on to Windows, run this script as root on the UNIX host:

(netlogon-dir)/netlogon.sh

Type the path and filename of the MS-DOS batch file that Windows runs.

Specify either a local path, or a drive letter to map to a network resource for users' home directories.

Type the path and filename of the UNIX script that VisionFS runs when users log onto the network.

SEE ALSO

"Placeholders" in the Help index.

"Using placeholders", later in this chapter.

The following placeholders are available to help you configure network logon services:

- **(netlogon-dir)** is replaced with the **netlogon** subdirectory of the SCO Vision2K shared directory (**/usr/local/vision**, by default).
- **(netlogonuser-name)** is replaced with the username a user types when they log onto the network.
- **(host-name)** is replaced with the VisionFS server's UNIX hostname.

SCO VisionFS SMB Client

SCO VisionFS SMB Client lets users access Windows files and folders from UNIX, using standard UNIX commands. Users can access shared folders on Windows 95, Windows 98, Windows 2000 and Windows NT PCs, as well as shared folders on VisionFS servers. Users can't access Windows for Workgroups PCs with SCO VisionFS SMB Client.

SCO VisionFS SMB Client users can only access the shared folders that they would be able to access from another Windows PC.

Note Before you can set up the SCO VisionFS SMB Client, you'll need an NFS server and client installed on the UNIX host, and at least one NFS exported directory.

To set up SCOVisionFS SMB Client

1. Log in as root on the UNIX host.
2. Type the following, replacing ***vision_dir*** with the name of the Vision2K shared directory, by default **/usr/local/vision**:

   ***vision_dir*/bin/visionfs clientadmin --setup**
3. Follow the instructions on your screen.

Passwords and SCO VisionFS SMB Client

SEE ALSO

"SCO VisionFS SMB Client, and passwords", in the Help index.

Just like connecting to shared folders from a PC, SCO VisionFS SMB Client users must be authenticated before they can access shared folders from UNIX. SCO VisionFS SMB Client must have a valid username and password for each resource a user wants to access.

Users can tell SCO VisionFS SMB Client their Windows usernames and passwords for different computers and shares by running the SCO VisionFS SMB Client Password wizard. SCO VisionFS SMB Client encrypts all the passwords it's told about, before storing them on the UNIX host.

Note Each user who wants to use SCO VisionFS SMB Client should run this command. Alternatively, Administrators can use the **visionfs client** command's **--password** option to configure users' usernames and passwords for them.

To configure your usernames and passwords

1. Log into the UNIX host.
2. Type the following, replacing ***vision_dir*** with the name of the Vision2K shared directory, by default **/usr/local/vision**:

   ***vision_dir*/bin/visionfs client --wizard**
3. Follow the instructions on your screen.

The passwords users configure here are only used by SCO VisionFS SMB Client. This command doesn't change VisionFS, UNIX or Windows—it just tells SCO VisionFS SMB Client about users' Windows usernames and passwords.

Users and Administrators can configure the following types of username and password:

- A username and password for a particular share. These details are only used when the user accesses that particular share.
- A username and password for a particular computer. These details are used whenever the user accesses a share on the specified computer *except when* a username and password for that particular share has been specified.
- A default username and password. These details are used when a user accesses a share on a computer that no other username and password applies to.

For example, if a user tries to access a shared folder **reports** on a computer **rome**, SCO VisionFS SMB Client looks for authentication information in the following order:

- A username and password for the shared folder **reports** on the computer **rome**.
- A username and password for the computer **rome**.
- A default username and password.

SCO VisionFS SMB Client will always use the most specific username and password available when authenticating users.

If an Administrator has used the **visionfs client** command to configure usernames and passwords for a user, the username and password specified by the Administrator takes precedence over user-supplied information*unless* the user has supplied more specific information.

For example, the user Fred wants to access the **reports** share on the computer **rome**. Fred runs the SCO VisionFS SMB Client Password wizard and specifies his username and password for the **reports** share on **rome**.

- If an Administrator configures Fred's username and password for the **reports** share on **rome**, these Administrator-specified details would be used when Fred accesses the share. This is because the details specified by Fred and the Administrator are equally specific, and Administrator-specified information takes precedence.
- If an Administrator configures Fred's username and password just for the computer **rome** (not for any particular share), the details specified by Fred would be used. This is because the information specified by Fred is more specific—it applies to a particular share, rather than just a computer.

Using SCO VisionFS SMB Client

When you set up SCO VisionFS SMB Client, Setup creates an empty directory at the mount point you specified (**/smb**, by default). This directory is the starting point for all users accessing Windows files and folders from UNIX.

Once a user's usernames and passwords have been configured, SCO VisionFS SMB Client creates a subdirectory of the mount directory with the same name as their UNIX username. Users access shared folders by using standard UNIX commands in their own subdirectory of the mount point.

For example, the UNIX user **fred** can list the shared folders available on a PC **moscow** by typing the following command:

```
ls /smb/fred/moscow
```

The same user could use the **vi** text editing program to edit a file called **99report.txt** in a shared folder **reports** using the following UNIX command:

```
vi /smb/fred/moscow/reports/99report.txt
```

When a user accesses remote filesystems in this way, SCO VisionFS SMB Client creates the appropriate directory (**moscow**, in the above example) in their user directory, and creates a connection to the remote computer.

The connection itself is only held for a relatively short time—it's disconnected after a few minutes. However, the user will continue to see the directory in their user directory.

SEE ALSO

"visionfs command, client option", in the Help index.

The **visionfs client** command lets you see which connections are in use and which have been disconnected. It also lets you disconnect connections and flush disconnected directory entries so that users no longer see them.

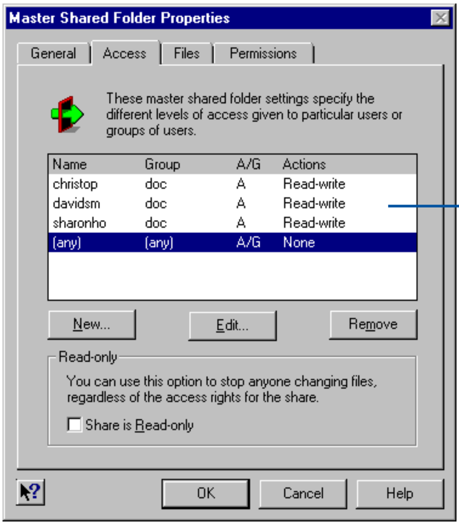
Note If a user can't access a share (perhaps because they haven't specified a valid username or password), they won't see an error message. The UNIX command appears to complete successfully, but doesn't display the expected output. If this happens, an appropriate error message will be added to the log files **vfsdata/clerr.log** (in the Vision2K shared directory) and **.vfserrors** (in the user's home directory).

Using links effectively

Links and master shares let you change settings in lots of shares at once. In fact, you'll probably want to leave most of your settings linked to the appropriate master share, and only change the settings that make the share different from the master.

If master shares reflect the most common settings for your site, making across-the-board changes is as simple as editing just the master shares.

For example, consider a VisionFS server dedicated to a particular team. In this case, a VisionFS Administrator should set up access rights for the team in the master shared folder, as shown in the picture below.



These master shared folder settings specify the different levels of access given to particular users or groups of users.

Name	Group	A/G	Actions
christop	doc	A	Read-write
davidsm	doc	A	Read-write
sharonho	doc	A	Read-write
(any)	(any)	A/G	None

Read-only

You can use this option to stop anyone changing files, regardless of the access rights for the share.

☐ Share is Read-only

The master shared folder's access rights.

In this way, when someone joins or leaves the team, a VisionFS Administrator just adds or removes an access right in the master shared folder, and all linked shares are automatically updated.

Also, when a VisionFS Administrator adds a new share, it automatically has the correct access rights for the team.

As a general rule, treat the shares you create as a collection of differences from the master shares, and use links as a form of "inheritance".

Overriding automatic user shares

Automatic user shares use the settings from the master user share, unless you've created a specific user share.

In other words, creating user shares for specific users lets you override the settings for those users. You only need to override the settings you want to—all the others retain their links to the master share.

So if you want to change just one setting for a particular user, it's as simple as creating a user share for that user, and changing that one setting.

The following sections show a few of the overrides you might want to use.

Show symbolic links for an advanced user

See Also

"PC and UNIX file differences", in Chapter 4, "Issues for Administrators".

Symbolic links could lead anywhere on the UNIX host. You can easily hide symbolic links in users' home directories, by clearing the Let Users Follow Symbolic Links box in the master user share. In this way, you can be sure that all automatically generated user shares will only grant access to subdirectories of home directories.

However, you can trust your advanced users—yourself included! You don't mind if those users can see symbolic links.

To give this custom behavior to your advanced users, all you need to do is create a user share for each one, and check the Let Users Follow Symbolic Links box.

Give a user access to another directory

If a particular user wants their user share to access a directory other than their home directory on the UNIX host, create a user share for that user and change the UNIX Directory setting.

See Also

"Placeholders" in the Help index.

"Using placeholders", later in this chapter.

By default, UNIX Directory is set to User's Home Directory. Next to Custom you'll see this setting shown another way, as **~(user-name)**. This uses the UNIX "~" notation for indicating home directories, together with the Profile Editor's placeholder **(user-name)** meaning the user the share's for.

To change the directory, click Custom, then type the directory. You can keep or remove the placeholder if you like.

