Snap! Server Administrator's Guide

Meridian Data, Inc.
5615 Scotts Valley Drive
Scotts Valley, California
95066

Copyright Notice

Trademarks

Revisions

Meridian Data, Inc. reserves the right to revise this publication and to make changes in the content hereof without the obligation of Meridian Data, Inc. to notify any person of such revision or changes.

Part Number: 70990001-001, Rev. A

Meridian’s No-Nonsense Warranty for Snap! Server

Meridian Data believes the Snap! Server to be the most reliable product of its kind available today. However, if for any reason you are unhappy with your Snap! Server during the first thirty (30) days following purchase, you may return it to Meridian for a full refund of your purchase price.

If your Snap! Server fails during the first three (3) years following purchase because of defects in materials or workmanship, Meridian Data, Inc. will repair or replace it (at Meridian’s option) at no charge.

There are, of course, some limitations to this Warranty. First, you must be the original end-user purchaser of the product and be able to provide proof of purchase showing the date and place of purchase if you submit a Warranty claim. Second, you must contact Meridian Data as indicated below, and upon request, ship the defective product to Meridian Data at your expense. Third, the product failure must not be the result of product abuse on your part, such as dropping the Snap! Server, using incorrect electrical current, or getting the Snap! Server wet.

There are also some legal limitations to this Warranty:

EXCEPT AS SET FORTH ABOVE, WITH RESPECT TO THE SNAP! SERVER, MERIDIAN DATA, INC. MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY AND DISCLAIMS ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

IN NO EVENT SHALL MERIDIAN DATA, INC. BE LIABLE FOR COST OF PROCUREMENT OF SUBSTITUTE HARDWARE, SOFTWARE, OR SERVICES, LOST PROFITS, OR ANY SPECIAL, INDIRECT, CONSEQUENTIAL OR INCIDENTAL DAMAGES, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY ARISING IN ANY WAY OUT OF THIS AGREEMENT OR THE SNAP! SERVER. THIS LIMITATION SHALL APPLY EVEN IF MERIDIAN DATA, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY PROVIDED HEREIN.

This Warranty will be governed in accordance with the laws of the State of California and the United States of America.

To obtain Warranty service for your Snap! Server, please contact Meridian Data Customer Service at:

Customer Service
Meridian Data, Inc.
5615 Scotts Valley Dr.
Scotts Valley, CA 95066
USA

Phone (within North America):	888-338-SNAP (7627)
Phone (outside North America):	918-610-2781

E-mail: snapsupport@meridian-data.com

END-USER LICENSE AGREEMENT FOR USE OF SNAP! SERVER AND RELATED INSTALLATION UTILITIES

1. SNAP! IP™ AND SNAP! UPDATE™ ("Installation Utilities") AND THE SYSTEM SOFTWARE EMBEDDED IN THE SNAP! SERVER™ ("Embedded Software") ARE PROPRIETARY COMPUTER SOFTWARE BELONGING TO MERIDIAN DATA, INC. ("MDI"). UNITED STATES COPYRIGHT AND OTHER FEDERAL AND STATE LAWS PROTECT THE INSTALLATION UTILITIES AND EMBEDDED SOFTWARE.

2. USE OF THE SNAP! SERVER, OR THE INSTALLATION UTILITIES IMPLY AGREEMENT TO THE TERMS AND CONDITIONS OF THIS LICENSE. BY USING THE INSTALLATION UTILITIES OR THE SNAP! SERVER YOU ARE ENTERING INTO A BINDING CONTRACT WITH MDI. IF YOU DO NOT AGREE WITH THESE TERMS AND CONDITIONS, YOU SHOULD PROMPTLY RETURN THIS ENTIRE PACKAGE TO THE COMPANY FROM WHICH YOU PURCHASED IT FOR A FULL REFUND.

3. Ownership and Copyright. The Snap! Server Installation Utilities and Embedded Software are licensed, not sold, to you for use only under the terms of this Agreement. MDI reserves any rights not expressly granted to you. Copying of the Software, unless specifically authorized in writing by MDI, is prohibited by law. You may not use, copy, modify, sell, lease, sublease or otherwise transfer the Installation Utilities or Embedded Software, or any copy or modification, in whole or in part, except as expressly provided in this Agreement.

4. License. You are given a non-exclusive license to use the Installation Utilities and Embedded Software in conjunction with a Snap! Server, copy the Installation Utilities for archival and backup purposes only, and/or transfer your Snap! Server and copies of the Installation Utilities and the accompanying documentation to a third party provided that you provide MDI written notice of the transfer within 30 days.

5. Reproduction of Proprietary Notices. Copies of the Installation Utilities must be labeled with the MDI copyright notice and other proprietary legends found on the original media.

6. Protection of Trade Secrets. The Software contains trade secrets, and in order to protect them you may not decompile, reverse engineer, disassemble, or otherwise reduce the Installation Utilities or Embedded Software to a human perceivable form.

7. Termination. This license will automatically terminate without notice from MDI if you fail to comply with any term or condition of this Agreement. You agree, upon termination, to return the Installation Utilities and the Snap! Server, along with any backups or other copies in your possession.

8. Export Laws. The Installation Utilities and/or Embedded Software may require a license from the U.S. Government before it may be exported. You agree to ascertain necessary licensing procedures and obtain required licenses before exporting either. You also agree to indemnify MDI and assume all financial responsibility for any losses it may suffer if you do not comply with this paragraph.

9. Government End-Users. The Installation Utilities, Embedded Software and accompanying documentation are deemed to be “commercial computer software” and “commercial computer software documentation,” respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use modification, reproduction release, performance, display or disclosure of the Installation Utilities or Embedded Software and accompanying documentation by the U.S. Government shall be governed solely by the terms of this Agreement and shall be prohibited except as expressly permitted by the terms of this Agreement.

10. Waiver. No delay or failure of MDI to exercise any right under this Agreement, nor any partial exercise thereof, shall be deemed to constitute a waiver of any rights granted hereunder or at law.

11. Unlawful Provision(s). If any provision of the Agreement is held to be unenforceable for any reason, all other provisions of this Agreement shall nevertheless be deemed valid and enforceable to the full extent possible.

12. Applicable Law. This Agreement will be governed by the laws of the State of California and the United States, including U.S. Copyright laws.

13. Entire Agreement. This Agreement constitutes the sole and exclusive agreement between the parties concerning the subject matter hereof.

14. Manufacturer. Meridian Data, Inc., 5615 Scotts Valley Drive, Scotts Valley, CA 95066, Telephone: 408-438-3100.

Contents

CHAPTER 1 Getting Started

The Snap! Server™ is a unique product that provides the quickest and easiest way to add additional hard disk storage for your network users. With the Snap! Server, you can add additional network storage and bypass the time-consuming processes of shutting down your file server, formatting the hard drives, and restarting the file server. You can install a Snap! Server in minutes.

While a traditional file server supports only one file sharing protocol, the Snap! Server simultaneously emulates the file sharing protocols of the most commonly used file servers available: Windows NT 4.0, Novell NetWare, NFS 2.0, and HTTP 1.0.

This chapter tells you how to:

- Use the *Snap! Server Administrator's Guide*
- Quickly register and set up your Snap! Server
- Contact Meridian Data Technical Support if you have questions

Using Snap! Server Administrator's Guide

Snap! Server Administrator's Guide is designed to help you quickly find the information you need. The following paragraphs explain how to use the chapters in this guide.

- Read Chapter 1 first to learn how to correctly unpack and set up the Snap! Server.
- If your site uses either Microsoft networking with the NetBEUI protocol or Novell networking, and you don't want to change any of Snap! Server's defaults, you can successfully use your Snap! Server without performing other tasks described in this guide. For a list of the server's default values, see Appendix B, "Snap! Server Default Configuration Parameters."
- If you need help connecting to your server, read Chapter 2.
- If your network uses Microsoft networking over TCP/IP, or NFS, or you want to modify Snap! Server's default configuration, then the Snap! Server must be assigned an Internet Protocol (IP) address. Read Chapter 3 for information about managing IP addresses.

- If you want to change your Snap! Server's default configuration or restrict access to your Snap! Server, you'll need to use Quick Configure. Read Chapter 4, "Using Snap! Server's Quick Configure." The HTML-based Quick Configure will guide you through configuration steps to help you specify key configuration parameters.
- If you are a system or network administrator who wants to access standard configuration utilities, read Chapter 5, "Server Administration."
- If your configuration isn't correct or you've encountered problems, read Chapter 6 for troubleshooting advice.
- Read the appendixes for technical information.

Conventions

The following table explains the conventions that *Snap! Server Administrator's Guide* uses.

This text	Looks like this
Messages that are displayed on your screen	`On-screen messages`
Commands or text that you must type	**Text that you type**
Variable values in commands and text that you type. (Note: You need to replace the variable with a value that is appropriate to your environment.)	***Values that you replace***
File, path, and share names	*Filename*

This icon	Means
IMPORTANT	Reader take notice of important information.
ADMINISTRATOR	System Administrator take notice of information intended specifically for you.
NOTE	Reader take note. Notes contain helpful suggestions.

Unpacking and Setting Up Your Snap! Server

You can set up your Snap! Server in a few easy steps.

1. Unpack the server and check the package contents (described on page 3).
2. Connect the Ethernet cable and power cord (described on page 4).
3. Verify LED status (described on page 5).

Checking the Package Contents

Check that your Snap! Server package contains each of the following items:

- Snap! Server
- Power cord
- RJ-45 Ethernet cable
- *Snap! Server Quick Start Guide*
- *Snap! Server Administrator's Guide*
- Snap! Server *Release Notes*
- Warranty registration card (attached to the manual's back cover)
- Snap! Utilities software CD-ROM containing the Snap! IP™ and Snap! Update™ utility programs

If any of these items is missing, notify your authorized reseller.

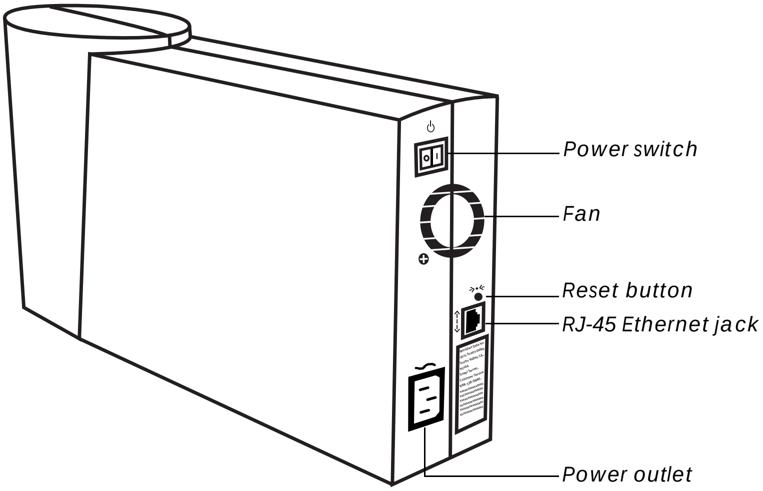
Registering Your Server

Register to receive Snap! Server product information bulletins. As a registered Snap! Server user, you will receive information on new product developments and special promotions as soon as they become available.

To save time, register online at: **http://www.snapserver.com/support**
Or, you can register by returning the registration card in your Snap! Server manual. When registering, be sure to include your server's serial number (for example, 20020), which you'll find on the back of the server.

Connecting the Cable and Power Cord

The cable for connecting the Snap! Server to your network is provided in your package. The following illustration of the Snap! Server's rear panel shows where to locate the RJ-45 jack for connecting the Ethernet cable.

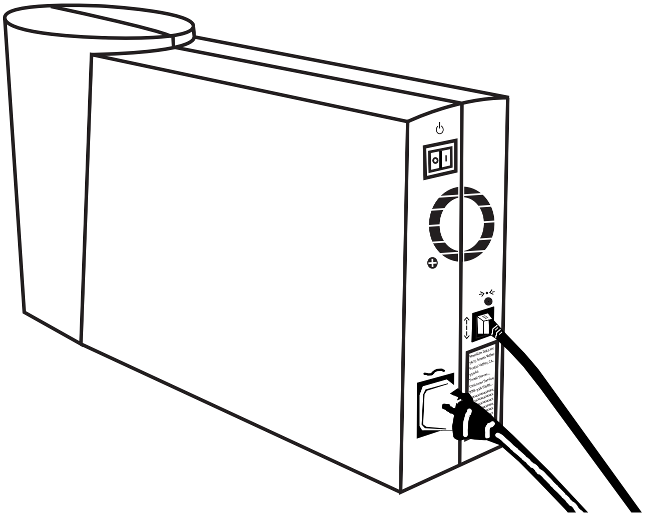


Follow these steps to connect the network cable and power cord to your Snap! Server.

1. Before you connect anything, make sure that the Snap! Server is turned off.
2. Plug the end of the Ethernet cable into the RJ-45 jack on the Snap! Server's rear panel.
3. Connect the other end of the cable to an active 10BaseT or 100BaseT hub port.

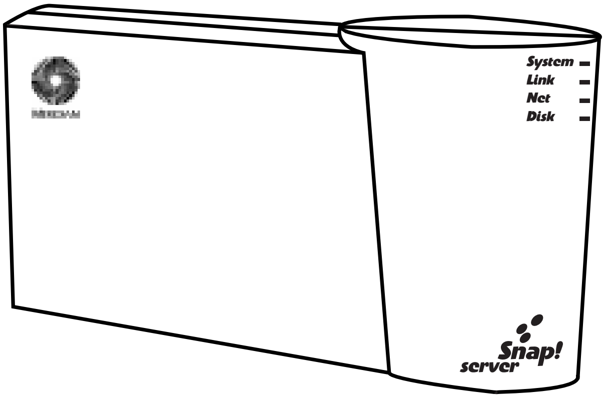
4. Connect the power cord from your Snap! Server to a 110V/220V power outlet.

   Your Snap! Server will automatically detect the correct 110/220 voltage setting and switch its internal power supply.



Verifying the Status of the LED Indicators

The Snap! Server has four LED status indicators which are located on the front of the unit.



The following table describes the LED status indicators. For more detailed information about the Snap! Server's LEDs, see Chapter 6, "Troubleshooting."

LED	Color	State	Indicates
System	Green	Blinking steadily	Server is operating
Link	Green	On	Server is properly connected to a 10BaseT or 100BaseT hub
Net	Amber	Blinking	Network activity
Disk	Amber	Blinking	Disk transfer in progress

To verify that your Snap! Server is operating correctly:

1. Turn on the power switch and wait about 30 seconds while the server boots. When the Disk LED stops blinking, the boot is complete.
2. Check that the System LED is blinking.
3. Check that the Link LED is on.

IMPORTANT

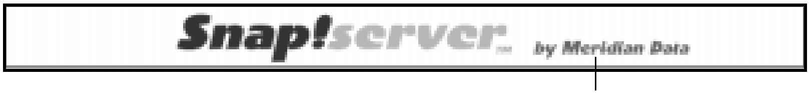
Whenever you turn *off* the Snap! Server's power, you must wait for all of the LEDs to turn off before you turn the server on again. After you turn off the Snap! Server, the LEDs will remain lit while the server completes its shutdown. If you don't turn off the server correctly, you may lose data.

Contacting Meridian Data Technical Support

Contact Meridian Data Technical Support if you have questions or comments about your Snap! Server or need help resolving a problem that isn't covered in Chapter 6, "Troubleshooting." Please have the following information available or include it in your message to Technical Support:

- Network vendor and version you are using
- Client operating system and version
- Snap! Server model and serial number (located on the back of the server)

- Snap! Server software, BIOS, and hardware version numbers. You can obtain this information by clicking the Meridian Data hyperlink at the top of the Snap! Server HTML pages described in Chapter 4 and Chapter 5.



Click here.

Providing this information helps Technical Support diagnose and solve your problem more quickly.

Electronic Services and Telephone Numbers

You can contact Technical Support by E-mail, the Internet, FAX machine, and telephone.

E-Mail

Send E-mail to Meridian Data Technical Support at the following Internet E-mail address: **snapsupport@meridian-data.com**

World Wide Web

Visit the Snap! Server home page on the World Wide Web at: **http://www.snapserver.com** for company and product information. You can also contact Technical Support from the home page.

FAX

Send a FAX to Meridian Data Technical Support at: **(918) 628-3222**

Telephone Numbers

In North America, call Meridian Data Technical Support toll-free at: **1-888-338-SNAP** (338-7627)

Outside North America, call Meridian Data Technical Support at: **(918) 610-2781**

CHAPTER 2 Connecting to the Snap! Server

In most cases, after connecting the Snap! Server to the network, you can successfully use the server in its default configuration without making changes. The Snap! Server appears on your network in the same way as any file server. You can make directories and store files.

The Snap! Server's default configuration is suitable for you if the following apply:

- You are using either Microsoft networking with the NetBEUI protocol, Novell networking, or TCP/IP with DHCP for automatic IP address assignment.
- You want the fastest, easiest configuration.
- You don't need to modify any of the Snap! Server's default configuration parameters (listed in Appendix B).

If you decide to change the default configuration, you'll need to assign an IP address to the server (as described in Chapter 3) and then use the Snap! Server's Quick Configure (as described in Chapter 4).

This chapter tells you how to connect to your Snap! Server from computers running:

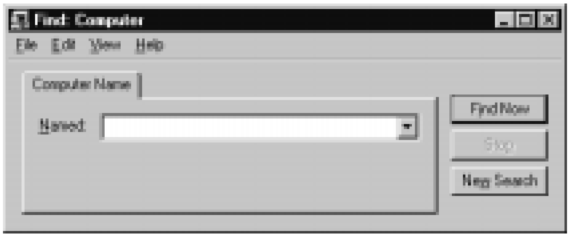
- Microsoft Windows NT 3.51 or 4.0
- Microsoft Windows 95
- Microsoft Windows for Workgroups 3.11
- Microsoft Windows 3.1
- DOS/LANMAN
- DOS/NetWare
- NFS/UNIX

Connecting from Microsoft Windows NT 4.0 and Windows 95

You can use either Find Computer or Network Neighborhood to locate the Snap! Server on your network. The server's default name is SNAP*nnnnn*, where *nnnnn* is the serial number on the back of the server. For example, SNAP20020.

To use Find Computer:

1. From the Start menu, choose Find and then choose Computer.



2. In the Named text box in the dialog box that appears, type:
   SNAP*nnnnn*

   replacing *nnnnn* with your Snap! Server serial number.

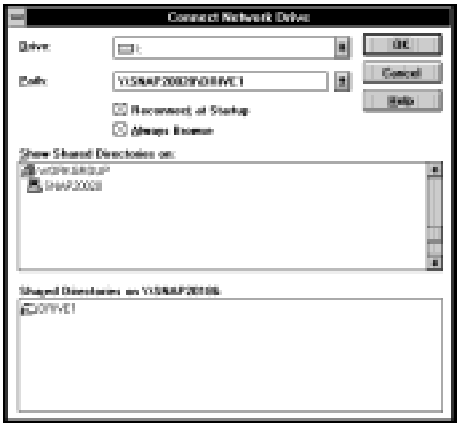
To use Network Neighborhood:

- Double-click Network Neighborhood and then locate the Snap! Server in the workgroup named WORKGROUP.

Connecting from Windows for Workgroups 3.11 and Windows NT 3.51

To connect Windows for Workgroups clients to the Snap! Server:

1. Open File Manager.
2. Choose the File menu’s Connect Network Drive command.



Connect Network Drive

Drive: I:

Path: \\SNAP20020\DRIVE1

☒ Reconnect at Startup

☐ Always Browse

Show Shared Directories on:

\\WORKGROUP

SNAP20020

Shared Directories on \\SNAP20020:

DRIVE1

3. In the dialog box that appears, use the Browse feature to locate your Snap! Server’s default name (for example, SNAP20020) within the workgroup named WORKGROUP.
4. If the server’s name doesn’t appear, then type your Snap! Server’s default name (SNAP*nnnnn*) in the Name field.

   The numbers in the server’s default name come from the Snap! Server’s serial number, which is on a label on the back of your server.

Connecting from Windows 3.1

Because Windows 3.1 does not directly support networking commands, use DOS networking as described in “Connecting from DOS-LANMAN Client” on page 12 and “Connecting from DOS-Novell VLM/NETX Client” on page 12.

Connecting from DOS-LANMAN Client

To connect a DOS-LANMAN client to the Snap! Server, follow this procedure.

1. Load the Microsoft LANMAN (LAN Manager) client software.
2. At the DOS prompt, type the following:

   net use *[drive letter]*: \\\\Snap*nnnnn*\Drive1

   replacing *[drive letter]* with an unused drive letter, and replacing *nnnnn* with your Snap! Server's serial number.

Connecting from DOS-Novell VLM/NETX Client

To connect a DOS-Novell VLM or NETX client to the Snap! Server, follow this procedure.

1. Load the Novell VLM or NETX client software.
2. Log into a Novell server on your network.
3. At the DOS prompt, type the following:

   map *[drive letter]*: = Snap*nnnnn*/Drive1:

   replacing *[drive letter]* with an unused drive letter, and replacing *nnnnn* with your Snap! Server's serial number.

Connecting from NFS/UNIX

To connect to the Snap! Server from UNIX via NFS, follow this procedure.

1. Verify the availability of the default shares and mount the share you prefer.
2. Use the UNIX showmount command to view the mount points that Snap! Server exports. For example, type:

   showmount -e Snap*nnnnn*

   When typing the command, do one of the following:

   - Replace *nnnnn* with the Snap! Server's serial number; for example, 20020.
   - Or, replace *Snapnnnnn* with the name that has been assigned to the Snap! Server. This will be either the server's default name (for example, SNAP20020) or the current name if the server was renamed.

   The showmount command syntax might differ depending on your version of UNIX.

3. Mount one of the Snap! Server’s mount points as you would normally mount any other file server’s mount points.

   By default, the Snap! Server exports the /Drive1 mount point. If your Snap! Server contains two hard drives, an additional default mount point, /Drive2, is available.

CHAPTER 3 *Managing IP Addresses*

An Internet Protocol (IP) address must be assigned to your Snap! Server if you are planning to do any of the following:

- Use Snap! Server’s HTML-based configuration pages to modify your server’s default settings.
- Permit network users to use their browsers to browse the Snap! Server’s shares.
- Use Microsoft networking over the TCP/IP protocol.
- Use Network File System (NFS).

If your network cannot resolve a TCP/IP name into a TCP/IP address, you must know your Snap! Server’s IP address in order to access it using either Microsoft networking or the Snap! Server’s HTTP (HTML) interface. Meridian Data recommends using the Snap! IP utility program to determine if your Snap! Server has an IP address, and then to determine the actual IP address. If there are any Snap! Servers on your network that have not been assigned an IP address, you can also use Snap! IP to assign IP addresses as well as the other TCP/IP parameters.

This chapter explains how to use Snap! IP to manage your Snap! Servers’ IP addresses.

Installing and Starting Snap! IP

To use Snap! IP, you’ll need:

- A computer that is running under the Microsoft Windows for Workgroups 3.11, Windows 95, or Windows NT operating system with a TCP/IP stack installed and properly configured.
- The Snap! Utilities CD-ROM, which is shipped with your server and contains the Snap! IP program.

NOTE If you don’t have a CD-ROM drive or you’ve misplaced the Utilities CD-ROM, you can download the Snap! IP executable from Meridian Data’s Snap! Server Web site at this address: **http://www.snapserver.com/download**

Installing the Snap! Utilities

To install Snap! IP from the Utilities CD-ROM, follow this procedure.

1. Put the Snap! Utilities CD-ROM into the CD-ROM drive.
2. Open one of the following:
    - Windows Explorer (Windows 95 or NT 4.0)
    - File Manager (Windows for Workgroups 3.11 or NT 3.51)
3. Locate and click on the CD-ROM drive where you put the Snap! Utilities CD.
4. Locate and double-click the setup.exe program.
5. Follow the instructions on your screen, and provide the information requested.

    You'll need to specify the destination path for the directory where you want to install the Snap! Utilities. The default destination is: c:\Meridian\Snap

To install Snap! IP using the file you downloaded from Meridian Data's Snap! Server Web site, follow this procedure.

1. Open one of the following:
    - Windows Explorer (Windows 95 or NT 4.0)
    - File Manager (Windows for Workgroups 3.11 or NT 3.51)
2. Locate and double-click the file that you downloaded.

    This file is usually named *WEBUTILS.EXE*.
3. Follow the instructions on your screen, and provide the information requested.

    You'll need to specify the destination path for the directory where you want to install the Snap! Utilities. The default destination is: c:\Meridian\Snap

Starting Snap! IP

When you have successfully installed the utilities, follow these steps to start the Snap! IP program.

1. If you are running Windows 95 or Windows NT 4.0, do the following:

    a. Click Start on the task bar to open the Start menu.

    b. Locate and click the Snap! Utilities folder.

    c. Click the Snap! IP icon IP.

    d. Skip to step 3 of this procedure.

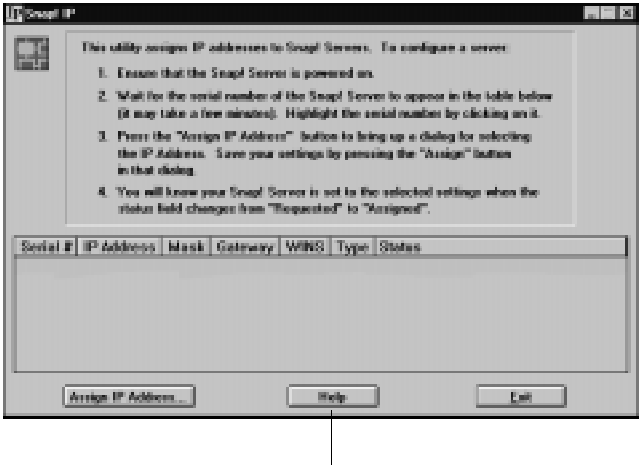
2. If you are running Windows for Workgroups 3.11 or Windows NT 3.51, do the following:

   a. Open the Program Manager.

   b. Double-click the Snap! Utilities folder.

   c. Double-click the Snap! IP icon IP.

3. The Snap! IP window appears.



This utility assigns IP addresses to Snap! Servers. To configure a server:

1. Ensure that the Snap! Server is powered on.
2. Wait for the serial number of the Snap! Server to appear in the table below (it may take a few minutes). Highlight the serial number by clicking on it.
3. Press the "Assign IP Address" button to bring up a dialog for selecting the IP Address. Save your settings by pressing the "Assign" button in that dialog.
4. You will know your Snap! Server is set to the selected settings when the status field changes from "Requested" to "Assigned".

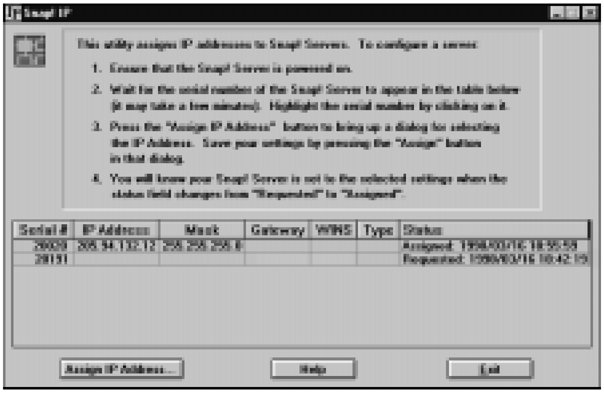
Serial #	IP Address	Mask	Gateway	WINS	Type	Status

Click Help for online information about Snap! IP and how to use it.

4. Verify that the Snap! Server is turned on and connected to the network.

The Snap! IP program will search the network for Snap! Servers. When it finds servers, it displays their serial numbers and current TCP/IP information in the Snap! IP window. This may take several minutes.

The Snap! IP window in the following illustration shows information for two Snap! Servers it found on the network.



This utility assigns IP addresses to Snap! Servers. To configure a server:

1. Ensure that the Snap! Server is powered on.
2. Wait for the serial number of the Snap! Server to appear in the table below (it may take a few minutes). Highlight the serial number by clicking on it.
3. Press the "Assign IP Address" button to bring up a dialog for selecting the IP Address. Save your settings by pressing the "Assign" button in that dialog.
4. You will know your Snap! Server is set to the selected settings when the status field changes from "Requested" to "Assigned".

Serial #	IP Address	Mask	Gateway	WINS	Type	Status
20020	205.94.132.12	255.255.255.0				Assigned: 1998/03/16 18:55:59
20151						Requested: 1998/03/16 10:42:19

The Snap! Server with serial number 20020 has already been assigned IP address 205.94.132.12. This address can be used to access that Snap! Server's HTML-based configuration pages by entering one of the following URLs.

Entering this URL	Jumps to these pages
http://205.94.132.12/quickconfig	Snap! Server Quick Configure (described in Chapter 4)
http://205.94.132.12/config	Snap! Server Administration (described in Chapter 5)

Assigning an IP Address

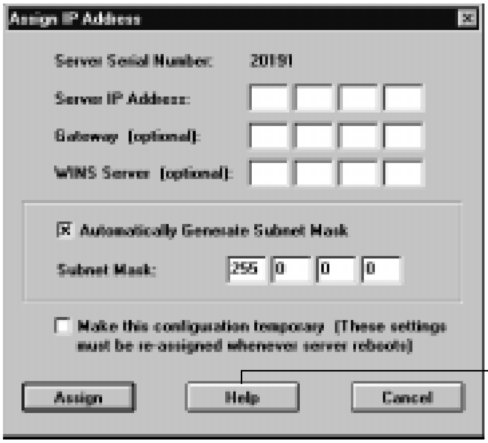
You can only assign an IP address to a Snap! Server that doesn't already have one. If the server already has an IP address and you want to change that address or any of the server's TCP/IP parameters, you must do so as described in "Changing the TCP/IP Address" on page 80. If you can't get to the Snap! Server Administration menu because of an error in the server's TCP/IP parameters, you must use the server's Reset button to clear the invalid TCP/IP parameters as described in "Diagnostic Modes" on page 105.

To assign an IP address to a Snap! Server that doesn't already have one, follow this procedure.

