Snap Server®
Administrator Guide

Snap OS v4.0

for Snap Servers 1100/2200/4100

SnapAppliance™

COPYRIGHT

Information in this document is subject to change without notice and does not represent a commitment on the part of Snap Appliance or any of its subsidiaries. The software described in this document is furnished under a license agreement. The software may be used only in accordance with the terms of the license agreement. It is against the law to copy the software on any medium. No part of this manual may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, for any purpose without the express written permission of Snap Appliance, Inc.

TRADEMARKS

Snap Appliance, the Snap Appliance logo, Snap Server, the Snap Server logo, and Guardian are trademarks or registered trademarks of Snap Appliance, Inc. registered in the U.S.A. and other countries.

Products mentioned herein are for identification purposes only and may be registered trademarks or trademarks of their respective companies. Snap Server is a trademark of Snap Appliance, Inc. DataKeeper is a trademark of PowerQuest Corporation. Backup Express is a trademark of Syncsort Incorporated. Windows, Windows NT, Internet Explorer, and Active Directory are registered trademarks of Microsoft Corporation. Java and Solaris, are registered trademarks of Sun Microsystems, Inc. Netscape is a registered trademark of Netscape Communications Corp. AppleShare, AppleTalk, Macintosh, and MacOS are registered trademarks of Apple Computer. AIX is a registered trademark of IBM Corporation. OpenView and HP-UX are trademarks or registered trademarks of Hewlett-Packard Company. BrightStor, Unicenter TNG, ARCserve, InoculateIT, and Unicenter are trademarks or registered trademarks of Computer Associates, Inc. Smart UPS and APC are registered trademarks of American Power Conversion Corporation. UNIX is a registered trademark of The Open Group. XFS is a trademark of Silicon Graphics, Inc. Backup Exec, VERITAS NetBackup BusinessServer, and VERITAS NetBackup Datacenter are trademarks or registered trademarks of VERITAS Software Corporation. Legato NetWorker is a trademark of Legato Systems, Inc. Linux is a registered trademark of Linus Torvalds. All other brand names or trademarks are the property of their respective owners.

REVISIONS

Snap Appliance, Inc. provides this publication “as is” without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability or fitness for a particular purpose. Snap Appliance and its subsidiaries reserve the right to revise this publication and to make changes in the content hereof without the obligation of Snap Appliance to notify any person of such revision or changes.

Part Number: 70990577-002

END USER LICENSE AGREEMENT (EULA)

FOR USE OF SNAP APPLIANCE STORAGE SOLUTIONS AND RELATED INSTALLATION UTILITIES

SNAP IP, ASSIST, AND NASMANAGER ("INSTALLATION UTILITIES"); THE SYSTEM SOFTWARE EMBEDDED IN THE SNAP SERVER STORAGE SOLUTION ("EMBEDDED SOFTWARE"); SOFTWARE MARKETED BY SNAP APPLIANCE OR THAT IS EMBEDDED IN OR OTHERWISE CONSTITUTES A PART OF SNAP APPLIANCE COMPUTER HARDWARE PRODUCT(S) (SOMETIMES REFERRED TO COLLECTIVELY HEREIN, TOGETHER WITH THE INSTALLATION UTILITIES AND THE EMBEDDED SOFTWARE, AS THE "LICENSED SOFTWARE"), EXCEPT WHERE EXPRESSLY PROVIDED OTHERWISE, ARE PROPRIETARY COMPUTER SOFTWARE BELONGING TO SNAP APPLIANCE, INC. OR ITS LICENSORS. UNITED STATES COPYRIGHT AND OTHER FEDERAL AND STATE LAWS AND INTERNATIONAL LAWS AND TREATIES PROTECT THE INSTALLATION UTILITIES AND EMBEDDED SOFTWARE.

USE OF THE SNAP SERVER STORAGE SOLUTION ("SERVER") OR THE INSTALLATION UTILITIES IMPLIES YOUR AGREEMENT TO THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. BY USING THE INSTALLATION UTILITIES OR THE SERVER, YOU ARE ENTERING INTO A BINDING CONTRACT WITH SNAP APPLIANCE, INC.. IF YOU DO NOT AGREE TO BE BOUND BY THESE TERMS AND CONDITIONS, YOU MAY NOT USE THE INSTALLATION UTILITIES, THE EMBEDDED SOFTWARE, OR THE SERVER AND SHOULD PROMPTLY RETURN THIS ENTIRE PACKAGE, INCLUDING THE INSTALLATION UTILITIES AND SERVER, TO THE PLACE WHERE YOU PURCHASED IT FOR A FULL REFUND.

1. Ownership and Copyright. The Installation Utilities and Embedded Software are licensed, not sold to you, for use only as permitted by the terms and conditions of this Agreement. Snap Appliance reserves any rights not expressly granted to you. The Licensed Software is composed of multiple, separately written and copyrighted modular software programs. Various Licensed Software programs (the "Public Software") are copyrighted and made available under the GNU General Public License or other licenses that permit copying, modification and redistribution of source code (which licenses are referred to as "Public Licenses").
   The Public Software is licensed pursuant to (i) the terms of the applicable Public License located in the related software source code file(s), and/or in its on-line documentation; and (ii) to the extent allowable under the applicable Public License. The source code is available at oss.snapappliance.com. To receive a copy of the GNU General Public License, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.
   All other Licensed Software programs (the "Restricted Software") are copyrighted by Snap Appliance or its licensors and are licensed pursuant to all of the terms of this Agreement.
   Copying of the Licensed Software, unless specifically authorized in writing by Snap Appliance, 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.

PROVISIONS APPLICABLE TO RESTRICTED SOFTWARE ONLY (ARTICLES 2 - 7):

2. License. In consideration of the premises of this License Agreement, your payment of any applicable license fee for Restricted Software, and/or your purchase of a Snap Appliance Server that the Licensed Software accompanies, for the term of intellectual property protection inhering in the Licensed Software, Snap Appliance hereby grants to you a limited, personal, and non-exclusive license to install and execute ("Use") the Restricted Software solely under the terms and conditions of this Agreement and only on the Server in connection with which Snap Appliance originally provided such Restricted Software. You are given a non-exclusive license to use the Installation Utilities and Embedded Software in conjunction with a Server, make one copy of the Installation Utilities for archival and backup purposes only, and/or transfer your Server and copies of the Installation Utilities and the accompanying documentation to a third party provided that you provide Snap Appliance written notice of the transfer within 30 days after the transfer date and you do not retain any copy of the transferred software. Any such transferee's rights and obligations with respect to the transferred software and documentation are as set forth in this Agreement.

3. Reproduction of Proprietary Notices. You may not sublicense, distribute, rent, lease, lend, or otherwise convey the Restricted Software or any portion thereof to anyone, and under no circumstance may you use or allow the use of the Restricted Software in any manner other than as expressly set forth herein. Copies of the Installation Utilities must be labeled with the Snap Appliance copyright notice and other proprietary legends found on the original media.

4. Protection of Trade Secrets. The Licensed Software contains trade secrets, and in order to protect them, you agree that you will not reverse assemble, decompile or disassemble, or otherwise reverse engineer any portion of the Restricted Software, or permit others to do so, except as permitted by applicable law, but then only to the extent that Snap Appliance (and/or its licensors) is not legally entitled to exclude or limit such rights by contract. Except with respect to online documentation copied for backup or archival purposes, you may not copy any documentation pertaining to the Licensed Software. You agree that your use and possession of the Licensed Software is permitted only in accordance with the terms and conditions of this Agreement.