Customize access to home directories

The most common ways to customize access involve granting read-only access, or denying access completely. You can use access rights to do these, but quicker—and easily reversible—ways exist:

- Deny access by clearing the Active option on the General tab.
- Give read-only access by checking the Read-only option on the Access tab.

See Also

You can get Help on an item by clicking the question mark button, then clicking the item.

Using placeholders

SEE ALSO

"Placeholders" in the Help index.

Placeholders give an extra level of control over some settings. For example, you can use **(share-name)** to stand for the name of the share.

Using placeholders in master shares means that some settings in automatically generated shares can include share-dependent information, like the name of the share. In this way automatic user shares give access to the user's home directory, using the placeholder **(user-name)** in the master user share's UNIX Directory setting.

Give all users a special Windows home directory

Normally, user shares give access to UNIX home directories. You might want to keep UNIX home directories safe, and set up a special "Windows home directory" for each user to keep their Windows files in. Placeholders let you do this easily.

In the master user share's properties, click Custom for the UNIX Directory. Then change the directory shown, preserving the placeholder **(user-name)** in some way.

For example, to keep UNIX home directories and "Windows home directories" independent, change the setting to something like/**winhome/(user-name)**. Then create directories under /**winhome** on your UNIX host for each user, and give them appropriate UNIX permissions and ownership—usually, exactly the same as the original UNIX home directories.

Alternatively, you could change the setting to **~(user-name)/windows** and create a directory called **windows** (with the right permissions) in every user's UNIX home directory.

Using shared printers for custom output

By default, VisionFS creates shared printers automatically for the printers on your UNIX host. When users list the shares on the VisionFS server, they'll see a shared printer for every system printer, with the same share name as the system printer in each case.

If you want, you can add shared printers that use the system printers in different ways. The details of how you do this will vary depending on your particular circumstances—for example, your flavor of UNIX system, and whether the printer is directly or indirectly connected to the UNIX host.

In general, you just need to change the command used to print the job. You could add a flag to the existing command, or use a different command entirely—preprocessing the print job using a separate program. Check your UNIX documentation for the different types of output you can generate.

SEE ALSO

"Placeholders, printers" in the Help index.

Some special printing placeholders are defined so you can include useful information in the commands, for example the name of the user who submitted the job.

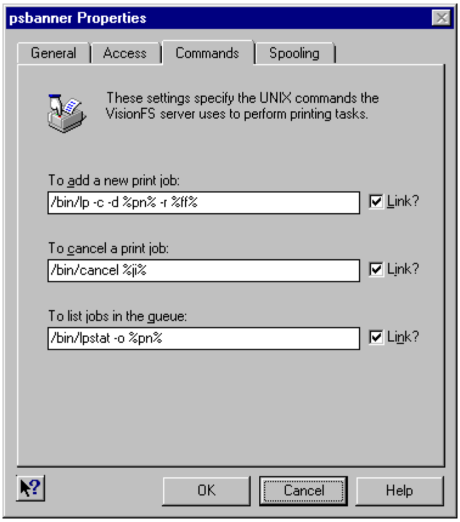
Using this technique, you can set up shared printers that:

- Print a banner page before every job.
- Print a header on each page.
- Print multiple pages of output on a single sheet of paper.
- Print with landscape instead of portrait orientation.

Remember that you can set up different shared printers with different access rights. For example, you could reserve some special output only for particular users, or restrict access to a color printer.

To customize printing commands

1 In the Profile Editor, double-click the shared printer you want to customize printing commands for. To customize every automatic shared printer, double-click **(Printers)**.



psbanner Properties

These settings specify the UNIX commands the VisionFS server uses to perform printing tasks.

To add a new print job: /bin/lp -c -d %pn% -r %ff% ☑ Link?

To cancel a print job: /bin/cancel %ji% ☑ Link?

To list jobs in the queue: /bin/lpstat -o %pn% ☑ Link?

2 Click the Commands tab.

3 Make any changes you want. Use Help to find out about the special printing placeholders you can use.

4 Click OK, then click Update Server on the Profile menu.

See Also

You can also get Help on an item by clicking the question mark button, then clicking the item.

Allowing multiple NetBIOS applications

Technically, VisionFS is a NetBIOS application that runs over TCP/IP—sometimes called an *NBT application*. When you look in your Network Neighborhood or use the Connect Network Drive dialog, the names you see and use are NetBIOS names.

If you want to use only a single NBT application on the UNIX host—VisionFS—then it works, straight out of the box. You don't need to make any changes at all.

However, you might want to run more than one NBT application on the host. You can set this up using the Profile Editor.

About NBT applications

Each NBT application:

- Has at least one name, to identify the application.
- Listens for connections on a UNIX TCP port.

An NBT application uses network broadcasts or WINS to announce, or *advertise*, its names. The naming doesn't need to be handled by the same program that listens for connections; they're independent. This means you could have an entirely separate program to advertise the names used by all NBT applications on the UNIX host. In fact, if you want to use more than one NBT application on the host, *only one* of the applications can advertise the names, as explained below.

With VisionFS, the naming process is part of, but distinct from, the rest of the server. The Profile Editor lets you name the server, and turn off naming altogether. It also lets you set up which TCP port the server listens to.

Primary and secondary NBT applications

If you have more than one NBT application on the UNIX host, then one of them must advertise all the names used for all NBT applications on the host. This is because only one application is allowed to use the appropriate naming ports, UDP ports 137 and 138 (different to the TCP port used to listen for connections).

Similarly, there's a standard port used for NBT connections, TCP port 139. Only one application can listen on this port. This application must make sure that connections intended for the other applications are rerouted, or *redirected* to the port each is listening on. This redirection happens only once, when the connection is first made.

The NBT application that advertises the names and handles redirections is called the *primary* application. All others are called *secondary* applications.

In summary:

- The primary NBT application advertises all names, and handles all redirections to secondary NBT applications, using the appropriate UDP and TCP ports.
- The secondary NBT applications don't advertise any names, and listen for connections on custom TCP ports, relying on the primary NBT application to redirect connections intended for them.

By default VisionFS tries to run as the primary NBT application, as it's highly likely VisionFS will be the only NBT application on the host. If another NBT application is already running as the primary, the VisionFS server won't start and will generate an error message explaining the problem.

SEE ALSO

"Other file and printer sharing or NBT applications", in Chapter 4, "Issues for Administrators".

Working with multiple NBT applications

The first task is to decide which NBT application is to be the primary, and which will be secondaries. You can configure VisionFS to be either; check the documentation for your other NBT applications to see if they prefer to be the primary or a secondary.

Once you've decided, make sure your users know the NBT applications will be out of action for a time—you'll need to stop VisionFS and the other NBT applications temporarily.

To find out whether a VisionFS server is running as the primary or a secondary application, start its Profile Editor and check the TCP Port number on the Advanced tab of Server properties: if it's 139, the server's the primary application; otherwise, it's a secondary.

To set up VisionFS as the primary NBT application

1. If VisionFS is already running as a secondary application, use the Profile Editor to change the TCP port it listens on to the default port, 139. You change the port in Server properties, on the Advanced tab. Update the server, but *don't* restart it.
2. Find out the port numbers used by all secondary applications, and make sure any existing primary application is set up to run as a secondary application.

Each secondary application must use a unique port number. Check the documentation for an application to find out how to configure the port number. Remember that port numbers less than 1024 are reserved for applications started as root.

3 Stop the VisionFS server if it is already running, then start it again. You can do this from the UNIX command line (remember to close the Profile Editor if it's running), or in the Profile Editor by clicking Restart Server on the Profile menu.

The server will now run as the primary application.

4 Use the Profile Editor to advertise the names used by each secondary application. You list all the names on the Identification tab of Server properties.

5 On the Advanced tab of Server properties, add NetBIOS Redirections for connections intended for the secondary applications.

6 Update the VisionFS server, and click Yes when the Profile Editor offers to restart it.

See Also

"Identifying the VisionFS server on the network", in Chapter 1, "The Basics".

"The visionfs command", in Chapter 4, "Issues for Administrators".

"Adding NetBIOS redirections", later in this chapter.

To set up VisionFS as a secondary NBT application

1 Make sure you stop any existing primary application before starting the VisionFS server.

The default profile tells the server to start as a primary application. If there's another primary application, the server cannot start. You need to be able to run the server to change some settings using the Profile Editor.

2 Use the Profile Editor to stop the VisionFS server from advertising any names. To do this, open Server properties, click the Advanced tab, and make sure Disable Naming is checked.

3 On the Advanced tab of Server properties, set up the server to listen for connections on a different TCP port from the default, 139. Remember that VisionFS must be started as root, so choose a port number less than 1024.

4 Update the server, and click Yes when the Profile Editor offers to restart it.

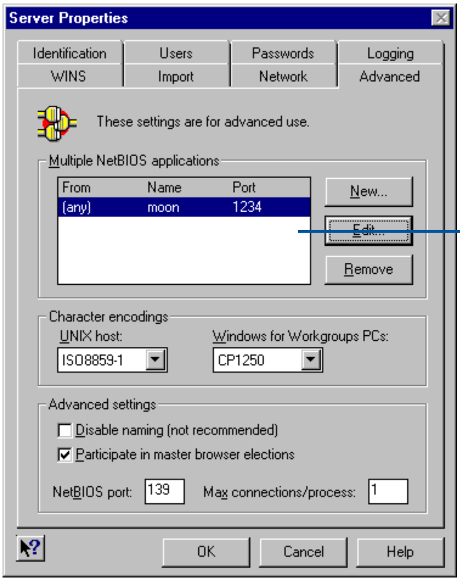
5 Now start your primary NBT application. Remember to set up the primary to redirect connections intended for the secondary applications to the ports they listen on, and to advertise all the names used for the secondary applications.