1. In the Snap! IP window, select a serial number that does not have an IP address—for example, serial number 20191 in the illustration on page 18.

   Notice that the IP Address field is empty and the Status field shows `Requested`.

2. Click the Assign IP Address button to open the Assign IP Address dialog box. (You can also double-click the serial number to open the dialog box.)



Assign IP Address

Server Serial Number: 20191

Server IP Address:

Gateway (optional):

WINS Server (optional):

☒ Automatically Generate Subnet Mask

Subnet Mask: 255 0 0 0

□ Make this configuration temporary (These settings must be re-assigned whenever server reboots)

Click Help for online information about using this dialog box.

3. In the fields provided, type the server IP address and optionally, the default gateway and WINS Server IP address.

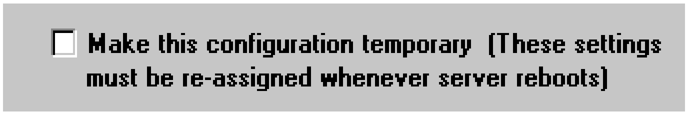
   Use the Tab key to navigate within the fields. You don't need to type the decimals in addresses.

4. By default, Snap! IP automatically generates the subnet mask.

   If you don't want this option, uncheck the box. When the box is not checked, you can type a specific subnet mask in the fields provided.

5. By default, Snap! IP assigns a permanent address.

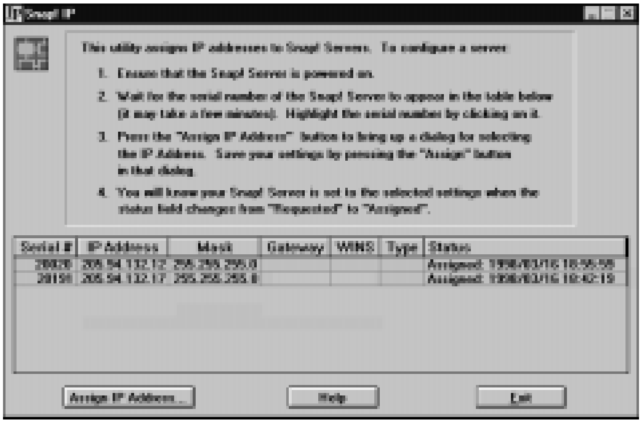
   If you don't want a permanent address, check this box to assign a temporary address (which will be lost when you reboot the server).



□ Make this configuration temporary (These settings must be re-assigned whenever server reboots)

   A temporary address might be useful if the server will be moved from network to network, or there is a small pool of network addresses to be shared among resources that use the network infrequently.

6. Click Assign to save the settings you specified.
7. Wait until the Status message in the Snap! IP window changes from `Requested` or `Assigning` to `Assigned`.



This utility assigns IP addresses to Snap! Servers. To configure a server:

1. Ensure that the Snap! Server is powered on.
2. Wait for the serial number of the Snap! Server to appear in the table below (it may take a few minutes). Highlight the serial number by clicking on it.
3. Press the "Assign IP Address" button to bring up a dialog for selecting the IP Address. Save your settings by pressing the "Assign" button in that dialog.
4. You will know your Snap! Server is set to the selected settings when the status field changes from "Requested" to "Assigned".

Serial #	IP Address	Mask	Gateway	WINS	Type	Status
20020	206.54.132.12	255.255.255.0				Assigned: 1998/03/16 18:56:58
20150	206.54.132.17	255.255.255.0				Assigned: 1998/03/16 18:42:15

8. Click Exit to quit the Snap! IP program.

CHAPTER 4 Using Snap! Server's Quick Configure

Quick Configure is an HTML-based configuration tool designed to guide you through a quick and easy way to configure your Snap! Server.

Use Quick Configure if you:

- Want to modify the server's default configuration (defaults are listed in Appendix B)
- Want to limit Snap! Server access only to explicitly authorized users (By default, the Snap! Server grants access to *any* user on your network.)

Snap! Server administrators should use Quick Configure first. To specify configuration parameters that are not available through the Quick Configure, use the configuration tools described in Chapter 5, "Server Administration."

Snap! Server's configuration tools support these Web browsers:

- Microsoft Internet Explorer 2.0 or greater
- Netscape Navigator 2.0 or greater

NOTE For optimum viewing, Meridian Data recommends using a display monitor with at least 800 x 600 resolution that can display at least 256 colors. You may also want to change your browser's Display Properties font size setting to small fonts.

This chapter explains how to:

- Use your Web browser to connect to your Snap! Server.
- Start Quick Configure.
- Specify key configuration parameters.

Accessing Snap! Server's Quick Configure

Once the IP address has been assigned, you can access Quick Configure in the following manner. (For information about IP address assignment, see Chapter 3.)

1. Open the browser that you want to use—either Microsoft Internet Explorer 2.0 or greater, or Netscape Navigator 2.0 or greater.
2. In the address box, enter one of the following Uniform Resource Locators (URLs).

   - If either a DNS or a Windows Internet Name Server (WINS) is available on your network and successfully translates the Snap! Server's name into an IP address, you can enter this URL:

     http://*ServerName*/quickconfig

     replacing *ServerName* with your Snap! Server's name.

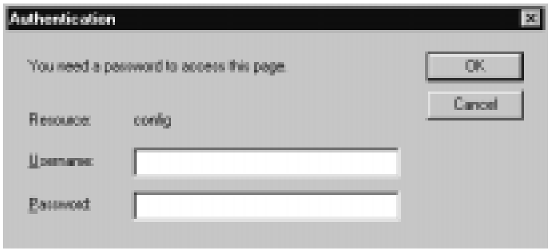
     Your Snap! Server's default name is SNAP*nnnnn*, where *nnnnn* represents the server's serial number; for example, SNAP20020.

   - Otherwise, enter this URL:

     http://*IP_address*/quickconfig

     replacing *IP_address* with your Snap! Server's IP address. For example, http://192.168.1.142/quickconfig.

   The Authentication dialog box appears.



Authentication

You need a password to access this page.

Resource: config

Username:

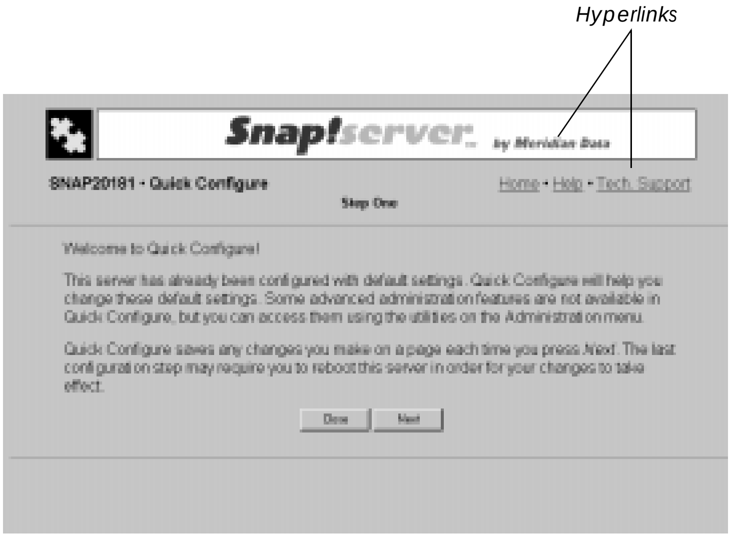
Password:

3. In the Username field, type:
   Administrator
   and then click OK.

   By default, no password is required. Meridian Data recommends that you change the Administrator's password during the Quick Configure (as described in "Changing the Administrator Password" on page 24).

The Snap! Server Quick Configure welcome page appears.

Using Quick Configure


Hyperlinks

SNAP20181 • Quick Configure

Step One

Welcome to Quick Configure!

This server has already been configured with default settings. Quick Configure will help you change these default settings. Some advanced administration features are not available in Quick Configure, but you can access them using the utilities on the Administration menu.

Quick Configure saves any changes you make on a page each time you press *Next*. The last configuration step may require you to reboot this server in order for your changes to take effect.

The following paragraphs describe how to use the hyperlinks at the top of Quick Configure pages.

- To view the Snap! Server information page, click Meridian Data in the title image.
- To go to the Snap! Server default home page, click Home.
- To get online help, click Help.
- To communicate with Meridian Data Technical Support, click Tech Support. To use this hyperlink, you must have access to the Internet.

Quick Configure will guide you from start to finish through a number of steps that help you:

- Configure server properties (date, time, and name).
- Verify the server's IP address, default gateway, subnet mask, and WINS address.

- Specify which network protocols to use and which not to use, and configure enabled protocol settings.
- Configure additional security if you want to restrict access to the server.

To navigate between pages, click Next to continue (advance to the next page or configuration step) or Prev to return to the previous page or step. Use the Tab key to navigate between fields on a page.

ADMINISTRATOR

The settings that you specify in each step are *saved* as soon as you click Next to advance to the next page. Clicking Prev does *not* undo changes you saved by clicking Next.

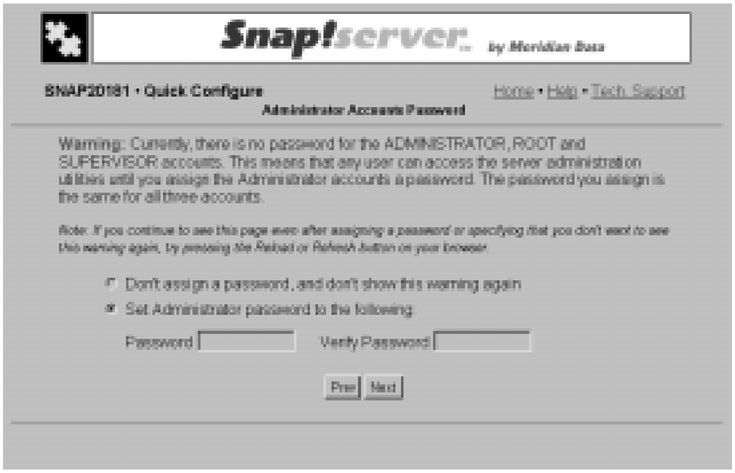
IMPORTANT

To avoid problems with the Snap! Server, once you start modifying the server's configuration, you should proceed to the end of the process. You can repeat Quick Configure as many times as needed.

On the Quick Configure welcome page, click Next to continue.

Changing the Administrator Password

Clicking Next opens the Administrator Accounts Password page, if you are using Quick Configure for the first time.



SNAP20181 • Quick Configure

Administrator Accounts Password

Warning: Currently, there is no password for the ADMINISTRATOR, ROOT and SUPERVISOR accounts. This means that any user can access the server administration utilities until you assign the Administrator accounts a password. The password you assign is the same for all three accounts.

Note: If you continue to see this page even after assigning a password or specifying that you don't want to see this warning again, try pressing the Reload or Refresh button on your browser.

○ Don't assign a password, and don't show this warning again

● Set Administrator password to the following:

Password □ Verify Password □

ADMINISTRATOR

The Snap! Server is preconfigured with a group named ADMIN that includes three administrator-level user accounts: ROOT, SUPERVISOR, and ADMINISTRATOR. (For more information about users and groups, see "Configuring Security" on page 32.) By default, no password is assigned to these user accounts. If you want to restrict unauthorized persons from accessing the Snap! Server Administration tools, you should change the Administrator accounts password now. Then, only those who have ADMIN access privileges will be able to open the Administration menu.

To assign a password:

1. Click the Set Administrator Password option.
2. Type the new password in the field provided.
3. The password is case-sensitive and can contain up to 14 alphanumeric characters.
4. Type the password again in the Verify Password field.
5. Click Next.

NOTE

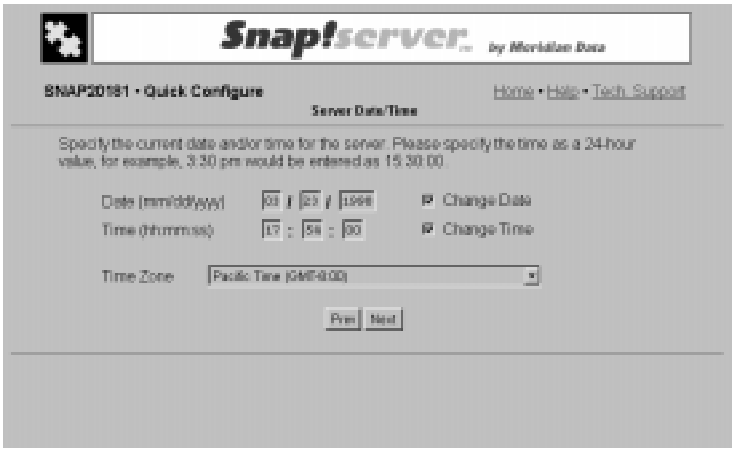
Setting the Administrator password in the Administrator Accounts Password page sets the password for all three of the preconfigured ADMIN accounts: ADMINISTRATOR, SUPERVISOR, and ROOT. If you continue with the Quick Configure, you will be prompted to log in with the new password.

If you don't want to assign a password:

1. Click the Don't Assign a Password option.
2. Click Next to continue.

Configuring Server Date and Time

The current date and time appear by default. To change the date or time, follow these steps.



Snap!server by Meridian Data

SNAP20181 • Quick Configure

Home • Help • Tech. Support

Server Date/Time

Specify the current date and/or time for the server. Please specify the time as a 24-hour value, for example, 3:30 pm would be entered as 15:30:00.

Date (mm/dd/yyyy) 03 / 23 / 1998 ☑ Change Date

Time (hh:mm:ss) 17 : 56 : 00 ☑ Change Time

Time Zone Pacific Time (GMT-8:00)

1. To change the date, type the new month, day, and year in the fields provided, and then check the Change Date box.
2. To change the time, type the new hour (24-hour format), minutes, and seconds in the fields provided, and then check the Change Time box.
3. To specify the time zone, select from the Time Zone list box.

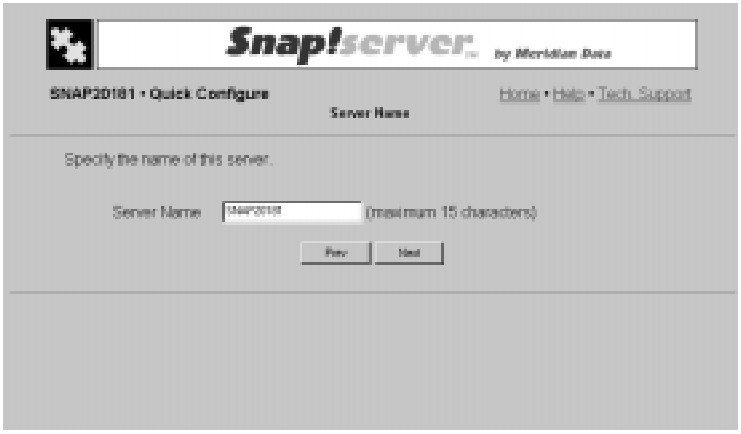
   The current release supports only time zones in the United States.
4. Click Next to continue.

IMPORTANT

Setting the correct date, time, and time zone is particularly important if you intend to use your Snap! Server with Novell network clients. Most Novell network clients do not compensate for differences in time zones. As a result, dates and times on files may be incorrect.

Configuring Server Name

To change the Snap! Server's default name, follow these steps.



SNAP20181 • Quick Configure

Server Name

Specify the name of this server.

Server Name: SNAP20181 (maximum 15 characters)

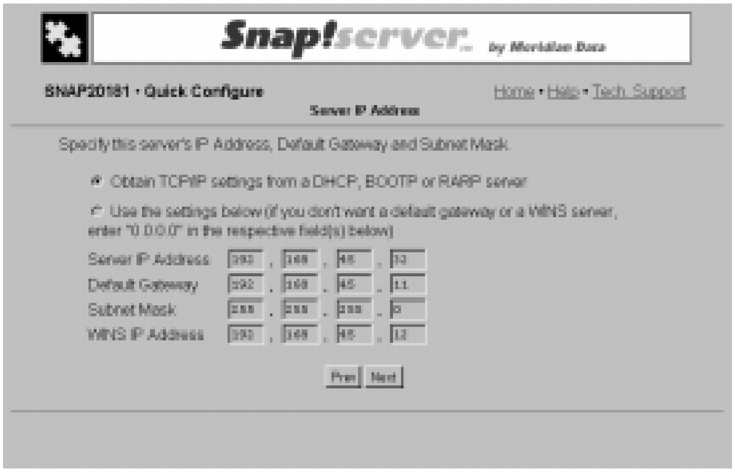
1. Type the new name in the Server Name field.

   The name can contain up to 15 alphanumeric characters.

2. Click Next to continue.

Verifying the Server's IP Address

The Server IP Address page shows the server's current TCP/IP settings. You can change these if you wish.



SNAP20181 • Quick Configure

Server IP Address

Specify this server's IP Address, Default Gateway and Subnet Mask.

● Obtain TCP/IP settings from a DHCP, BOOTP or RARP server

○ Use the settings below (if you don't want a default gateway or a WINS server, enter "0.0.0.0" in the respective field(s) below)

Server IP Address: 192 . 168 . 45 . 32
Default Gateway: 192 . 168 . 45 . 11
Subnet Mask: 255 . 255 . 255 . 0
WINS IP Address: 192 . 168 . 45 . 12

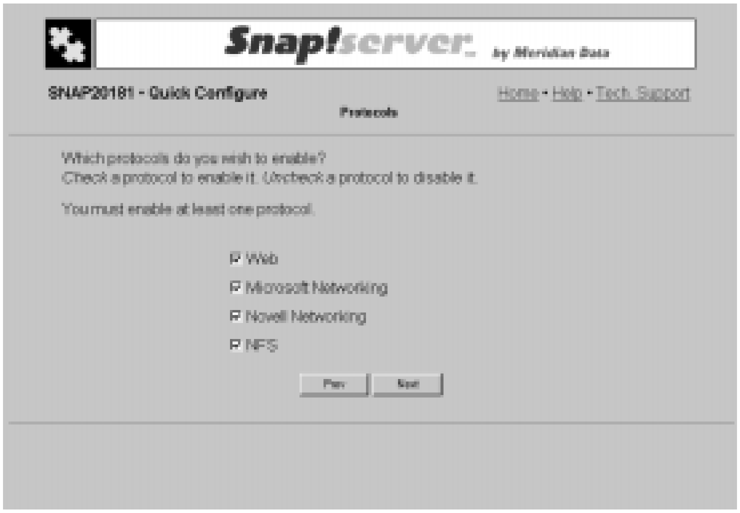
The first option, if selected, verifies that a dynamic IP address was automatically obtained from a DHCP, BOOTP, or RARP server on the network.

The second option, if selected, verifies the IP address you assigned using the Snap! IP utility program. If you select this option to manually configure TCP/IP, you must specify at least the TCP/IP address and the subnet mask. The default gateway and WINS server are optional parameters.

Click Next to continue.

Specifying Network Protocols

All protocols are enabled by default.



SNAP20181 - Quick Configure

Protocols

Which protocols do you wish to enable?
Check a protocol to enable it. Uncheck a protocol to disable it.

You must enable at least one protocol.

☑ Web
☑ Microsoft Networking
☑ Novell Networking
☑ NFS

To disable a protocol, uncheck the box beside its name. You must enable at least one protocol.

The following table describes the protocols.

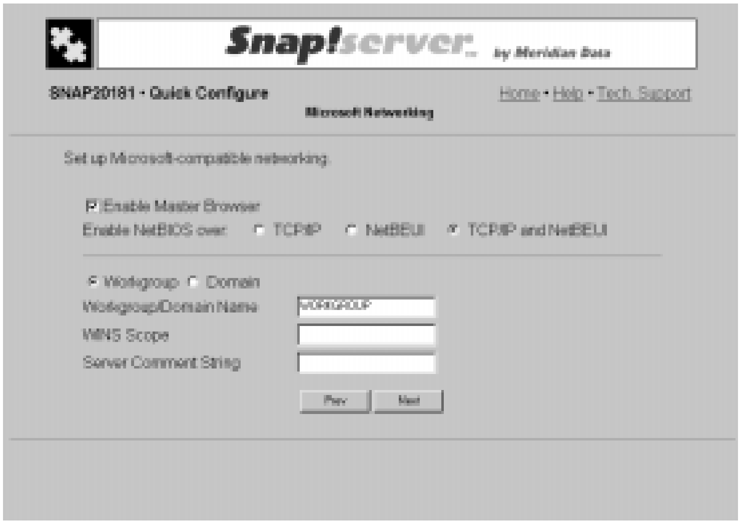
Select this protocol	To enable
Web	Snap! Server as an HTTP file server ADMINISTRATOR If you disable the Web protocol, you can access the Administration menu by entering this URL: **http://*IP_address*/config**
Microsoft Networking	Microsoft-compatible networking
Novell Networking	Novell-compatible networking
NFS	Network File System operation

After making your protocol selections, you need to configure parameters for them. The network configuration pages that appear depend on the protocols you've enabled.

Click Next to continue.

Configuring Microsoft Networking

If you enabled the Microsoft Networking protocol, clicking Next opens the page for setting up Microsoft-compatible networking.



Snap!server by Meridian Data
SNAP20181 • Quick Configure
Home • Help • Tech. Support
Microsoft Networking

Set up Microsoft-compatible networking.

☑ Enable Master Browser

Enable NetBIOS over: ○ TCP/IP ○ NetBEUI ● TCP/IP and NetBEUI

● Workgroup ○ Domain

Workgroup/Domain Name: WORKGROUP

WINS Scope:

Server Comment String:

The following table describes the parameters and their defaults.

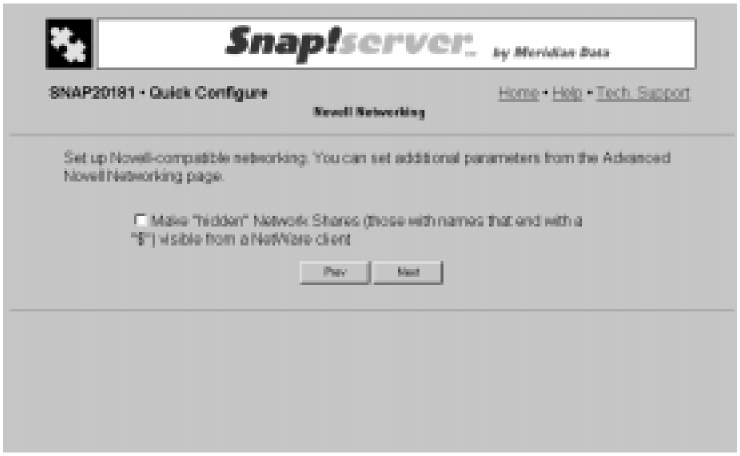
Parameter	Default	Description
Master Browser	Enabled	The Snap! Server can maintain the master list of all computers belonging to a specific workgroup if there is no Master Browser available in that workgroup. Disabling this feature prevents the Snap! Server from ever becoming the Master Browser. Disable this feature *only* if you're sure that there is another machine in that workgroup that serves as the Master Browser.
NetBIOS over:		Specifies the transport layer used in Microsoft networking
TCP/IP	Disabled	
NetBEUI	Disabled	
TCP/IP and NetBEUI	Enabled	
Workgroup Domain	Workgroup	Specifies either workgroup-based or domain-based operation **ADMINISTRATOR** If you select Domain, then you must enter all relevant group names for the domain into the Snap! Server group list. See "Configuring Security" on page 32.
Workgroup/Domain Name	Workgroup	Specifies the name of the workgroup or domain within which the Snap! Server will appear

Parameter	Default	Description
WINS Scope	None	Specifies the Windows Internet Name Service scope identifier (used to manage NETBIOS name resolution); the string can contain up to 63 characters (letters, numbers, and hyphens only).
Server Comment	None	Optional descriptive comment; can contain up to 48 printable characters

Clicking Next to continue.

Configuring Novell Networking Settings

If you enabled the Novell Networking protocol, clicking Next opens the page for setting up Novell-compatible networking.



Snap! server by Meridian Data
SNAP20181 • Quick Configure
Home • Help • Tech. Support
Novell Networking
Prev
Next

Set up Novell-compatible networking. You can set additional parameters from the Advanced Novell Networking page.

□ Make "hidden" Network Shares (those with names that end with a "$") visible from a NetWare client

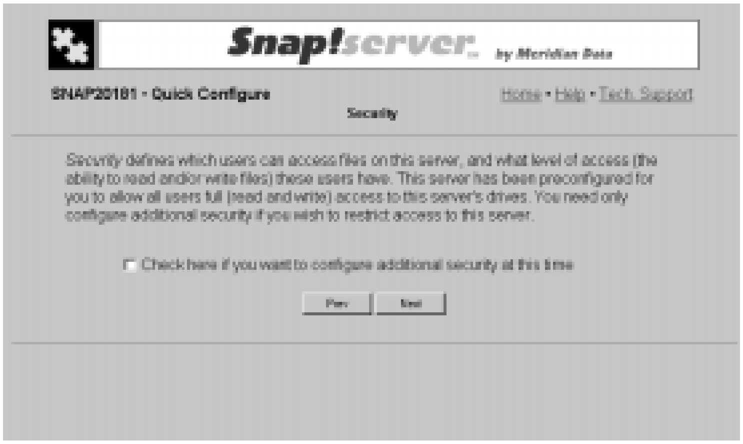
If you want to make hidden network shares (or volumes) visible from a NetWare client, check the box. Shares (or volumes) that end with the dollar-sign character ($) are normally hidden. Checking this box enables NetWare users to browse and map to these shares.

For information about setting additional parameters from the Advanced Novell Networking page, see "Reconfiguring Novell Networking" on page 84.

Clicking Next on the Novell Networking page opens the Quick Configure Security page (described in "Configuring Security," next).

Configuring Security

Use the Security configuration parameters to control network users' access to resources on the Snap! Server and to define groups' access permissions—read only, full, or deny access. By default, all users have full (read and write) access to the server's drives.



SNAP20181 - Quick Configure

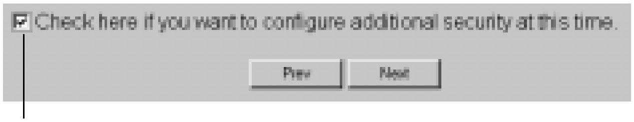
Security

Security defines which users can access files on this server, and what level of access (the ability to read and/or write files) these users have. This server has been preconfigured for you to allow all users full (read and write) access to this server's drives. You need only configure additional security if you wish to restrict access to this server.

□ Check here if you want to configure additional security at this time

If you want to restrict access to the server, you can configure additional security by doing the following.

1. Check the Check Here box.



☑ Check here if you want to configure additional security at this time.

Check this box to configure additional security.

2. Click Next.

   You are presented with four information pages that describe how to:

   a. Create a user.

   b. Create a group (a collection of users who all have the same access to a network share).

c. Assign users as members of specific groups.

d. Create a network share (a virtual folder to a directory on one of the Snap! Server's drives that is accessible to users on the network).

Depending on the model, your Snap! Server has either one or two preconfigured network shares named Drive1 and Drive2, to which all users have full access.

e. Specify which groups have access to each network share.

3. Click Next to continue viewing pages that provide descriptions and examples for configuring security.

About Users and Groups

ADMINISTRATOR

This topic provides information for Snap! Server and system administrators. The Snap! Server has a default user named GUEST. The GUEST user is a member of the default group named EVERYONE. A GUEST user is anyone who is:

- Not recognized by the Snap! Server
- Not recognized by the domain controller
- A member of a group that is recognized by the domain controller but is *not* recognized by the Snap! Server

These unrecognized users, now recognized by the system as GUEST users, will have access to network shares that grant access to the EVERYONE group. (For information about deleting the GUEST user, see Chapter 5, "Server Administration.")

The EVERYONE group includes all users. Any new user that you create automatically becomes a member of the EVERYONE group. You can't delete or modify this group directly. However, you can change access rights associated with the EVERYONE group.

The Snap! Server has another default group named ADMIN that includes these three user names that all reference the same Administrative account: ROOT, SUPERVISOR, and ADMINISTRATOR. You can add a user to the ADMIN group, but you cannot do the following:

- Delete the three administrator-level users.
- Remove the three default users from the ADMIN group.
- Delete the ADMIN group.

Only members of the ADMIN group can access the Snap! Server Administration tools (described in Chapter 5).

For more information about the Snap! Server's security method, see Appendix C, "Security and Access Control."

The Snap! Server supports using a Microsoft networking domain controller to authenticate a user. For such authentication to work properly, you must have done the following:

- Enabled Microsoft networking.
- Selected the Domain option on the Microsoft Networking page (as described in "Configuring Microsoft Networking" on page 29).

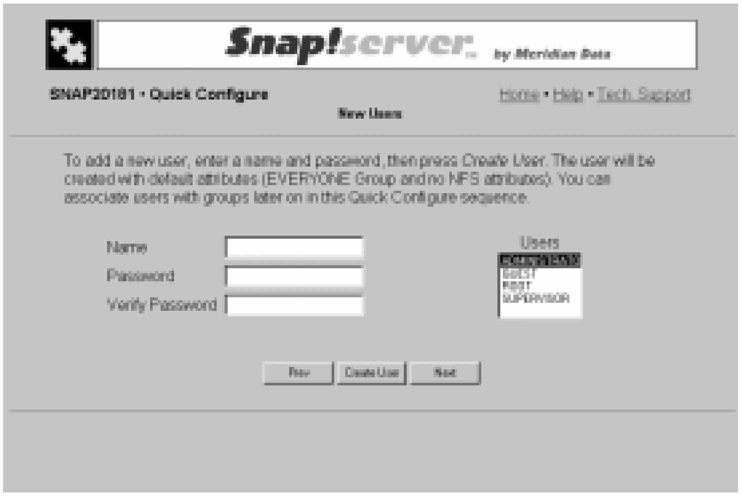
  The name of the domain specified on the Microsoft Networking page will be used for user authentication. If you've selected the Domain option, it is *not* necessary to create the users contained in the domain. The Snap! Server will communicate with the domain controller directly to authenticate a user. However, it will be necessary to create each group in the domain on the Snap! Server. This is required so that you can assign access rights to the Snap! Server shares using a group name.

NOTE The group name must exactly match the group names in the domain. Otherwise, a user will not be granted access to a share.