5. Ownership of Restricted Software. You agree and acknowledge that, (i) Snap Appliance transfers no ownership interest in the Restricted Software, in the intellectual property in any Restricted Software or in any Restricted Software copy, to you under this Agreement or otherwise, (ii) Snap Appliance and its licensors reserve all rights not expressly granted to you hereunder, and (iii) the Restricted Software is protected by United States Copyright Law and international treaties relating to protection of copyright, and other intellectual property protection laws of the U.S. and other countries.

6. Termination. If you fail to fulfill any of your material obligations under this Agreement, Snap Appliance and/or its licensors may pursue all available legal remedies to enforce this Agreement, and Snap Appliance may, at any time after your default of this Agreement, terminate this

Agreement and all licenses and rights granted to you hereunder. You agree that any Snap Appliance suppliers referenced in the Restricted Software are third-party beneficiaries of this Agreement, and may enforce this Agreement as it relates to their intellectual property. You further agree that, if Snap Appliance terminates this Agreement for your default, you will, within thirty (30) days after any such termination, deliver to Snap Appliance or render unusable all Restricted Software originally provided to you hereunder and any copies thereof embodied in any medium.

7. 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, Commercial Computer Software-Restricted Rights at 48 CFR 52.227-19, and FAR Section 12.212, and successor provisions thereof, 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.

PROVISIONS APPLICABLE TO RESTRICTED SOFTWARE AND, SUBJECT TO SECTION 1, TO PUBLIC SOFTWARE (ARTICLES 8 - 15):

8. Export Laws. Notwithstanding any provision of any Public License to the contrary, Snap Appliance shall have no duty to deliver or otherwise furnish source code of any Public Software if it cannot establish to its reasonable satisfaction that such delivery or furnishing will not violate applicable US laws and regulations. You hereby assure that you will not export or re-export any Licensed Software except in full compliance with all applicable laws, regulations, executive orders, and the like pertaining to export and/or re-export, including without limitation USA versions of the same. No Licensed Software may be exported or re-exported into (or to a national or resident of) any country to which the U.S. embargoes goods, or to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Table of Denial Orders. You agree to ascertain necessary licensing procedures and obtain required licenses before exporting or re-exporting either. You also agree to indemnify Snap Appliance and assume all financial responsibility for any losses it may suffer if you do not comply with this paragraph.

9. Disclaimer of Warranties. THE INSTALLATION UTILITIES AND EMBEDDED SOFTWARE ARE LICENSED "AS IS" WITHOUT WARRANTY OF ANY KIND. SNAP APPLIANCE HEREBY DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, RELATING TO THE INSTALLATION UTILITIES AND THE EMBEDDED SOFTWARE INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT.

10. Limitation of Liability. IN NO EVENT WILL SNAP APPLIANCE OR ITS LICENSORS' LIABILITY UNDER THIS AGREEMENT EXCEED THE PRICE THAT YOU PAID FOR THE INSTALLATION UTILITIES AND EMBEDDED SOFTWARE. FURTHERMORE, IN NO EVENT WILL SNAP APPLIANCE OR ITS LICENSORS BE LIABLE FOR ANY LOST PROFITS, LOST DATA, COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, INDIRECT, OR PUNITIVE DAMAGES ARISING OUT OF OR UNDER THIS AGREEMENT OR THE APPLICABLE PUBLIC LICENSE. The limitation of liability set forth in this paragraph will apply whether or not Snap Appliance or its licensor was advised of the possibility of the loss, liability, or damages and notwithstanding any failure of essential purpose of any limited remedy. Since some states do not allow exclusions or limitations of liability for consequential or incidental damages, this provision may not apply to you.

11. Waiver. No delay or failure of Snap Appliance 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.

12. 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 fullest extent possible.

13. Applicable Law. Except with respect to any Public Software program for which the applicable Public License contains provisions expressly stating the applicable governing law (with respect to which the law so specified shall govern all aspects of such agreement, including the provisions incorporated into such Public License hereunder), the terms of this Agreement (including, to the extent allowable under the Public License, all software governed by a Public License which does not specify a governing law) will be governed by the laws of the State of California, without reference to its choice of law rules, and the United States, including U.S. Copyright laws.

14. Entire Agreement. This Agreement and all applicable Public Licenses supersede all proposals, negotiations, conversations, discussions, all other agreements, oral or written, and all past course of dealing between you and Snap Appliance relating to the Licensed Software or the terms of its license to you, and may only be modified in writing signed by you and Snap Appliance.

15. Contractor/Manufacturer. Snap Appliance, Inc., 2001 Logic Drive, San Jose, CA 95124, USA

Contents

Preface

The Snap Server can be customized to suit your needs. Use this administrator guide to make the most of your Snap Server.

Audience

This guide is intended for individual users or system administrators who need to install and maintain one or more Snap Servers on their network. This guide assumes a basic understanding of file server functionality.

Purpose

This guide provides information on the installation, configuration, security, and maintenance of Snap Servers. It also provides information on installing and using the following utilities and software components:

- Assist
- Administration Tool

Tips and Cautions

This manual uses the following conventions:

Tip A tip presents time-saving shortcuts related to the main topic.

Caution A cautions alerts you to potential hardware or software hazards in the configuration or operation of Snap Servers.

Document Organization

This document is organized as follows:

- **Chapter 1, Installing the Snap Server** shows you the basics of installing your Snap Server onto your network.
- **Chapter 2, Using Your Snap Server** explains how to connect to your network using all of the supported platforms.
- **Chapter 3, Customizing Your Snap Server** teaches you how to set up security, to create local Snap Server users, and to customize your Snap Server.
- **Chapter 4, Managing Your Snap Server** further explains how to maintain and modify your Snap Server.
- **Chapter 5, Troubleshooting** provides tips and tricks that do not appear in other chapters. These items will provide more information when things do not happen in the manner which you expect.

A complete index is available at the end of the guide to help you locate specific topics more quickly.

Typographical Conventions

This manual uses the following conventions.

Font convention	Usage
Bold	Emphasis
Italic	• Emphasis • The introduction of a new terms • Settings you select in the Administration Tool
Arial Bold	Menu commands, command buttons, and navigational links.
Arial	• **Text** that you type directly into a text field, a command line, or web page • Buttons on a keyboard
`Courier Italic`	A variable for which you must substitute a value
`Courier Bold`	Commands you enter in a command-line interface

Related Documents

Documents related to Snap Server models 1100, 2200, and4100 are shown below.

Document No.	Title	Description
70990562-001	Snap Server 1100 Quick Start Guide	Installation and initial configuration instructions for the Snap Server 1100
70990564-001	Snap Server 2200 Quick Start Guide	Installation and initial configuration instructions for the Snap Server 2200
70990566-001	Snap Server 4100 Quick Start Guide	Installation and initial configuration instructions for the Snap Server 4100
70990588-001	Snap Server UI Online Help	Help for the Administration Tool installed on the Snap Server
70990576-001	Snap Server Assist Online Help	Help for the Snap Server Assist utility
70980580-001	ReadMeFirst.html	Describes Snap Server documentation
70980581-001	ReleaseNotes.html	Contains important, late-breaking information not included in other documentation
70980582-001	UpgradeNotes.html	Upgrade procedures for Snap OS
70980583-001	UpgradeNotes2.html	Upgrade procedures for Snap OS
70980584-001	UpgradeNotes3.html	Upgrade procedures for Snap OS
70980585-001	UpgradeNotes4.html	Upgrade procedures for Snap OS
70980586-001	UpgradeNotes5.html	Upgrade procedures for Snap OS

Contacts

Snap Appliance company contacts are listed below.