Adding NetBIOS redirections

NetBIOS redirections allow a VisionFS server to act as a primary NetBIOS application, redirecting connections intended for other, secondary NBT applications. You can set up VisionFS to redirect connections based on the name of the computer connecting to the VisionFS server, or the name it's using to connect.

To redirect a connection to another NBT application

1 In the Profile Editor, open Server properties and click the Advanced tab.



These settings are for advanced use.

Multiple NetBIOS applications

From	Name	Port
(any)	moon	1234

Character encodings

UNIX host: ISO8859-1

Windows for Workgroups PCs: CP1250

Advanced settings

☐ Disable naming (not recommended)

☑ Participate in master browser elections

NetBIOS port: 139 Max connections/process: 1

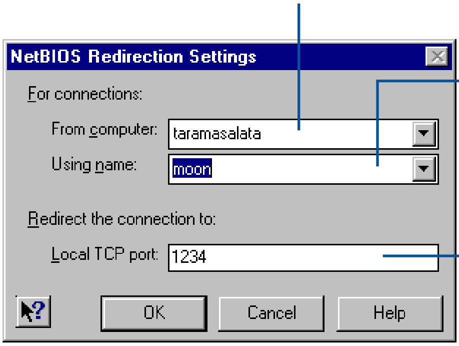
The list of current redirections. Redirections earlier in the list take precedence. To move a redirection, drag the list entry up or down.

2 To add a new redirection, click New.

To edit an existing redirection, click it in the list, then click Edit.

3 In the NetBIOS Redirection Settings dialog, first specify which connections are affected by this redirection. Then, specify where those connections are redirected to.

The NetBIOS name of the computer making the connection. Click **(any)** in the list to mean any computer.



From computer: taramasalata
Using name: moon
Local TCP port: 1234

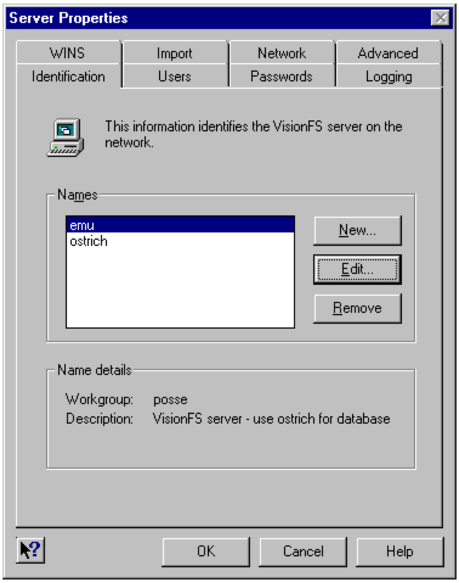
The NetBIOS name used by the connecting computer to access the VisionFS server. Click **(any)** in the list to mean any of the server's names.

The TCP port number to redirect to on the UNIX host. The primary NBT application on a host uses port 139.

Example

For example, consider a UNIX host running two NBT applications: VisionFS (the primary), and a database server (a secondary, running on TCP port 2345). You'd like the VisionFS server to use the NetBIOS name "emu", and the database server to use "ostrich".

In this case, you'd first set up the VisionFS server to advertise the names **emu** and **ostrich**, using the Identification tab of Server properties as shown below:

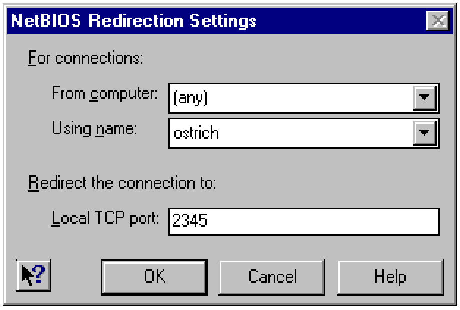


This information identifies the VisionFS server on the network.

emu
ostrich

Workgroup: posse
Description: VisionFS server - use ostrich for database

Then you need to add a NetBIOS redirection, so that people can use the database server. On the Advanced tab of Server properties, click New. In the NetBIOS Redirection Settings dialog, specify that connections from any computer, that use the name **ostrich** to make the connection, are redirected to TCP port 2345. Your NetBIOS Redirection Settings dialog should look like this:



NetBIOS Redirection Settings

For connections:

From computer: (any)

Using name: ostrich

Redirect the connection to:

Local TCP port: 2345

Finally, you need to update and restart the server for the new names and redirections to take effect.

Using more than one VisionFS server

You might want to use more than one VisionFS server, for example to enable Internet workgroups between two independent subnets, or to dedicate one server to deploy Vision2K PC products in read-only license mode, while another server for more general use runs in fully licensed mode.

SEE ALSO

"License management", in Chapter 4, "Issues for Administrators".

Single authentication server

You can dedicate one VisionFS server to be an authentication server, authenticating users for all your VisionFS servers.

SEE ALSO

"Passwords and authentication", in Chapter 2, "Beyond the Basics".

To do this, first decide which server you want to authenticate users, and then use the Passwords tab of Server properties on all other servers to point to that server. The authentication server can use UNIX (unencrypted) or VisionFS (encrypted) passwords to authenticate users, but it can't "chain" to a third server for authentication.

Moving mappings and passwords between servers

The VisionFS password database and username mappings are fully portable between servers, even servers running on different flavors of UNIX.

- The VisionFS password database is the file ***vision_dir*/vfsprofile/authfile**
- The VisionFS username mappings are stored in the file ***vision_dir*/vfsprofile/mapfile**

SEE ALSO

"The visionfs command", in Chapter 4, "Issues for Administrators".

where ***vision_dir*** is the name of the Vision2K shared directory, by default **/usr/local/vision**.

Note These filenames may change in future versions of VisionFS.

To allow you to modify its contents easily, the username mappings file is in ASCII format.

The VisionFS password database is a binary file. However, the **visionfs password** UNIX utility lets you add and remove passwords.

Configuring multiple servers from one Profile Editor

You can configure multiple VisionFS servers from the same Profile Editor, as long as all servers have the same version number.

To change the server you're configuring, click Change Server on the Profile menu, and type the name of the new server. If the server you're currently configuring needs updating with any changes you've made, the Profile Editor will prompt you.

Issues for Administrators

4

Look in this chapter to learn how to control the VisionFS server from the UNIX host, and find information about things that matter to you, such as security, licensing and troubleshooting.

Contents

Controlling VisionFS on UNIX

Setup installs files in the Vision2K shared directory, by default **/usr/local/vision**. You use one of these files, a program called **visionfs** in the **bin** subdirectory, to control VisionFS. Any user can run this program, but most functions are restricted only to the UNIX superuser.

Note Don't try to control the server by running binaries directly, or by using **kill**. Using the **visionfs** command is the only supported way of controlling the server.

The visionfs command

The **visionfs** command has the following syntax:

visionfs *option* [*option-specific-arguments*]

The options let you control the server in different ways, or produce information about the server. The table briefly describes each option.

TIP

Every option has an argument "--help".

Option	Description
archive	Archives the VisionFS server's log files
client	Configures the shared folders users can access with SCO VisionFS SMB Client, and their passwords
clientadmin	Controls SCO VisionFS SMB Client
election	Forces an election to choose a new master browser in a workgroup
help	Displays information about the usage of the **visionfs** command
information	Gives detailed information about the VisionFS server's configuration and operation
license	Adds license numbers for the VisionFS server, and converts an evaluation or read-only installation to fully licensed
lockinfo	Reports which files are locked, and in what way
lookup	Displays information about a particular network (NetBIOS) name
message	Sends a WinPopup message to a user or workgroup
nameinfo	Gives information about names on your network
netinfo	Gives information about UNIX network interfaces
password	Imports, creates or changes VisionFS passwords in the VisionFS password database

SEE ALSO

"Logging" and "License management", later in this chapter.

"Printing from the UNIX host", in Chapter 2, "Beyond the Basics".

"visionfs command", in the Help index.

Option	Description
print	Provides access to shared printers on the network
query	Examines the VisionFS server's log files
restart	Stops then restarts the VisionFS server
setup	Modifies or fixes the VisionFS server configuration.
share	Adds, removes and lists shared folders
start	Starts the VisionFS server
status	Reports VisionFS server details: the current license mode, server names, the current authentication method, which users are VisionFS Administrators, whether the server's running, and who's connected
stop	Stops the VisionFS server
uninstall	Uninstalls VisionFS

Security and authentication

In this section, we'll give information about how VisionFS authenticates users, and how you can be sure your server is as secure as possible while making access by your users as transparent as possible.

How users are authenticated

Authentication effectively starts when the user logs into the PC with a particular username. This username is the name by which the PC knows the user, but plays an important part in authenticating the user to the VisionFS server.

This is because VisionFS uses *user level* security: the user must be authenticated by the server (logged in) before access is granted, but once authenticated can connect to any shares on the server, assuming the access rights for each share allow it. The Windows username is sent to the server during authentication, as described below.

User level security contrasts with *share level* security, which allows for different passwords for each share, and doesn't involve usernames. This means that actions aren't associated with a particular user, making it impossible to distinguish between users. For example, Windows for Workgroups operates in share level security.