Creating Users

To add a new user:

1. On page 4 of the Security description, click Next to open the Quick Configure New Users page.



To add a new user, enter a name and password, then press Create User. The user will be created with default attributes (EVERYONE Group and no NFS attributes). You can associate users with groups later on in this Quick Configure sequence.

2. Type the new user name in the Name field.

   The name can contain up to 20 alphanumeric characters.

3. Optionally, type the new user's password in the Password field.

   The password is case-sensitive and can contain up to 14 alphanumeric characters.

4. Type the password again in the Verify Password field.
5. Click Create User.

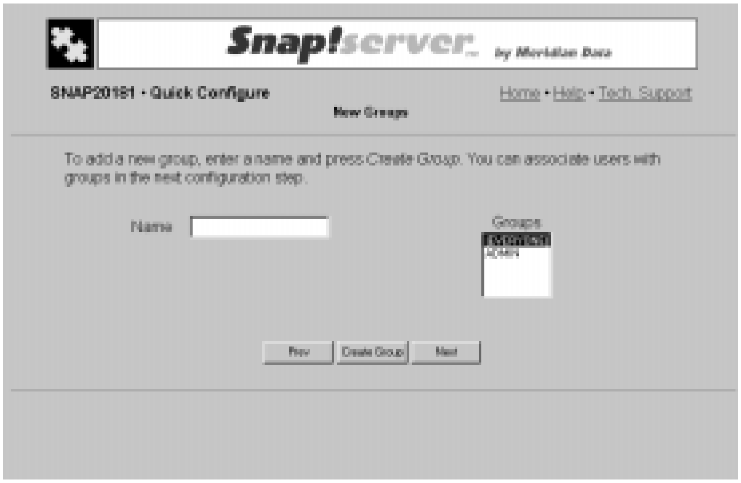
   The user name you added appears in the Users list.

6. To add another new user, repeat steps 2 through 5 of this procedure.
7. Click Next to advance to the New Groups page.

NOTE If you use the Microsoft Windows 95 Client for NetWare Networks to connect to the Snap! Server with the default GUEST account, and later set up security and user accounts, you may have problems reconnecting to the Snap! Server. The client for NetWare Networks automatically tries to reconnect using the stored GUEST account information. The connection may fail because of the new security restrictions that you have created. In this case, change the password for the Snap! Server's GUEST account. Then request those using the Windows 95 workstations affected by this problem to log off their machines and then log in again. Then remove the GUEST password if you want to allow controlled access to unregistered users.

Creating Groups

To add a new group, follow this procedure.



Snap!server by Meridian Data
SNAP20181 • Quick Configure
Home • Help • Tech. Support
New Groups
Name
Groups
EVERYONE
ADMIN
Prev
Create Group
Next

To add a new group, enter a name and press Create Group. You can associate users with groups in the next configuration step.

1. Type the name of the new group in the Name field.

   The name can contain up to 48 alphanumeric characters.

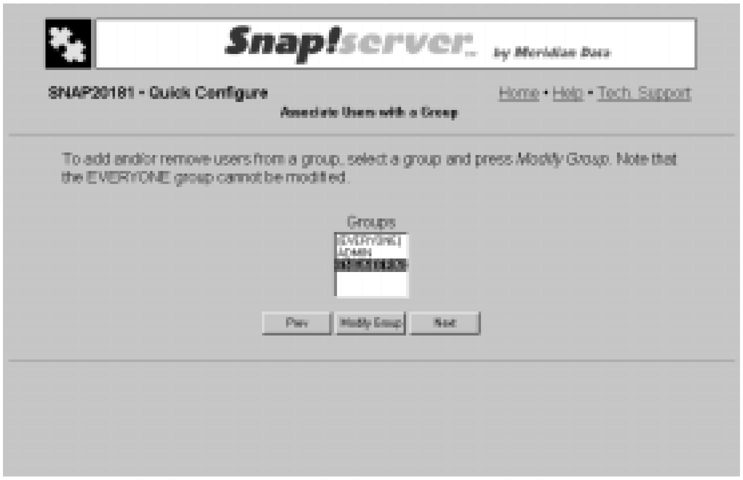
2. Click Create Group.

   The group name you added appears in the Groups list.

3. To add another new group, repeat steps 1 through 2 of this procedure.
4. Click Next to advance to the Associate Users With a Group page.

Associating Users With Groups

To associate users with a group, follow this procedure.



SNAP20181 - Quick Configure

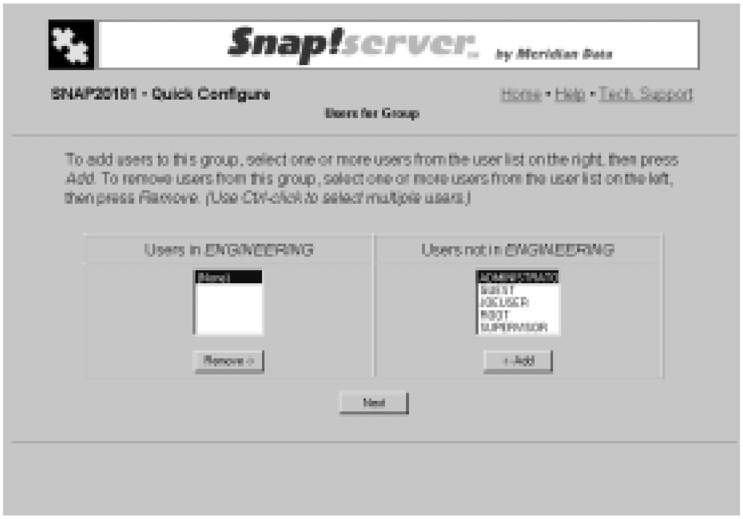
Associate Users with a Group

To add and/or remove users from a group, select a group and press *Modify Group*. Note that the EVERYONE group cannot be modified.

1. To modify a group by adding or removing users, select the group's name in the Groups list, and then click Modify Group.

   You can't modify the EVERYONE group. In this example, a group named ENGINEERING is modified.

   The Users for Group page appears.



SNAP20181 - Quick Configure

Users for Group

To add users to this group, select one or more users from the user list on the right, then press *Add*. To remove users from this group, select one or more users from the user list on the left, then press *Remove*. *(Use Ctrl-click to select multiple users.)*

2. To add users to the group you're modifying, select one or more names from the list of Users Not In that group.
3. Click Add.

   The user name(s) you added appear in the list of Users In the group you're adding to.
4. To remove users from this group, select one or more user names from the list of Users In the group.
5. Click Remove.

   The user name(s) you removed appear in the list of Users Not In the group you're modifying.
6. Click Next to return to the Associate Users With a Group page.
7. To modify another group, return to step 1 and repeat the procedure for adding or removing users.
8. Click Next to advance to the New Network Shares page.

About Network Shares

A network share is linked to a folder on one of the Snap! Server's drives that it makes available to users on your network. By default, your server has either one or two network shares named Drive1 and Drive2. You can create new shares and make them available to network users or restrict users' access to them by associating groups with shares and assigning access permissions.

Shares provide your only means of restricting users' access to a folder on the Snap! Server. When a user connects to a share, he has the same access rights to every file and folder within the share. When defining shares, be careful that you don't inadvertently grant access to a restricted file or folder. The following example illustrates how access can be inadvertently granted to a restricted file or folder.

Suppose that you have the following directory structure:
\Path1
\Path1\Path2

You have two shares—share1 and share2—with the following attributes:

share1:	full access,	references \Path1
share2:	read-only access,	references \Path1\Path2

A user who connects to share1 will have *full* access to every file and folder within \Path1 *as well as* within \Path1\Path2, even though \Path1\Path2 is restricted by share2. However, if the same user connects to share2, he will have read-only access to every file and folder within \Path1\Path2.

You can resolve the problem by moving the contents of the \Path1\Path2 folder to a new folder that is not contained within \Path1. For example, the new directory structure might be:

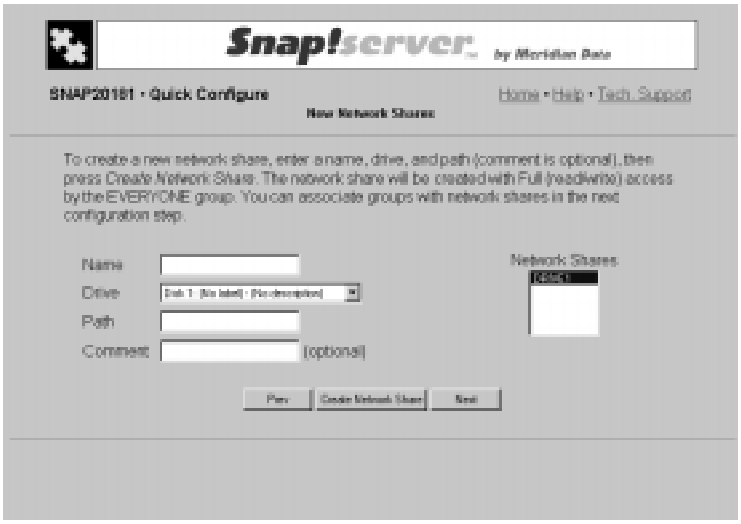
\Path1 ⟵ share1
\Path2 ⟵ share2

and share2 would now reference \Path2. Users cannot circumvent the read-only access on share2 by connecting to share1.

For more information about shares and setting up security, see Appendix C, "Security and Access Control."

Creating Network Shares

To create a new network share, follow this procedure.



Snap! server by Meridian Data
SNAP20181 • Quick Configure
Home • Help • Tech. Support
New Network Shares

To create a new network share, enter a name, drive, and path (comment is optional), then press Create Network Share. The network share will be created with Full (read/write) access by the EVERYONE group. You can associate groups with network shares in the next configuration step.

Name
Drive Disk 1 : [No label] : [No description]
Path
Comment (optional)

Network Shares
SHARE1

Prev
Create Network Share
Next

1. On the New Network Shares page, type the name of the new share in the Name field.

   The name can contain up to 12 alphanumeric characters.

2. From the Drive list box, select the drive on which to create the share.

3. Type the path in the Path field, where the backslash character (\) represents the root of the drive you selected in step 2.

   The path can contain up to 254 alphanumeric characters. The directory you specify must exist on the drive you selected. Otherwise, the share will not be available to network users. If the directory does not exist, you will be prompted to create it.

4. Optionally, you can add a descriptive comment containing up to 47 printable characters.

5. Click Create Network Share.

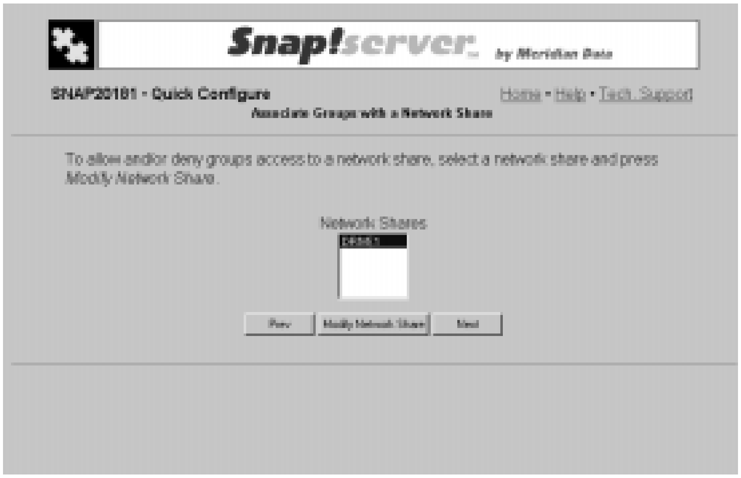
   The name of the share you created appears in the Network Shares list. By default, the group named EVERYONE has full (read/write) access to the new share you created.

6. To create another new share, repeat steps 1 through 5 of this procedure.

7. Click Next to advance to the Associate Groups With a Network Share page.

Associating Groups With a Network Share

To associate groups with a network share, follow this procedure.



SNAP20181 • Quick Configure

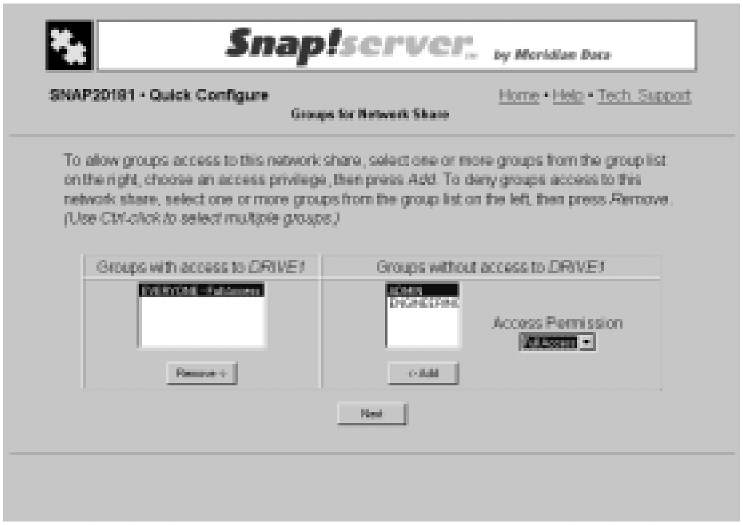
Associate Groups with a Network Share

To allow and/or deny groups access to a network share, select a network share and press *Modify Network Share*.

Network Shares: DRIVE1

1. To modify a network share by allowing or denying access to groups, select the share's name in the Network Shares list, and then click Modify Network Share.

   The Groups for Network Share page appears.



SNAP20181 • Quick Configure

Groups for Network Share

To allow groups access to this network share, select one or more groups from the group list on the right, choose an access privilege, then press *Add*. To deny groups access to this network share, select one or more groups from the group list on the left, then press *Remove*. *(Use Ctrl-click to select multiple groups.)*

Groups with access to *DRIVE1*	Groups without access to *DRIVE1*
EVERYONE - Full Access	ADMIN ENGINEERING

Access Permission: Full Access

2. To assign groups access rights to the share you're modifying, do the following:

   a. Select one or more names from the list of Groups Without Access to that share.

   b. From the Access Permission list box, select Full Access, Deny Access, or Read Only for each group that should be granted access rights to the share.

   c. Click Add.

   The group name(s) you added appear in the list of Groups With Access to the share you're modifying. Each group name is followed by its access permission.

3. To deny groups access to the share you're modifying, select one or more names from the list of Groups With Access to that share.

4. Click Remove.

   Any group names you remove appear in the list of Groups Without Access to the share you're modifying.

5. Click Next to return to the Associate Groups With a Network Share page.

6. To modify another share, repeat steps 1 through 5 of this procedure.

7. Click Next to proceed to the final configuration step.

Completing the Last Configuration Step

The last step in the configuration procedure depends on the settings you specified.

- If the changes you made do not require the server to restart, you are prompted to click Finish.

  Clicking Finish takes you to the Snap! Server's Administration menu. If you are a system or network administrator who wants to make additional configuration changes, see Chapter 5 for information.

- If the system requests that you reboot the server so that the changes you configured take effect, click Reboot to restart the server.

CHAPTER 5 Server Administration

This chapter provides information for users who install and administer networks.

Meridian Data recommends that you use Quick Configure first, as described in Chapter 4. Use the Snap! Server administration tools to reconfigure specific components that you want to change.

Server Administration Tools

Once the Snap! Server's IP address has been assigned, you can access the Administration menu in the following manner. (For information about IP address assignment, see Chapter 3.)

1. Open the browser that you want to use—either Microsoft Internet Explorer 2.0 or greater, or Netscape Navigator 2.0 or greater.
2. In the address box, enter one of the following Uniform Resource Locators (URLs).
   - If either a DNS or a Windows Internet Name Server (WINS) is available on your network and successfully translates the Snap! Server's name into an IP address, you can enter this URL:

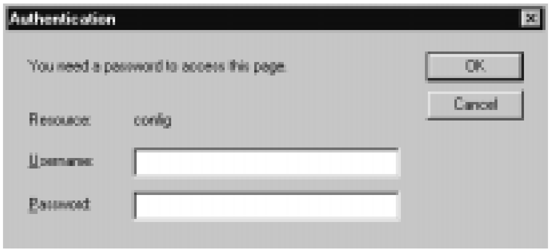
     http://*ServerName*/config

     replacing *ServerName* with your Snap! Server's current name.
   - Otherwise, enter this URL:

     http://*IP_address*/config

     replacing *IP_address* with your Snap! Server's IP address. For example, http://192.168.1.142/config.

The Authentication dialog box appears.



You need a password to access this page.

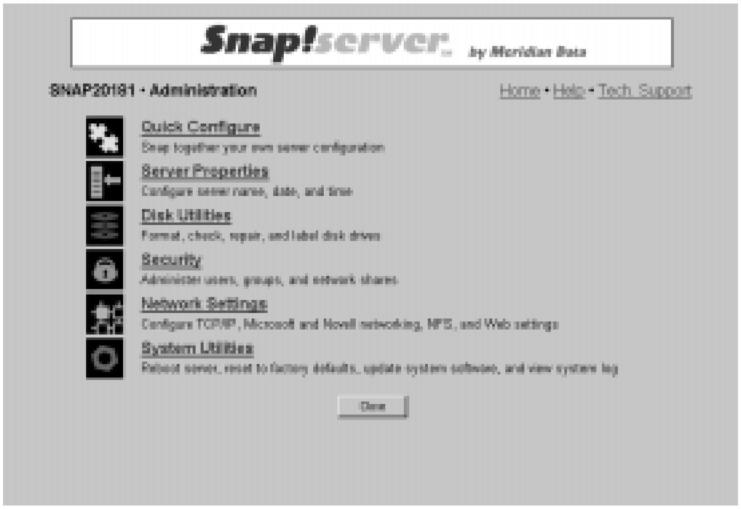
Resource: config

Username:

Password:

3. In the Username field, type:
   Administrator
4. In the Password field, type the current password, if any, for the Administrator account.
5. Click OK.

The Snap! Server Administration menu appears.



Snap!server by Meridian Data
SNAP20181 · Administration
Home • Help • Tech. Support
Done

Quick Configure
Snap together your own server configuration

Server Properties
Configure server name, date, and time

Disk Utilities
Format, check, repair, and label disk drives

Security
Administer users, groups, and network shares

Network Settings
Configure TCP/IP, Microsoft and Novell networking, NFS, and Web settings

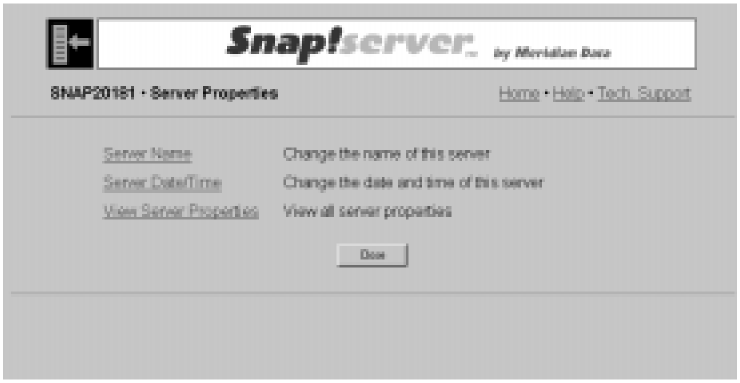
System Utilities
Reboot server, reset to factory defaults, update system software, and view system log

Clicking the Server Properties, Disk Utilities, Security, Network Settings, and System Utilities hyperlinks opens menus with hyperlinks to tools for customizing the configuration of specific, key parameters and administering the Snap! Server. The topics that follow describe these administration tools.

Configuring and Viewing Server Properties

Open the Server Properties menu to do the following.

- Rename the Snap! Server.
- Change the server’s date, time, and time zone.
- View Server Properties.



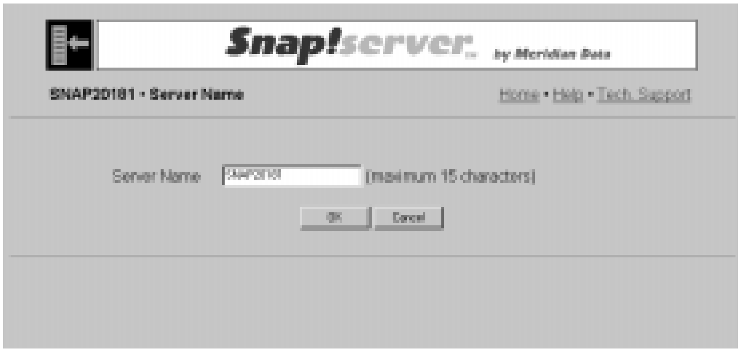
SNAP20181 • Server Properties

Server Name	Change the name of this server
Server Date/Time	Change the date and time of this server
View Server Properties	View all server properties

Changing the Server’s Name

To rename the Snap! Server:

1. On the Server Properties menu, click Server Name to open the Server Name page.



SNAP20181 • Server Name

Server Name SNAP20181 (maximum 15 characters)

2. Type the new name in the Server Name field.

   The name can include up to 15 alphanumeric characters.

3. Click OK to accept your change.

   The Reboot Server page appears to advise you that you must reboot the server so that your name change takes affect. The page also lists the names of users currently logged onto the server so that you can warn them before the server reboots.

4. On the Reboot Server page, click Reboot Now.

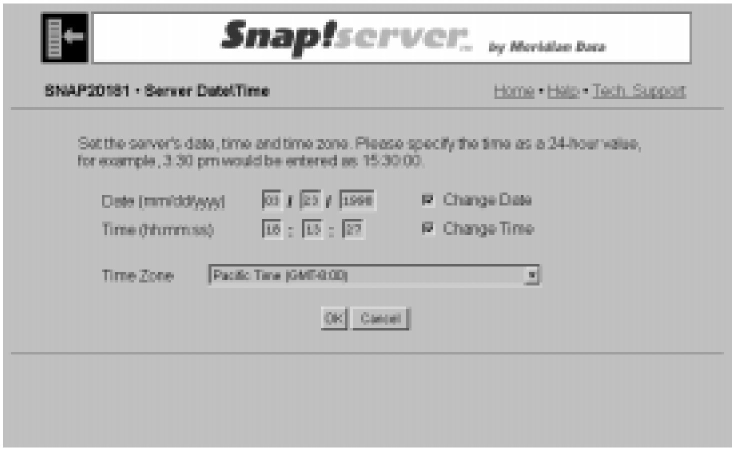
   The Snap! Server restarts itself.

   If you click Reboot Later instead of Reboot Now, your changes are saved, but they won't take effect until you reboot the server.

Changing the Date and Time

To change the Snap! Server's date and time parameters:

1. On the Server Properties menu, click Server Date/Time to open the Server Date/Time page.



SNAP20181 • Server Date/Time

Set the server's date, time and time zone. Please specify the time as a 24-hour value, for example, 3:30 pm would be entered as 15:30:00.

Date (mm/dd/yyyy) 03 / 23 / 1998 ☑ Change Date

Time (hh:mm:ss) 18 : 13 : 27 ☑ Change Time

Time Zone Pacific Time (GMT-8:00)

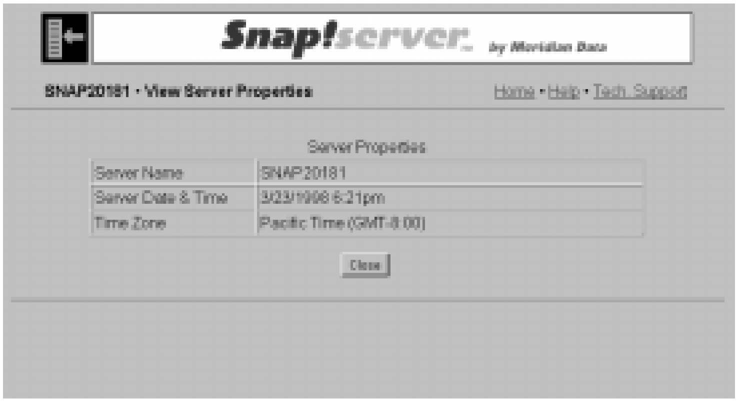
2. To change the date, type the new month, day, and year in the fields provided, and then check the Change Date box.
3. To change the time, type the new hour (24-hour format), minutes, and seconds in the fields provided, and then check the Change Time box.
4. To specify the time zone (only for the United States of America in the current release), choose from the Time Zone list box.
5. Click OK to accept the parameters and return to the Server Properties menu.

IMPORTANT Setting the correct date, time, and time zone is particularly important if you intend to use your Snap! Server with Novell network clients. Most Novell network clients do not compensate for differences in time zones. As a result, dates and times on files may be incorrect.

Viewing Server Properties

To see the server's properties settings:

1. On the Server Properties menu, click View Server Properties.


Snap!server
by Meridian Data
SNAP20181 • View Server Properties
Home • Help • Tech. Support
Close

Server Properties

Server Name	SNAP20181
Server Date & Time	3/23/1998 6:21pm
Time Zone	Pacific Time (GMT-8:00)

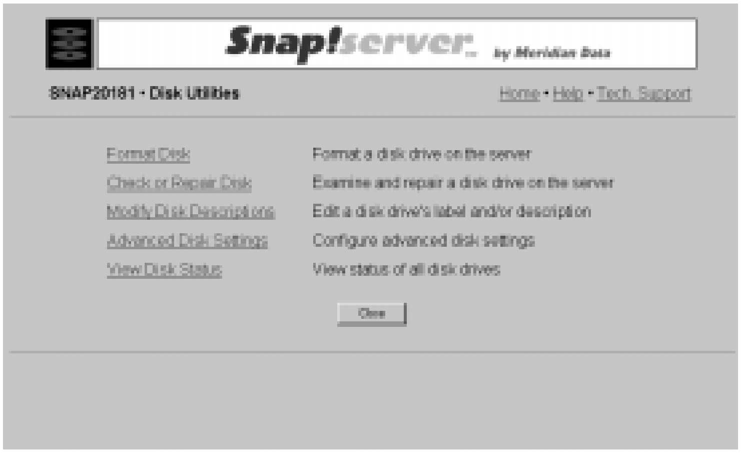
2. Click Close to return to the Server Properties menu.

Using Disk Utilities

The Snap! Server Disk Utilities menu provides hyperlinks to utilities for formatting, checking and repairing, and changing the labels and descriptions of disk drives on the server. It also provides the ability to check the status of the disk drives.

To use the disk utilities:

1. On the Snap! Server Administration menu, click Disk Utilities to open the Disk Utilities menu.



SNAP20181 • Disk Utilities

Format Disk	Format a disk drive on the server
Check or Repair Disk	Examine and repair a disk drive on the server
Modify Disk Descriptions	Edit a disk drive's label and/or description
Advanced Disk Settings	Configure advanced disk settings
View Disk Status	View status of all disk drives

2. On the Disk Utilities menu, click the name of the utility you want to use:
   - Format Disk
   - Check or Repair Disk
   - Modify Disk Descriptions
   - Advanced Disk Settings
   - View Disk Status

Formatting a Disk

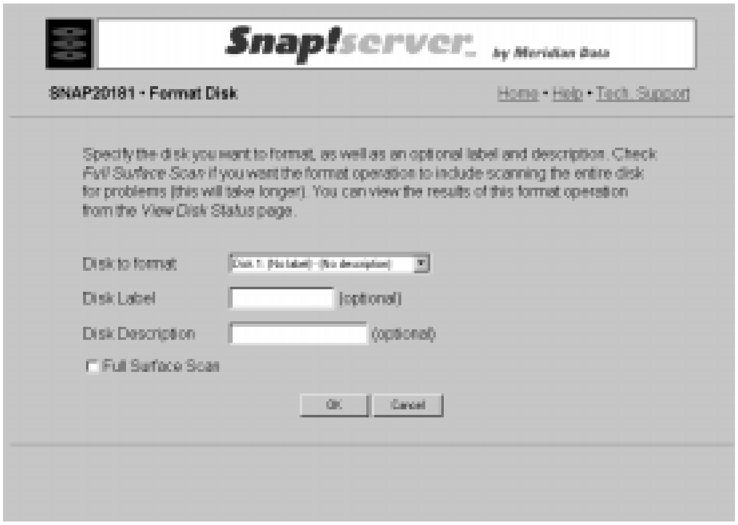
The Snap! Server ships with all drives formatted and ready to use. If you want to format a disk, use the Format Disk utility. Formatting a disk requires the Snap! Server to reboot. Before rebooting, the server does the following.

- Warns you if the disk is not blank.
- Displays a list of users who are currently logged on, so that you can warn them before the server reboots itself.

The disk reformats immediately after the server reboots.

To format a disk, follow these steps.

1. On the Disk Utilities menu, click Format Disk to open the Format Disk page.



Specify the disk you want to format, as well as an optional label and description. Check *Full Surface Scan* if you want the format operation to include scanning the entire disk for problems (this will take longer). You can view the results of this format operation from the View Disk Status page.

Disk to format: Disk 1: (No label) - (No description)

Disk Label: (optional)

Disk Description: (optional)

☐ Full Surface Scan

2. Select the disk to format from the list box.
3. Optionally, type a label for the disk in the Disk Label field.

   The label can contain up to 12 alphanumeric characters.
4. Optionally, type a description of the disk in the Disk Description field.

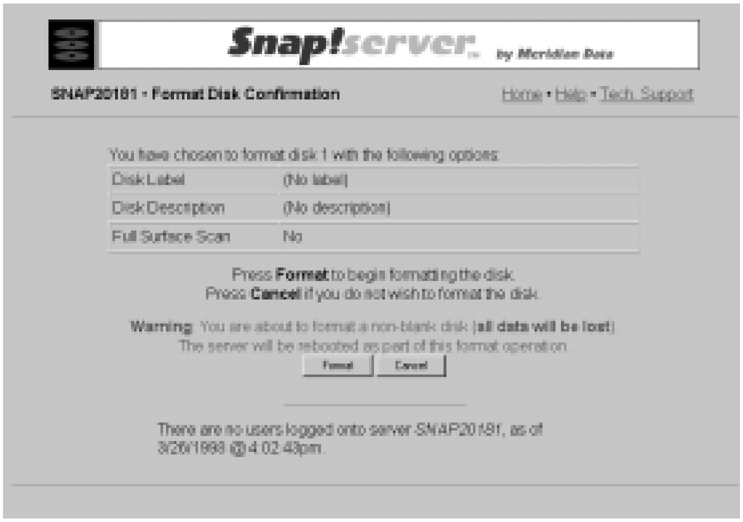
   The description can contain up to 63 printable characters.