Snap Appliance Corporate Headquarters

Snap Appliance, Inc.
2001 Logic Drive
San Jose, CA 95124

1.888.310.SNAP (7627) (North America)
1.408.879.8700 (International)

Snap Appliance Web Site

http://www.snapappliance.com

Service and Technical Support

For an immediate response to a service inquiry, use our Expert Knowledge Base System at http://www.snapappliance.com/support. Simply type in your question to view a list of possible resolutions to known issues. However, if none of the listed topics resolves your inquiry, you can forward the question to our Technical Support department who will then e-mail you with a response. To obtain additional service or technical support for your Snap Server, call 1.888.338.SNAP (7627) (North America) or 1.408.558.4657 (International).

Chapter 1

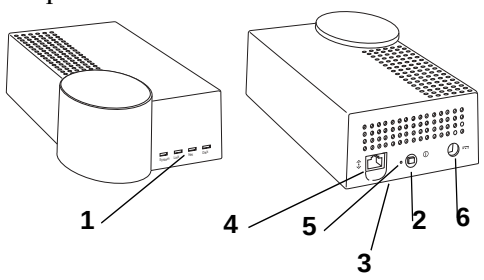
Installing the Snap Server

To install a Snap Server, locate the connectors and controls, connect the Snap Server to your network, turn the server on, and assign the server an IP address

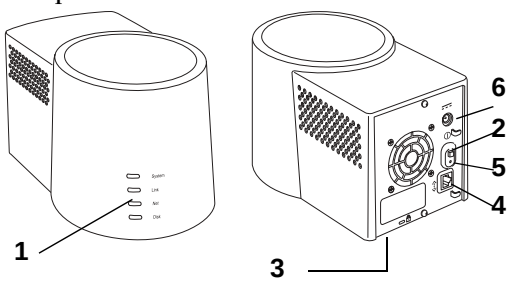
Connectors and Controls

All Snap Servers have the following connectors and controls. These may be in different locations on the server, depending on the model.

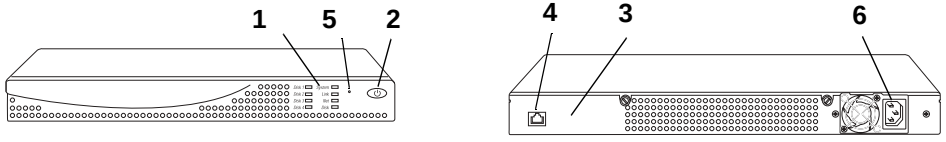
Snap Server 1100



Snap Server 2200



Snap Server 4100



1 Status lights
2 Power button
3 Server number label[1]
4 Network connector
5 Reset button
6 Power connector

1.There are two numbers on the label: a 6 digit server number and a 10 digit serial number. The 10 digit serial number usually starts with FC, JB or CX.

Tip The Snap Server 4100 also has rack mount ears for rack mount installation.

Cord Holder and Kensington Lock Slot (Snap Server 2200 Only)

The Snap Server 2200 has two features not available in the Snap Server 1100 or the Snap Server 4100; the power cord retainer and the Kensington® lock slot.

Power Cord Retainer

Two clips are used to hold the power cord in place. These two clips can be found on the far right of the back of the machine. Use these clips to hold the power cord tight against the back of the Snap Server.

Kensington Lock Slot

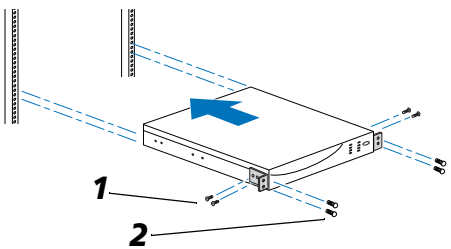
The Kensington Lock slot can be used to secure a Kensington lock on your Snap Server 2200. Kensington locks can be used to secure your server to another object, as well as securing your server to the chassis. With a Kensington lock in place, even unscrewing the case will not open the server. For more information about Kensington locks, see the Kensington Web site at www.kensington.com.

Rack Installation (Snap Server 4100 Only)

You can install the Snap Server 4100 in a standard 19-inch rack.

1. Install the mounting brackets onto the server as shown using the *black* screws.

   It is important that you use the *black* screws, and double-check that the mounting brackets are securely connected to the unit. These brackets will hold the entire weight of the unit.



2. Carefully slide the server into a shelf space in the rack. Use the *silver* screws to secure the server in place on the rack.

If you choose not to install your server in a rack, you can place the Snap Server on a desktop or workstation.

1. Peel the five rubber feet off the backing sheet.
2. Attach the rubber feet onto the markings on the bottom of the unit.

Caution Do not put heavy objects on top of the mounted server.

Connecting Your Server to Your Network

You can connect your Snap Server to a 10BaseT or 100BaseTX network.

1. Connect the server to your network using the Ethernet cable provided.
2. Connect the provided AC power cord to your Snap Server, then connect the server to an AC wall outlet.

Turning On Your Snap Server

Press the power button until the System light turns on, then release the button and wait for the server to start up.

When the System light starts blinking at a steady rate (about once a second), the startup is complete.

Turning Off Your Snap Server

You can turn off your Snap Server using the power button, or by using the Web Administration Tool.

To turn off the Snap Server using the button:

1. Press the power button until the System light blinks three times (about one second). Release the button and wait for the lights to turn off.
2. After you turn off the Snap Server, the lights remain lit while the server completes its shutdown. You must wait for all of the lights to turn off before you turn on the server again or disconnect it from the power source. The Snap Server should never take more than thirty seconds to shut down.

Tip It is important to shut down your server properly to avoid the possibility of data corruption.

To turn off your Snap Server using the Web Administration Tool (not available on Model 2000):

1. In your browser, open the Web Administration Tool by opening your browser to the Snap Server name. For example, if you are connecting to the server named SNAP30123, you would enter the URL http://SNAP30123. For more details, see the Quick Start Guide.
2. Select **Server Settings**.
3. Select **Power Off**. You can see any open files by clicking **Show Open Files**. This lets you ensure that users have time to close files before the server is turned off.

4 Click **Power Off** to begin the power off process. A confirmation page appears.

Tip To turn the server on again, you must physically engage the power switch as described in "Turning On Your Snap Server" on page 7.

Assigning an IP Address

To configure the Snap Server and use it in some network environments, it must have an IP address. (An IP address is a network address and is required for TCP/IP.)

Your Snap Server can automatically obtain an IP address from a DHCP, BOOTP, or RARP server. If your network assigns IP addresses automatically, skip to Chapter 3, "Using Your Snap Server" on page 11.

Tip Your Snap Server must be configured to use the same subnet as the Windows® domain controller if WINS is not in use on the network.