In general, authentication involves these steps:

- The user tries to connect to the VisionFS server in some way, for example displaying the list of shares or trying to access a share.
- If another server is being used to authenticate users, this VisionFS server acts as a "go-between" for Windows and the authentication server: this VisionFS server passes user and password information from Windows to the authentication server, and sends responses from the authentication server back to Windows.
- Windows and the authentication server negotiate the details of the connection, including whether or not to encrypt passwords on the network. Encrypted passwords are used if the authentication server is Windows 2000 or Windows NT, or a VisionFS server using VisionFS passwords. Unencrypted passwords are used if the authentication server is a VisionFS server using UNIX passwords.
- Windows and the authentication server will attempt to authenticate the user, taking into account the current authentication method, and (if the authentication server is a VisionFS server in UNIX password mode) whether or not the user has a Windows-to-UNIX username mapping. Windows may prompt the user for a password, or the user may be denied access.

Negotiation

In some cases, Windows doesn't give users the option of entering a password if the passwords it tries aren't accepted. For example, File Manager on Windows for Workgroups will display an Access Denied dialog if you try to list the shares on a server before you've been authenticated.

In general, if you connect to a share by name—using \server\share—Windows will either authenticate you, or prompt you for a password.

Summary

This section summarizes important points about authentication. For more information, read the sections that follow.

- You should set up username mappings so that VisionFS knows which Windows usernames correspond to which UNIX users, and/or use identical Windows and UNIX usernames.

  If you're using another VisionFS server to authenticate users by their UNIX passwords, you need to set up username mappings on the authentication server as well as this VisionFS server.
- A user without a password on the authentication server is logged in with guest permissions (that you define), and the supplied password is ignored.
- A user with a password on the authentication server is authenticated if the supplied password matches their password in the appropriate database.
- The VisionFS password database stores passwords (which are case-insensitive) for Windows usernames.
- With the UNIX password authentication method, VisionFS applies any username mapping before checking in the standard UNIX password database. As UNIX passwords are case-sensitive, but Windows sends case-insensitive passwords, VisionFS allows for different capitalization of UNIX passwords.
- A user is denied access if the supplied password doesn't match the password in the appropriate database.

Authentication methods

The authentication method you use controls:

- Which server performs the authentication.
- Which passwords are used to authenticate users.

You can authenticate users on:

- This VisionFS server, by their VisionFS or UNIX password.
- Another VisionFS server, by their VisionFS or UNIX password.
- A Windows 2000 or Windows NT server, by their password for that server.

Authenticating users on this (or another) VisionFS server using VisionFS passwords

- Passwords are encrypted before transmission on the network, and are case-insensitive.
- Passwords are stored in this (or the other) VisionFS server's VisionFS password database, which stores passwords for Windows usernames.
- Passwords are checked against users' Windows usernames, without taking any username mappings into account.
- Users without a password in this (or the other) VisionFS server's VisionFS password database are granted guest access only, whether or not they have an account on the UNIX host.
- You change these passwords from Windows, using the authentication server's Profile Editor or a separate program in the authentication server's **visiontools**share,**password.exe**.

Authenticating users on this (or another) VisionFS server using UNIX passwords

- Passwords are transmitted unencrypted on the network, and are case-sensitive. Windows sends case-insensitive passwords, so VisionFS tries different combinations of upper-case and lower-case characters.
- Passwords are stored on this (or the other) VisionFS server's UNIX host, in the UNIX password database, which stores passwords for UNIX usernames.
- Passwords are checked against users' UNIX usernames, taking into account any username mappings.
- Users without an account on this (or the other) UNIX host are granted guest access only and the password is ignored.
- You change these passwords on the UNIX host.

Note that the authentication server's username mappings list is used to authenticate users, but this VisionFS server's username mappings list is used when a user performs an action.

Important You can have a username mapping from a Windows user to a UNIX user that doesn't exist. These users will only be granted guest access.

Authenticating users on a Windows 2000 or Windows NT server

- Passwords are encrypted before transmission on the network, and are case-insensitive.
- Passwords are stored in the Windows server's user database, which stores passwords for Windows usernames.
- Passwords are checked against users' Windows usernames. Username mappings don't apply to Windows servers.
- Users without a password for this Windows server are granted guest access only, whether or not they have an account on the UNIX host.
- You change these passwords using standard Windows tools.

Usernames

The usernames sent by Windows are case-insensitive. However, the usernames stored in the UNIX user database are case-sensitive. The authentication server converts all Windows usernames to lower-case before working with them.

This means you must set up username mappings for all users with mixed-case UNIX usernames. If the authentication server can't work out the user's UNIX username—for example, if there's no username mapping—then the user is granted guest access.

Otherwise, passwords are checked against users' Windows usernames.

The UNIX user database

The VisionFS server uses the standard UNIX mechanisms for accessing the UNIX user database. For example, it doesn't matter if your UNIX host uses **/etc/passwd** or NIS—VisionFS will check whatever you're using.

Passwords

You should be aware of some general password issues that affect the security of your UNIX host.

How passwords are sent

Passwords may be encrypted or unencrypted, depending on the authentication method of the authentication server:

- If a VisionFS server uses UNIX passwords to authenticate users, or forwards username and password information to another VisionFS server that uses UNIX passwords for authentication, then Windows will send passwords in plain text—not encrypted. Although both Windows and UNIX provide facilities for the encryption of passwords, the encryption mechanisms used are incompatible.
- With all other authentication methods, Windows will encrypt passwords before transmitting them on the network.

SEE ALSO

"Authentication methods", earlier in this chapter.

Using UNIX passwords to authenticate users may present a security problem in environments where very high security is required, though in most environments it does not affect the security of your system. Using VisionFS with UNIX passwords is no less secure than using the UNIX telnet program, for instance.

Mixed-case passwords on UNIX

Windows sends case-insensitive passwords to the VisionFS server. If you're using VisionFS passwords to authenticate users, this doesn't matter: the VisionFS password database stores case-insensitive passwords, like Windows. However, UNIX passwords are case-sensitive. Consequently, with the UNIX password method VisionFS tries different capitalizations of the password.

For example, if Windows sends the password **FOO**, VisionFS would try the passwords **foo**, **foO**, **fOo**, **Foo**, **fOO**, **FoO**, **FOo**, and **FOO**.

This decreases security, by effectively making UNIX passwords case-insensitive, and increases the time taken to authenticate users. There is no real alternative solution other than enforcing lower-case UNIX passwords, which decreases security still further.

SEE ALSO

"Case sensitivity", in the Help index.

However, you can use the Profile Editor to reduce the number of characters in the password the VisionFS server will change the case of. This increases security (as the server will try fewer passwords) and reduces the time taken to authenticate users, but restricts the acceptable range of passwords. By default this is 8, as most UNIX systems only use the first eight characters of passwords for authentication. Check your UNIX documentation to see if you should change it.

For example, if you change the setting to 2, then VisionFS will match a password with at most two upper-case characters in an otherwise lower-case password (or two lower-case characters in an upper-case password).

If one of the password combinations matches, the user is authenticated. If no match is found, the user is denied access.

Using Windows passwords to access the VisionFS server

Often, Windows sends the VisionFS server a user’s Windows password to try to authenticate the user. This means that if a user’s Windows password is the same as their password for the server, the user might not be prompted for a password.

However, be aware that using identical passwords decreases security:

- If the user leaves their PC unattended, other users can access the UNIX host.
- In some cases, the Windows password list can be decrypted easily.

The Windows password list

A security flaw present in the first release of Windows 95 means it is computationally easy to decrypt the Windows password list file. This file contains all the passwords that Windows caches for the user, including the password for accessing the VisionFS server. Password caching is enabled by default.

This flaw is fixed in later releases of Windows 95 (which you may be able to obtain from the Microsoft web site, **www.microsoft.com**) and in Windows 98. Windows 2000 and Windows NT do not use password lists, and so do not have this flaw.

If you use versions of Windows that suffer from this security flaw, you can disable password caching so that the password for the VisionFS server is not stored on the PC, and can’t be decrypted in this way.

To disable password caching in Windows 95

1. Delete all ***username*.pwl** files in the Windows directory.
2. Create a file called **nocache.reg**, containing the following:

   ```
   REGEDIT4

   [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\
   CurrentVersion\Policies\Network]
   "DisablePwdCaching"=dword:00000001
   ```

   Important The text between **[** and **]** must be on a *single line* in the file.
3. Double-click the **nocache.reg** file.

Filtering unwanted connections

You may want to allow only computers in your organization to access your VisionFS server, and automatically reject all other computers. Similarly, you may want to allow access through a particular network interface on the UNIX host, and reject accesses using other interfaces.

The Profile Editor lets you do both of these easily, by setting up a list of *filters*: a list of DNS names or IP addresses (not NetBIOS names), which can include wildcards, and whether those computers are allowed or denied access.

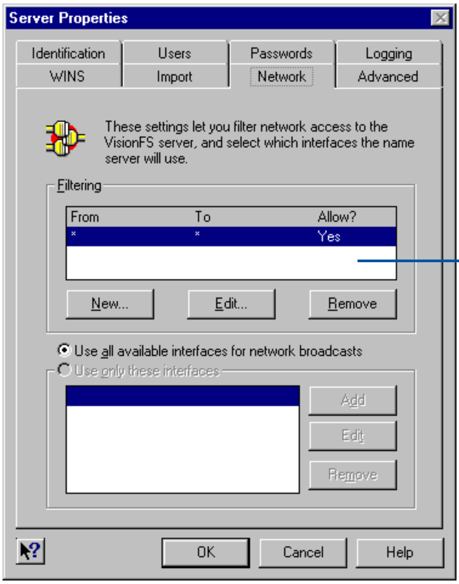
When a computer tries to access the server, VisionFS checks the list of filters. The first filter that matches determines whether the connection is allowed or denied.