5. If you want the entire disk scanned for potential problems, check the Full Surface Scan box.

NOTE Surface Scan will take approximately two hours, depending on the size of the disk. The scan finds any unusable disk sectors and prevents them from being used in the future.

6. Click OK.

   The Format Disk Confirmation page appears, showing what you specified.



SNAP20181 • Format Disk Confirmation

You have chosen to format disk 1 with the following options:

Disk Label	(No label)
Disk Description	(No description)
Full Surface Scan	No

Press **Format** to begin formatting the disk.
Press **Cancel** if you do not wish to format the disk.

Warning: You are about to format a non-blank disk (**all data will be lost**).
The server will be rebooted as part of this format operation.

There are no users logged onto server *SNAP20181*, as of 3/26/1998 @ 4:02:43pm.

7. Check for accuracy, and then click Format to reboot the server and start formatting the disk.

After the Snap! Server reboots, which takes abut 30 seconds, you can view the progress of the formatting operation on the View Disk Status page described on page 57.

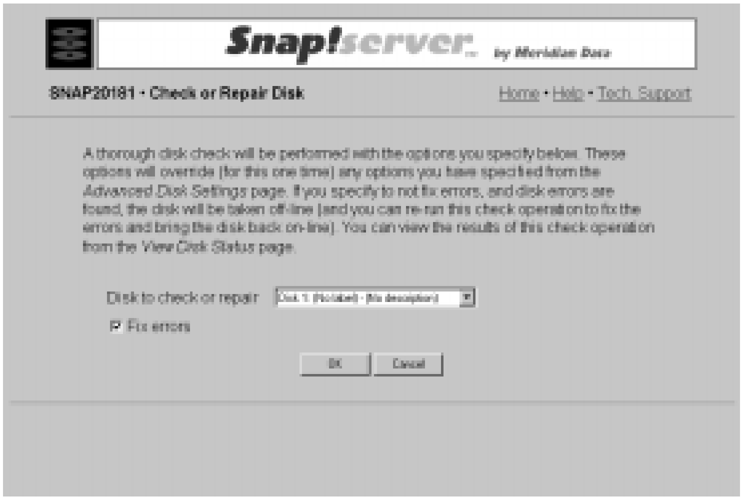
NOTE You can change a disk's label and description without having to format the disk. See "Modifying Disk Labels and Descriptions" on page 55.

Checking and Repairing a Disk

Use this utility when you want to perform a disk check. The options selected during the Disk Check operation temporarily override the Advanced Disk Settings options you have specified (described on page 56).

To check or repair a disk drive on the server with the options you specify, follow these steps.

1. On the Disk Utilities menu, click Check or Repair Disk.



SNAP20181 • Check or Repair Disk

A thorough disk check will be performed with the options you specify below. These options will override (for this one time) any options you have specified from the *Advanced Disk Settings* page. If you specify to not fix errors, and disk errors are found, the disk will be taken off-line (and you can re-run this check operation to fix the errors and bring the disk back on-line). You can view the results of this check operation from the *View Disk Status* page.

Disk to check or repair: Disk 1 (No label) - (No description)

☑ Fix errors

2. Select the disk to check or repair from the list box.

NOTE If the description of the drive appears as `unable to be queried`, then the drive is currently busy. Check the drive's status using the Disk Status page described on page 57.

3. Do one of the following:

   a. To check the disk and repair any errors encountered, verify that the Fix Errors box is checked, and then click OK.

      Fix Errors is checked by default.

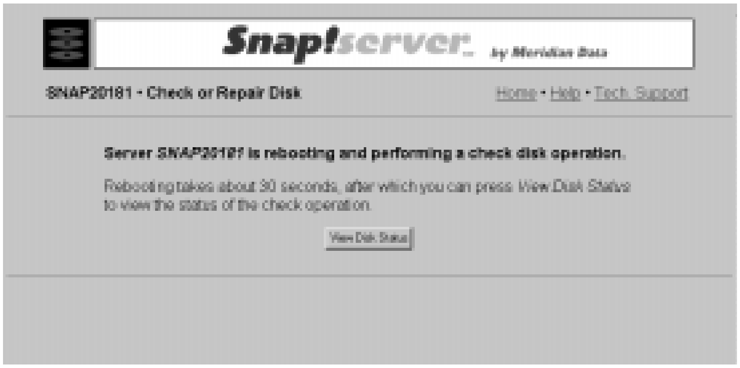
   b. To check the disk without fixing errors, uncheck the Fix Errors box, and then click OK.

IMPORTANT If disk errors are found, the disk will not be mounted. You must then run Check or Repair disk again with Fix Errors turned on to repair the disk and make it available to users.

4. When the Check Disk Confirmation page appears showing what you specified, verify your Disk Check options.

NOTE Checking a disk requires the Snap! Server to reboot. The names of users currently logged onto the server appear at the bottom of the Check Disk Confirmation page so that you can warn them before the server reboots.

5. Click Check to reboot the server and start checking the disk. A page similar to this one appears.

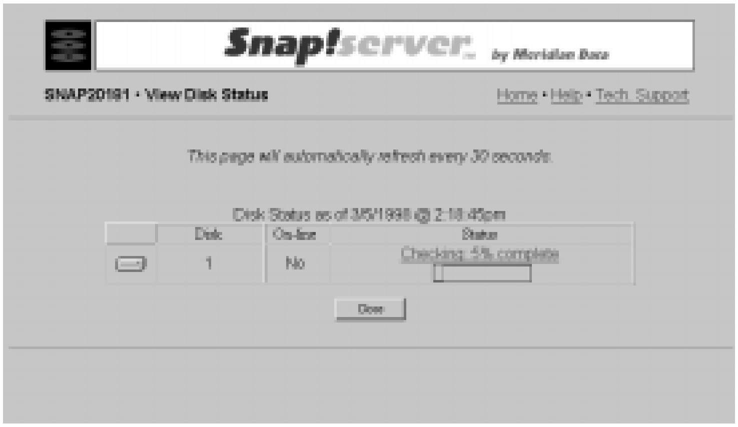


SNAP20181 • Check or Repair Disk

Server *SNAP20181* is rebooting and performing a check disk operation.

Rebooting takes about 30 seconds, after which you can press *View Disk Status* to view the status of the check operation.

Wait about 30 seconds for the server to reboot, and then click View Disk Status for the status of the check operation.



SNAP20191 • View Disk Status

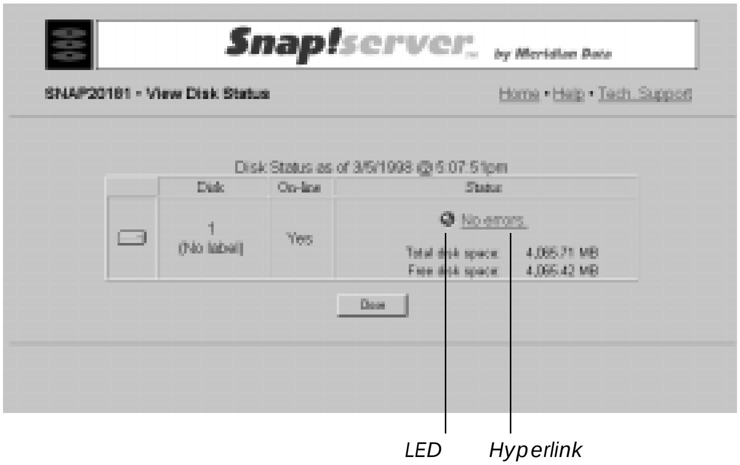
This page will automatically refresh every 30 seconds.

Disk Status as of 3/5/1998 @ 2:18:45pm

	Disk	On-line	Status
▭	1	No	Checking: 5% complete

The status page refreshes every 30 seconds. The message in the Status field is a hyperlink that you can click to view the Disk Log, which provides a chronological list of the operations performed on the disk.

When the check operation is finished, messages in the Status field will indicate whether errors were found, as shown in the following example.



Snap!server by Meridian Data

SNAP20181 • View Disk Status

Home • Help • Tech. Support

Disk Status as of 3/5/1998 @ 5:07:51pm

	Disk	On-line	Status
	1 (No label)	Yes	No errors Total disk space: 4,095.71 MB Free disk space: 4,095.42 MB

Messages in the Status field are hyperlinks, which you can click to view the Disk Log for more information on the Disk Check operation. The messages are preceded by different colored LEDs.

- Green indicates that no problems were found.
- Yellow indicates a warning; problems were found and repaired, and you should check the Disk Log for details.
- Red indicates a problem; problems were found but not repaired, and you should check the Disk Log for details.

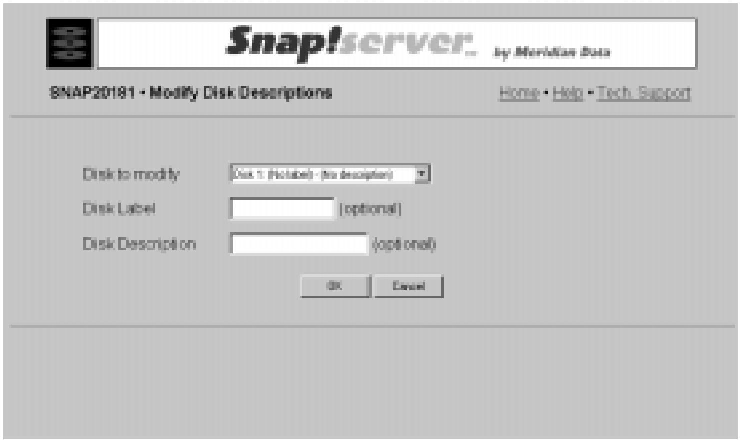
IMPORTANT If errors were found and the Fix Errors option was not selected, then the disk is not mounted. You must check the disk again with the Fix Errors option selected. Once the disk is repaired, it will be mounted and made available to users.

For more information about the Disk Check error messages in the Status field, see Chapter 6, “Troubleshooting.”

Modifying Disk Labels and Descriptions

To change the labels and descriptions of disk drives, follow these steps.

1. On the Disk Utilities menu, click Modify Disk Descriptions.



SNAP20181 • Modify Disk Descriptions

Disk to modify: Disk 1: (No label) - (no description)

Disk Label: (optional)

Disk Description: (optional)

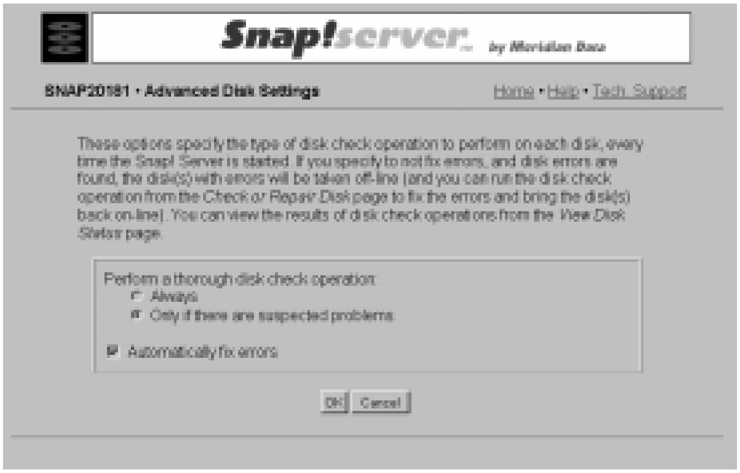
2. Select the disk to modify from the list box.
3. Optionally, type the new disk label and/or description in the appropriate field(s).

   Whatever values are specified in the Disk Label and Disk Description fields are the values that will be assigned. Leaving a field blank *removes* the current value.
4. Click OK to save your changes and return to the Disk Utilities menu.

Advanced Disk Settings

To specify the type of disk check operation to perform on each disk whenever the Snap! Server is booted, follow these steps.

1. On the Disk Utilities menu, click Advanced Disk Settings.



SNAP20181 • Advanced Disk Settings

These options specify the type of disk check operation to perform on each disk, every time the Snap! Server is started. If you specify to not fix errors, and disk errors are found, the disk(s) with errors will be taken off-line (and you can run the disk check operation from the *Check or Repair Disk* page to fix the errors and bring the disk(s) back on-line). You can view the results of disk check operations from the *View Disk Status* page.

Perform a thorough disk check operation:
○ Always
● Only if there are suspected problems

☑ Automatically fix errors

2. To specify the options to use for a disk check operation at bootup, do one of the following:

   a. Click Always if you always want a thorough check at every reboot.

   b. Click Only If Suspected Problems, if you want the server to boot faster.

      This option is on by default.

3. To specify whether to repair disks, do one of the following:

   a. To check disks and repair them, check the Automatically Fix Errors box.

      This option is on by default.

   b. To check disks without fixing errors, uncheck the Automatically Fix Errors box.

IMPORTANT

If disk errors are found, those disks will not be mounted. To repair the disks and make them available, run Check or Repair disk (described on page 51) with Fix Errors turned on.

---

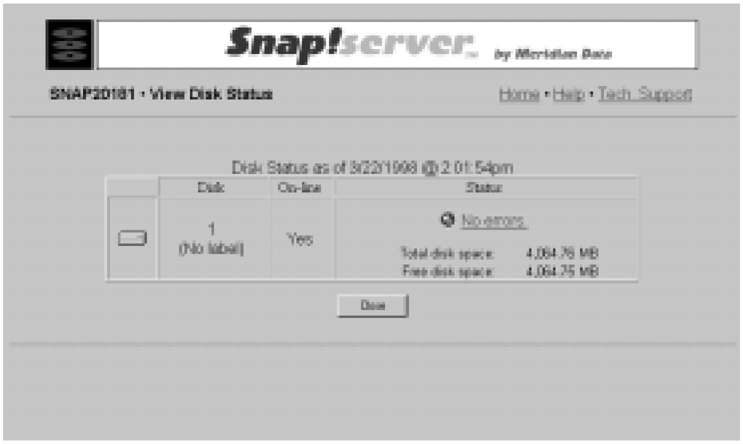
4. Click OK to save your settings and return to the Disk Utilities menu.

For information on how to temporarily override the Advanced Disk settings, see “Checking and Repairing a Disk” on page 51.

Viewing Disk Status

To view the status of the disk drives on the server:

1. On the Disk Utilities menu, click View Disk Status.



Disk Status as of 3/22/1998 @ 2:01:54pm

	Disk	On-line	Status
	1 (No label)	Yes	No errors. Total disk space: 4,084.76 MB Free disk space: 4,084.75 MB

2. To view the Disk Log associated with the drive, click the hyperlink next to the LED in the Status column.
3. Click Close to return to the Disk Utilities menu.

Administering Security (Users, Groups, and Network Shares)

On the Administration menu, click Security to open the Snap! Server Security menu. This menu provides hyperlinks to tools for:

- Listing and viewing information about active users
- Creating, modifying, and deleting user accounts
- Creating, modifying, and deleting groups

  A group is a collection of users. You use groups to define access rights to shares on the Snap! Server.

- Creating, modifying, and deleting network shares

  A network share is a reference to a folder on one of the Snap! Server's drives that is accessible to users on the network.

- Viewing security information about users, groups, and network shares

The Snap! Server supports using a Microsoft networking domain controller to authenticate a user. For such authentication to work properly, you must have done the following:

- Enabled Microsoft networking.
- Selected the Domain option on the Microsoft Networking page, as described in "Configuring Microsoft Networking" on page 29.

  The name of the domain specified on the Microsoft Networking page will be used for user authentication. If you've selected the Domain option, it is *not* necessary to create the users contained in the domain. The Snap! Server will communicate with the domain controller directly to authenticate a user. However, it will be necessary to create each group defined in the domain on the Snap! Server. This is required so that you can assign access rights to the Snap! Server shares using a group name.

NOTE The group name must exactly match the group names defined in the domain. Otherwise, users within the group will *not* be granted access to a share.

The Snap! Server has a default user named GUEST. The GUEST user is a member of the default group named EVERYONE. A GUEST user is anyone who is:

- Not recognized by the Snap! Server
- Not recognized by the domain controller
- A member of a group that is recognized by the domain controller but is *not* recognized by the Snap! Server

These unrecognized users, now recognized by the system as GUEST users, will have access to network shares that grant access to the EVERYONE group.

The EVERYONE group includes all users. Any new user that you create automatically becomes a member of the EVERYONE group. You can't delete or modify this group directly. However, you can remove all access rights associated with the EVERYONE group.

The Snap! Server has another default group named ADMIN that includes these three Administrator accounts: ROOT, SUPERVISOR, and ADMINISTRATOR.

For more information about Snap! Server security, see Appendix C, “Security and Access Control.”

The following tables summarize the Snap! Server’s default users and groups.

User	Member of group(s)	Changeable?
GUEST	EVERYONE	User can be deleted
ROOT	ADMIN EVERYONE	Cannot be deleted or removed from the Admin or Everyone group
ADMINISTRATOR	ADMIN EVERYONE	Cannot be deleted or removed from the Admin or Everyone group
SUPERVISOR	ADMIN EVERYONE	Cannot be deleted or removed from the Admin or Everyone group

Group	Includes	Changeable?
EVERYONE	All users	New users are automatically added; group cannot be deleted or modified
ADMIN	ROOT, ADMINISTRATOR, and SUPERVISOR	Users can be added to the group, but the group cannot be deleted

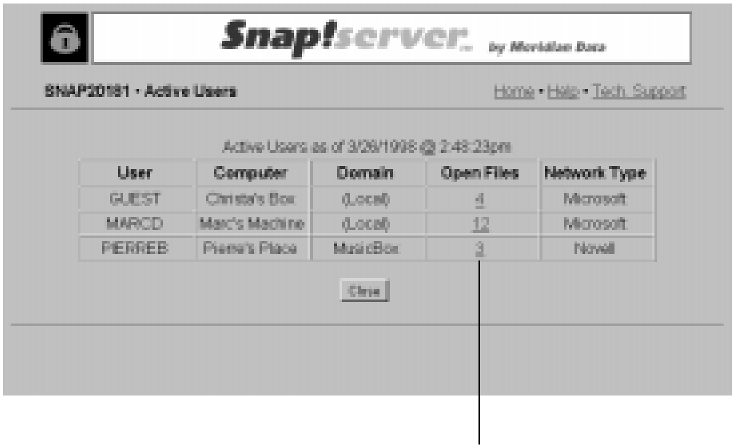
Listing Active Users

This topic describes how to list and view detailed information about all users who are currently connected to the Snap! Server.

NOTE NFS and HTTP users won't be listed on the Active Users page because these file sharing protocols are connectionless.

1. On the Security menu, click Active Users.

   The Active Users page appears, listing: all currently active users, the workstation from which they logged in, number of open files, and network protocol.



SNAP20181 • Active Users

Active Users as of 3/26/1998 @ 2:48:23pm

User	Computer	Domain	Open Files	Network Type
GUEST	Christa's Box	(Local)	4	Microsoft
MARCD	Marc's Machine	(Local)	12	Microsoft
PIERREB	Pierre's Place	MusicBox	3	Novell

Hypertext link to list of user's open files

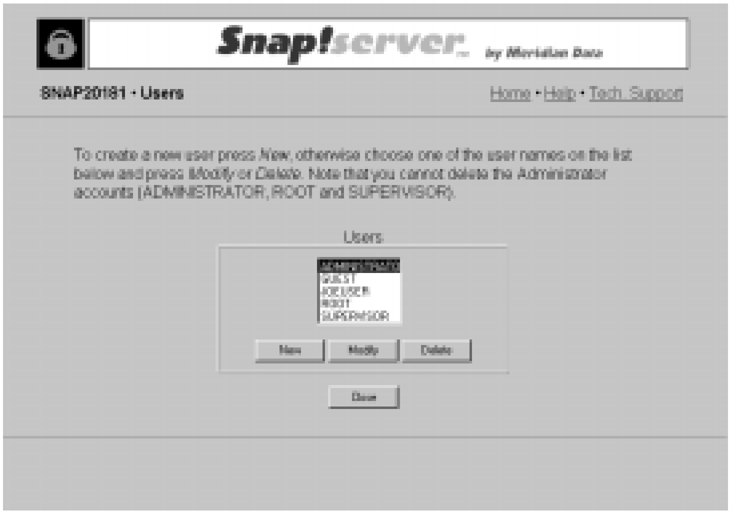
2. To view the list of open files for a user, click the number in the Open Files field.

   The list may include files that you believe to be closed. Opportunistic locking, if used, causes this. It's normal system behavior, which you can ignore. For information on opportunistic locking, see "Advanced Microsoft Networking" on page 83.

3. To return to the Security menu, click Close.

Creating, Modifying, and Deleting User Accounts

Click Users on the Security menu to open the page where you create, modify, and delete user accounts.



SNAP20181 • Users

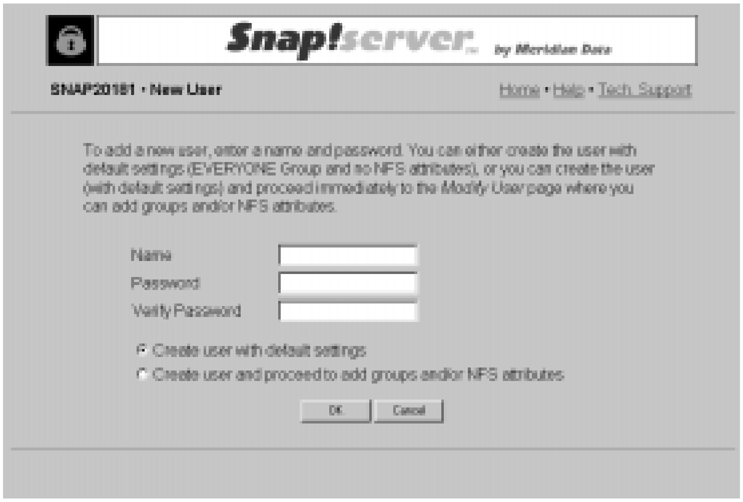
To create a new user press *New*, otherwise choose one of the user names on the list below and press *Modify* or *Delete*. Note that you cannot delete the Administrator accounts (ADMINISTRATOR, ROOT and SUPERVISOR).

NOTE The GUEST user allows any user who is not explicitly defined on the Snap! Server to gain access to the server and thereby gain access to any share that permits access to groups that GUEST is a member of. GUEST is a member of the EVERYONE group. Deleting the GUEST user (or setting a password for GUEST) will prevent any user who is not explicitly known to the Snap! Server or the domain controller, if applicable, from gaining access to the Snap! Server or any of its shares.

Creating New Users

To create a new user account, you need to provide a user name and a password, and designate the groups to which the user belongs.

1. On the Users page, click New to open the New User page.



SNAP20181 • New User

To add a new user, enter a name and password. You can either create the user with default settings (EVERYONE Group and no NFS attributes), or you can create the user (with default settings) and proceed immediately to the *Modify User* page where you can add groups and/or NFS attributes.

Name

Password

Verify Password

● Create user with default settings

○ Create user and proceed to add groups and/or NFS attributes

2. On the New User page, type the user name in the Name field.

   The name can contain up to 20 alphanumeric characters.

3. Optionally, type the new user’s password in the Password field.

   The password is case-sensitive and can contain up to 14 alphanumeric characters.

4. Type the password again in the Verify Password field.

5. Choose the default settings option (see “Using the Default Account Settings,” next) or specify your own settings (see “Specifying Your Own Account Settings” on page 63).

Using the Default Account Settings

To set up the user account with the default account settings:

1. Select the Create User with Default Settings option.

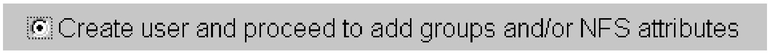
2. Click OK.

   Clicking OK returns you to the Users page. The new user name appears in the Users list. By default, the user account you created is a member of the group named EVERYONE and has no NFS attributes.

Specifying Your Own Account Settings

To set up the user account with new default settings:

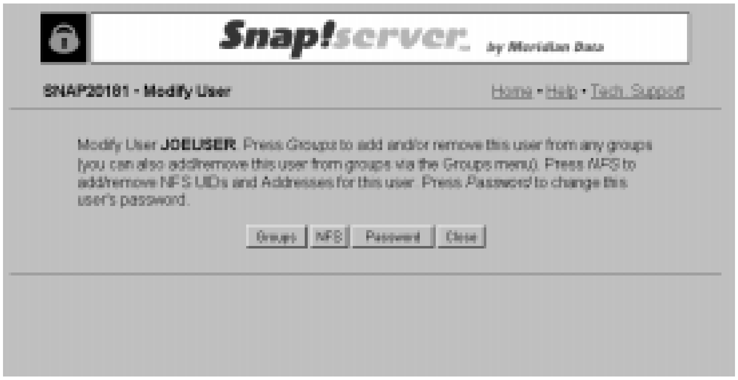
1. Select this option.



● Create user and proceed to add groups and/or NFS attributes

2. Click OK.

   The Modify User page appears.



SNAP20181 - Modify User

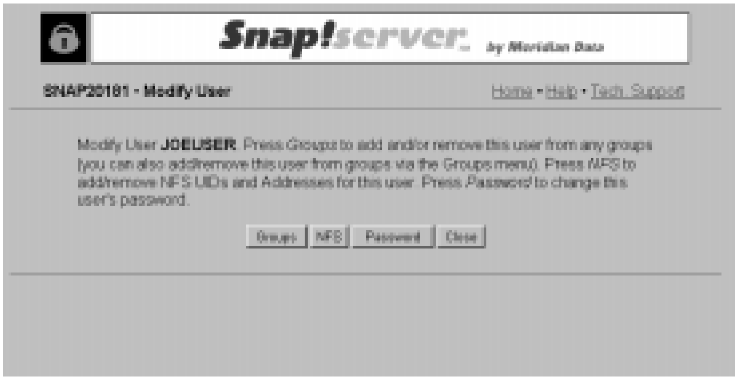
Modify User **JOEUSER**. Press *Groups* to add and/or remove this user from any groups (you can also add/remove this user from groups via the Groups menu). Press *NFS* to add/remove NFS UIDs and Addresses for this user. Press *Password* to change this user's password.

On this page, you can set up the user's group memberships and add or remove NFS properties. See "Modifying User Accounts," next.

Modifying User Accounts

To modify a user account, do the following.

1. On the Snap! Server Users page, select the user name from the Users list.
2. Click Modify to open the Modify User page.



SNAP20181 - Modify User

Modify User **JOEUSER**. Press *Groups* to add and/or remove this user from any groups (you can also add/remove this user from groups via the Groups menu). Press *NFS* to add/remove NFS UIDs and Addresses for this user. Press *Password* to change this user's password.

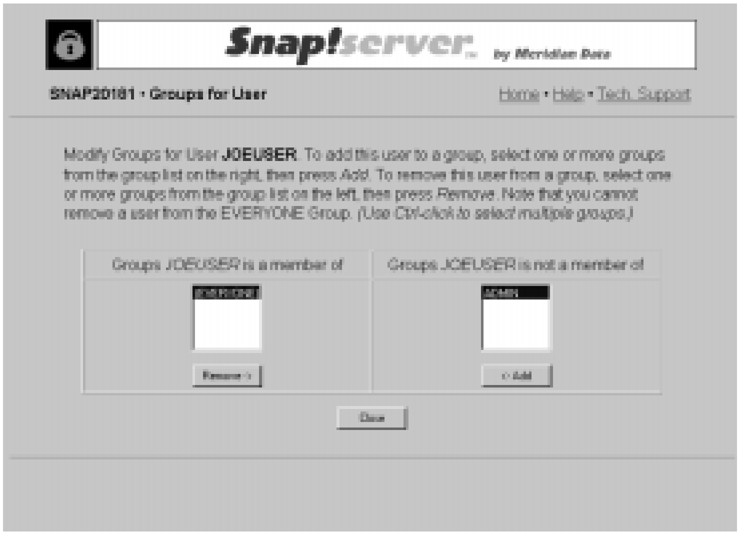
On this page, you can:

- Set up the user’s group memberships (see “Setting Up Group Membership,” next).
- Add or remove NFS properties (see “Modifying NFS Properties” on page 66).
- Change the user’s password (see “Changing the User’s Password” on page 70).

Setting Up Group Membership

To set up the user’s group membership:

1. On the Modify User page, click Groups to open the Groups for User page.



SNAP20181 • Groups for User

Modify Groups for User **JOEUSER**. To add this user to a group, select one or more groups from the group list on the right, then press *Add*. To remove this user from a group, select one or more groups from the group list on the left, then press *Remove*. Note that you cannot remove a user from the EVERYONE Group. *(Use Ctrl-click to select multiple groups.)*

Groups *JOEUSER* is a member of	Groups *JOEUSER* is not a member of
EVERYONE	ADMIN

2. To add the user to one or more groups, select the group(s) from the list of groups the user is not currently a member of, and then click Add.
3. To remove the user from one or more groups, select the group(s) from the list that the user currently has membership in, and then click Remove.
4. Click Close to return to the Modify User Page.

Modifying NFS Properties

Use the NFS properties to set up security and access rights for NFS users. The NFS protocol identifies its users by a combination of host IP address and UID, as described in the following paragraphs.

- Host IP address

  The host IP address is the IP address of the system (usually UNIX) from which the user is connecting. However, the host could also be a DOS or Windows workstation running PCNFS software. Note that the Snap! Server allows system administrators to group multiple hosts together by means of the IP address mask.

- UID

  All UNIX users are assigned a UID (user identification number). After authenticating a user by his user name and password, UNIX then uses the UID to identify the user internally or when issuing requests to a NFS server. Unlike UNIX, PCNFS hosts rely on the Snap! Server both to authenticate users (by their user name and password) and to assign them a UID.

The NFS properties associate one or more NFS user identities to a Snap! Server user. This allows the Snap! Server to recognize an NFS user as a local user. By virtue of this recognition, the NFS user is granted the same privileges on the Snap! Server as the corresponding local user.