If your network does not assign IP addresses automatically, follow the procedure below for your computer type to assign one manually. You can also use these procedures to look up an automatically assigned address.

Tip To change the server's IP address once it is assigned, use the Snap Server's Web user interface.

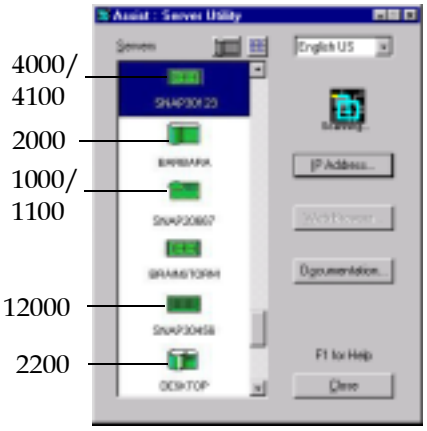
Windows Computers

To assign or look up an IP address on a Windows computer:

1 Load the User CD into your computer's CD-ROM drive.

On most computers Assist starts automatically when you load the CD-ROM. If it does not start, view the contents of the CD-ROM drive, then double-click the **Assist** program icon.

2 Select a server to install from the list of Snap Servers that Assist displays (it might take a few minutes for the server to appear on the list). To view an automatically assigned IP address, double-click the server name and read the address on the Details window. If no address is assigned, continue to step 3.



Tip Assist shows you the model type for each server found on the network.

The icon for servers found mimics the outline of that model's physical appearance, and may show older Snap Servers that are on your network.

3 Click **Initial Setup** or **IP Address** to begin the configuration. If these buttons are not visible, then the server you selected has already been configured with an IP address.

4 If the IP Address window is displayed, select the server and enter the desired IP address. Click **Apply**. Otherwise, follow the instructions presented by the Initial Configuration Wizard. For more information about any setting, press the F1 key for help.

5 Finish the Initial Configuration Wizard by clicking **Finish** to apply your changes. This will also restart the Snap Server if necessary.

Macintosh Computers

To assign or view an IP address on a Macintosh® computer:

1 Load the User CD into the computer's CD-ROM drive and double-click the **Snap** icon to display the Snap Server Selection window. A new window appears.

2 Double-click the **SnapIP** icon.

3 If you use zones with AppleTalk®, select the zone for the server you want to configure.

4 Select the Snap Server you want to configure, then click **OK** to display the TCP/IP Settings dialog box.

If the TCP/IP settings are blank, you must assign the following settings appropriately for your network:

- IP address of the Snap Server
- Your network's subnet mask

- IP address of your network's default gateway (router). If you do not want to assign a default gateway, enter 0 (a zero) in each field.

If necessary, ask your Network Administrator for help in determining appropriate settings.

5 Click **OK** to assign the TCP/IP settings.

Technical Reference

You can always find more detailed information about your Snap Server in the Technical Reference, available at http://www.snapappliance.com/support.

You can also find more information in the online help. Both the main user interface and the Assist utility contain helpful information. To access the Web Administration online help, click the **Help** link. To access the Assist online help, press the F1 key.

Chapter 2

Using Your Snap Server

Once installed on your network, the Snap Server appears as a server with shared folder(s). You can use it to organize and store files in the same way that you use the folders on your local hard disk drive.

The default server name is SNAP followed by a series of digits based on your server number. The actual number of digits depends on your server type; please check the server number on your unit to confirm the default name.

This means that one server might have the default name SNAP300020 while another might have the default name SNAP30020. For Novell® NetWare® users, the default server name is *SNAPnnnNW,* where *nnn* is the server number, regardless of the number of digits.

In general, you can use the following procedures to connect to the Snap Server. The remainder of this chapter describes these procedures in more detail.

To connect to the server using:	Do this:
Microsoft Windows 2000/Me/XP®	Look for the server in My Network Places. If the default settings were not changed during installation, it will appear under Workgroup.
Microsoft Windows 95/98/NT®	Look for the server in Network Neighborhood. If the default settings were not changed during installation, it will appear under Workgroup.
Macintosh	Connect to the server using the Chooser, Network Browser, or Connect to Server.
Web browser	Enter the server name or IP address in your Web browser's location or address box.

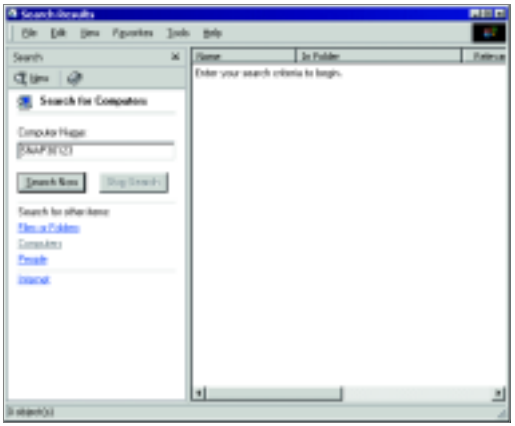
To connect to the server using:	Do this:
NFS	Mount the desired share using the server name or IP address.
FTP	Enter the server name or IP address in your FTP client application.

Windows Users

Windows 2000 and Me

The Snap Server should automatically appear in My Network Places under Workgroup if the default setup was accepted during installation. If it does not appear, follow the steps described here:

1. On the Start menu, click **Search** and then **For Files or Folders**.
2. In the Search Results window, select **Computers**.
3. In the Search for Computers dialog box, enter the server name and click **Search Now**. By default your server name is based on the server number. For example, a Snap Server with the server number 30123 would by default be named SNAP30123.



4. Wait for the server to appear (you may need to try again after a few minutes if you have just turned on the server).
5. Double-click the Snap Server icon to see a folder that represents the network disk drive(s). (NetWare users also see a SYS volume.)

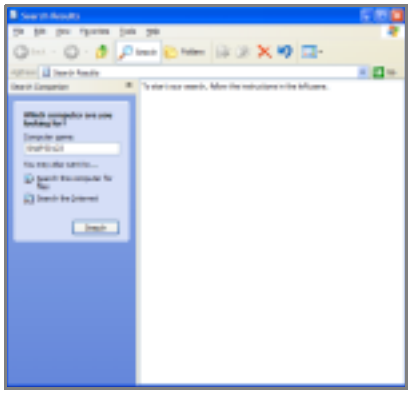
Windows XP

The Snap Server should automatically appear in My Network Places under Workgroup if the default setup was accepted during installation. If it does not appear, follow the steps described here:

1. On the Start menu, click **Search** and then **Computers or People**.
2. In What Are You Looking For, select **Computers on the Network**.

3 In the Search for Computers dialog box, enter the server name and click **Search Now**. By default your server name is based on the server number. For example, a Snap Server with the server number 30123 would by default be named SNAP30123.

4 Wait for the server to appear (you may need to try again after a few minutes if you have just turned on the server).

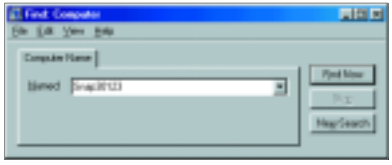


Double-click the Snap Server icon to see a folder that represents the network disk drive(s). (NetWare users also see a SYS volume.)