If none of the filters match, the connection is denied.

Note Computers which are denied access to the VisionFS server will be unable to make use of Internet workgroups.

To filter unwanted connections

1 In the Profile Editor, open Server properties and click the Network tab.



These settings let you filter network access to the VisionFS server, and select which interfaces the name server will use.

From	To	Allow?
*	*	Yes

● Use all available interfaces for network broadcasts

○ Use only these interfaces

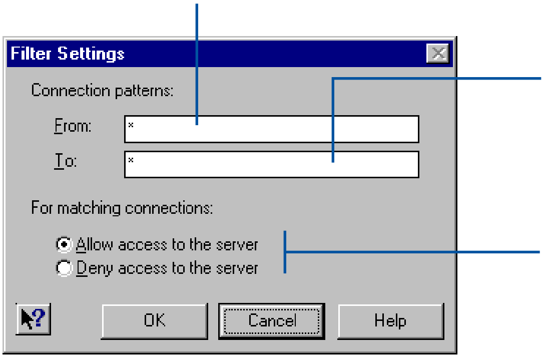
The list of current filters. Filters earlier in the list take precedence. To move a filter, drag the list entry up or down.

2 To add a new filter, click New.

To edit an existing filter, click it in the list, then click Edit.

3 You'll see the Filter Settings dialog.

Type the IP address or DNS name of the computer trying to connect to the VisionFS server.



Filter Settings

Connection patterns:

From: *

To: *

For matching connections:

● Allow access to the server

○ Deny access to the server

Type the IP address or DNS name of the network interface on the UNIX host that the computer's connecting through.

Specify whether connections that match are allowed or denied.

You can use the wildcard "*" to match more than one IP address or DNS name. If you're using DNS names in filters, but a computer that tries to connect doesn't have a DNS name, the reverse name lookup will fail, after some time, and the attempt to connect may time out before VisionFS allows or denies it.

VisionFS and firewalls

As a standard NetBIOS over TCP/IP application, VisionFS uses UDP ports 137 and 138 for naming, and TCP port 139 (by default) to listen for connections.

You should configure your firewall to prevent external access through these ports. If you do this, then computers outside your firewall won't be able to set up a CIFS Bridge to a computer on your network, or set up Internet workgroups with your workgroups.

How to tell if an action will succeed

When a user tries to perform an action in a share on the VisionFS server, whether that action succeeds depends on a number of things.

To find out if an action will succeed

- **Check whether connections are automatically rejected**

  See “Filtering unwanted connections”, earlier in this chapter.

- **Check whether the user has a Windows-to-UNIX username mapping**

  See “Username mappings”, in Chapter 2, “Beyond the Basics”.

- **Check the VisionFS server’s authentication method**

  See “Passwords and authentication”, in Chapter 2, “Beyond the Basics”. See also “Security and authentication”, earlier in this chapter.

- **Check the user’s access rights in the share**

  See “Controlling access”, in Chapter 2, “Beyond the Basics”.

- **Check the UNIX permissions**

  See “Controlling access”, in Chapter 2, “Beyond the Basics”.

PC and UNIX file differences

In this section, we'll cover the differences between how PCs view files, and how UNIX views them. We'll explain how VisionFS helps smooth the way, and where circumstances conspire to make it impossible.

Filenames

With VisionFS, each file or directory effectively has three names:

- The UNIX filename.
- A long name.
- A short name, for compatibility with DOS and older versions of Windows.

When a long or short name is used in Windows, VisionFS uses the correct UNIX filename.

Potentially, there are fewer long names than UNIX filenames, and fewer short names than long names. This means that the process of converting UNIX filenames to long names, then to short names, may result in two unique UNIX filenames losing their uniqueness.

You can specify that when VisionFS truncates a filename, VisionFS generates a suffix for that filename to help keep it unique. To do this, make sure the Try To Make Truncated Names Unique box on the share's Files tab is checked.

The next sections describe the two conversion processes, and how VisionFS generates suffixes.

Converting UNIX filenames to long names

This involves the following steps:

- Removing trailing dots.
- Removing the characters not allowed in long names: **? " / \ < > * | :**
- Appending "_" to the MS-DOS reserved basenames. These basenames are: **aux com1 com2 com3 com4 con lpt1 lpt2 lpt3 nul prn clock$**

Converting long names to short names

This involves the following steps:

- Removing all dots but the last.
- Removing the additional characters not allowed in short names: **[ ] ; = + ,**
- Converting to upper-case.
- Truncating the basename to 8 characters, and the extension to 3 characters.

- Adding suffixes to the basename, as described below, if the filename was truncated.
- Adding an underscore "_" if there's no basename—for example, one would be added for the UNIX filename **.cshrc**.

Making filenames unique

If you've configured VisionFS to try to keep filenames unique, VisionFS first generates a 32-bit checksum for each, based on the original UNIX filename. The checksum is converted to a printable form.

Then, a suffix is formed for each truncated filename, using the special character for the share (by default, ~) and the specified number of characters from the printable checksum (by default, 2).

Finally, the suffixes are added to the basenames of the truncated filenames, replacing the final characters to ensure the basenames don't exceed 8 characters in length.

Permissions

UNIX permissions are richer than MS-DOS (Windows) file attributes, but MS-DOS file attributes aren't a subset of UNIX permissions.

Of the four standard MS-DOS file attributes—Archive, Hidden, System and Read-only—VisionFS directly supports the Read-only attribute. The other attributes don't easily map onto UNIX permissions.

Windows 2000 or Windows NT Access Control Lists aren't supported on most flavors of UNIX, and aren't supported by VisionFS.

Read-only attribute

The Read-only attribute of a Windows file is set if the user accessing a share isn't allowed to write to the file, according to the UNIX permissions. Similarly, changing the Read-only attribute in Windows sets or clears the three UNIX write permissions for owner, group and others.

Remember that even if the access rights for a user allow a particular action, the UNIX permissions determine whether that action succeeds or fails.

Archive, Hidden and System attributes

SEE ALSO

"DOS attributes", in the Help index.

VisionFS includes indirect support for the Archive, Hidden and System attributes. For each share, you can define when VisionFS reports each attribute as being set, in one of two ways:

- For filenames matching particular patterns that you specify.
- For files with a particular UNIX permission bit set.

Semantics

Some actions on files will have different effects in Windows than UNIX users might expect.

Deleting symbolic links

On UNIX, deleting a symbolic link deletes the directory entry, and doesn't affect the file or directory referenced by the symbolic link. However, Windows doesn't have the concept of a symbolic link.

For files shown in Windows that, in reality, are symbolic links on the UNIX host:

- Deleting a symbolic link to a file will just delete that link. The referenced file is unaffected.
- Deleting a symbolic link to a directory will delete all files and subdirectories in the directory pointed to by the link, then delete the symbolic link. This is because Windows tells VisionFS to delete the contents of the directory, then delete the directory.

See Also

"Hiding symbolic links", in the Help index.

Important For an experienced UNIX user this is not the expected behavior, but is beyond the control of VisionFS. Be careful to ensure that directories are not deleted accidentally. If necessary, hide symbolic links in shares.

Renaming and deleting files

On UNIX, the permissions of a directory determine whether you can rename or delete files in that directory.

In Windows, the Read-only attribute on a file determines whether you can rename or delete it.

Deleting files in use

On UNIX, you can delete or rename a file in use. In Windows, you can't.

This is because UNIX keeps file information separately from directory information, whereas Windows keeps them together.

VisionFS allows files to be deleted or renamed while in use.

Free disk space

Windows will report the free disk space based on the root directory of each share on the VisionFS server. However, there may be symbolic links in the share pointing to other file systems, which means the effective free disk space is larger.

Also, as UNIX allows multiple directory entries per file, deleting a file may not necessarily increase the amount of available disk space.

File locking

In this section, we'll describe VisionFS file locking, which lets a program be sure it can read and write to a file (or part of a file) without another program doing so at the same time.

Overview

When you edit a file, you perform at least three actions on that file: you open the file in your editing program, you make changes, and finally you save the file.

Imagine that two people want to edit the same file. The first person opens the file in an editor and starts making changes. Then the second person opens the file, makes changes and saves the file *before* the first person has finished editing. Later, the first person finishes editing the first copy of the file and saves it.

The second person's changes are lost: they weren't in the file when the first person started editing. Ideally, the second person should have been prevented from editing the file until the first person had finished.

The process of controlling which actions users are allowed to perform on a file while another user is performing an action on a file is called *file locking*.

For example, if you're reading a file but don't intend to make changes, it may be acceptable for others to *read* the same file. However, it may not be acceptable for others to *modify* the file while you're reading it.

File locking lets users be sure that files they work with are up-to-date, and that all their changes will be preserved.

UNIX and Windows file locking

UNIX and Windows offer different file locking facilities. UNIX offers only rudimentary file locking, which isn't used by many applications. In contrast, Windows provides rich and flexible file locking.