For example, user Joe has user account *joeuser* on a UNIX system. To allow Joe to access files on the Snap! Server, you first create the Snap! Server account *JOEUSER* and assign it a password. The user name and password need not match those used on the UNIX host. To make this account usable from NFS, you then create an NFS property for the account, using Joe's UID and the IP address from the UNIX system. If Joe also uses a PC workstation running PCNFS, you can create a second NFS property entry with the IP address from Joe’s PC and a unique UID that you assign to him for use with the Snap! Server.

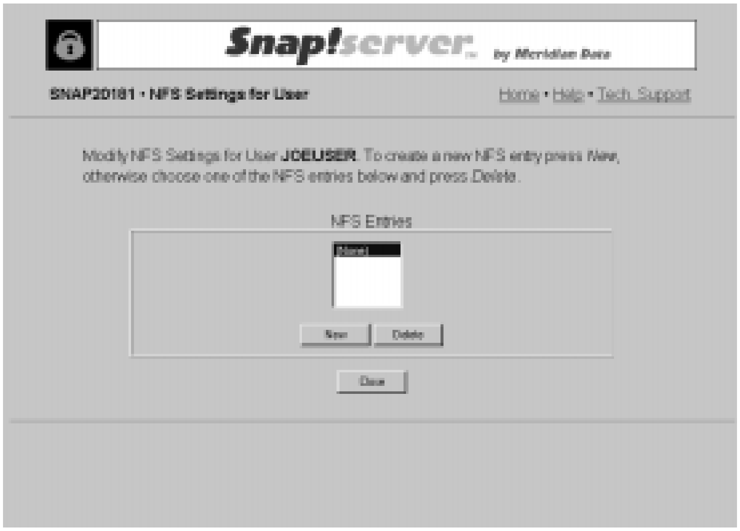
To create or modify a user's NFS properties, specify the user's UID, IP address, and IP address mask. Multiple NFS properties can be defined for a user. However, each NFS property must differ from the other NFS properties defined in your Snap! Server by at least one of the following:

- A unique IP address (or range of IP addresses, as determined by the combo of IP address and IP address mask)
- A unique UID

For example, you may have multiple users from the same UNIX host. All of these users share the same IP address. However, each user’s UID will be different. Similarly, two separate users may have the same UID on their respective UNIX hosts. Their host's IP address, however, will be different. In either of these cases, you can use the combination of IP address and UID to specify a unique NFS property for these users.

To set up the NFS property, use the following procedure.

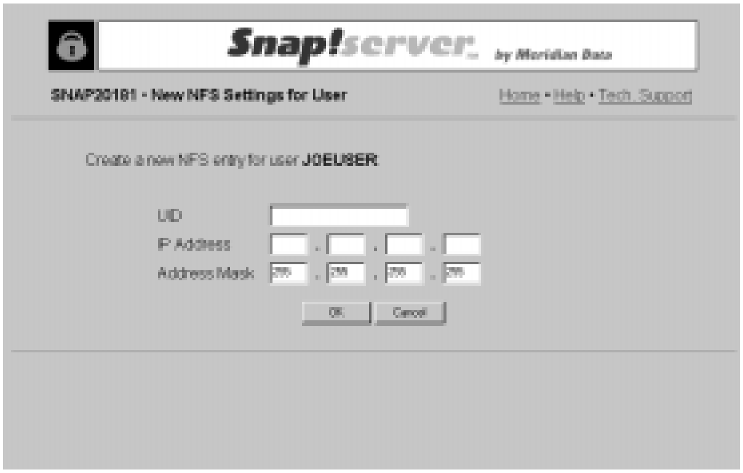
1. On the Modify User page, click NFS to open the NFS Settings for User page.



SNAP20181 • NFS Settings for User

Modify NFS Settings for User **JOEUSER**. To create a new NFS entry press *New*, otherwise choose one of the NFS entries below and press *Delete*.

2. To create a new NFS entry, click New.



SNAP20181 - New NFS Settings for User

Create a new NFS entry for user **JOEUSER**

UID

IP Address . . .

Address Mask 255 . 255 . 255 . 255

3. On the New NFS Settings for User page, do the following.

   a. Type the user’s UID in the field provided.

      On a UNIX host, the UID for a specific user can be found in the */etc/passwd* file, in an NIS (yp) passwd map, or in an NIS+passwd table. You can also find the UID on a UNIX host by logging into the system as the specified user and typing: **id**.

      PCNFS hosts rely on the Snap! Server to provide them with a UID. In this case, you can assign any arbitrary number as a UID, as long as this number, in combination with the IP address, uniquely identifies your NFS user.

   b. In the IP Address field, type the IP address of the host on which the NFS user referenced by the UID will be logging in.

   c. Type the address mask in the field provided.

      The address mask, which is similar to an IP netmask, identifies the portion of the IP address that you are interested in. The default value for the address mask—255.255.255.255—indicates that the full IP address must be matched. When the address mask is set to this value, an NFS user with the UID you entered in step 3a will match only if its host IP address is exactly the same as the IP address you entered in step 3b.

If the address mask is set to 255.255.255.0, the user can log in with the UID that you entered in step 3a from any host in the subnet whose IP address matches the first three numbers of the IP address you entered in step 3b. In this case, the address mask is applied to the IP address before checking for duplicate IP addresses.

This combination	Matches
UID = 101	UID = 101
IP = 192.168.45.2	IP = 192.168.45.174
IP mask = 255.255.255.0	IP mask = 255.255.255.0

d. Click OK to save the NFS setting and return to the NFS Settings for User page.

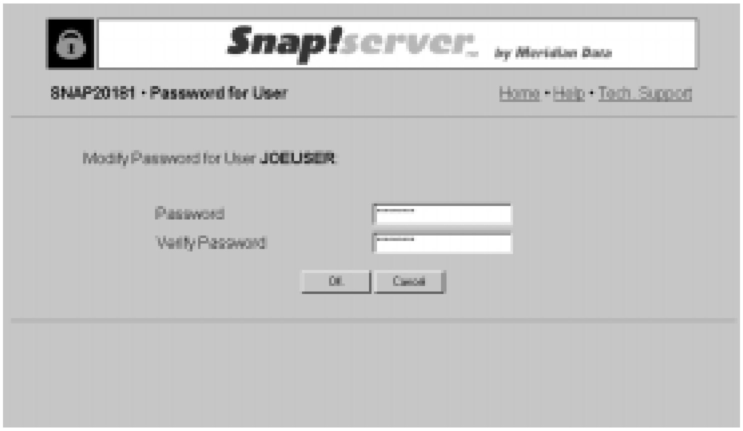
4. To delete an NFS entry, select the entry from the NFS Entries list box, and then click Delete.
5. Click Close to return to the Modify User Page.

IMPORTANT If you delete the GUEST account or restrict access to it, you must create one or more NFS properties for ROOT. Without these, NFS users cannot access shares on the Snap! Server.

Changing the User's Password

To change the password:

1. On the Modify User page, click Password to open the Password for User page.



SNAP20181 • Password for User

Modify Password for User JOEUSER

Password

Verify Password

2. Type the new password in the Password field.

   The password is case-sensitive and can contain up to 14 alphanumeric characters.

3. Type the password again in the Verify Password field.
4. Click OK to return to the Modify User page.

NOTE Changing the password for either the ADMINISTRATOR, ROOT, or SUPERVISOR account changes the password for all three accounts.

Deleting User Accounts

To delete a user account, do the following:

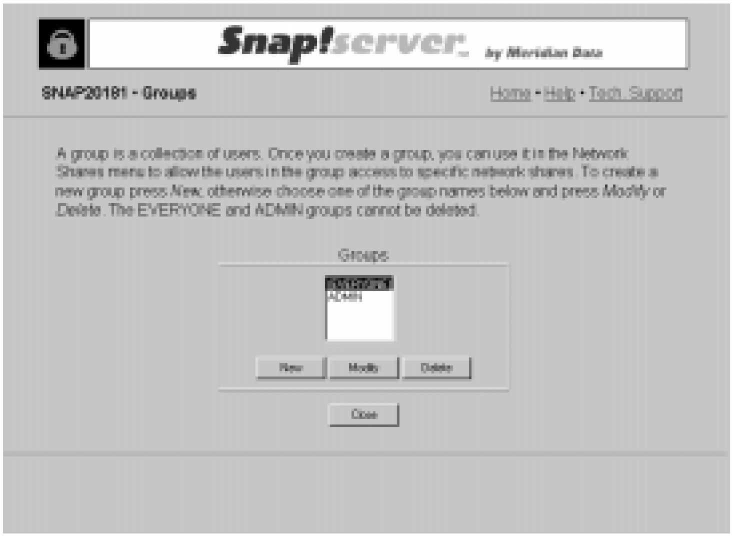
1. On the Users page, select the user name from the Users list.
2. Click Delete.
3. Click Yes to confirm that you want to delete the user account.

NOTE You cannot delete the ADMINISTRATOR, ROOT, and SUPERVISOR accounts.

Clicking Yes returns you to the Users page. Then click Close to return to the Snap! Server Security menu.

Creating, Modifying, and Deleting Groups

To create, modify, and delete groups, click Groups on the Snap! Server Security menu. The Groups page appears.



SNAP20181 - Groups

A group is a collection of users. Once you create a group, you can use it in the Network Shares menu to allow the users in the group access to specific network shares. To create a new group press *New*, otherwise choose one of the group names below and press *Modify* or *Delete*. The EVERYONE and ADMIN groups cannot be deleted.

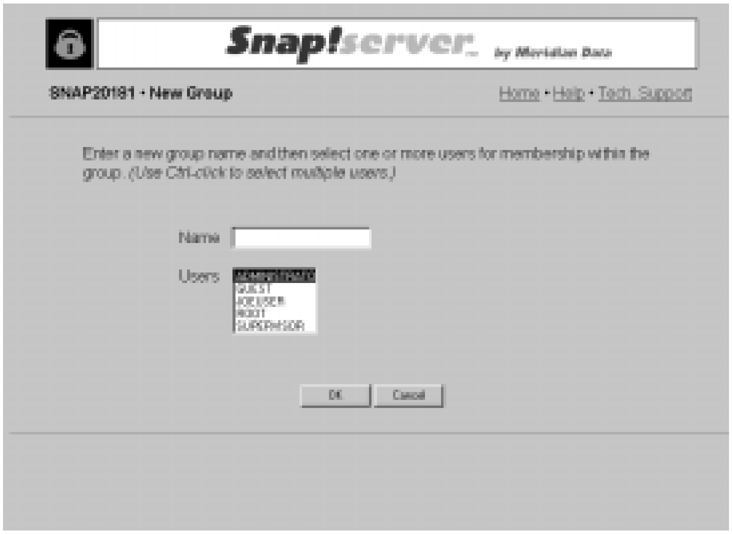
Groups

EVERYONE
ADMIN

Creating Groups

To create a group, do the following.

1. On the Groups page, click New.



SNAP20181 - New Group

Enter a new group name and then select one or more users for membership within the group. *(Use Ctrl-click to select multiple users.)*

Name

Users

ADMINISTRATOR
GUEST
JOEUSER
ROOT
SUPERVISOR

2. On the New Group page, type the name for the group in the Name field.

   The name can contain up to 48 alphanumeric characters.

3. From the Users list, select one or more users to add to the group.

   If you're using a domain controller for authentication, you can skip this step.

4. Click OK.

   Clicking OK returns you to the Groups page. The new group name appears in the Groups list.

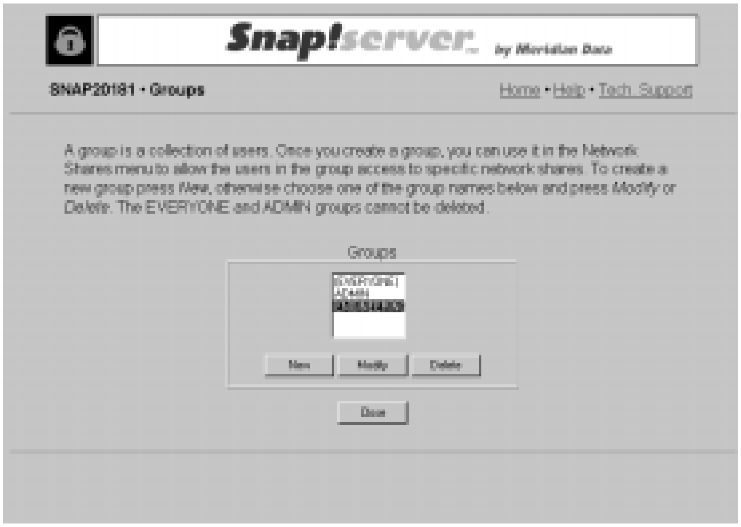
After creating a group, you can grant the group and all of its associated users access to specific network shares. For more information, see "Administering Network Shares" on page 74.

Changing Group Membership

To modify a group, do the following.

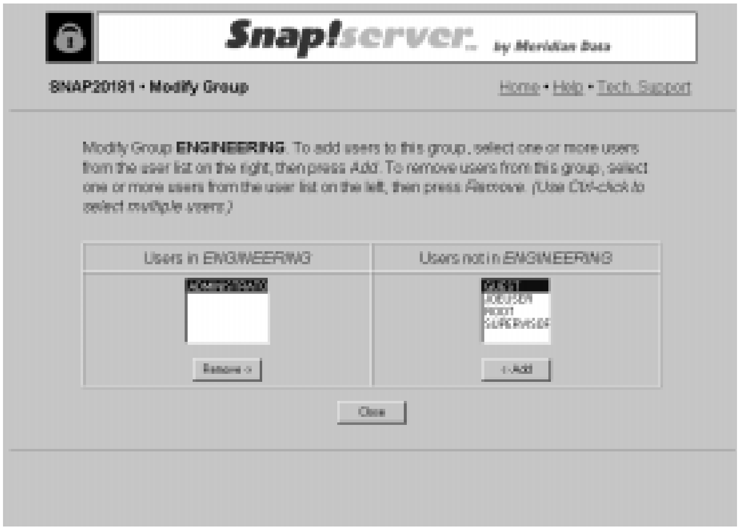
1. On the Snap! Server Groups page, select the group to modify from the Groups list.

   You cannot modify the EVERYONE group. The example uses a group named ENGINEERING.



A group is a collection of users. Once you create a group, you can use it in the Network Shares menu to allow the users in the group access to specific network shares. To create a new group press *New*, otherwise choose one of the group names below and press *Modify* or *Delete*. The EVERYONE and ADMIN groups cannot be deleted.

2. Click Modify to open the Modify Group page.



SNAP20181 • Modify Group

Modify Group **ENGINEERING**. To add users to this group, select one or more users from the user list on the right, then press *Add*. To remove users from this group, select one or more users from the user list on the left, then press *Remove*. *(Use Ctrl-click to select multiple users.)*

3. To add one or more users to the group, select the name(s) from the list of users who are not currently in the group, and then click Add.
4. To remove one or more users from the group, select the name(s) from the list of users who currently have membership in the group, and then click Remove.
5. To return to the Snap! Server Groups Page, click Close.

NOTE If you have set up your Snap! Server as part of a Microsoft network domain, you do not need to add domain users to the Snap! Server groups that are defined on the domain controller.

Deleting Group

To delete a group, do the following.

1. From the Groups list on the Snap! Server Groups page, select the group to delete.

   You cannot delete the ADMIN or EVERYONE groups.

2. Click Delete.

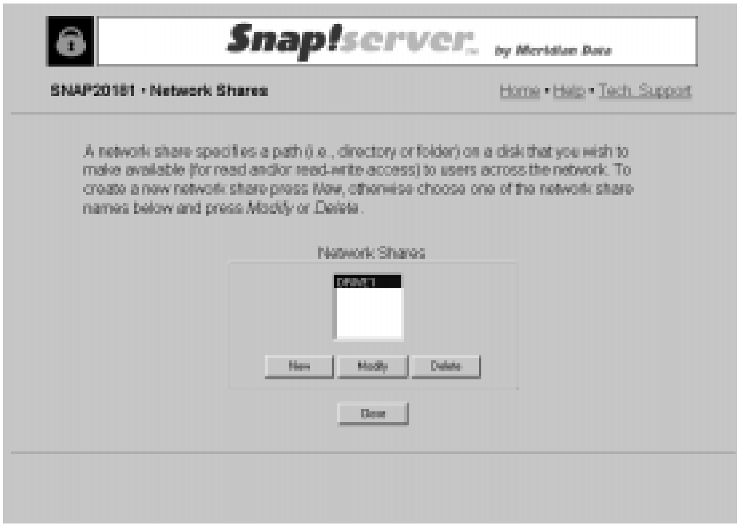
3. Click Yes to confirm that you want to delete the group.

   Clicking Yes returns you to the Groups page. Then click Close to return to the Snap! Server Security menu.

Administering Network Shares

A network share is a reference to a folder on one of the Snap! Server's disks that you want to make available for read and write access to users on the network.

To administer network shares, click Network Shares on the Snap! Server Security menu. On the Network Shares page that appears, you can create a new share or modify or delete an existing share.



A network share specifies a path (i.e., directory or folder) on a disk that you wish to make available (for read and/or read-write access) to users across the network. To create a new network share press *New*, otherwise choose one of the network share names below and press *Modify* or *Delete*.

Shares provide your only means of restricting users' access to a folder on the Snap! Server. When a user connects to a share, he has the same access rights to every file and folder within the share. When defining shares, be careful that you don't inadvertently grant access to a restricted file or folder. The following example illustrates how access can be inadvertently granted to a restricted file or folder.

Suppose that you have the following directory structure:
\Path1
\Path1\Path2

You have two shares—share1 and share2—with the following attributes:

share1:	full access,	references \Path1
share2:	read-only access,	references \Path1\Path2

A user who connects to share1 will have *full* access to every file and folder within \Path1 *as well as* within \Path1\Path2, even though \Path1\Path2 is restricted by share2. However, if the same user connects to share2, he will have read-only access to every file and folder within \Path1\Path2.

You can resolve the problem by moving the contents of the \Path1\Path2 folder to a new folder that is not contained within \Path1. For example, the new directory structure might be:

\Path1 ← share1
\Path2 ← share2

and share2 would now reference \Path2. Users cannot circumvent the read-only access on share2 by connecting to share1.

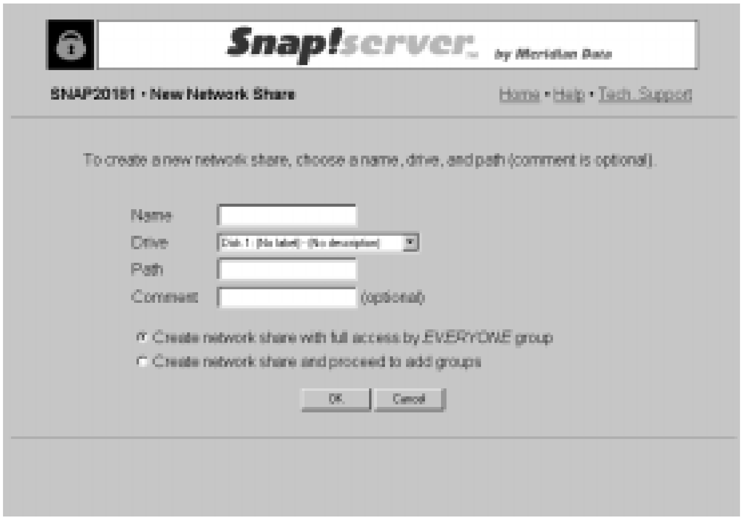
For more information about shares and setting up security, see Appendix C, “Security and Access Control.”

Creating a New Share

To create a new network share, you need to define the name, drive, and path for the share, and then designate the groups that can or cannot access the share. Follow these steps.

1. Click New on the Network Shares page.

   The New Network Share page appears.



Snap!server by Meridian Data
SNAP20181 • New Network Share
Home • Help • Tech. Support
OK
Cancel

To create a new network share, choose a name, drive, and path (comment is optional).

Name
Drive: Disk 1 : (No label) - (No description)
Path
Comment (optional)

● Create network share with full access by *EVERYONE* group
○ Create network share and proceed to add groups

2. Type the share name in the Name field.

   The name can contain up to 12 alphanumeric characters.

3. From the Drive list box, select the drive on which to create the share.
4. Type the path in the Path field.

   For example, type: \DATADIR

   The path can contain up to 254 alphanumeric characters.

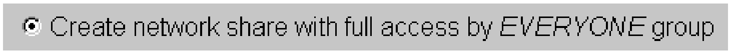
   If you type a path that doesn’t exist, a warning appears prompting you to create the path. Creating a share to a directory that doesn’t exist results in an inaccessible share.

5. Optionally, type a descriptive comment, which can contain up to 47 printable characters.
6. Choose the default option (see “Assigning the Default Group Access,” next) or designate your own access permissions (see “Assigning Your Own Group Access Specifications” on page 76).

Assigning the Default Group Access

To create the new network share with the default group access:

1. Check this box.



● Create network share with full access by *EVERYONE* group

   Full access indicates read and write privileges.

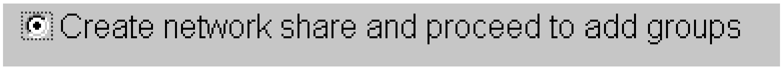
2. Click OK.

By default, the EVERYONE group has full read and write access to the new share you created.

Assigning Your Own Group Access Specifications

To create the new network share with your own group access specifications:

1. Check this box.



● Create network share and proceed to add groups

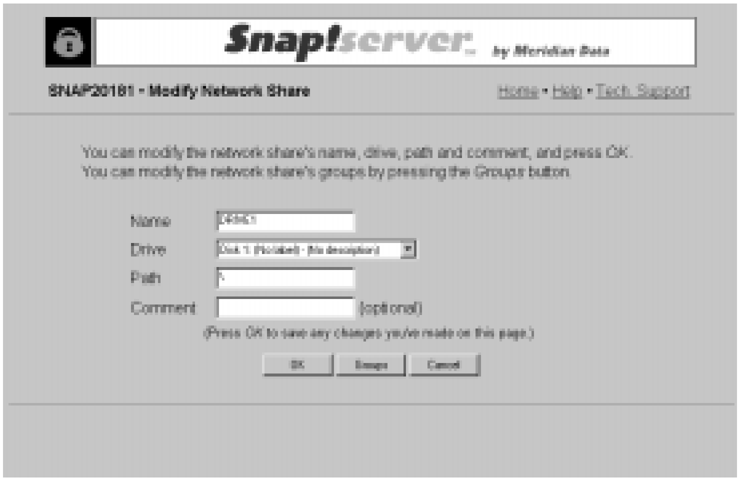
2. Click OK.

3. On the Groups for Network Share page that appears, you can specify the groups that have access to the new share as well as their access privileges. For more information, see “Changing a Group’s Access Rights to a Network Share” on page 78.

Modifying a Network Share

You can change the name, drive, and path of a network share, as well as the groups that can access the share. To modify a network share, follow these steps.

1. From the Network Shares list on the Network Shares page, select the name of the share to modify.
2. Click Modify to open the Modify Network Share page.



SNAP20181 - Modify Network Share

You can modify the network share's name, drive, path and comment, and press OK.
You can modify the network share's groups by pressing the Groups button.

Name: [illegible]
Drive: Disk 1 (No label) - (No description)
Path: \
Comment: (optional)

(Press OK to save any changes you've made on this page.)

3. To change the share name, type the new name in the Name field.

   The name can contain up to 12 alphanumeric characters.
4. To change the drive, select a new drive from the Drive list box.
5. To change the path, type the new path in the Path field.

   The path can contain up to 254 alphanumeric characters.
6. To change the descriptive comment, type your changes in the Comment field.

7. Do one of the following:

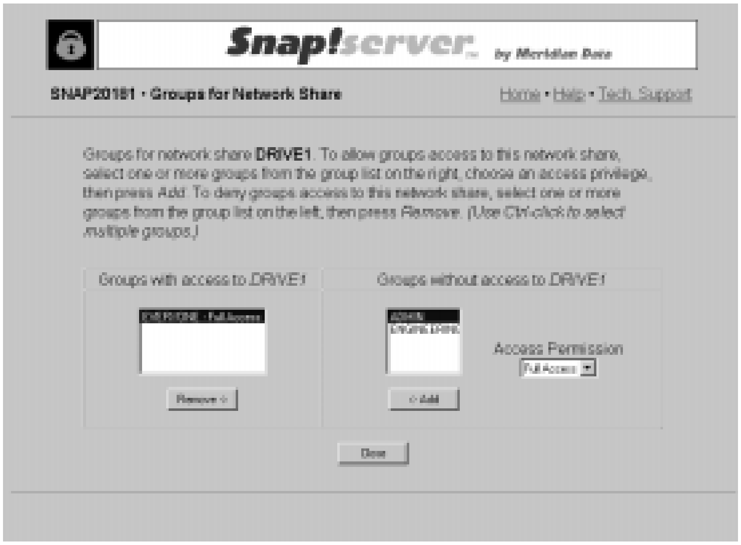
   a. If you’re finished making changes, click OK to return to the Snap! Server Network Shares page.

   b. If you want to allow or deny a group’s access to the share, click Groups to open the Groups for Network Share page.

   To continue, see “Changing a Group’s Access Rights to a Network Share,” next.

Changing a Group’s Access Rights to a Network Share

Click Groups on the Modify Network Share page to open the Groups for Network Share page.



Snap!server by Meridian Data
Home • Help • Tech. Support
Groups with access to DRIVE1
EVERYONE - Full Access
Groups without access to DRIVE1
ADMIN
Access Permission
Full Access
Remove ->
<- Add
Done

SNAP20181 • Groups for Network Share

Groups for network share **DRIVE1**. To allow groups access to this network share, select one or more groups from the group list on the right, choose an access privilege, then press *Add*. To deny groups access to this network share, select one or more groups from the group list on the left, then press *Remove*. *(Use Ctrl-click to select multiple groups.)*

NOTE If you’re creating a new network share and you’ve chosen not to use the default group access settings, the Groups for Network Share page appears when you click OK on the New Network Share page.

To allow one or more groups access to the share, follow these steps.

1. Select one or more names from the list of groups that don’t have access to the network share you’re modifying.

2. Select an access privilege from the Access Permission list box.

3. Click Add.

   The group(s) and permission you specified appear in the list of groups that currently have access to the network share you're modifying.

NOTE Granting access to the EVERYONE group permits any Snap! Server user or any user with domain controller authentication to access the share. If the GUEST account exists, any user—even those not recognized by the Snap! Server—will have access to the share.

To deny one or more groups access to the share, follow these steps.

1. Select one or more names from the list of groups that currently have access to the network share you're modifying.
2. Click Remove.

   The name(s) of the group(s) you removed appear in the list of groups that currently do not have access to the network share you're modifying.

NOTE Removing a group from the list of groups that have access to a share is not the same as adding the group to the list and assigning Deny Access as the group's access permission. Users in a group that is explicitly denied access to a share may not access that share even if other groups they belong to are granted access to the same share.

Deleting a Network Share

To delete a network share, follow these steps.

1. From the Network Shares list on the Network Shares page, select the name of the share to delete.
2. Click Delete.
3. Click Yes to confirm that you want to delete the network share.

   Clicking Yes returns you to the Network Shares page. To return to the Snap! Server Security menu, click Close.

Viewing Security

To see detailed information about all users, groups, and network shares, do the following.

1. On the Security menu, click View Security.
2. To return to the Security menu, click Close.

Changing Network Settings

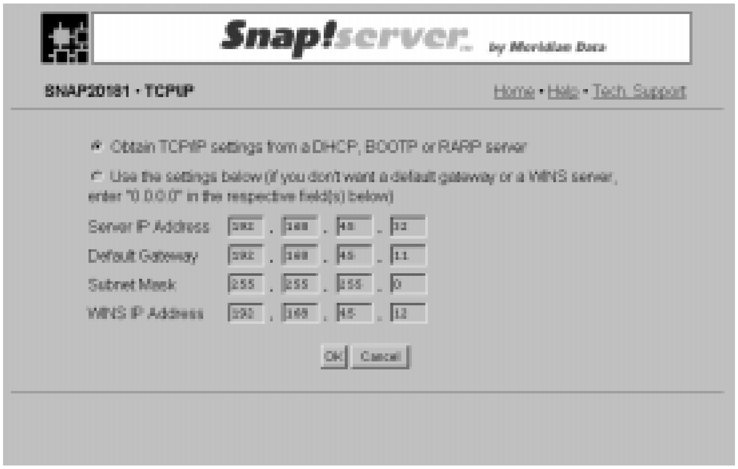
To change the Snap! Server's TCP/IP address and reconfigure network protocols, click Network Settings on the Snap! Server Administration menu.

NOTE Many network configuration changes do not take effect until the server reboots. You will be notified you when you make changes that require rebooting. If you press Reboot Later, your changes are saved but won't take affect until the server is rebooted.

Changing the TCP/IP Address

To change the Snap! Server's TCP/IP address:

1. Click TCP/IP on the Network Settings menu.



● Obtain TCP/IP settings from a DHCP, BOOTP or RARP server

○ Use the settings below (if you don't want a default gateway or a WINS server, enter "0.0.0.0" in the respective field(s) below)

Server IP Address 192 . 168 . 45 . 12

Default Gateway 192 . 168 . 45 . 11

Subnet Mask 255 . 255 . 255 . 0

WINS IP Address 192 . 168 . 45 . 12

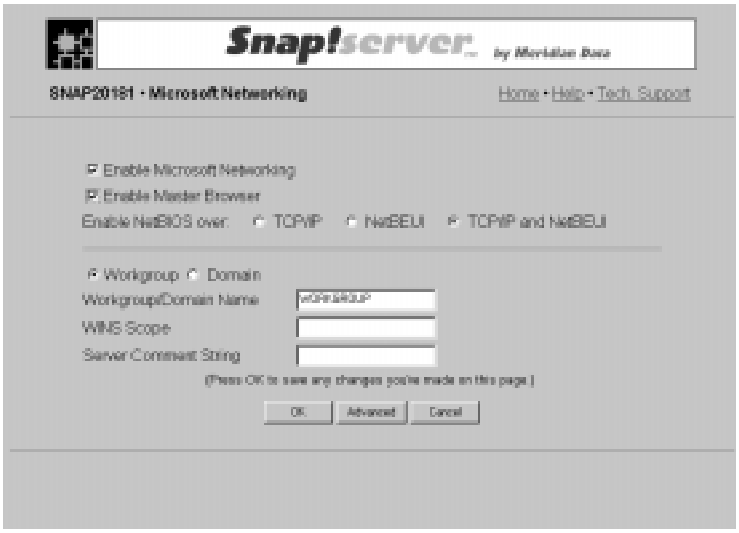
2. On the TCP/IP page, do one of the following:
   a. To obtain an automatically assigned address, gateway, and subnet mask from a DHCP, BOOTP, or RARP server on the network, select the first option.
   b. To manually configure a specific address, select the second option.