Windows 95, 98, or NT

The Snap Server should automatically appear in your Network Neighborhood under Workgroup (if the default settings were used). If it does not, follow the steps described here:

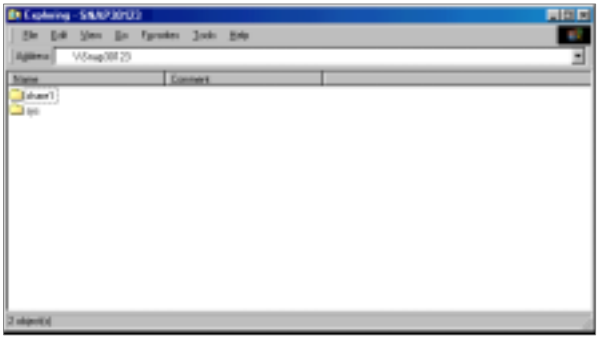
1 On the Start menu, click **Find** and then **Computer**.



2 Enter the server name. By default your server name is based on the server number. For example, a Snap Server with the server number 30123 would by default be named SNAP30123.

3 Click **Find Now** and wait for the Snap Server to appear (you may need to try again after a few minutes if you just turned on the server).

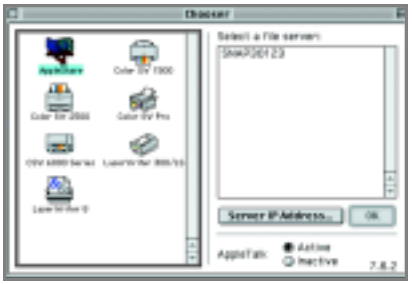
4 Double-click the Snap Server icon to see a folder that represents the network disk drive(s). (NetWare users also see a SYS volume.)

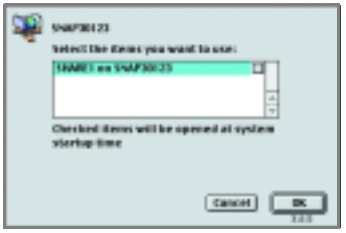


Macintosh Users

To connect to the Snap Server:

1. Select the Network Browser, Chooser, or Connect to Server from the Apple menu. In the Chooser, click the **AppleShare**® icon.
2. If you use zones with AppleTalk, select the default zone in the AppleTalk Zones® list.
3. Scroll through the list of servers in the Select a file server list and select your Snap Server, then click **OK**. In MacOS X, you may need to enter the IP address.
4. When asked for a user name or password, click **GUEST**, then click **OK**.
5. In the server dialog box, select **SHARE1 on SNAP*nnnnnn***.
6. Click **OK** to mount the server on your desktop.





With Macintosh MacOS X, you can mount via NFS as described in "Connecting From an NFS Mount (UNIX® systems only)" on page 15.

Connecting From the Web

By default, you can view folders and files on the Snap Server from the Web. To connect from a Web browser:

1. Type the server's name or IP address in your browser's Location or Address box.
2. Press **Enter**. This will connect you to the server's Home page.

To browse the contents of the server, click the SHARE1 link. Additional links appear if you add network shares. If you restrict access to a network share, you must log in with the right privileges to browse the contents of the share.

Tip If you plan to use your Snap Server as a Web server (hosting static Web content), you can customize the server's Home page and change other Web-related settings. From the server's Administration page, first click **Network Settings** and then click **Web**. The instructions are available through the **Help** link.

Connecting From an NFS Mount (UNIX® systems only)

To connect to the server using an NFS mount:

1. From a command line, type
   mount *server_name:/share_name /local_mount*
   where *server_name* is the name or IP address of the server, *share_name* is the name of the share to which you want to mount, and *local_mount* is the name of the mount target directory.
2. Press **Enter**. You are now connected to the specified share on the server.

   For more details about working with UNIX NFS Networks, see the Technical Reference.

Connecting From an FTP Application

To connect to the server using FTP:

1. Type the server's name or IP address in your FTP program's Location or Address box.

   To connect via a command line, type

   `ftp server_name`

   To connect via a Web browser, type

   `ftp://server_name`

   where *server_name* is the name or IP address of the server.
2. Press **Enter**. This connects you to the server's FTP root directory. All shares and subdirectories will appear as links or folders.

If you restrict access to a network share, you must log in with the right privileges to browse the contents of the share. You cannot manage files or folders in the FTP root directory.

Chapter 3

Customizing Your Snap Server

You can use your Snap Server in its default configuration, or you can customize its name, disk configuration, and other features.

By default, no security restrictions are in place for accessing the files and folders within the Snap Server. Anyone who can connect to the Snap Server from your network or from the Internet can access any of the server's files. If you are concerned about the security of your files, set up users and access restrictions.

Use a Web browser to enable security on your Snap Server and to perform other management functions. For detailed instructions, see the online Help.

You can always find more detailed information about your Snap Server in the Technical Reference, available at http://www.snapappliance.com/support.

Tip The first time you access the Snap Server from a Web browser, you are asked to select your preferred language.

Using Quick Configure

1. Start your browser and enter the server's name or IP address in the Location or Address box. Press **Enter** to display the Snap Server Home page.
2. On the Home page, click **Administration**.
3. When asked to log in, enter Administrator as the user name and enter the Administrator password (leave the password blank if you have not changed it from its default).
4. On the Administration menu, click **Quick Configure** for the initial setup procedure.
5. Follow the Quick Configure's instructions to customize the server. For more information about the settings on any page, click the **Help** link on that page.
6. When you complete the initial setup, click **Finish** to apply your changes, and if necessary, restart the server.
7. At this point, you may want to register your Snap Server online. The link listed on this page will allow you to do so. A new browser window will open to the Snap Server registration page.

After you complete the Quick Configure process, you might want to return to the Administration menu to change the disk configuration or set up security. The remainder of this chapter describes this process.

Changing the Disk Configuration

Your Snap Server's disk configuration was preset at the factory, and the default disk settings depend on the Snap Server.

Tip Make changes to the disk configuration before you store any files on the server. Changing the configuration will erase all data stored on the disk drives.

- **Snap Server 2200 —** By default, the two disk drives on a Snap Server 2200 are combined into a single larger disk (or *disk array*). This configuration is called disk striping or RAID 0. When you connect to the server, you see a single disk. This configuration provides the best performance, but does not protect your data from disk failure.

  You may want to configure your disks differently:

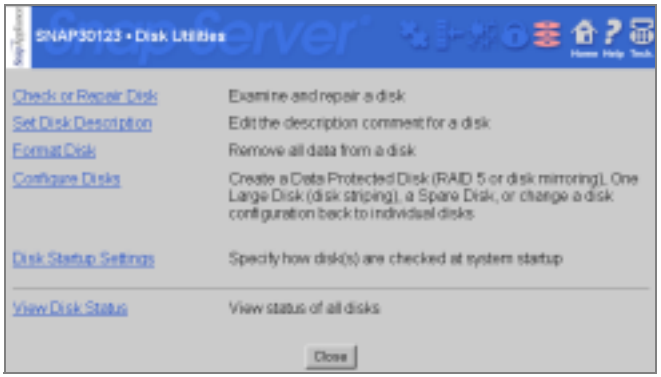
  - You can configure each disk as an individual unit, which network users can access as an independent storage device (JBOD).
  - To protect your data from disk failure, you can use one disk to duplicate the data stored on the other disk. This configuration is called disk mirroring or RAID 1. In this configuration, if a disk fails, the remaining disk automatically takes over and the server continues operating without interruption or loss of data.