Comparing Windows and UNIX file locking in detail reveals two important differences:

- UNIX doesn't allow open locks or opportunistic locks. Windows does.
- Windows uses 32-bit range locks, whereas UNIX is restricted to 31-bit range locks. Also, the NFS lock daemon becomes unreliable with range locks above 29 bits long.

The different types of lock are explained in more detail below.

VisionFS file locking

VisionFS has an independent component, called the *lock daemon*, which provides full Windows locking semantics. The lock daemon manages lock requests from PCs and maintains a lock database which contains information about all file locks which are currently in place. When a PC requests access to a file in a share, VisionFS consults the lock daemon for the availability of that file, and access is granted or denied as appropriate.

VisionFS provides three types of locks for PCs to use with files.

Lock type	Description
Open lock	Used when a file is first opened. These locks let you specify exactly which actions other users are allowed to perform on a file while you are using it.
Record lock	Used to prevent other users from accessing a particular portion of a file while you are using it.
Opportunistic lock	Gives the user complete control over a file while they are using it. If another user needs to edit the file, the client with the opportunistic lock is asked to relinquish its lock and lock again with an Open lock or a Record lock.

Should I use opportunistic locks?

Opportunistic locks give great performance benefits: one user has complete control over the entire file at one time and can edit a local copy, only updating the file on the server immediately before the lock is removed.

However, opportunistic locks don't provide protection from simultaneous editing by a PC user and a UNIX user.

You should use opportunistic locks in the following cases:

- If the files in a share will only be modified by PC clients.
- If the files in a share will be read by PC and UNIX clients, but never modified by either, for example with a CD-ROM drive.

You shouldn't use opportunistic locks if the files in a share might be modified by both PC and UNIX clients.

Logging

VisionFS log files contain useful information about who uses (and who tries and fails to use) the server. In this section, you'll learn how to examine the VisionFS log files, how to customize what's logged, and how to archive log files.

Checking the logs

See Also

"The visionfs command", earlier in this chapter.

"Customizing what's logged", later in this chapter.

You use the **visionfs** command's **query** option to examine the VisionFS log files, and find out about server usage.

Important Remember that you can customize what's logged: if the information doesn't seem to be correct, make sure the server was logging the information in the first place.

Arguments to the **query** option let you view the information in different ways, as described in the table.

Note Each argument is prefixed by two dashes, "--", not one.

Argument	Description
--conns	Displays information about successful and failed connections to the VisionFS server, and shows the maximum number of simultaneous connections.
--err	Displays the error log.
--shares	Displays information about usage at the share level, showing counts and percentages. You must supply one of the arguments**--byuser**, **--byshare** or**--bymachine**, to show the information by user, share or machine.
--ops	Displays information about usage at the operation level, with success/failure ratios shown for each operation. You must supply one of the arguments**--byuser**, **--byshare** or **--bymachine**, to show the information by user, share or machine.
--all	Displays all information (the default). You can omit a section of information from the output by using the appropriate argument with the**--all** flag. For example, **visionfs query --all --err** displays all information except the error log.

Customizing what's logged

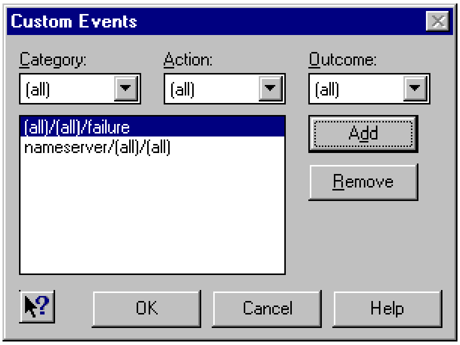
You use the Profile Editor to customize the information the VisionFS server writes to log files. If you want, you can choose to log just failed operations, or just particular operations you're interested in.

To customize what's logged

1. In Server properties, click the Logging tab.
2. In Logged Events, click Custom, then click Define. The Custom Events dialog appears.

TIP

On the Logging tab, click All, Failures or None in the Logged Events box to use the most common logging settings.



Category: (all)
Action: (all)
Outcome: (all)

(all)/(all)/failure
nameserver/(all)/(all)

3. To log something new, click the Category, Action and Outcome you want to log, then click Add. Click **(all)** in the lists to mean all Categories, Actions or Outcomes as appropriate.

   To remove something you don't want to log, click an entry in the list, then click Remove.

4. When you're done, click Update Server on the Profile menu, and restart the server.

Archiving log files

Log files can use a significant amount of disk space on the UNIX host. Archiving the logs compresses the files, freeing disk space. Setup automatically configures your host to perform a "checkpoint" every Sunday at 4am, which archives the log files.

Log files are stored in the **vfsdata/logs** subdirectory of the Vision2K shared directory (by default, **/usr/local/vision**). Each server uses multiple log files, which it may write to at any time. If you want to examine the logs, use the **visionfs query** command.

Note Do not delete any files in the **logs** directory. If you delete a file the server still has open, the directory entry will disappear but the disk space won't be freed until the server exits. To reclaim some disk space, first archive the logs, then delete the archive.

To archive the logs

1 Log in as root on the UNIX host.

2 Type the following, replacing ***vision_dir*** with the name of the Vision2K shared directory, by default **/usr/local/vision**:

```
vision_dir/bin/visionfs archive
```

Archiving the logs compresses the files and moves them to a numbered subdirectory of the **logs** directory. A file **summary.txt** in this directory contains the results of performing **visionfs query** at the time of the archive.

You can delete archived log files without affecting the server.

Note In earlier versions of VisionFS, you could only use **visionfs archive** when the server wasn't running. The **visionfs checkpoint** command would stop the server, archive the logs, and restart the server. In this release, **visionfs checkpoint** and **visionfs archive** are identical, but **visionfs checkpoint** is deprecated.

License management

In this section, we'll explain how VisionFS licensing works, and how you can use License Manager to add and remove license numbers, and monitor license usage.

Overview

On a distributed network, it can be difficult to keep track of what software is installed. Vision2K products are therefore licensed on a concurrent user basis, not on the basis of the number of computers the software is installed on. For example, a 100 user VisionFS license number means that up to 100 people may use VisionFS at any one time, with perhaps each person using several VisionFS servers at once.

The License Administrator, named when you install Vision2K products on the UNIX host, is responsible for policing license agreements. To help, the License Administrator can use:

- License Manager, a Windows program
- **licadmin**, a UNIX utility

SEE ALSO

"License Manager" and "License Server", later in this chapter.

A License Server (called **licsrv**) manages licenses on the UNIX host. Vision2K products contact the License Server to request and release licenses. The License Server is installed automatically when you install VisionFS. Only one License Server runs on a subnet at a time.

License modes

VisionFS can run in three different license modes:

- *Read-only* mode is used only to deploy the PC components of Vision2K software through the **vision2k** shared folder. In Read-only mode you are restricted to one VisionFS Administrator. All other users can only read information from the UNIX host; they can't write or change files on the UNIX host, or print to the server.
- *Evaluation* mode is used to evaluate the product. Evaluation mode provides the full functionality of VisionFS, but only for 30 days.
- *Fully licensed* mode provides the full functionality of VisionFS, with no restrictions. You need a license number to use VisionFS in fully licensed mode.

Licenses are stored with the License Server, not with the PC or the VisionFS server.

Changing the license mode

SEE ALSO

"The visionfs command", earlier in this chapter.

To change the license mode, use ***vision_dir*/bin/visionfs license**, replacing ***vision_dir*** with the name of the Vision2K shared directory, by default **/usr/local/vision**. You must be root to do this.

To change from read-only to evaluation mode, you don't need a license number.

To change from read-only or evaluation to fully licensed mode, you must make sure a valid license number is available or add one, and then change the license mode.

There are three ways you can add license numbers:

SEE ALSO

"License Manager", later in this chapter.

- Using **visionfs license**.
- Using the License Manager Windows program.
- Using the ***vision_dir*/bin/licadmin** UNIX utility, replacing ***vision_dir*** with the name of the Vision2K shared directory on the UNIX host, by default **/usr/local/vision**. Use **licadmin -A** to add license numbers.

To add or remove licenses using License Manager or **licadmin** you must be root or have license administration privileges. To run **visionfs license**, you must be root.

If you use License Manager or **licadmin** to add a license number, you must still change the VisionFS license mode using **visionfs license**.

License Manager

License Manager lets you add and remove license numbers, monitor license usage, and control the behavior of the License Server. For example, you can make the License Server automatically email the License Administrator when a Vision2K product runs out of licenses.

To run License Manager

SEE ALSO

For help on License Manager, click Help Topics on its Help menu.

‣ Open the **visiontools** shared folder on the VisionFS server, open the **licmgr** folder, and then double-click **licmgr.exe**.

Alternatively, you can insert the Vision2K CD in a PC's CD drive, and, when the Setup wizard starts, choose Browse. Open the **licmgr** folder, and then double-click **licmgr.exe**.

To run License Manager, you must be root or have license administration privileges on the UNIX host running the License Server.

License Server

SEE ALSO

"License Manager", earlier in this chapter.

The License Server, which runs on a UNIX host, grants or denies licenses when users try to connect to the VisionFS server (or use another Vision2K product). To configure the behavior of the License Server, use License Manager.

If you have Vision2K products installed on more than one UNIX host, only one License Server will run on a subnet at a time. VisionFS will request licenses from the running License Server. Similarly, License Manager will contact the running License Server for licensing information.

Soft and hard licensing

The License Server can use "soft" licensing or "hard" licensing.