      Type the appropriate values in the fields provided. If you don't want to specify a default gateway or WINS IP address, type the value *zero* (0) in each field.

3. Click OK to return to the Network Settings menu.

Reconfiguring Microsoft Networking

Click Microsoft Networking on the Network Settings menu to open the page for reconfiguring Microsoft-compatible networking.



Snap! server by Meridian Data
SNAP20181 · Microsoft Networking
Home • Help • Tech. Support

☑ Enable Microsoft Networking
☑ Enable Master Browser
Enable NetBIOS over: ○ TCP/IP ○ NetBEUI ● TCP/IP and NetBEUI

● Workgroup ○ Domain
Workgroup/Domain Name: WORKGROUP
WINS Scope:
Server Comment String:

(Press OK to save any changes you've made on this page.)

- To enable an option (described in the table that follows), check the box next to its name.
- To disable an option, uncheck the box next to its name.
- To save your changes, click OK.
- To open the Advanced Microsoft Networking page, click Advanced.

NOTE If you intend to continue with Advanced Microsoft networking (described on page 83), you must first save any changes you've made on the Microsoft Networking page.

The following table describes the options on the Microsoft Networking page.

Options	Description	Default
Microsoft Networking	Enables or disables Microsoft-compatible networking	Enabled
Master Browser	The Snap! Server can maintain the master list of all computers belonging to a specific workgroup. At least one Master Browser must be active per workgroup. If no Master Browser is active for the workgroup, leave this option enabled.	Enabled
NetBIOS over: TCP/IP NetBEUI TCP/IP and NetBEUI	Specifies the transport layer used. NetBIOS over NetBEUI is suitable for small, unrouted networks. Larger, routed networks need to enable NetBIOS over TCP/IP. **NOTE** If you enable only NetBEUI for Microsoft networking, TCP/IP will still be available for HTTP and NFS file-sharing protocols.	TCP/IP and NetBEUI
Workgroup Domain	Specifies either workgroup-based or domain-based operation **NOTE** If you enable the Domain option, you must enter all relevant groups defined by the domain. Use the Snap! Server's Security page to do so. See "Creating Groups" on page 71.	Workgroup

Options	Description	Default
Workgroup/Domain Name	Specifies either: the name of the workgroup for workgroup-based operation; or your Microsoft networking domain name for domain-based operation. The name can contain up to 15 alphanumeric characters.	WORKGROUP
WINS Scope	Specifies the Windows Internet Name Service scope identifier (for managing NETBIOS name resolution). The string can contain up to 63 characters (letters, numbers, and hyphens only).	(None)
Server Comment String	Optional descriptive comment; can contain up to 48 printable characters.	(None)

Advanced Microsoft Networking

Click Advanced at the bottom of the Microsoft Networking page to open the Advanced Microsoft Networking page.

To use the advanced features, you must have already saved any changes you've made on the Microsoft Networking page.

On the Advanced Microsoft Networking page, you can do one of the following:

- Enable Opportunistic Locking by checking the box.

  By default, this parameter is selected to enhance system performance.

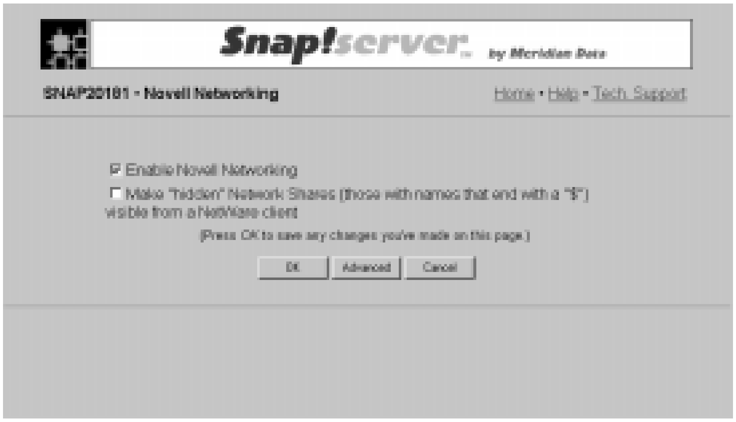
- Disable Opportunistic Locking by unchecking the box.

  Some software may require that opportunistic locking be disabled.

Click OK to return to the Microsoft Networking page.

Reconfiguring Novell Networking

Click Novell Networking on the Network Settings menu to open the page for reconfiguring Novell-compatible networking.



SNAP20181 - Novell Networking

☑ Enable Novell Networking

□ Make "hidden" Network Shares (those with names that end with a "$") visible from a NetWare client

(Press OK to save any changes you've made on this page.)

- To enable Novell Networking, check the box.

  By default, this parameter is on.

- To disable Novell Networking, uncheck the box.
- To make hidden network shares visible from a NetWare client, check the box.

  Normally, network share names that end with the dollar-sign character are hidden from users. These shares cannot be browsed (they will not appear in a server’s volume list) or mapped to. If you make hidden network shares visible, Novell users can browse and map them.

- To save your changes, click OK.

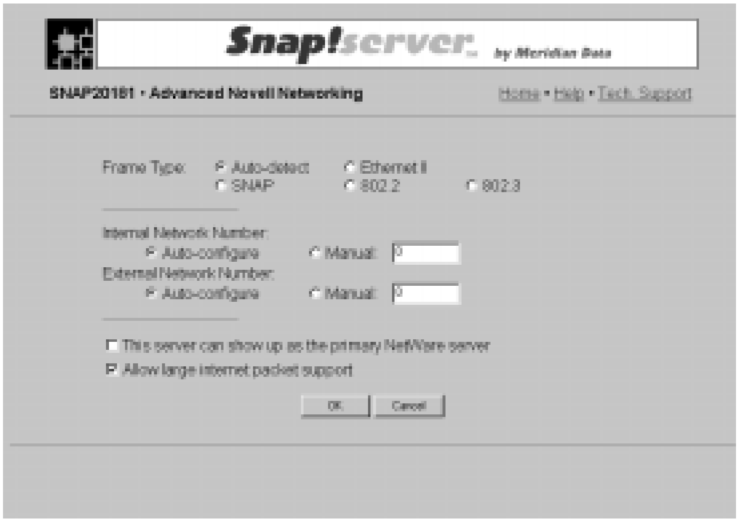
  If you intend to continue with Advanced Novell Networking (described next), you must first save any changes you’ve made on the Novell Networking page.

- To open the Advanced Novell Networking page, click Advanced.

Advanced Novell Networking

For most of its setup parameters, the Snap! Server relies on other NetWare servers already configured for Novell networking. In cases where the default settings are not sufficient, you can change the server’s configuration. For more detailed information on advanced Novell networking, see Appendix E, “Novell Networking: Advanced Setup.”

Click Advanced at the bottom of the Novell Networking page to open the Advanced Novell Networking page.



SNAP20181 • Advanced Novell Networking

Frame Type: ● Auto-detect ○ Ethernet II ○ SNAP ○ 802.2 ○ 802.3

Internal Network Number:
● Auto-configure ○ Manual: 0

External Network Number:
● Auto-configure ○ Manual: 0

☐ This server can show up as the primary NetWare server

☒ Allow large internet packet support

Specifying the Frame Type

The Snap! Server supports the four standard Ethernet frame types used with Novell networking: Ethernet SNAP, Ethernet II, 802.2, and 802.3. To change the Ethernet Frame Type, select one of the following:

- Auto-detect (the default)
- SNAP
- Ethernet II
- 802.2
- 802.3

When the frame type is set to Auto-detect, the server can accept incoming packets of all frame types currently configured on your Novell network and generate outgoing packets with the correct frame. However, if a server supports multiple frame types, Novell networking requires that each frame type be assigned a separate external network number. (See “Specifying the External Network Number,” next.) When you reconfigure the Snap! Server to support a specific frame type, it only responds to incoming packets of that frame type.

Specifying the Internal Network Number

The internal network number uniquely identifies a file server on a Novell network. Your Snap! Server has been preconfigured with a default internal network number (set to the lowest four bytes in the server's Ethernet host number). If this number conflicts with that of another server on the network, you'll need to change it manually.

To manually specify the internal network number:

1. Select Manual.
2. Type the number in the field provided.

NOTE Setting the internal number to a number that is already used by another Snap! Server or NetWare server can cause problems with Novell networking clients. By default, the internal network number is set to the last eight hexadecimal characters in the Snap! Server's Ethernet address, which can be found on the View Network Settings page. See Appendix E, "Novell Networking: Advanced Setup," for more information.

Specifying the External Network Number

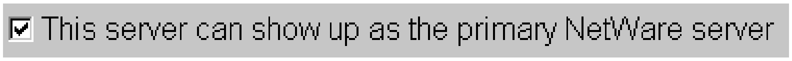
The external network number identifies each logical network segment in a Novell network. The Snap! Server can operate on one to four network segments—one for each Ethernet frame type that the server is configured to support. By default, the Snap! Server automatically configures its external network number(s) by listening to SAP broadcasts from other NetWare servers. However, in situations where the auto-configuration option is inadequate, you can set the external network number manually. Meridian Data generally recommends that you do this only when the Snap! Server is configured to support a single Ethernet frame type, or if your Snap! Server is the only NetWare server on the network.

To manually specify the number:

1. Select Manual.
2. Type the number in the field provided.

Configuring Snap! Server to Show Up as the Primary Server

If you want your Snap! Server to operate without other NetWare servers present on the same network, then you need to enable the option that allows it to show up as the primary NetWare server. To do so, check this box.



☑ This server can show up as the primary NetWare server

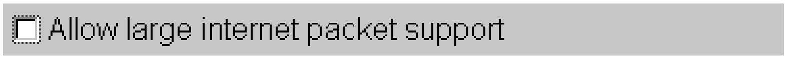
NOTE Select this option *only* if you have replaced the virtual SYS share with a true SYS share. See Appendix E, “Novell Networking: Advanced Setup,” for more information. Typically, you will also need to manually specify an external network number.

Allowing Large Internet Packet Support

For optimal file transfer performance, the Snap! Server is preconfigured to negotiate the maximum packet size with clients on the same network as the server.

However, in the case of routers that do not support Ethernet packets that contain more than 512 bytes of data, you may need to disable large internet packet support. Doing so forces the Snap! Server to negotiate a smaller packet size with clients that are not on the same network segment as the server.

To disable large internet packet support, uncheck this box.

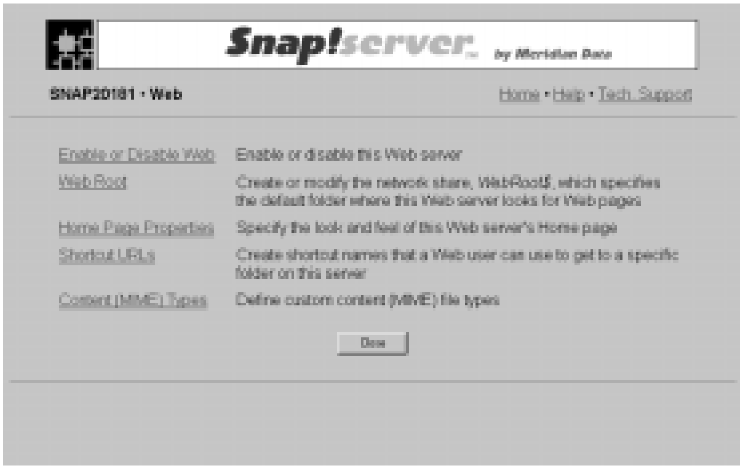


☐ Allow large internet packet support

Click OK to return to the Novell Networking page.

Changing Web Parameters

To reconfigure the Snap! Server's Web settings, click Web on the Network Settings menu. The Snap! Server Web menu appears.



Enable or Disable Web	Enable or disable this Web server
Web Root	Create or modify the network share, WebRoot$, which specifies the default folder where this Web server looks for Web pages
Home Page Properties	Specify the look and feel of this Web server's Home page
Shortcut URLs	Create shortcut names that a Web user can use to get to a specific folder on this server
Content (MIME) Types	Define custom content (MIME) file types

Web Services

To enable or disable the server's Web services:

1. On the Web menu, click Enable or Disable Web.

   The Enable or Disable Web page appears.

2. To enable the server as a Web server, check the Enable this Web Server box.

3. To disable the Snap! Server's directory browsing Web services, uncheck the box.

   By disabling Web services, you can prevent users from accessing the Snap! Server's home page. However, system administrators can still access the Snap! Server's Administration menu using one of the following URLs:

   - http://*IP_address*/config

     Replace *IP_address* with your server's IP address.

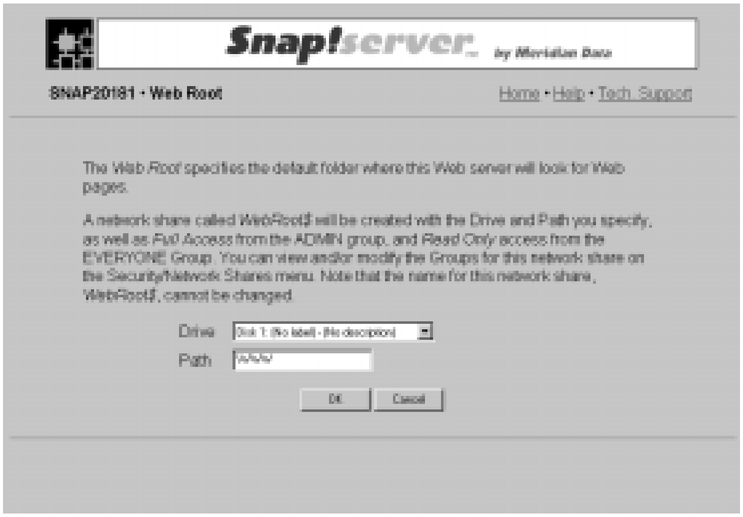
   - http://*SnapServerName*/config

     Replace *SnapServerName* with your server's name.

Web Root

The network share named *WebRoot$* specifies the default folder where the server searches for HTML pages.

Click Web Root to open the page where you can make changes to the existing *WebRoot$* share or create one if none currently exists.



SNAP20181 • Web Root

The Web *Root* specifies the default folder where this Web server will look for Web pages.

A network share called *WebRoot$* will be created with the Drive and Path you specify, as well as *Full Access* from the ADMIN group, and *Read Only* access from the EVERYONE Group. You can view and/or modify the Groups for this network share on the Security/Network Shares menu. Note that the name for this network share, WebRoot$, cannot be changed.

Drive: Disk 1: (No label) - (No description)

Path: \www\

If the *WebRoot$* share already exists, you can change the drive and path to which it points. You cannot change the name of the share, however.

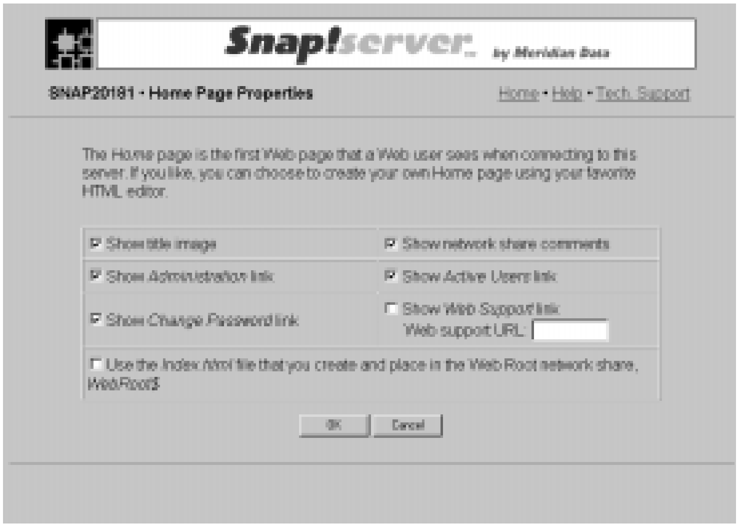
1. On the Web Root page, select the drive from the Drive list box.
2. Type the path in the Path field and click OK to save your changes.

   If you change the path to *WebRoot$*, the Snap! Server's HTML Help files will be unavailable unless you move them to the new *WebRoot$* location.

Home Page Properties

To reconfigure the Snap! Server's home page properties, click Home Page Properties on the Web menu.

The Home Page Properties page appears.



SNAP20181 • Home Page Properties

Home • Help • Tech. Support

The Home page is the first Web page that a Web user sees when connecting to this server. If you like, you can choose to create your own Home page using your favorite HTML editor.

☑ Show title image

☑ Show network share comments

☑ Show Administration link

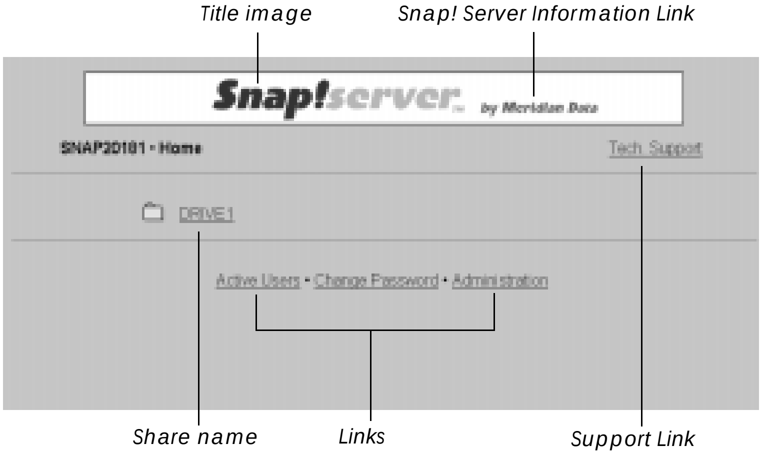
☑ Show Active Users link

☑ Show *Change Password* link

□ Show Web Support link
Web support URL:

□ Use the *Index.html* file that you create and place in the Web Root network share, *WebRoot$*

When Web users connect to the Snap! Server, the first Web page they see is the Home page. The Meridian Data Snap! Server's default home page looks like this.



SNAP20181 • Home

Tech Support

DRIVE1

Active Users • Change Password • Administration

The following paragraphs describe the hyperlinks on this default Home page.

- To view the Snap! Server information screen, click Meridian Data in the title image.
- To communicate with Meridian Data Technical Support, click Tech Support. To use this hyperlink, you must have access to the Internet.
- To look at the contents of a network share, click its name.

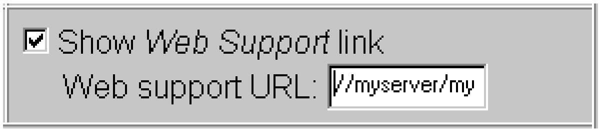
  A network share is a resource that is available to users on your network. Depending on the model, your Snap! Server has either one or two preconfigured network shares named Drive1 and Drive2. For more information, see “About Network Shares” on page 38.
- To see a list of the users who are logged onto the server, click Active Users.
- To change their password, users can click Change Password to open a page with instructions.
- To open the Administration menu, authorized users can click Administration.

System or network administrators can modify the default home page or create their own. If you do create your own home page, you must:

- Name your file *index.html*.
- Put your *index.html* file in the Web Root network share (named *WebRoot$*) on the Snap! Server.

You specify your home page’s appearance by enabling or disabling the Home Page Properties (shown on page 90). To enable a property, check the box beside its name; to disable a property, uncheck the box. For example, to show a link, check its box; to hide a link, uncheck its box.

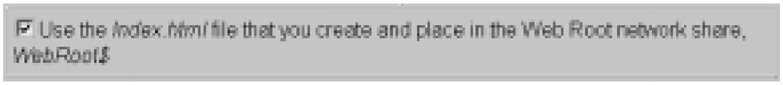
- You can show or hide a Web Support hyperlink to a URL that you define. Just check this box and type the URL in the field provided.



☑ Show *Web Support* link

Web support URL: //myserver/my

- To use the *index.html* file that you create and put in the Web Root network share (named *WebRoot$*), check this box.



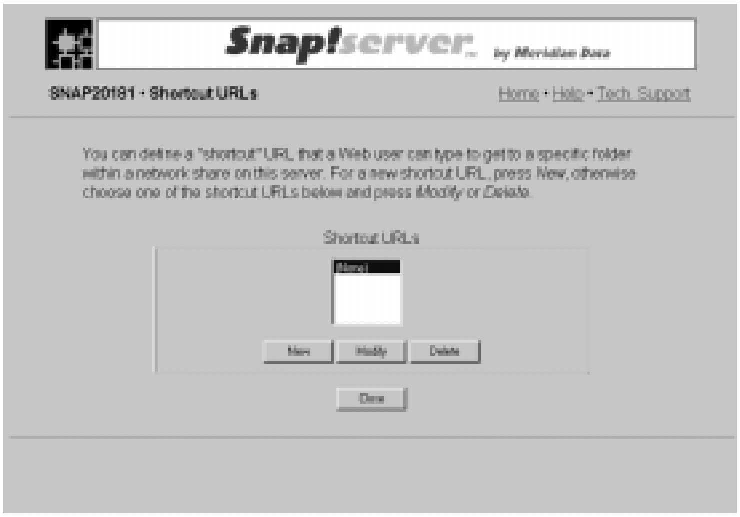
☑ Use the *index.html* file that you create and place in the Web Root network share, *WebRoot$*

Now, when users connect to the Snap! Server via their browser, they will see your *index.html* file instead of Meridian Data's default Snap! Server home page.

Defining Shortcut URLs

You can define a shortcut URL that Web users can type to access a specific folder within a network share on the server. Instead of typing the complete URL (the full path to the folder), users can type an abbreviated URL. For example, suppose you have a network share named *Sales*, and within that share is a folder with the path name */products/instruments/classical/violins*. You could create a shortcut URL called *violins* that points to */products/instruments/classical/violins* so that users could access the *violins* folder by typing only http://*servername*/violins.

On the Web menu, click Shortcut URLs to open the page where you can define a new shortcut URL, or change or delete an existing one.



SNAP20181 • Shortcut URLs

You can define a "shortcut" URL that a Web user can type to get to a specific folder within a network share on this server. For a new shortcut URL, press *New*, otherwise choose one of the shortcut URLs below and press *Modify* or *Delete*.

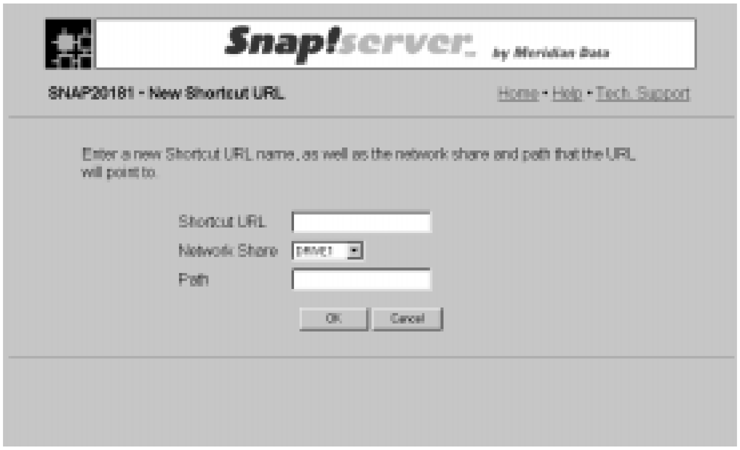
Shortcut URLs

[None]

Defining a new shortcut URL

To define a new shortcut URL:

1. Click New to open the New Shortcut URL page.



SNAP20181 - New Shortcut URL

Enter a new Shortcut URL name, as well as the network share and path that the URL will point to.

Shortcut URL

Network Share DRIVE1

Path

2. In the Shortcut URL field, type the name.

   The name can contain up to 254 alphanumeric characters.

3. Select the appropriate network share from the list box.
4. Type the path that the URL points to.

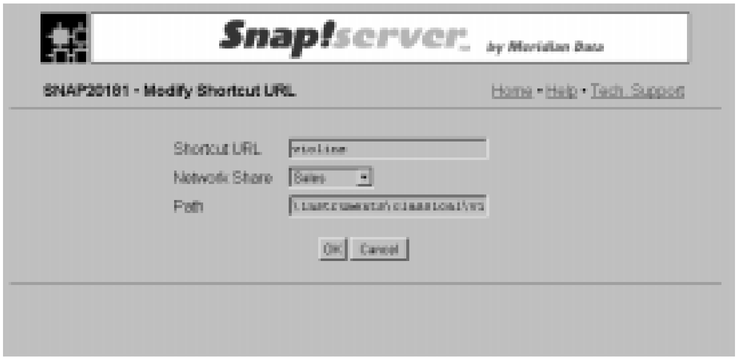
   The path is relative to the network share you select and can contain up to 254 alphanumeric characters.

5. Click OK.

Changing an existing shortcut URL

To change an existing URL:

1. Select the URL from the Shortcut URLs list.
2. Click Modify.



SNAP20181 - Modify Shortcut URL

Shortcut URL: violins

Network Share: Sales

Path: \instruments\classical\vi

3. On the Modify Shortcut URL page that appears, edit the name of the URL in the Shortcut URL field.
4. Select the appropriate share from the Network Share list box.
5. Edit the URL path in the Path field.
6. Click OK.

Deleting an existing shortcut URL

To delete an existing shortcut URL:

1. Select the URL from the Shortcut URLs list.
2. Click Delete.
3. Click Yes to confirm that you want to delete the URL.

   Clicking Yes returns you to the Shortcut URLs page. Click Close to return to the Web menu.

Working With Content (MIME) Types

A Content (MIME) type gives the client browser information about what a file contains and how to handle the file. For example, a particular content type might inform the browser on a client workstation to open a special viewer when it accesses the file. By convention, the file extension indicates the content type. For example, the extension *.gif* maps to content (MIME) type *image/gif*. The Snap! Server is preconfigured with a list of common content types. You can add a new content type or change or delete an existing one.

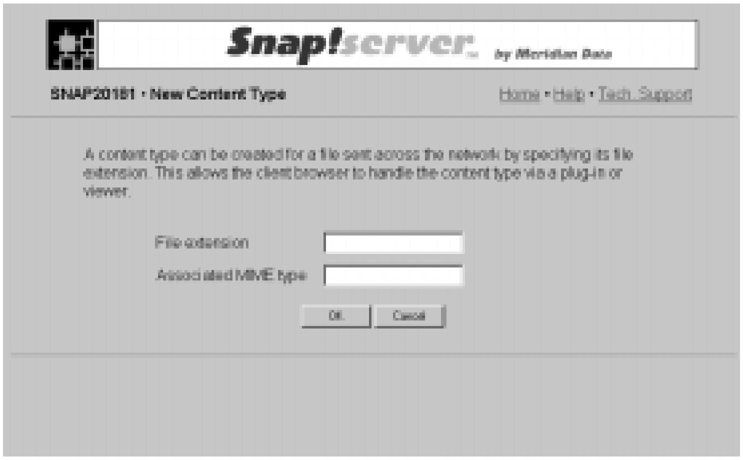
On the Web menu, click Content (MIME) Types to open the page where you can:

- Define custom content (MIME) file types.
- Change existing content types.
- Delete existing content types.

Defining a new content type

To define a new content type:

1. Click New to open the New Content Type page.



SNAP20181 • New Content Type

A content type can be created for a file sent across the network by specifying its file extension. This allows the client browser to handle the content type via a plug-in or viewer.

2. In the File Extension field, type the extension of the file type that you want to add.

   The file extension can contain up to 63 characters.

3. In the Associated MIME Type field, type the file type that you're adding.

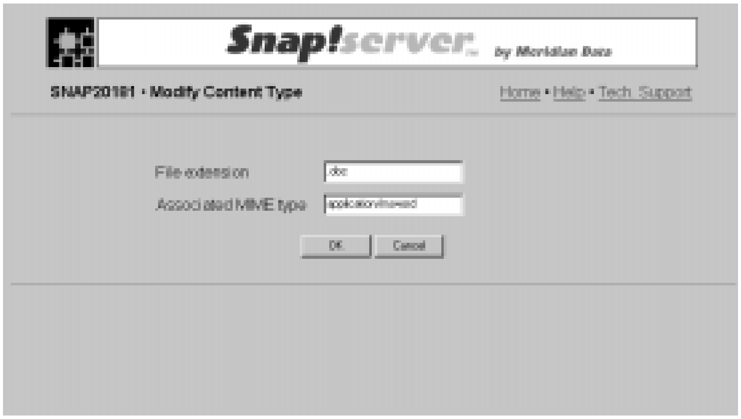
   The MIME type name can contain up to 63 characters.

4. Click OK.

Modifying an existing content type

To change an existing content type:

1. Select the type from the Content Types list.
2. Click Modify to open the Modify Content Type page.



SNAP20181 • Modify Content Type

File extension: .doc

Associated MIME type: application/msword

3. Type a new file extension and associated MIME type in the appropriate fields.

   The file extension and the MIME type name can contain up to 63 characters each.

4. Click OK to return to the Content (MIME) Types page.

Deleting an existing content type

To delete an existing content type:

1. Select the type from the Content Types list.
2. Click Delete.
3. Click Yes to confirm that you want to delete the content type.

Enabling/Disabling NFS

To enable or disable Network File System operation:

1. On the Network Settings menu, click NFS.
2. On the NFS page, turn Enable NFS on or off by checking or unchecking the box.
3. Click OK to accept your change and return to the Network Settings menu.

Viewing Network Settings

To see detailed information about all network settings:

1. On the Network Settings menu, click View Network Settings.
2. To return to the Network Settings menu, click Close.

NOTE Instead of showing the currently active settings, this page may show the most recently changed settings. In this case, the server must be rebooted for the changes to take effect.