- **Snap Server 4100 —** By default, the four disk drives on a Snap Server 4100 are combined into one large, data-protected disk. This configuration is called RAID 5. The total capacity of the combined disks (known as a disk array) is equivalent to the capacity of three individual disks. The remaining disk space is used for data protection. If any single disk in the array fails, the array automatically recovers from the failure and the server continues operating without interruption or data loss.

  According to your needs, you may want to configure your Snap Server disks differently:

  - You can configure each disk as an individual unit, which network users can access as an independent storage device (JBOD).
  - You can combine any two to four disks to make a single larger disk that has no data protection. This configuration is called disk striping, or RAID 0. Disk striping is best suited for applications where maximum performance and highest capacity are more important than data protection.
  - You can combine any two disks, using one disk to duplicate the data stored on the other. This configuration is called disk mirroring, or RAID 1. If either disk in the configuration fails, the other automatically takes over; the server continues operating without interruption or data loss. Disk mirroring sacrifices disk capacity, which is reduced by half, to provide a high level of data protection.

- **All models —** To change disk settings, use the Disk Utilities menu from the Snap Server Administration menu.



Failure Notification via E-mail

If there is a failure of any kind, an e-mail notification can be sent to the administrator. To configure this feature, do the following:

1. From the Administration page, click **Server Settings**.
2. Click **Failure Notification**.
3. Under the Failure Notification screen you can choose when the server will send an error message and to whom. Fill in all the appropriate information and click OK.

Tip You may want to send a test e-mail to confirm your settings. Make sure the "Send a test e-mail..." box is checked to do so.

You can also set up a failure notification using SNMP. Refer to the Technical Reference for more information.

Setting Up Security

Security restrictions control who can access the files and folders stored on the server.

The default configuration allows all users on your network full access to all disks on the server. If you have Web access enabled, this could include Internet users as well, depending on your network setup. If you intend to store sensitive data, define tighter security restrictions before putting it on the server.

If you want to enforce security, define users and user groups and identify which of these may access your Snap Server.

When planning how to enforce security at your location, consider the following Snap Server features:

- You do not need to define users and groups that are already known to a Microsoft Windows network domain or to a Novell NetWare bindery server. See "Defining Snap Server Users" on page 21.
- You can secure a share, an entire disk, selected folder, or individual files.
- You can control how much disk space a user can consume by assigning usage quotas.

To set up security on your server, use the settings on the Security menu. You access the Security menu from the Administration menu.

See the Technical Reference (available at http://www.snapappliance.com/support) for additional information on security topics.

Defining Snap Server Users

Before you can give or deny access to a server, you need to identify the users. Your server allows you to use pre-existing Network Users or define Local Users and Groups.

Network Users

Network Users are users whose information the server obtains from a Microsoft Windows domain or a Novell NetWare bindery server. These network services allow you to define users in a central location and use those definitions across your network.

To access network user lists, click **Security Guides** on the Security menu, and then do one of the following:

- Click **Using Windows domain security** to add Microsoft Windows and Macintosh network users that are part of the domain. Read the initial screen, then click **Next** to continue. You are guided step-by-step to add desired users. See "Configuring Microsoft Windows Domain Security" on page 22 for details.
- Click **Using the security from another Netware server** to add NetWare users. Read the initial screen, then click **Next** to continue. You are guided step-by-step to add desired users.

After Network Users are added, they appear in Share, File, and Directory Security list for Access Right Assignment.

Local Users

Local Users are users whom you define on a specific Snap Server. All of their user information is stored on the server. If you have other Snap Servers on your network, you must define a user on each server, or import users from one server to another using the Assist program on your User CD.

To define Local Users, click **Users** on the Security menu and then click **New**. You can use other buttons on this page to manage Local Users.

User Groups

You can define User Groups and you can also give or deny access to the entire group. If you have defined network users, any groups defined in the Microsoft Windows domain service or Novell network bindery service are available for you to use on the server.

To define groups of Local Users, move to the Security menu, click **Groups** on the Users & Groups menu selection. Click **New**. You can use the other buttons on the Security page to manage local user groups.

Configuring Microsoft Windows Domain Security

You can configure your server to take advantage of Microsoft Windows domain security. In this configuration, you do not need to set up Microsoft Windows (or Macintosh) network users and groups that are already recognized by the domain.

For example, if user JohnD is a member of the domain, you do not need to create a Local User called JohnD in order to connect to the server using Microsoft (or Macintosh) networking. When assigning access privileges, JohnD (along with all other domain users) appears in the list of available users.

You configure domain security from the Security menu by clicking **Security Guides**, then clicking **Using Windows domain security**, and follow the instructions (click the **Help** link if you need more information).

You can configure the server to be part of a "resource" domain (which is where your server appears when browsing the network via Network Neighborhood or My Network Places) and a "security" domain (which is the domain that contains all your users and groups). These two domains could be one and the same (which is typically recommended for smaller networks) or separate (which may be better suited for larger networks).

If you configure your server to use separate domains, the "security" domain must be a domain "trusted" by the "resource" domain. In other words you will need to establish "trust relationships" between the two domains. (For information on configuring trust relationships, see the Windows NT/2000/XP Server documentation.)

As part of the configuration procedure, you must provide a user account (user name and password). This user account must belong to the security domain. The account is used by the server to log in to the security domain and obtain information on users and groups. The user account does not need administrative privileges for Windows domains, but it does need these privileges when accessing Active Directory domains.

After enabling domain security, domain users and groups show up when you assign access rights to network shares. However, domain users and groups do not appear in configuration pages which are used to manage local Snap Server users and groups.

If a user is already part of the domain, do not create a Snap Server local account with the same name and password. This can cause confusion when assigning access rights to network shares.

If you have a large domain (more than 2000 users or groups), the server cannot automatically download the entire list of users (or groups) from the Domain Controller. You can download the entire list of users and groups by checking **Import user/group list from large security domain** in the Large User/Group List tab in Assist's Advanced window. This function downloads the full list of users/groups into the server. The workstation running Assist must be part of the same resource domain as the Snap Server. When using this functionality, Assist must be run on a Windows NT/2000/XP machine. In addition, the Snap Server must be in domain mode for this feature to work.

You can also use the UGUpdate.exe command line program. This has been provided so that this update process can be automated and scheduled. See the Technical Reference for details.

Checking **Import user/group list from large security domain** prevents the Snap Server from downloading the list of domain users/groups automatically. As a result, if the list has changed since you last imported it, you need to "Refresh" it from the Large User/Group List tab in Assist.

Assigning User Access to Network Shares

Network shares are virtual folders that map to an actual directory on the server. They are equivalent to Microsoft networking shares, Macintosh networking shared folders, Novell networking volumes, and NFS exported file systems. Unlike standard NetWare or AppleShare servers, it is possible to share folders contained in a folder that is already shared on a Snap Server.

Snap Servers are configured at the factory with one share for each disk drive or disk array. (For more information on disk configurations for models with multiple disks, see "Changing the Disk Configuration" on page 19.) You can create additional shares that represent an entire disk or a folder within a disk.

You can also assign users or groups access permissions (full access, read only, or access denied) to shares. These access permissions apply to all files and folders accessible through the share.