- With soft licensing, users can connect to the VisionFS server even if the number of concurrent users has reached the limit defined by your VisionFS license number.
- With hard licensing, users are denied access once the limit has been reached.

On Windows 2000 and Windows NT, users will see an error message explaining why they're denied access. On other versions of Windows, users may see a message explaining that an extended error has occurred, or that the request was not accepted by the network. These messages are displayed by Windows, and aren't under the control of VisionFS.

Troubleshooting

As soon as you connect two computers together, you need to make careful decisions about how the computers interact. As networks grow, the potential for trouble increases dramatically.

VisionFS works seamlessly for most networking environments. But no two networks are identical. In this section, we'll point out some of the areas that could lead to problems.

SEE ALSO

"Troubleshooting" in the Help index.

Be sure to check the Help for other troubleshooting information about the VisionFS server and the Profile Editor.

General problems

If you can't start the VisionFS server or the Profile Editor, the profile may be corrupt, or you may have accidentally changed some settings that mean you are no longer allowed to access the Profile Editor.

You can fix a profile by running VisionFS Setup.

To fix a corrupt or invalid profile

SEE ALSO

"The visionfs command", earlier in this chapter.

1 Log in as root on the UNIX host.

2 Type the following, replacing ***vision_dir*** with the name of the Vision2K shared directory, by default **/usr/local/vision**:

***vision_dir*/bin/visionfs setup**

3 Follow the instructions on your screen.

Remember to check the **README.vfs** file, installed in the **docs** subdirectory of the Vision2K shared directory (by default, **/usr/local/vision**). It may contain late-breaking information that couldn't make this book or the online Help.

If you need to contact Support

VisionFS can output detailed diagnostic information about your network environment. If you need to contact Support, this information may help to solve your problem more quickly.

- From the Profile Editor, click About on the Help menu, click the Information tab, then click Save.
- From the UNIX command line, use the **visionfs information** command.

Making sure PCs can access VisionFS

To access a VisionFS server, Windows needs to use standard networking software, the same as it can use to access other Windows PCs on the network.

Note If a PC uses NetBEUI but not TCP/IP, then it can talk to other Windows PCs on the network, but not VisionFS servers.

Windows 95 and 98 requirements

- Client for Microsoft Networks. To check, open Windows Control Panel, double-click Network, and look in the list under The Following Network Components are Installed.
- TCP/IP. See later in this chapter.

Windows NT requirements

- NetBIOS Interface and Workstation services. To check, open Windows Control Panel, and double-click Network. On Windows NT 3.51, look in the Installed Network Software list. On Windows NT 4, look in the list on the Services tab.
- TCP/IP Protocol. See later in this chapter.

Windows 2000 requirements

- Client for Microsoft Networks. To check, open Windows Control Panel, open Network and Dial-up Connections, right-click Local Area Connection and choose Properties. Look in the list of components.
- TCP/IP Protocol. See later in this chapter.

Installing Microsoft TCP/IP

To access a VisionFS server, PCs must use TCP/IP as one of their transport protocols. All versions of Windows supported by this release of VisionFS include a TCP/IP protocol stack as part of the operating system.

To install Microsoft TCP/IP on Windows 95 and 98

1. Open Windows Control Panel and double-click Network.
2. Click Add. Click Protocol, and then click Add.
3. In the Manufacturers list, click Microsoft. In the Network Protocols list, click TCP/IP. Click OK to return to the Configuration tab.
4. In the network components list, click TCP/IP and then click Properties.
5. Fill in the required details in the Properties dialog box.

To install Microsoft TCP/IP on Windows NT 4

1. Open Windows Control Panel, double-click Network, and then click the Protocols tab. The dialog box shows the installed protocols.
2. Click Add.
3. In the Network Protocols list, click TCP/IP Protocol, and then click OK.
4. Windows NT Setup displays a message asking if you wish to use DHCP to dynamically provide an IP address. If DHCP is in use at your site, click Yes, and you can ignore step 7 in these instructions. Otherwise, click No.
5. Windows NT Setup displays a message asking for the full path to the Windows NT distribution files. Provide the appropriate location, and click Continue. All necessary files are copied to your hard disk.
6. Click Close.
7. Fill in the required details in the Microsoft TCP/IP Properties dialog box.

To install Microsoft TCP/IP on Windows 2000

1. Open Windows Control Panel and then open Network and Dial-up Connection.
2. Right-click Local Area Connection and choose Properties.
3. Click Install. Click Protocol, then click Add.
4. In the Network Protocol list, click Internet Protocol (TCP/IP). Click OK.
5. In the components list, click Internet Protocol (TCP/IP) and then click Properties.
6. Fill in the required details in the Properties dialog box.

Checking your PC and UNIX broadcast addresses

VisionFS uses NetBIOS naming, which broadcasts names using the UNIX host’s broadcast address. It’s important that this broadcast address is correct, or the VisionFS server won’t appear in workgroups.

On your UNIX host, you can use the **visionfs netinfo** command to display information about the network interfaces. This command will tell you if your UNIX host seems to be using an incorrect broadcast address or subnet mask.

Windows works out the broadcast address based on the subnet mask. Most sites use a Class C subnet mask even if they have a Class B network. However, Windows defaults the subnet mask based on the class of network. This means you may need to change subnet masks of 255.255.0.0 (Class B network) to 255.255.255.0 (Class C network).

The UNIX host and your PCs must use the same broadcast address. Some flavors of UNIX (for example, SunOS) use the wrong broadcast address by default. See your UNIX documentation on the **ifconfig** command to find out how to set broadcast addresses and subnet masks.

Accessing the server and shares

Windows 95 or 98 denies access

Windows 98 and later releases of Windows 95 don't allow the use of unencrypted passwords by default. This results in an Access Denied dialog when a user tries to access a VisionFS server which is using unencrypted (UNIX) passwords. (By default VisionFS uses encrypted passwords.)

To fix the problem, either use encrypted passwords to authenticate users (recommended), or do the following:

1 On Windows 95 or 98, run Registry Editor.

2 From the **HKEY_LOCAL_MACHINE** subtree, go to the following key:

\System\CurrentControlSet\Services\VxD\VNETSUP

3 Click New on the Edit menu, then click DWORD Value.

4 Type **EnablePlainTextPassword**, then press Return.

5 Click Modify on the Edit menu, then type **1** in the Value Data box.

6 Click OK, quit Registry Editor, then restart Windows.

Note The Windows 98 CD includes two files to enable and disable the transmission of plain text (unencrypted) passwords easily. These files are **ptxt_on.inf** and **ptxt_off.inf**, in the **\tools\mtsutil** folder on the CD. Read the **mtutil.txt** file for instructions.

Account not authorized to login

See Also

"Soft and hard licensing", earlier in this chapter.

"Passwords", later in this chapter.

Windows 2000 and Windows NT 4.0 Service Pack 3 and later don't allow the use of unencrypted passwords by default. This results in an error message "The account is not authorized to log in from this station" when a user tries to access a VisionFS server which is using unencrypted (UNIX) passwords. (By default VisionFS uses encrypted passwords.)

To fix the problem, either use encrypted passwords to authenticate users (recommended), or follow one of the procedures below.

For Windows 2000:

1 Open Control Panel, and double-click Administrative Tools.
2 Double-click Local Security Policy.
3 In the Security Settings tree, open Local Policies and click Security Options.
4 Change the setting "Send unencrypted password to connect to third-party SMB servers" to "Enabled".

For Windows NT:

1 Run Registry Editor.
2 From the **HKEY_LOCAL_MACHINE** subtree, go to the following key:
\System\CurrentControlSet\Services\Rdr\Parameters
3 Click New on the Edit menu, then click DWORD Value.
4 Type **EnablePlainTextPassword**, then press Return.
5 Click Modify on the Edit menu, then type **1** in the Value Data box.
6 Click OK, quit Registry Editor, then restart Windows.

Not Browsable means not Active in Windows 95 and Windows NT 4

If you configure a share to be not browsable, using the box on the General tab of the share's properties, then in Windows 95 and Windows NT 4 Explorer, it is also not active: Windows won't let you connect to the share, even if you know its name. This is a problem with Windows 95 and Windows NT 4.

However, you can access the share from MS-DOS, for example by mapping a drive. Windows Explorer on Windows 98 does not have this problem.

Problems reconnecting at logon on Windows NT 4

If you're having problems with the Reconnect at Logon box on Windows NT 4 in domains, you should switch to VisionFS (encrypted) passwords, or use another VisionFS server (in VisionFS password mode) or Windows NT server for authentication, and use the same passwords for Windows and VisionFS.

Find Computer fails

In Windows, you can click Find Computer on the Start menu to locate computers on the network.

On Windows 95 and 98, this can sometimes fail to locate a VisionFS server. This can happen if you haven't connected to the VisionFS server in that Windows session, and Windows hasn't cached your password for the VisionFS server, and your Windows password is different to your password for accessing the VisionFS server.

Other supported versions of Windows successfully locate VisionFS servers in Find Computer.

In Windows 95 and 98, clicking Run on the Start menu and typing \server works more reliably than searching for a computer named *server* in the Find Computer dialog.

Passwords

Using VisionFS with HP-UX 10+ trusted systems

SEE ALSO

"Restarting the VisionFS server", in the Help index.

VisionFS determines whether HP-UX 10+ is running as a trusted system when it starts up. However, you can change between a trusted and non-trusted system without rebooting your UNIX host. If you do this, VisionFS will treat all passwords as invalid until you restart the VisionFS server.