System Utilities

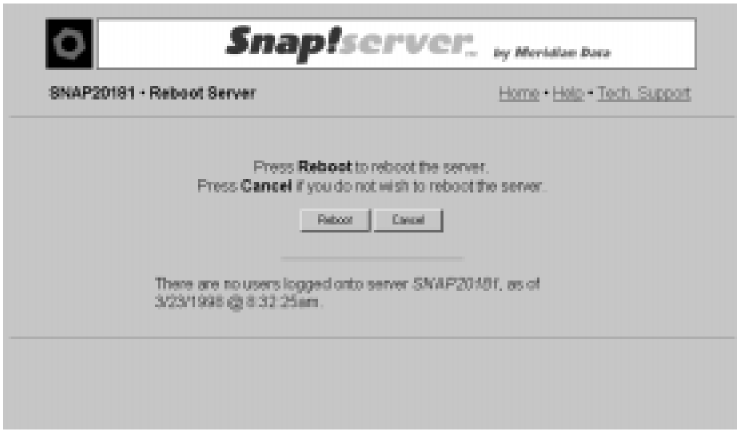
The System Utilities menu includes hyperlinks to various utility programs for restarting the server, restoring your Snap! Server's factory default settings, updating the server software, and viewing system status and statistics.

Rebooting the Server

To reboot the server:

1. On the System Utilities menu, click Reboot Server.

   The Reboot Server page appears showing the names of users currently logged onto the server so that you can warn them before you reboot the server.



SNAP20181 • Reboot Server

Press **Reboot** to reboot the server.
Press **Cancel** if you do not wish to reboot the server.

There are no users logged onto server *SNAP20181*, as of 3/23/1998 @ 8:32:25am.

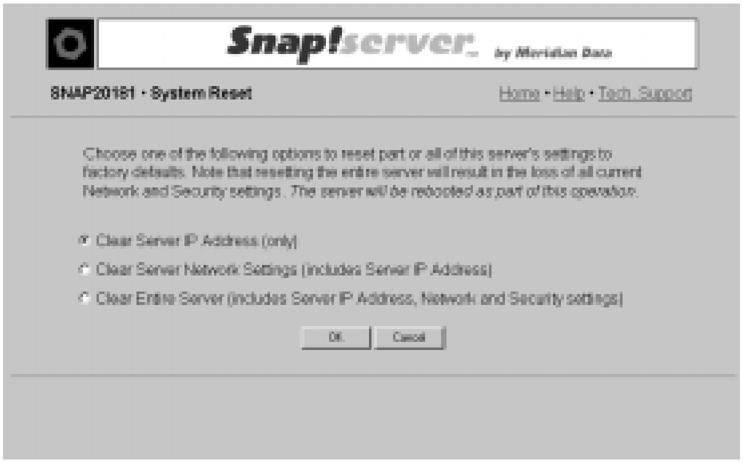
2. On the Reboot Server page, click Reboot.

   The Snap! Server restarts itself. It takes approximately 30 seconds to reboot.

Resetting Factory Defaults

To reset some or all of the Snap! Server's parameters to their factory default settings:

1. On the System Utilities menu, click System Reset.



SNAP20181 • System Reset

Choose one of the following options to reset part or all of this server's settings to factory defaults. Note that resetting the entire server will result in the loss of all current Network and Security settings. *The server will be rebooted as part of this operation.*

● Clear Server IP Address (only)
○ Clear Server Network Settings (includes Server IP Address)
○ Clear Entire Server (includes Server IP Address, Network and Security settings)

2. On the System Reset page, select the option that meets your needs.

Select	To reset the server's
The first option	IP addresses (IP address, gateway, WINS, and subnet mask)
The second option	Network settings and the IP address (If you select this option, you will lose all of the server's current network settings.)
The third option	IP address, network settings, and security settings (If you select this option, you will lose all of the server's current network and security settings.)

3. Click OK.

   A confirmation page appears and lists users who are currently logged on so that you can warn them before the server reboots.

4. When prompted to confirm that you want to clear settings and reboot the server, click Yes.

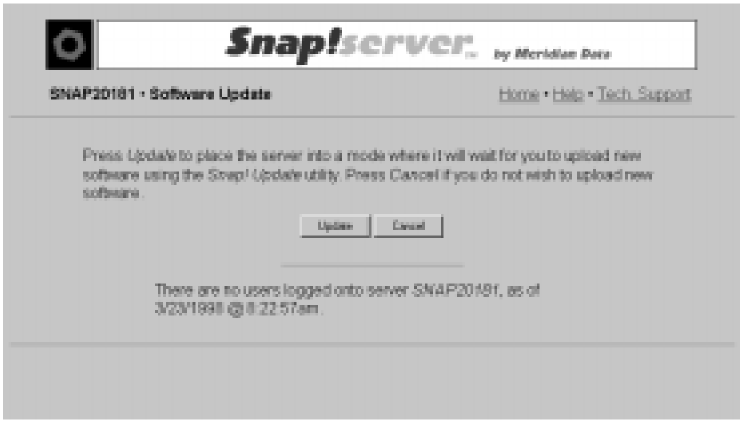
   The Snap! Server reboots so that your changes take effect.

Updating System Software

Meridian Data may make upgrades to the Snap! Server available at the following Internet address: **http://www.snapserver.com/download**

To prepare the server for a software update, click Software Update on the System Utilities menu.

The Software Update page appears.



SNAP20181 • Software Update

Press Update to place the server into a mode where it will wait for you to upload new software using the Snap! Update utility. Press Cancel if you do not wish to upload new software.

There are no users logged onto server SNAP20181, as of 3/23/1998 @ 8:22:57am.

At the bottom of the page, Snap! Server lists the names of users currently logged on so that you can warn them before you disconnect them from the server. When you're ready, click Update.

Clicking Update puts the server in software update mode. Wait at least 30 seconds before you start the Snap! Update™ utility program to update your Snap! Server's flash memory. For further instructions, turn to Appendix D, "Updating System Software with Snap! Update."

Viewing the System Log

On the System Utilities menu, click System Log to view a log of system messages displayed in chronological order. These messages may contain useful troubleshooting information.

On the System Log page, click Close to return to the System Utilities menu.

Viewing System Status

On the System Utilities menu, click System Status to view system diagnostic statistics.

On the System Status page, click Close to return to the System Utilities menu.

Backing Up Files

You should back up files stored on the Snap! Server in the same manner that you back up any other file server. Snap! Servers are fully compatible with Windows 95 and Windows NT backup software. From Novell and UNIX file systems, you must use backup software that supports remote volumes without requiring remote system support. For example, the UNIX tar and cpio utilities will properly back up the Snap! Server.

CHAPTER 6 *Troubleshooting*

It's a good idea to look for problem resolutions in this chapter before you contact Meridian Data Technical Support. If you don't find the information you need here, see "Contacting Meridian Data Technical Support" on page 6.

This chapter provides information about the following topics.

- Status messages that appear on the:
  - Snap! Server Home page
  - Disk Status page
  - Disk Log page
- Using the Reset button to enter diagnostic modes
- Snap! Server's LED patterns

Network Share Status Messages

This topic describes messages that may appear next to a network share on the Snap! Server Home page. These messages indicate that the share is unavailable for viewing from the Home page as well as unavailable to network users.

Unavailable: disk is being checked

This message indicates that the share is unavailable because the drive that the share references is currently being examined by Disk Check. If the Disk Check operation finds no errors, the share automatically becomes available when the Disk Check finishes.

Unavailable: disk is being formatted

This message indicates that the share is unavailable because the drive that the share references is currently being reformatted. When formatting is finished, the share will remain unavailable because the subdirectory that the share references will not exist unless it references the root path. To make the share available again, wait for the formatting operation to finish, and then create the subdirectory that the share references.

Unavailable: disk is off-line

This message indicates that the share is unavailable because the drive that the share references is off-line. This usually occurs when the Disk Check operation finds errors during boot up. To bring the drive on-line, run the Disk Check operation with the Fix Errors box checked. For more information, see “Checking and Repairing a Disk” on page 51. For information about viewing disk errors, see “Viewing Disk Status” on page 57. For a detailed description of the errors you may find when reviewing the Disk Log, see “Disk Log Messages” on page 103.

Unavailable: folder does not exist

This message indicates that the subdirectory that the share references no longer exists. You can either delete the share or create the subdirectory that the share references. For information on deleting a share, see “Administering Security (Users, Groups, and Network Shares)” on page 57.

Disk Status Messages

The following messages may appear on the View Disk Status page. They indicate the current status of the disk drive(s).

No Errors

This message (preceded by a green LED) indicates that the:

- Disk Check operation examined the drive during boot up and did not find any indication of a damaged file system
- File system was successfully mounted and is available for use

Disk needs repair; recheck using *Fix* option

This message (preceded by a yellow LED) indicates that the Disk Check operation suspects that there may be errors on the disk and that a more comprehensive examination of the disk is necessary. Run the Disk Check operation with the Fix Errors box checked. For more information, see “Checking and Repairing a Disk” on page 51.

Disk successfully repaired; see log for details

This message (preceded by a yellow LED) indicates that the Disk Check operation found and successfully repaired problems on the disk. Most likely, these errors were caused when the Snap! Server was improperly shut down. Open the Disk Log by clicking the hyperlinked error message in the Status field on the View Disk Status page. Check the log for error messages. For a detailed description of the errors you may find when reviewing the Disk Log, see “Disk Log Messages” on page 103.

Fatal error during disk check; see log for details

This message (preceded by a red LED) indicates that the system was not able to mount the disk because of an error on the disk. Open the Disk Log by clicking the hyperlinked error message in the Status field on the View Disk Status page, and check for error messages. For a detailed description of the errors you may find when reviewing the Disk Log, see “Disk Log Messages” on page 103. The recommended error resolution is to go to the Check or Repair Disk page, check the Fix Errors box, and run another Disk Check.

Disk Log Messages

This topic supplements the information in “Using Disk Utilities” on page 48. It describes the more important error messages reported by disk checking operations (see “Checking and Repairing a Disk” on page 51) and recommends problem resolutions when appropriate. The error messages are reported in the System and Disk Logs and appear in alphabetical order.

Clean Flag not set in Superblock (Fixed)

This message appears *only* when the Snap! Server was *not* shut down properly. It indicates that the Snap! Server file system may be in an inconsistent state, which may result in errors or lost information. The Disk Check operation fixes such inconsistencies. When the Disk Check is finished, the clean flag is set to indicate that the file system is now consistent and ready for use.

*****File System Was Repaired*****

This message appears *only* when the Snap! Server was *not* shut down properly and the Disk Check operation was run with the Fix Errors option turned on. This message confirms that the Disk Check completed successfully and that the errors found during the check were fixed.

Free Block Count(s) Wrong in Superblock (Salvaged)

This message appears *only* when the Snap! Server was *not* shut down properly. It indicates that there are File System Blocks which have been used but are also listed in the system’s free list. The Check Disk operation has adjusted the free list to reflect that the File System Blocks in question are no longer available.

FSCK Fatal Error = *x*

This message indicates that the Disk Check operation found an error that requires Meridian Data's Technical Support assistance to repair. Contact Technical Support and provide them with the exact text of the error message as well as the error code (represented by *x* in the message described here). For contact information, see "Contacting Meridian Data Technical Support" on page 6.

Modified Flag Set in Superblock (Fixed)

This message appears *only* when the Snap! Server was *not* shut down properly. It indicates that the Snap! Server did not complete an update transaction to the disk. When the Disk Check is finished, the modified flag is cleared to indicate that the file system is now consistent and ready for use.

Partition is clean

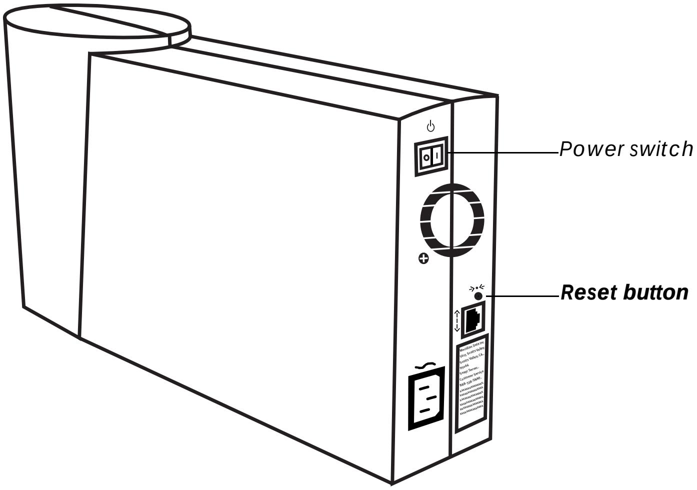
This message indicates that the Snap! Server was shut down correctly.

Partition is NOT clean

This message indicates that the Snap! Server was *not* shut down correctly. To shut down the server correctly, turn off its power switch and *wait for all of the LED lights to turn off*.

Diagnostic Modes

This topic explains how to use the Snap! Server's Reset button to enter diagnostic modes.



You may need to use a procedure described here as a workaround if the normal procedure described in "System Utilities" on page 97 doesn't work for some reason.

1. Turn off the Snap! Server and wait for all of the LEDs to go out.
2. Press and hold down the Reset button while you turn the Snap! Server on; wait until both the System and Disk LEDs start flashing in sync.
3. Release the Reset button.
4. To select the appropriate diagnostic mode, briefly press the Reset button:
   - Once to clear the server's IP address
   - Twice to clear the Administrator password
   - Three times to clear the server's network settings
   - Four times to clear all system settings
   - Five times to put the server into software update mode

5. Watch the Disk LED—the number of times it flashes corresponds to the number of times you pressed the Reset button.

   For example, if you pressed Reset three times to clear the network settings, the Disk LED should flash three times repeatedly to indicate that you are in the proper diagnostic mode.

   If the number of flashes is not as described here, repeat steps 1 through 5 of this procedure.

6. When the LED indicates that you are in the correct mode, press down and hold the Reset button until both the System and Disk LEDs turn off, and then release the Reset button.

   The Snap! Server enters the appropriate diagnostic mode.

Led Patterns

This topic describes the Snap! Server's LED patterns.

- System LED (green) indicates whether the system is operating properly; for more specific information, see the table that follows
- Link LED (green) is on when the Snap! Server is connected to an Ethernet hub
- Net LED (amber) indicates network activity when the Snap! Server transmits, and when it receives either network broadcasts or information directed to itself
- Disk LED (amber) indicates either disk activity during normal operation, or a specific operating failure mode; for more specific information, see the table that follows.

Synchronized System and Disk LED Patterns

System LED	Disk LED	Indicates
Steady light	Irregular flashing	System is loading
Steady light	1 - 6 sequential flashes	System in diagnostic mode
Slow flashing	Irregular flashing	Disk activity
Slow flashing	Flashing concurrently with the system light	System in diagnostic mode

Synchronized System and Disk LED Patterns

System LED	Disk LED	Indicates
Double flashes	Reflects disk activity	System is running and performing a Disk Check operation
Triple flashes	Reflects disk activity	System is shutting down
Rapid flashing	1 - 4 sequential flashes	Failure mode Note: Report the number of flashes to Meridian Data Technical Support
Continuous dimming/ brightening	1 - 4 sequential flashes	Failure mode Note: Report the number of flashes to Meridian Data Technical Support
Blinks off	Blinks off	Update progress For information, see “Software Update LED Patterns,” next.

Software Update LED Patterns

During a software update, the Snap! Server’s LEDs are usually on, but they blink off to indicate the status of the software update. The following table describes the LED patterns during a software update.

# of System LED blinks	# of Disk LED blinks	Meaning
1	1	Waiting for software download to the Snap! Server IP address
	2	Snap! Server does not have an IP address; waiting for a download in broadcast mode
	3	New software is downloading over the network
	4	Snap! Server is storing the new software in memory; this can take up to 5 minutes

# of System LED blinks	# of Disk LED blinks	Meaning
2	1	Software download failed due to a network problem; waiting for another software download to the Snap! Server IP address
	2	Software download failed due to a network problem, and the server does not have an IP address; waiting for a download in broadcast mode
3	1	Software update completed successfully; system will restart automatically
	2	Software update aborted due to numerous network errors Note: Turn off the unit and try again.
	3	Software update aborted due to memory programming errors Note: Turn off the unit and try again.
	4	Software update aborted due to internal error Note: Turn off the unit and try again.
	5	Software update aborted due to a checksum error in the transmitted data Note: Turn off the unit and try again.
	6	Software update aborted due to an attempt to download incorrect software for this type of Snap! Server Note: Turn off the unit and try again.

APPENDIX A *Software and Network Compatibility*

This appendix presents information about clients and applications that the Snap! Server supports. It also notes exceptions.

Supported Clients

The Snap! Server supports the same clients that Windows NT 4.0, NetWare 3.12, and NFS 2.0 servers support. However, the server does not support any Macintosh client. Supported clients are listed in the following tables.

Microsoft Windows Networking
Windows NT 4.0
Win 95
Windows for Workgroup 3.11
Windows NT 3.51
Windows 3.1 with LAN Manager client
OS/2 Warp
DOS 6.22 with LAN Manager client

Novell Networking
NT 4.0 with either the Microsoft or Novell NetWare client
Win 95 with Microsoft and Novell 32-bit clients
Windows for Workgroups 3.11 with Novell 32-bit clients, VLM, NETX clients
Windows 3.1 with VLM, NETX clients
DOS 6.22 with VLM, NETX clients

NFS
SCO Open View UNIX
SPARC Solaris
HP-UX
IBM AIX

Supported Applications

The Snap! Server supports the same applications that Windows NT 4.0, NetWare 3.12, and NFS 2.0 servers support.

Incompatible Applications

The Snap! Server is not compatible with:

- Disk maintenance utilities, such as Windows 95 defragmenters
- NetWare-specific backups and programs that run as a VLM on the server

Windows NT Compatibility

The Snap! Server operates in a manner that is similar to a Windows NT 4.0 file server, with a few minor differences in the following areas:

- Administration
- File security
- Other differences

Administration

The Snap! Server is administered through the HTML-based configuration. Standard Windows NT administration utilities are not supported. Use the HTML-based configuration to set up shares and security and to monitor the server. You can access the configuration from any computer with a Web browser. For more information, see Chapter 4, "Using Snap! Server's Quick Configure."

File Security

Groups are denied or allowed access to shares on the Snap! Server. Access checking is not performed at the file level. Users are allowed access when they are part of a group that has access. The Snap! Server supports three types of access to a share: deny access, read-only access, or full access.

You can create users and groups on the Snap! Server or authenticate them using a domain controller. If you are using a domain controller, you must create groups on the Snap! Server with the same names as the groups on the domain controller. For more information on setting up the Snap! Server to authenticate users using a domain controller, see “Configuring Microsoft Networking” on page 29. For instructions on creating users and groups, see “Configuring Security” on page 32.

Other Differences

- Share names cannot be longer than 12 characters (NT allows up to 80 characters). This limitation allows Windows for Workgroups to access the share.
- Microsoft networking clients can use only the NETBEUI or TCP/IP protocols to access the Snap! Server (NetBIOS over IPX is not supported).
- There is no printer port; print services are not supported.

NFS Compatibility

The Snap! Server supports NFS clients in a manner similar to PC/NFS running on an NT server. Because the underlying file system is similar to a Windows NT file system, there are some differences from standard UNIX.

This topic describes differences between Snap! Server NFS capabilities and standard NFS capabilities in the following areas:

- NFS protocol versions
- Administration
- Mount points
- User authentication and security
- File attributes
- Unsupported features

Protocol Versions

The Snap! Server supports the following versions of the NFS protocol.

Protocol	Version	Source
NFS	2.0	RFC 1094
Mount	1.0, 2.0	RFC 1094, Appendix A
PC/NFS	2.0	Protocols for X/Open PC networking: (PC) NFS

Administration

Use the HTML-based automated configuration to configure and manage the server. You can access the configuration from any Web browser. For instructions, see Chapter 4, “Using Snap! Server’s Quick Configure.” The Snap! Server allows you to associate user accounts on one or more UNIX host systems to a Snap! Server’s local user account. The user is authenticated on the UNIX system but has the same rights as the local user. This feature lets the same user connect from different workstations and lets multiple users connect from the same workstation. For more information, see “Modifying NFS Properties” on page 66.

Mount Points

The Snap! Server exports shares as mount points. Shares are virtual folders that map to an actual directory on the Snap! Server. Shares are defined using the HTML-based configuration. For more information, see “About Network Shares” on page 38.

In the default configuration, there is one share for each drive in the Snap! Server. The default shares are named /Drive1, /Drive2, and so on.

NFS users can use the following capabilities when mounting Snap! Server shares:

- Connect to the same mount point from different IP addresses and user IDs.
- Mount a subdirectory of a share.
- Use dynamic mounting with automount and static mounting.
- Use mount points for home directories, applications, and file storage.
- Automatically remount when the server restarts after being shut down.

After mounting, NFS users can create, delete, write, and rename files and create and remove directories if they have read-write access to the mount point.

User Authentication and Security

The Snap! Server controls access to files at the share level. When a user connects to a share, the Snap! Server checks whether that user belongs to a group that is authorized for read-only access or read-write access to a specific share. Users who are authorized have access to all files within the share. The Snap! Server does not check or save user permissions at the file level.

When a Snap! Server is first installed, all users have access to all shares through the GUEST account. If an NFS user (or any user) fails to connect with a specific user name and password, the Snap! Server connects the user through the GUEST account. By default, GUEST has read-write access to all shares on the server. To prevent unauthorized access by NFS (and other) users, you must reconfigure the shares you want to protect so that GUEST is not allowed access to them.

File Attributes

UNIX sets read (r), write (w), and execute (x) permissions for each file. These permissions can be set independently for the owner, group, and other (world). The Windows NT file system supports only one level of file attributes (not three). As a result, when NFS users set read, write, or execute permission at any level for a file on the Snap! Server, the permission gets set at all three levels. For example, if you turn on read permission at the group level, it is also turned on at the owner and other level.

The file system on the Snap! Server uses one attribute, read-only, to set permissions at the file level. If a file is set to read-only, then the UNIX write attribute is turned off at all three levels. If a file is not set to read-only, then read-write permission is allowed.

Access restrictions set at the share level override those set at the file level. For example, if a user is allowed read-only access to a share, files within that share may report read-write access, however the user will only be allowed to read them.

The following table shows mappings between Snap! Server and UNIX file attributes and how they interact with permissions set at the share level.

Snap! Server file attributes	UNIX file attributes	User has read-write access to share	User has read-only access to share
read-only	r-x r-x r-x	User can read only	User can read only
read-write	rwx rwx rwx	User can read and write	User can read only

In addition to rwx permissions, the NFS file system also stores owner (user ID) and group ID attributes. These are not supported in the Snap! Server file system. The Snap! Server sets the owner ID to the current user's ID and the group ID to root (0) for all files. NFS users can issue commands that change the user or group ID, but their changes will have no effect.

Unsupported Features

The following NFS features are not supported in this version of the Snap! Server file system:

- Symbolic and hard links
- File locking support via the Network Lock Manager
- File ownership
- Access Control list (ACLs)

Novell NetWare Compatibility

For detailed compatibility information, see Appendix E, "Novell Networking: Advanced Setup."

APPENDIX B *Snap! Server Default Configuration Parameters*

The following table lists the Snap! Server's preset configuration defaults.

Parameter	Default Value
Server Name	SNAP*nnnnn* (where *nnnnn* represents the serial #)
Server Date and Time	1/1/1980 12:00 AM
Time Zone	Greenwich Time, no daylight savings (GMT)
Stacks: TCP/IP	Enabled
TCP/IP: Auto Generate TCP/IP Address	Enabled
Stacks: NetBEUI	Enabled
Stacks: IPX	Enabled
File Sharing: Microsoft Networking (SMB)	Enabled
File Sharing (SMB): Master Browser	Enabled
File Sharing (SMB): Workgroup/Domain	Workgroup
File Sharing (SMB): Workgroup/Domain Name	WORKGROUP
File Sharing (SMB): Server Comment	(none)
File Sharing (SMB): Opportunistic Locking	Enabled
File Sharing: Novell Networking (NCP)	Enabled
File Sharing (NCP): Show Hidden Shares	Disabled
File Sharing (NCP): Frame Type	Auto-Detected
File Sharing (NCP): Internal Network Number	Auto-Configured
File Sharing (NCP): External Network Number	Auto-Configured
File Sharing (NCP): Primary NetWare server	Disabled
File Sharing (NCP): Large Packets (Burst Mode)	Enabled
File Sharing: Network File System (NFS)	Enabled
File Sharing: Hypertext Transfer Protocol (HTTP)	Enabled

Parameter	Default Value
File Sharing (HTTP): Web Root	\WWW on first drive
File Sharing (HTTP): Shortcut URLs	(none)
File Sharing (HTTP): Home Page	Show Snap! Server Default
Shares:	WebRoot$ and Drive1
Shares:	Drive2, if a second drive is present
Users (No Passwords):	ADMINISTRATOR, SUPERVISOR, ROOT
Groups:	EVERYONE, ADMIN
FSCK: Automatically Fix Drive Errors If Detected	Enabled
FSCK: Examine Disk	Only If Errors Are Suspected

APPENDIX C Security and Access Control

The file server security method used by Snap! Server is similar to that of other Microsoft network servers, such as Windows NT. Access control is based on the user's login identity and applied at a share level. In order to restrict access to Snap! Server drives or folders, you need to create user accounts and groups, then create network shares, and finally assign access rights to these shares. Instructions are provided in Chapter 5, starting with "Administering Security (Users, Groups, and Network Shares)" on page 57. This appendix provides the background and practical information you need to set up security on your Snap! Server and make it work for you.

Microsoft Network Server Security and your Snap! Server

The Microsoft network uses more than one scheme for security and access control. Servers for small workgroups, such as Windows for Workgroups and Windows 95, typically restrict access by associating a password to each network share that needs to be secured. This scheme is typically referred to as "share level security." More robust Microsoft server products, such as Windows NT, associate access rights with user accounts. With "user level security," a user's login determines what information he or she can access. Access rights are configured via access control lists (ACLs). These are lists of users and groups that are allowed or denied access to certain information. ACLs are typically associated with network shares. In some cases, such as NTFS partitions on Windows NT servers, ACLs can also be associated with folders and files.

Snap! Server supports user-level security, but differs from a Windows NT server in the following ways:

- Access control on a Snap! Server can only be associated with network shares, but not with arbitrary folders or files. (This is the same as a Windows NT server configured with FAT partitions.)
- Access control on a Snap! Server can only be configured for groups (that is, ACLs may only include groups). Individual user rights are determined based on the groups they belong to. Snap! Server ACLs are referred to as group access lists.

- Only the following access rights may be associated with a group:
  - Allow full read and write access.
  - Allow read only access.
  - Deny read and write access.

To facilitate server security setup, a Snap! Server can be associated with a Microsoft network domain. In this case, users are authenticated and group membership is established by the domain controller. Domain groups whose names match one of the local Snap! Server groups are recognized by Snap! Server and can be used to access information on its drives.

Setting Up Snap! Server for Unrestricted Access for all Users

By default, Snap! Server is set up to allow unrestricted access for all users. The server is configured with one network share per drive, typically referred to as the "root share" for the drive. By default, root shares allow full read and write access to all members of the EVERYONE group. This means that all users have full access to all of the drives, including all Microsoft network users authenticated through the domain controller and, if the GUEST account is enabled, all users who failed to authenticate and are logged in as GUEST.

NOTE To only allow users who have been authenticated from a "trusted source" (that is, users recognized as local users by the Snap! Server, NFS users authenticated on a UNIX host, or Microsoft network users authenticated through the domain controller) simply delete the GUEST account. As an alternative, to keep the GUEST account so that you may allow unregistered users to access other network shares, you can specifically deny access to GUEST, as explained in “Restricting Access to a Snap! Server Drive,” next.

Restricting Access to a Snap! Server Drive

You can restrict access to the entire contents of a Snap! Server drive through its default network share (Drive1 or Drive2). How you do this depends on exactly what you’re trying to accomplish. The following paragraphs describe some common scenarios.

To allow full read and write access only to users who have been authenticated from a trusted source (thus excluding the GUEST account and with it, all users who failed to authenticate at login), follow these steps.

1. Create a new Snap! Server group.
2. Add GUEST to the group you created as part of step 1.
3. Add the group you just created to the group access list for the share (for example, Drive1) and deny it all access rights.

To allow full read and write access to only a small group of Snap! Server users or to a single user, follow these steps.

1. Create a new Snap! Server group for the users you want to grant access to.
2. Add these users to the group you created as part of step 1 of this procedure.
3. Add the group you just created to the group access list for the share (for example, Drive1) and allow it full read and write access.
4. Remove the EVERYONE group from the group access list for the network share.
5. If you want Snap! Server ADMIN users to have access to the information on this drive, add ADMIN to the group access list, granting it full read and write access.

To allow read-only access to everyone and full read and write access to only a small group of users or to a single user, follow this procedure.

1. Create a new Snap! Server group for the users you want to grant full read and write access to.
2. Add these users to the group you created as part of step 1 of this procedure.
3. Add the group you just created to the group access list for the share (for example, Drive1) and allow it full read and write access.
4. Modify access rights for the EVERYONE group, restricting it to read-only.
5. If you want Snap! Server ADMIN users to have access to the information on this drive, add ADMIN to the group access list, granting it full read and write access.

To allow full access to everyone *except* a small group of Snap! Server users, follow this procedure.

1. Create a new Snap! Server group for the users you want to deny access to.
2. Add these users to the group you created as part of step 1 of this procedure.

   If you have not deleted the GUEST account, you should also add GUEST to this group. Otherwise, users can bypass the security you are trying to establish simply by logging in as GUEST.
3. Add the group you just created to the group access list for the share (for example, Drive1) and deny it all access rights.

To allow full read and write access to all Microsoft network users belonging to a specific group in a domain, follow this procedure.

1. Create a new Snap! Server group with exactly the same name as the domain group.

   You don't need to add users, as this is done on the domain controller, which is where you would continue to manage this group.
2. Add the group you just created as part of step 1 of this procedure to the group access list for the share (for example, Drive1) and allow it full read and write access.
3. Remove the EVERYONE group from the group access list for the network share.
4. If you want Snap! Server ADMIN users to have access to the information on this drive, add ADMIN to the group access list, granting it full read and write access.