To assign access permissions, click **Security Guides** on the Security menu and then click **Give or deny users access to an entire disk** or **Give or deny users access to a folder on a disk**. Follow the instructions to select (or create) a share and then give or deny access to that share.

When restricting access to a share, consider the following:

- If you leave a share configured with full access to EVERYONE, all users (except those who are denied access to the share) can still read and write files and folders accessible through the network share.
- Security changes made to Snap Server network shares may not take effect until users log off and back on. Restart the Snap Server if you absolutely need security changes to take effect immediately.
- Denying access to a share overrides any file or directory access granted to a user or group.
- If your network has over 1000 user and group names, the users may be displayed as a range, for example [USR_1000..USR_2000]. Select **Expand Range** to see all of the users within the selected range.

Assigning Users Access to Files and Folders

If desired, you can assign the following access permissions to specific files and folders on your Snap Server:

No Access	User/group is denied access to the file/folder.
Read	User/group can only read the contents of the files or folders.
Add	User/group can create files and folders but not read or modify them.
Write	User/group can create files but not read them.
Add & Read	User/group can create and read the files and folders but not modify them.
Read & Write	User/group can read and write files but not delete them.
Change	User/group can create, read, modify and delete files and folders, but cannot change the access rights.
Full Control	User/group has full access privileges.

For example, you may have a network share open for full access by EVERYONE. You can prevent certain files (or folders) from being overwritten by changing their access rights from "Full Control" to "Read." You can also control access to individual files (or folders) by adding users (or groups) with specific rights to the list of who can access the files (or folders).

To assign access permissions:

1. Click **File/Folder Security** on the Security menu. The server displays a list of network shares that you have defined.
2. Browse the contents of the shares to locate files or folders you want to secure.
3. To view and/or modify the security settings for a file or folder, click the corresponding security icon (it looks like a key).
4. Select the users and groups you wish to add, pick the appropriate security level, and click **Add** to add them to the security list. To change the access permissions for a user (or group), remove the user (or group) from the list, then re-add it to the list with the correct settings.
5. When assigning access rights to a folder, you can click **Apply this folder's security to all sub-files and folders** to propagate the access rights for the folder to all files and folders it contains.

If your network has over 1000 user and group names, the users may be displayed as a range, for example [USR_1000..USR_2000]. Select **Expand Range** to see all of the users within the selected range.

Tip The access permissions you assign to specific files and folders work in conjunction with access permissions you assign to a network share. When access rights for a user or group to a share differ from those to a file or folder in the share, the most restrictive access right is enforced.

For example, you may have a network share where you have denied access to GUEST. GUEST cannot access this share regardless of access permissions assigned to individual files. You may also have a network share where the group Sales has read only access. Members of Sales cannot modify files they access through this share even if these are configured for "Full Control" by EVERYONE.

Assigning File Ownership

The person who creates a file is the registered owner of that file. Owners always have full access to their own files, regardless of access settings. File ownership information is also used to calculate disk space usage for disk quotas. For better file control, you can change file ownership.

For example, a file may exist on the server that was created by one person or a third party, but afterwards the project for which the file was created is transferred to a new employee. You may then want to transfer file ownership to a new person.

1. Click **File/Folder Security** on the Security menu. Select **Set File/Folder Security**. The server displays a list of network shares that you have defined.
2. Browse the contents of the shares to locate files or folders for which you want to modify the registered owner.
3. To view and/or modify the ownership for a file or folder, click the corresponding ownership icon (it looks like a face).
4. Select the person to whom you want to assign ownership of the file or folder, then click **Set Owner**. To apply ownership to an entire folder or subfolder, click **Apply this folder's ownership to all files and subfolders**.

If your network has over 1000 user and group names, the users may be displayed as a range, for example [USR_1000..USR_2000]. Select **Expand Range** to see all of the users within the selected range.

Assigning Disk Usage Quotas

If desired, you can control how much disk storage space a user can consume on the Snap Server.

For example, you may want to prevent some of your users from consuming more than 100 MB of disk space each, while allowing other users to operate without any restrictions.

To assign disk usage quotas:

1. Click **Disk Quotas** on the Security menu and then click **Modify/View Disk Quotas**. The server displays a list of users along with their current disk space allocation and consumption. Disk Quotas must be enabled in order to set quotas for users.

   The Enable Disk Quotas page displays the current quota enabled/disabled state of each disk. The current quota statistics for each user are displayed on the User Disk Quota page. Usage percentage values are rounded up to the nearest whole number.

2. Click on a user name to change the disk quotas for that user.

If you have enabled the Snap Server e-mail notification feature, the server informs you whenever users fills up their available disk space.

If your network has over 1000 user and group names, the users may be displayed as a range, for example [USR_1000..USR_2000]. Select **Expand Range** to see all of the users within the selected range.

Quotas use file ownership to calculate disk space consumed per user. In some cases, it may be desirable to change file ownership in order to fairly distribute disk usage.

Accessing the Snap Server with GUEST Privileges

By default, a Snap Server has a predefined local user named GUEST that allows anyone to use the Snap Server. If a user tries to access the Snap Server and is not recognized, then that user is identified as GUEST and has whatever access privileges that have been allowed to GUEST. This is equivalent to using an anonymous login to access those shares made available to GUEST. Depending on the level of security you require, you may want to restrict GUEST privileges when accessing some (or all) network shares.

How Users Can Auto-Connect with GUEST Privileges

When a user tries to connect with a name that is not recognized as a local user, the Snap Server checks to see if network users are enabled. If so, it lets the Windows domain (or external NetWare server) decide what to do. If network users are not enabled, the Snap Server auto-connects the user as GUEST.

For example, assume that your Snap Server still has its default security settings. If user JaneD tries to connect to the server, she is allowed in with GUEST privileges. In other words, she is listed as JaneD in the server's active user lists, but is treated as if she were GUEST when accessing information on the server. Since, by default, EVERYONE has full access to the server, JaneD has full access to all Snap Server files and folders.

If you configure JaneD as a local user (or use a pre-defined user account, such as Administrator), JaneD (or Administrator) is only allowed to connect to the server by supplying the correct password. However, once connected, JaneD and Administrator have their own user identity. As a result, these users may be allowed access to files or folders that are denied to GUEST.

If you now enable Windows domain security (for both Microsoft and Macintosh network users), the server behaves differently depending on which network protocol is used to connect.

For example, user JohnD (who is not configured as a local user) tries to connect from a Macintosh, the Snap Server lets the domain decide if he is allowed access. However, if JohnD is using a Web browser, the Snap Server auto-connects him with GUEST privileges (because the Web is not enabled for domain security).

Security Tips for GUEST Users

If you are not comfortable with the "auto-connect" feature, simply delete the GUEST account or assign a password to it. If you decide to leave the GUEST account unchanged, consider the following:

- Change access restrictions for Share1. In most cases, you should only allow network administrators to access this share. (Delete "EVERYONE" from the access list and add the local group "Admin" instead.)
- For a small set of users, enter these as local users. When restricting access to a network share, allow full access to EVERYONE but deny access to GUEST. All local users, except GUEST, now have full access to the share.

Chapter 4

Managing Your Snap Server

If you are the administrator of a Snap Server, you can use your Web browser to connect to the server and perform administrative tasks such as checking who is using the server, checking the disk status, and changing configuration options. This chapter gives you a brief introduction to these administrative tools. It also covers special concerns for backing up the data stored on your Snap Server and using the Snap Server in different network environments.