Passwords and Windows NT or Windows 2000

Windows 2000 and Windows NT don't cache passwords. If a VisionFS server is using UNIX (unencrypted) passwords for authentication, or another VisionFS server that's using UNIX passwords, then users will always have to type a password to access the VisionFS server.

To allow users to access a VisionFS server from Windows 2000 or Windows NT without typing a password, the VisionFS server must use one of the other authentication methods. In addition, a user's Windows password must be the same as their password for accessing this VisionFS server.

If you switch to using UNIX passwords from another authentication method, users must log out of Windows and log in again, otherwise Windows won't allow them to connect to the server.

Passwords and network logon services

SEE ALSO

"Network logon services", in Chapter 3, "The Possibilities".

If you've configured the VisionFS server to provide network logon services, users can't use Windows tools (Passwords in Control Panel, for example) to change their Windows password. Instead, they must use the **password.exe** program.

File protection

Opportunistic locks give great performance benefits over other file locking methods.

However, opportunistic locks don't provide protection from simultaneous editing by a PC user and a UNIX user.

If there is any chance that the files in a share might be modified by both PC and UNIX clients, you should turn off opportunistic locks. If you allow opportunistic locks in these circumstances, data loss could occur.

By default, opportunistic locks are turned off.

CD-ROM drives

You can set up a shared folder that accesses your UNIX CD-ROM drive, if you have one.

On some flavors of UNIX, files on the CD-ROM have version numbers, such as ";1", added to the end of the name. This can cause problems with Windows, which uses the file extension to determine the type of a file. For example, using Windows 98 a file called **program.exe** might appear as **program.exe;1**, and Windows would not recognize it as an executable program.

If possible, make sure the CD-ROM is mounted so that version numbers aren't shown. Check your UNIX documentation for the correct mount command to use.

Printing

Printer driver

Make sure your users have installed the correct Windows printer driver for your UNIX printer. Be careful to give the correct make and model. In some cases, print jobs may fail to appear even with a similar make and model of printer.

Some users may need extra permissions in their domain to install a printer driver.

Double-conversion

Windows printer drivers output data intended for the printer itself. Similarly, UNIX printers can use "filters" to convert print jobs to printable data, in much the same way. When printing using VisionFS, it's important that the UNIX host *doesn't* perform any filtering. Otherwise, the print output may not appear as expected.

If you see, for example, a PostScript file printed as text, then your UNIX printer is filtering raw printer data unnecessarily.

By default, the VisionFS print command for shared printers tries to use "raw" mode, which bypasses any filters you might have for that printer. However, not all systems support filter bypassing.

Watch out for filters that identify a PostScript print job by looking for "%!" as the first two characters in the job: Windows often puts a CTRL+D character, or other data, before the PostScript.

Feedback from printers

Some printers return information about their current status, for example that they're out of paper. Unfortunately, this information is not returned to UNIX, and so doesn't appear in Windows when printing using VisionFS.

SEE ALSO

"Using shared printers for custom output", in Chapter 3, "The Possibilities".

Other problems

If you're having problems printing using VisionFS, try printing to a file from Windows. Then you can copy the resulting file to your UNIX host, and try different variations of print command from a shell prompt. When you find one that works, you can set up the shared printer to use that print command.

Networking

PC networking commands

SEE ALSO

"Making sure PCs can access VisionFS", earlier in this chapter.

Windows and MS-DOS contain some useful tools for mapping drives, and changing and displaying a PC's network settings. You may find the following commands helpful:

- **net**
- **nbtstat**
- **winipcfg** on Windows 95 and 98
- **ipconfig /all** on other versions of Windows

In each case, you can use the command-line option **/?** to get help on the command. For example:

- To find out all the NetBIOS names a computer has registered, type **nbtstat -a** *netbiosname* or **nbtstat -A** *ipaddress*
- Use **net view** \server to show the shares on a server

Names

In networking, a computer may have many different names, each used in particular circumstances. This section summarizes the types of name a computer may have, and where each type fits with the other types.

A computer may have:

- Exactly one hostname.
- Zero or more network interfaces (for example, ethernet adapters), each with a single hardware address. Typically, there'll be a "loopback"

interface (a software interface local to the computer, used to do networking to itself), and a physical network card (for networking with other computers).

- Zero or more IP addresses, each mapping to a single hardware address. Typically, there'll only be a single IP address.
- Zero or more DNS names, each mapping to one or more IP address. Typically, there'll only be a single DNS name.

VisionFS will work as expected, no matter how many DNS names, IP addresses and network interfaces you have on your UNIX host.

Additionally, an application may have zero or more NetBIOS names. (NetBIOS names belong to applications, not computers, though typically there's only a single NetBIOS application per computer.)

VisionFS advertises all NetBIOS names over the network interfaces you specify on the Network tab of Server properties: either through network broadcasts, or by registering with a WINS server. When other computers try to access VisionFS, the NetBIOS name will be resolved to the relevant IP address (as VisionFS uses NetBIOS over TCP/IP).

A typical UNIX host might use its different names in the following way:

- A hostname **jelly**.
- An IP address, 192.168.5.44, that maps to a single ethernet address corresponding to the UNIX host's only ethernet card.
- A DNS name, **jelly.sales.indigo-insurance.com**, that maps to the single IP address.

The UNIX host may also be running a single NetBIOS application, with name **jelly**, that maps onto the single IP address.

Working with your existing software

In this section, we'll explain how VisionFS can work alongside your networking software.

PC TCP/IP stacks

PCs and the VisionFS server communicate using the SMB protocol, which runs over NetBIOS.

Technically, NetBIOS can run over multiple network transports, for example NetBEUI, IPX/SPX and TCP/IP. In fact, any number of transports could be used simultaneously.

To connect to a VisionFS server, a PC requires a TCP/IP stack that supports the NetBIOS protocol. All versions of Windows supported by VisionFS are supplied with compatible TCP/IP stacks.

See Also
"Installing Microsoft TCP/IP on PCs", earlier in this chapter.

TCP/IP stacks from other vendors will work if they support the NetBIOS interface. You may find that although a particular PC can communicate with another PC, it can't connect to a VisionFS server. This may be because the PCs are using NetBIOS over NetBEUI or another network transport. In this case, the TCP/IP stack does not fully support the NetBIOS interface.

Other file and printer sharing programs or NBT applications

VisionFS will coexist with other file and printer sharing programs on UNIX, such as Samba, without customization, as long as those programs don't conflict with VisionFS as the primary NetBIOS over TCP/IP (NBT) application.

You can set up VisionFS to work alongside other NBT applications, by designating one as the primary and the others as secondaries.

On SCO OpenServer Release 5, you can't use VisionFS if you're running SCO NetBIOS over TCP/IP, for example with SCO Advanced File and Print Server (AFPS) or LAN Manager Client (**lmc**). This is because SCO NetBIOS over TCP/IP conflicts with the NetBIOS over TCP/IP used by VisionFS.

SEE ALSO

"Allowing multiple NetBIOS applications", in Chapter 3, "The Possibilities".

To use VisionFS alongside AFPS or **lmc**, you can:

- Remove SCO NetBIOS over TCP/IP from your UNIX host before running VisionFS. You can do this using the Network Configuration Manager. You can still use AFPS or **lmc** over NetBEUI.
- Stop SCO NetBIOS over TCP/IP using the command **/etc/netbios stop**. To make sure SCO NetBIOS over TCP/IP doesn't start when the UNIX host reboots, remove or edit the **/etc/rc2.d/S86netbios** UNIX boot script.

PCs can run more than one file and printer sharing client at the same time.

Performance

A number of factors may affect the apparent performance of the VisionFS server.

- The theoretical maximum bandwidth for standard ethernet traffic is 1Mbyte/second (10Mbps).
- In practice, the real speed is dependent on the speed of the client and the speed of the UNIX file system. If NFS is also involved (for example, a shared folder might access a directory mounted over NFS) speeds will reduce further.
- VisionFS does not buffer data. However, both UNIX and Windows do.

Connections per process

Each VisionFS process on the UNIX host can handle a number of connections from PCs, up to a maximum. Once the maximum is exceeded, a new process starts. Only one connection can be attended to in each process at a time.

See Also

"Optimizing process usage", in the Help index.

By changing the maximum number of connections per process, you can trade off response time against resource usage. More connections per process makes more efficient use of server resources, but may result in decreased performance for users. Fewer connections per process increases performance for users, but uses server resources less efficiently.

Locking

See Also

"VisionFS file locking", earlier in this chapter.

Two changes can improve the performance of the VisionFS server:

- If a share gives access to a CD-ROM drive then no files will ever be modified, so you can turn off locking completely for that share.
- If you are sure that files in a share won't be edited by UNIX users as well as PC users, then turn on opportunistic locking in that share.

International characters

Windows is available localized into multiple languages. Your users may want to name files using characters not found in English, for example characters with accents. If not, you can skip this section.

VisionFS supports Unicode, as do newer versions of Windows. Typically, UNIX hosts and Windows for Workgroups PCs support a limited number of character encodings, but not Unicode.

You can configure VisionFS to use particular character encodings when talking to the UNIX host and to Windows for Workgroups PCs. This helps to ensure that filenames appear the same whether you view them from Windows or UNIX.

To set the encodings, start the Profile Editor, open Server properties and click the Advanced tab.

Index