NOTE In all of the scenarios previously described, if the drive contains *WebRoot$* (see page 88), make sure that this share maps to a folder and not to the root of the drive. This allows you to assign different access rights to *WebRoot$* without compromising security for the rest of the drive. For more information, see "Restricting Access to Folders on a Snap! Server Drive" on page 121.

It is possible to set up more complicated group access lists for a share, allowing full read and write access to some users, read-only access to others, and denying access to yet others. If you intend to do this, you need to be aware of the rules that the Snap! Server uses to determine effective access rights. These rules come in to play when a user is a member of more than one group.

- If a user is granted read-only access through one group and full read and write access through another, the user has full read and write access to all of the information in the network share.
- If a user is denied access through one group, the user has no access to the network share regardless of what access rights are granted via membership in other groups.

For example, consider the following scenario. User JOHND is a member of a group called USERS, and USERS has read-only access to Drive1, while EVERYONE still has read and write access to Drive1. JOHND has full read and write access to all of the information in Drive1 because he is a member of EVERYONE. Now add a group called EXCEPTIONS, and make JOHND a member of this group. Next, add EXCEPTIONS to the access group list for Drive1 with access denied. JOHND no longer has access rights to Drive1. However, if you have not deleted the GUEST account or included it in EXCEPTIONS, JOHND could "sneak in" by logging in as GUEST. To close this major security hole, delete the GUEST account or add GUEST to the EXCEPTIONS group.

Restricting Access to Folders on a Snap! Server Drive

Although Snap! Server controls access only at a share level, it is possible to set up multiple shares for the same drive, each with different group access lists. This allows you to restrict access to certain folders on the Snap! Server drive while leaving other folders open to everyone. In fact, you can use this approach to set up relatively complex access control schemes. To do so:

1. Restrict access to the root of the drive (Drive1 or Drive2).

   Typically, you only want to allow members of the ADMIN group to access the drive through its root share.

2. Create the folders that you want to secure.
3. Set up shares for each of these folders, with the access restrictions you want to impose.

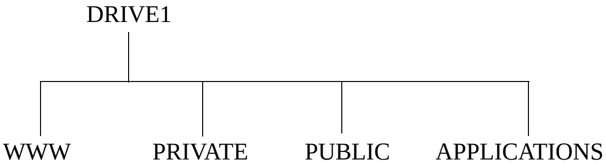
   Create access control lists for each share following the same rules that you would use when securing the entire drive.

Step 1 is particularly important. If you create a network share that grants certain users access to a folder, these users can access all other folders within this share, no matter what other network shares you create and restrictions you impose on them. The most common mistake you can make is to restrict access to a share that maps into a folder on Drive1 while leaving full access to Drive1 itself.

For example, suppose that you create a PRIVATE folder on Drive1 and a PRIVATE share that maps into the folder you just created. You then restrict access to PRIVATE, so that only members of the ADMIN group may access it, but you leave Drive1 to its default setting, which allows EVERYONE full read and write access. Users may not be able to access the contents of the PRIVATE share, but they can still access the PRIVATE folder through Drive1. In other words, you have not achieved what you wanted—to restrict access to PRIVATE. You need to restrict Drive1 so that only members of the ADMIN group may access it, and then create a PUBLIC folder and corresponding share. Now configure PUBLIC with full read and write access for EVERYONE. In this case, the PRIVATE share is not needed unless you want other groups to access it, too.

NOTE If your system is configured for Web access through HTTP, you need to set up a special share called *WebRoot$* (see page 88 for more information). This share is typically configured with read-only access for EVERYONE (including GUEST), and full read and write access to a selected group (mostly ADMIN users). *WebRoot$* is preconfigured at the factory to map to a folder on your Snap! Server drive so that you can secure access to the rest of the drive while opening up access to your Web pages.

The following example shows how you could set up access control on a typical single-drive Snap! Server using multiple folders.



In the example, WWW is the folder used for *WebRoot$*, PRIVATE is an area containing sensitive data that only certain users can access, PUBLIC is a storage area available to all users for exchanging files, and APPLICATIONS is a folder containing applications for general use. You could set up security as follows:

1. Create a group called PRIVILEGED_USERS and add to it all of the users who are allowed to access the PRIVATE folder.
2. Create a group called WEBMASTERS and add to it all of the users responsible for maintaining the Web content on the Snap! Server.
3. Create a group named UNAUTHORIZED and add GUEST to this group.

4. Change access rights for Drive1.

   a. Add the ADMIN group with full read and write access.

   b. Remove the EVERYONE group.

   Only system administrators can now access the drive from its root.

5. Change the access rights for *WebRoot$* as follows:

   a. Change access rights for EVERYONE to read-only.

   b. Add both the ADMIN and the groups with full read and write access.

6. Create a new network share named PRIVATE and map it to the PRIVATE folder.

   Set up access rights so that only the ADMIN and PRIVILEGED_USERS groups have full read and write access to this share. Make sure that the EVERYONE group is not included in the group access list for this share.

7. Create a new network share named PUBLIC and map it to the PUBLIC folder.

   Set up access rights so that the EVERYONE group has full read and write access, and the UNAUTHORIZED group is denied access.

8. Create a new network share named APPS and map it to the APPLICATIONS folder.

   Set up access rights so that the ADMIN group has full read and write access, the EVERYONE group has read-only access, and the UNAUTHORIZED group is denied access.

APPENDIX D *Updating System Software with Snap! Update*

Meridian Data may make available upgrades to the Snap! Server. This appendix describes how to perform a system software upgrade using the Snap! Update™ utility program.

Upgrading involves two main steps:

1. Put the Snap! Server in software update mode. (See “Preparing the Server” on page 126.)
2. Run the Snap! Update utility on an attached network machine. (See “Starting Snap! Update and Performing the Upgrade” on page 127.)

   Snap! Update must be installed and run on a TCP/IP client/workstation that’s running under the Windows for Workgroups 3.11, Windows 95, or Windows NT operating system.

If you have already installed the Snap! Utilities, skip to “Preparing the Server” on page 126. Otherwise, continue with “Installing Snap! Update,” next.

Installing Snap! Update

Install the Snap! Utilities from the CD-ROM that is shipped with your Snap! Server. If you don’t have a CD-ROM drive, or you have misplaced the Snap! Utilities CD-ROM, you can download Snap! Update from Meridian Data’s Snap! Server Web site at this address:
http://www.snapserver.com/download

To install the Snap! Update utility program from the CD-ROM:

1. Put the Snap! Utilities CD-ROM into your local CD-ROM drive.
2. Click Start on the taskbar, and then click Run.
3. In the dialog box that appears, type:

   ```
   A:\setup.exe
   ```

   and then click OK.

4. Follow the instructions on your screen, and provide the information requested. For example, you'll need to specify the destination path for the directory where you want to install the Snap! Utilities.

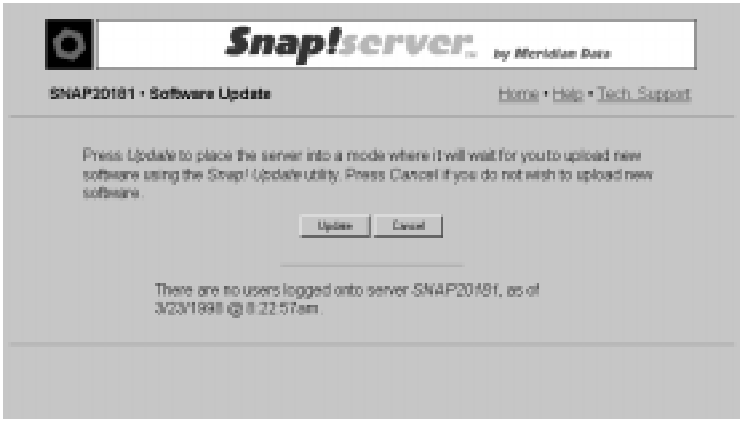
When you have successfully installed the utilities, you can prepare it for the upgrade.

Preparing the Server

The Snap! Server must be correctly installed, must have an IP address, and you must have access to the Snap! Server Administration menu via your browser.

To prepare the server for a software update, click Software Update on the System Utilities menu. You can access the System Utilities menu from the Snap! Server's Administration menu.

The Software Update page appears.



Press Update to place the server into a mode where it will wait for you to upload new software using the Snap! Update utility. Press Cancel if you do not wish to upload new software .

There are no users logged onto server SNAP20181, as of 3/23/1998 @ 8:22:57am .

At the bottom of the page, Snap! Server lists the names of users currently logged on so that you can warn them before you disconnect them from the server. When you're ready, click Update.

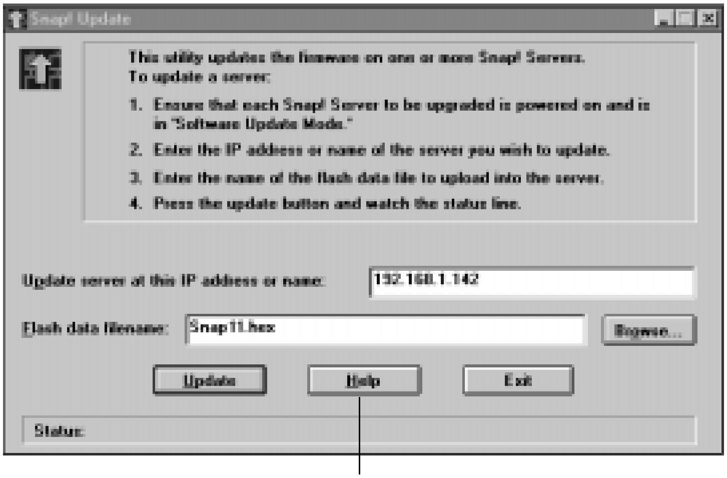
Clicking Update puts the server in software update mode. Wait at least 30 seconds before you start the Snap! Update™ utility program to update your Snap! Server's flash memory.

Starting Snap! Update and Performing the Upgrade

To start Snap! Update, follow these steps:

1. In Windows Explorer (Windows NT, Windows 95) or Program Manager (Windows for Workgroups), open the Snap! Utilities folder.
2. Locate and double-click the Snap! Update application icon to start the utility program.

The Snap! Update window appears.



Snap! Update

This utility updates the firmware on one or more Snap! Servers.
To update a server:

1. Ensure that each Snap! Server to be upgraded is powered on and is in "Software Update Mode."
2. Enter the IP address or name of the server you wish to update.
3. Enter the name of the flash data file to upload into the server.
4. Press the update button and watch the status line.

Update server at this IP address or name: 192.168.1.142

Flash data filename: Snap11.hex

Click Help for online information about Snap! Update and how to use it.

To update the server's flash memory:

1. In the first field, type either the IP address or the name of the server to be upgraded.
2. In the next field, type or browse for the name of the flash data file to upload into the server.

   When Meridian Data recommends an upgrade, it will supply this .HEX file, which contains the new Snap! Server software.
3. Click Update to perform the upgrade.

4. Watch the Status field for information about the upgrade’s progress. When the status message changes to `Upload successful! Server is updating... Server will reboot when complete`, click Exit to quit the Snap! Update program.

5. Wait at least five minutes for the Snap! Server to reprogram itself with the new software, and then reboot.

IMPORTANT

Do not turn off the Snap! Server during the update process, or you will damage the Flash ROM!!!

APPENDIX E Novell Networking: Advanced Setup

This appendix provides a more detailed definition of the Snap! Server's Novell networking emulation functionality.

This version of Snap! Server provides network-based storage to workstations that are configured for Novell networking, and is not designed to operate as a stand-alone server in a Novell network. Those who intend to use the Snap! Server as their primary or sole server are advised to take advantage of the Snap! Server's Microsoft networking functionality, which is better suited for stand-alone operation. The Novell network support that is built into the Snap! Server is designed to extend the storage available on existing Novell networks. To automatically configure itself, the Snap! Server takes advantage of NetWare servers that are already connected to the network.

The Snap! Server will work on most existing networks without special setup requirements. However, the server's default configuration may not be adequate for all situations. This appendix provides the background information necessary for dealing with such situations. It also describes how to perform system administration tasks on a Snap! Server, such as adding users and granting trustee rights on volumes, using standard NetWare utilities.

Novell Network Functional Compatibility

This version of Snap! Server emulates a Novell NetWare 3.12 Server. It provides the file services as well as all of the support functions, such as login and access control, required for disk storage. However, the Snap! Server does not provide the *full* functionality of a Novell NetWare 3.12 Server. The following paragraphs describe the areas in which this version of Snap! Server generally differs from a Novell NetWare 3.12 Server.

- The Snap! Server does not have a "console" and does not support NLMs, print services, transaction tracking, accounting, or any of the other services typically provided by a NetWare 3.12 Server.

- The Snap! Server only supports DOS name space for files and directories, meaning that file names are restricted to “8.3 format.” Files with longer names are recognized by file searches and file open operations, but the names are converted to 8.3 format in accordance with the Windows NT name mangling conventions.
- Snap! Server supports unified login from multiple protocols. In other words, the same user name and password is valid regardless of the protocol used to connect to the server. While the Snap! Server does allow Novell network clients to use encrypted passwords when validating a user account, the clients may not change their passwords using the standard Novell networking client tool (SETPASS or GUI-based utilities). In some cases, the utility may appear to be working, but the password is not actually changed. As a workaround, Meridian Data suggests using the Snap! Server’s Web-based Administration utilities (see Chapter 5, “Server Administration”). Users may also change their passwords by clicking the Change Password hyperlink on the Snap! Server’s home page.
- The volume structure and related security model used by this version of Snap! Server differ from those of a NetWare 3.12 Server. A *volume* on the Snap! Server is equivalent to a *share* on a Windows NT server. The Snap! Server’s shares are created and managed through its Web-based Administration utilities. Because multiple shares can be created for the same physical device, it is possible for the same file or directory to be located on more than one volume.
- When a Snap! Server share is deleted, the corresponding NetWare volume is replaced by a “phantom volume” named WAS_DELETED. This is used as a placeholder so that NetWare volumes following the one that was deleted need not be renumbered. Phantom volumes are reclaimed when new shares are created and disappear if the server reboots.
- This version of Snap! Server is preconfigured with a “default” SYS volume that contains empty LOGIN, SYSTEM, and PUBLIC directories. The volume is read-only and does not map to an actual drive. It is possible to create a “real” SYS volume (a share named SYS). This volume takes precedence over the “default” SYS volume and can be populated with directories and files as desired. The “real” SYS volume is required to support DOS clients (NETX and VLM) and some DOS-based system administration utilities such as SYSCON.

- Access restrictions (trustee rights) in this version of Snap! Server are applied at a volume level only, and not at a directory or file level. This is equivalent to user-level security on a Windows NT server FAT partition. With user-level security, it is possible for multiple volumes to provide access to the same directory structure but with different security restrictions. Typically, this is done by providing access at different levels in the directory tree. The root is normally restricted to privileged users, while selected subdirectories are opened up for general access.
- This version of Snap! Server does not support trustee rights for an individual user. Trustee rights can only be assigned to groups. Individual user trustee rights are determined based on the groups the user belongs to.
- With this version of Snap! Server, granting and/or revoking trustee rights to a volume does not affect users who are already mapped to that volume. A user would have to unmap and remap the volume for the new rights to take effect.
- You can only assign the following access rights with this version of Snap! Server:
  - Full access, which is equivalent to read, write, open, create, delete, search, and modify
  - Read-only access, which is equivalent to read, open, and search
  - Deny all access (all access rights are denied)

  For example, you cannot set up trustee rights for a group and just include search rights on a volume. Although this assignment might be accepted by some Novell network setup utilities such as SYSCON, the Snap! Server will translate it into read-only access (meaning that read and open rights are also assigned automatically). Similarly, revoking search rights for a group on a volume configured for read-only access has no effect unless read and open rights are also revoked at the same time.
- The NetWare “supervisory” right does not get assigned as part of the trustee rights. All Snap! Server volumes, however, can be accessed as “supervisory” volumes.
- The file system on the Snap! Server uses one attribute, read only, to set access permissions at the file level. Therefore, the execute attribute is not supported.

- The Snap! Server does not provide any of the standard NetWare 3.12 DOS utilities for server access or server management. However, the following Novell DOS utilities are partially or fully supported. For more information on individual programs, see the *Snap! Server Release Notes*.

ATTACH	CASTON	CASTOFF	FCONSOLE
FILER	FLAG	GRANT	LISTDIR
LOGIN	LOGOUT	MAP	NCOPY
NDIR	NVER	REMOVE	RENDIR
REVOKE	SEND	SESSION	SLIST
SMODE	SYSCON	SYSTIME	TLIST
USERLIST	VOLINFO	WHOAMI	

None of the printer related functions work with this version of Snap! Server. In addition, the following are known to fail when used with the Snap! Server.

ACONSOLE	ALLOW	CHKDIR	CHKVOL
DSPACE	PURGE	RCONSOLE	SALVAGE
SETPASS	MAKEUSER	USERDEF	

- Snap! Server also supports IntraNetWare 4.11 utilities, such as NLIST and NWADMIN, which operate on NetWare 3.1x and NetWare 4.x servers.

Advanced Setup Options

This topic provides information on the setup options available from the Novell Networking Advanced Setup page in the Snap! Server's Web-based Administration utilities. (See Chapter 5, "Server Administration.")

Ethernet Frame Type

Snap! Server supports all four standard Ethernet frame types used with Novell networks:

- Ethernet-II
- Ethernet 802.2 LLC
- Ethernet 802.2 SNAP
- Ethernet 803.3

The Auto-detect option, which is selected by default, allows the server to accept incoming packets of all frame types and to generate outgoing packets with the correct frame.

When Snap! Server is reconfigured to support a single frame type, the server only accepts incoming packets of the desired frame type. Although this is somewhat more restrictive, it may be the preferred option in some network configurations, as it allows better control over external network number assignment.

Internal Network Number

The internal network number is used to uniquely identify a file server on a Novell network. By default, the internal network number for a Snap! Server is auto-configured to a unique value (the last eight hexadecimal characters in the server's Ethernet host number). If the default internal network number conflicts with that of another server on the same network, it needs to be set manually to a value that does not conflict. Your Snap! Server's Ethernet number is shown on the View Network Settings page. (See "Viewing Network Settings" on page 97.)

External Network Number

The external network number is used to identify each logical network segment in a Novell network. The Snap! Server can operate on up to four network segments—one for each Ethernet frame type supported.

Novell networking requires that each frame type be assigned a separate external number on each physical segment. By default, the server auto-configures its external network number(s) by listening to SAP broadcasts from other NetWare servers. The Snap! Server uses the contents of these broadcast packets to determine the external network number associated with the frame type of the broadcast. Once the external network number is known, the corresponding network segment is activated—the server starts broadcasting its own SAP advertisement for that frame type.

In most cases, a Snap! Server can auto-configure itself in minutes on all network segments where other NetWare servers are active. However, Snap! Server cannot initialize its external network number(s) on inactive segments, or network segments where there are no NetWare servers actively broadcasting SAP packets. SAP broadcasts received through routers are not used to set the external network address. As a result, it is possible for a Snap! Server to only partially auto-configure itself, or to activate itself only for some of the Ethernet frame types it supports. Generally, this is not a problem, as the uninitialized external network number(s) typically correspond to unused frame type(s). Also, a Snap! Server can respond to some Novell networking clients even if they are using a network segment that has not been activated; the server uses a network number of 0 in this case.

To deal with situations where auto-configuration is inadequate, you can set the external network number manually. Meridian Data generally recommends that this be done only when the server is configured for a specific Ethernet frame type. If this is the case, when a specific external network number is selected, the number corresponds to the Ethernet frame type supported by the server.

If you are configuring your Snap! Server to operate in a stand-alone mode, you can assign external network addresses for all four frame types. Accept the Ethernet frame type default setting (Auto Detect) and select an external network number. In this case, the Snap! Server uses the external network number selection as the start of a sequence of four external network numbers, each assigned to a different frame type. The first network number (the number actually selected) is used for Ethernet 802.2 LLC; the next number (the number selected plus one) is used for Ethernet 802.3; the next number (the number selected plus two) is used for Ethernet-II; and the last number (the number selected plus three) is used for Ethernet 802.2 SNAP.

Note that a more serious problem can occur if more than one logical network address is in use on the same physical network segment (multiple servers are broadcasting on this segment using different external network addresses for the same frame type). NetWare servers will report this as an error on the console. Also, other Snap! Servers will auto-configure to the external network address of the first local SAP broadcast they receive. This is not guaranteed to be the same each time the server starts up.

Allow Large Internet Packet Support

By default, a Snap! Server is set up to always negotiate the maximum packet size with client workstations attaching to it. This assures optimal performance when transferring files to or from the server. This setting, however, can cause problems with some of the older routers, which do not support Ethernet packets that contain more than 512 bytes of data. (Most routers, especially newer ones, do not have this problem.) If necessary, you can disable the Allow Large Internet Packet Support option on the Advanced Novell Networking page (described on page 87). This forces the Snap! Server to negotiate a smaller packet size with clients that are not on the same network segment as the server (those that require the service of a router). The maximum packet size is still used with clients that do not require routers.

Allow Server to Show Up as Primary Server

By default, the Snap! Server is set up *not* to respond to “get nearest server” SAP queries. This is equivalent to configuring a NetWare 3.12 Server with the Reply to Get Nearest Server option turned *off*. In either case, the server cannot be selected by a Novell network client as its primary server. This also implies that the Snap! Server cannot be the only server on the Novell network.

In the default configuration, 32-bit Windows clients should authenticate using a pre-existing NetWare server, and then connect to the desired Snap! Server volumes. Older DOS clients (NETX and VLM, for example) should LOGIN to a pre-existing NetWare server and then ATTACH to the desired Snap! Server and MAP its volumes.

If the Snap! Server is configured to show up as the primary server, it replies to SAP “get nearest server” queries. (This configuration option is described on page 87.) These broadcast packets are used by Novell network clients to locate a primary server, which provides the information needed to log in (not necessarily to the same server). This setting causes problems for Novell network clients that need access to the standard DOS-based NetWare utilities, such as LOGIN, SLIST, and MAP. These utilities, which are typically located in the SYS volume of a NetWare server, are *not* provided with this version of Snap! Server. 32-bit Windows clients do not need to have access to these DOS utilities as long as GUI utilities (such as Network Neighborhood) are used to log in to the server and access or map its volumes.

Also note that most Novell network clients synchronize their date and time to their primary NetWare server without adjusting for the time zone.

The Default SYS Volume

The Snap! Server is preconfigured with a default SYS volume that contains empty LOGIN, SYSTEM, and PUBLIC directories. This volume is read-only and does not map to an actual drive. Instead, the volume is part of the electronic root file system. The default SYS volume is only seen by Novell network clients and is not visible from Snap! Server’s Web-based Administration utility or through other networking protocols. Snap! Server’s default SYS volume is provided for compatibility purposes only, as some Novell network clients expect volume 0 to be SYS. Since the default SYS volume does not contain any of the standard DOS-based NetWare utilities, DOS clients such as NETX and VLM cannot use a Snap! Server as their primary login server, even if it has been configured to show up as the primary server. Also, some of the NetWare 3.12 DOS-based system administration utilities, such as SYSCON, do not operate properly unless a real SYS volume is available.

If necessary, you can create a real SYS volume on a Snap! Server. To do so, use Snap! Server’s Web-based Administration utilities to create a share named SYS and map it to a subdirectory on one of the Snap! Server’s drives. In most cases, the SYS share should be set up with full permission for the ADMIN group and read-only permission for the EVERYONE group. However, to support SYSCON, the SYS share must be assigned full permission for the EVERYONE group.

When the real SYS volume is made available, it replaces the default SYS volume. The real SYS volume can be populated with directories and files as desired. Typically, SYS should include LOGIN, SYSTEM, and PUBLIC directories in its root. SYSCON also requires a MAIL directory. Programs can be copied to these directories, *as long as their licensing restrictions are satisfied*.

Access Security and the GUEST Account

When used as a network storage device, Snap! Server offers an opportunity to shorten the otherwise time-consuming configuration tasks of setting up user accounts and trustee rights for volumes. You can take advantage of this as long as access to data located on the Snap! Server does not need to be restricted.

By default, your Snap! Server's drives are accessible as Drive1 and Drive2, if a second drive is available. These volumes are set up with full access granted to EVERYONE. Instruct your users to log into the Snap! Server using the GUEST account. Alternatively, they can use the Novell DOS ATTACH utility with their own user ID and password. If a user's name does not correspond to one of the Snap! Server's accounts, that user is automatically logged in as GUEST.

For more information on security issues, see Appendix C, "Security and Access Control."

NOTE If you use the Microsoft Windows 95 Client for NetWare Networks to connect to the Snap! Server with the default GUEST account, and later set up security and user accounts, you may have problems reconnecting to the Snap! Server. The client for NetWare Networks automatically tries to reconnect using the stored GUEST account information. The connection may fail because of the new security restrictions that you have created. In this case, change the password for the Snap! Server's GUEST account. Then request those using the Windows 95 workstations affected by this problem to log off their machines and then log in again. Then remove the GUEST password if you want to allow controlled access to unregistered users.

Stand-alone Server Operation

Although this version of Snap! Server is not designed to operate as the only server in a Novell network, you can configure it as such, but only if no DOS-based clients are present on the network. To set up a Snap! Server to support

32-bit Windows clients in stand-alone mode, follow these steps:

1. Set the external network number to an arbitrary non-zero value. (See "Advanced Setup Options" beginning on page 132.)

   Meridian Data recommends that you leave the Ethernet Frame Type as Auto-detect when operating in stand-alone mode. As a result, the value selected begins a sequence of four external network numbers, each of which is assigned to a different frame type.

External network number	Frame type
First	Ethernet 802.2 LLC
Second	Ethernet 802.3
Third	Ethernet-II
Last	Ethernet 802.2 SNAP

   If the Snap! Server is the only server on the Novell network, then the external network number can be arbitrary.

2. Enable the Snap! Server to show up as the primary server. (See "Advanced Setup Options" beginning on page 132.)

   Doing this allows clients to locate the Snap! Server without assistance from other NetWare servers. 32-bit Windows clients can locate the Snap! Server and access or map its volumes by using GUI utilities such as Network Neighborhood. You cannot set up 32-bit Windows clients to log in using standard NetWare DOS client utilities such as LOGIN and MAP.

This configuration does not support older DOS clients, such as NETX and VLM, that require the standard NetWare DOS utilities (typically located in a NetWare server's SYS volume). Because these utilities are not provided with the Snap! Server, only clients that can log in to the server without them are supported in stand-alone mode.

Using NetWare 3.12 Utilities for System Administration

Snap! Server does not provide any of the standard NetWare 3.12 DOS utilities for server administration. However, you can use some of these utilities, such as SYSCON, to manage a Snap! Server. Instead of these programs, Meridian Data recommends that you use the Snap! Server's Web-based Administration tools, which are simpler to use, offer a protocol-independent view of the Snap! Server, and support certain operations (for example, creating volumes and changing user passwords) that cannot be performed using the NetWare utilities.

Traditional DOS-based NetWare programs for system administration (such as SYSCON) should only be used by Novell CNEs or system administrators who understand NetWare server operation.

When using DOS-based system administration utilities with a Snap! Server, you should understand the differences between Snap! Server and a NetWare 3.12 Server. (For more information, see "Novell Network Functional Compatibility" on page 129.) The differences in the security model and the NetWare bindery implementation are particularly important. The following issues apply to most of the system administration utilities that the Snap! Server supports.

- This version of Snap! Server provides *some* of the bindery functions of a NetWare 3.12 Server. Bindery support is limited to those functions that are required to support file services and related login and user administration functions. Therefore, not all of the bindery objects and properties are supported. In addition, the EVERYONE group is not a bindery object, but rather an "implied group" (all users are automatically members of the EVERYONE group).
- System administration privileges in a Snap! Server are extended to all members of the ADMIN group. Therefore, adding a user to the ADMIN group is equivalent to granting SUPERVISOR privileges to the user (or adding SUPERVISOR to the SECURITY EQUALS list for the user).
- This version of Snap! Server has three preconfigured system administration accounts: ADMINISTRATOR, ROOT, and SUPERVISOR; all three user accounts belong to the ADMIN group. All members of the ADMIN group have system administration privileges in a Snap! Server. The ADMINISTRATOR, ROOT, and SUPERVISOR accounts also have the following special characteristics, which do not apply to other members of the ADMIN group:
  - They share a single password. For example, changing the password for one user account changes the password for the other two as well.

  - They cannot be deleted or removed from the ADMIN group.
  - The SUPERVISOR account is assigned ownership of all files created on the Snap! Server.
- The Snap! Server reports all of the trustee rights associated with a volume, including those associated with the EVERYONE group. Consequently, DOS utilities such as TLIST, GRANT, REVOKE, and REMOVE can be used to show, add, or delete privileges. Note that when showing the trustee rights for a user, Snap! Server derives the information based on the group the user belongs to. It is not possible to change trustee rights for a user.
- You can grant and revoke individual access rights such as delete, but the Snap! Server can track only the following rights:

These rights	Mean
Full access	Equivalent to read, write, open, create, delete, search, and modify
Read-only access	Equivalent to read, open, and search
Deny all access	All access rights are denied

  Although the user interface for some programs (SYSCON, for example) shows individual trustee rights and allows the user to change them individually, the system database does not reflect these changes. Therefore, granting rights to *either* read, open or search is equivalent to granting *all three* of these rights. To revoke read access, all three of these rights must be null. Revoking only the open permission, for example, has no effect because the read and search permissions remain set, leaving read-only access enabled. Similarly, granting rights to *either* write, create, delete, or modify is equivalent to granting *all* applicable rights. To revoke full access, *all four* of these rights must be revoked at the same time.

- To use SYSCON and some of the other systems administration utilities, you must first create a real SYS volume by creating a new share named SYS. Set up this SYS volume with read+write permissions (or trustee rights) for the EVERYONE group and with MAIL, LOGIN, SYSTEM, and PUBLIC subdirectories in its root.

Index