Language Support for File and Folder Names

Documents saved on a Snap Server may be written in any language that the client operating system supports. File and folder name support is provided only for languages that are compatible one or both of Code Pages 437 (US English, Indonesian), or 850 (Western Europe including Afrikaans, Basque, Catalan, Danish, Dutch, English, Finnish, French (excluding Canadian), German, Italian, Norwegian, Spanish and Swedish) and Secondary Code Page 865.

Caution Use of file and folder names in other languages not listed above may not be fully supported. Thus, files and folders may be impossible to open or delete if named using unique characters in unsupported languages. Cyrillic characters are an example of characters that are not supported for use in file or folder names.

If you are running Microsoft Windows you can find the active code page currently used by the client. To find the code page, open a command line and type `chcp`, then press **Enter**. The active code page is displayed.

Using the Home Page

To display the Snap Server Home page, start your Web browser, enter the server's name or IP address in the Address or Location box, and press **Enter** or **Return**.

On the Home page, you can:

- Click a share icon to access the folders and files within that share.
- Click the **Active Users** link to see who is currently using the server.
- Click the **Change Password** link to change the password for a local user. (Local users are described in "Defining Snap Server Users" on page 21.)
- Click the **Administration** link to display the Administration menu where you can access additional server management features.

Using the Administration Menu

From the Administration menu you can:

- Click **Quick Configure** if you would like step-by-step instructions that help you customize your server by changing basic configuration settings from their factory defaults. (See "Using Quick Configure" on page 18.)
- Click **Server Settings**, **Network Settings**, **Security**, or **Disk Utilities** to review your server's configuration settings, make configuration changes as needed, and monitor your server's operation.

For example, you can use Disk Utilities to check a disk or change its description.

- View information about users (click **Active Users**), files (click **Open Files**), and the server log (click **Server Log**).

To learn more about the links and buttons on the Administration menu, click **Help** at the top of the page.

Using the Virtual Machine

Your Snap Server comes with a virtual machine already installed. This lets applications based on Java™ technology run on the Snap Server. The virtual machine is a software module that converts the platform independent code based on Java technology into code that is specific to the Snap Server's microprocessor. Once the code is converted, the virtual machine executes the converted code.

What is a SnapExtension?

A SnapExtension is an application designed to run on the Snap Server. SnapExtensions are integrated using the framework created specially for them. The Snap Server framework allows you to access an application based on Java technology from the Snap Server Web Administration Tool. Only applications developed and integrated for the Snap Server can be accessed this way.

You can find installed SnapExtensions on the SnapExtension page; open the main page of the Web Administration Tool and click **SnapExtensions**.

Check the Snap Appliance Web site at http://www.snapappliance.com for other available SnapExtensions.

Enabling the Virtual Machine

By default, the virtual machine is turned off. To turn it on and begin using SnapExtensions and other applications based on Java technology:

1. Start the Snap Server Web Administration Tool and click **SnapExtensions**.
2. Click **Start Java** to start the virtual machine. You are then prompted to confirm that you want to start Java.
3. Click **Yes** to restart the Snap Server with the virtual machine enabled.

What is Secure Server?

Secure Server uses Secure Sockets Layer (SSL) to let you transmit private data over TCP/IP. The data is encrypted using a private key prior to transmitting the data. By encrypting the data prior to transmission, it will be secure and can only be read by the user requesting the data via a web browser. The secure server is supported by all major browsers. To access the Snap Server using SSL, the Uniform Resource Locator (URL) will begin with https: instead of http:

Enabling Secure Server (SSL)

To enable Secure Server, the virtual machine must be enabled. Use the Snap Server Web Administration Tool's advanced administration features to start Secure Server.

1. If Java is not already active, start Java and restart the machine as described in "Enabling the Virtual Machine" on page 31.
2. Open the Web Administration Tool in your Web browser and click **Network Settings**.
3. Click **Web**, then **Secure Server**.
4. Click **Enable/Disable SSL**, then click **OK** and log in again.

Backing Up the Snap Server

The easiest way to maintain an automatic backup on your Snap Server is with the Server-to-Server SnapExtension. This SnapExtension uses Java-based technology to synchronize two Snap Servers. The synchronization can be fully automated and works with all Snap Servers with a virtual machine installed. For details, please visit us on the internet at http://www.snapappliance.com.

If you choose not to use this SnapExtension, you can back up your Snap Server in the same manner that you back up any other file server. You can use any of several commercial backup programs to copy the data stored on your server to backup media such as tape, another disk drive, another Snap Server, or CD-ROM. Most backup programs store the data in a special format and include a restore function for retrieving files from backups.

Some special considerations for backing up from different operating systems are detailed in this section.

Windows Systems

The Snap Server is compatible with all major backup software for Microsoft Windows NT and Microsoft Windows 2000 servers.

UNIX Systems

You can back up your Snap Server using UNIX backup applications, such as **tar** and **cpio**. However, you must use backup software that supports remote volumes without requiring remote system agent support.

Macintosh Systems

To back up data on your Snap Server from a Macintosh computer, you must first mount the appropriate network shares (volumes) on the desktop. Doing so allows

Macintosh backup programs to operate without a remote agent running on the Snap Server.

Novell Networking Systems

You can back up a Snap Server using applications that are compatible with the Novell SMS (Storage Management System) and TSA (Target Service Agent) protocols. Supported network backup programs include Computer Associates® ARCserve*IT*™ and Veritas Backup Exec™ for NetWare.

When using Novell-based networking backup applications with a Snap Server, you need to be aware of the following issues:

- If the Snap Server does not appear on the list of servers available for backup, you may need to reconfigure the backup software to recognize the server. With some software packages, the only way to do this is to reinstall the backup program.
- Some backup applications do not operate if your server supports more users than allowed by your backup software license. By default, the Snap Server is configured for 250 Novell networking users; you may need to reduce this number to match your license restrictions.

For example, if you purchased a 25-user version of Computer Associates ARCserve*IT*, you need to change the number of Novell networking users to 25 or fewer. (From the Novell Networking page, click **Advanced**, then change the **Number of user licenses**. This setting has no effect on other networking environments.)

- The Snap Server does not currently support data compression. Therefore, you cannot back up data from a NetWare 4.x or 5.x volume with data compression enabled and restore it to a Snap Server. (Compressed files are restored as zero length files to the Snap Server volume.) If you want to transfer your data to a Snap Server, you must decompress it on the NetWare server before you perform the backup.

You can always find more detailed information about your Snap Server in the Technical Reference, available at http://www.snapappliance.com/support.

Tips for Specific Network Environments

This section contains additional tips for using your Snap Server in specific network environments. See the Technical Reference for additional information on this topic.

Microsoft Networks

The Snap Server operates like a Microsoft Windows NT 4.0 file server.

By default, the Snap Server is configured as part of Workgroup. You can reconfigure the server for a different workgroup or domain through Quick Configure or Network Settings (see "Using the Administration Menu" on page 30).

If you configure your Snap Server to use Microsoft Windows domain security (as described in "Configuring Microsoft Windows Domain Security" on page 22), you do not need to set up all your network users as local Snap Server users.

UNIX NFS Networks

The Snap Server supports version 2.0 and 3.0 of the NFS protocol. The Snap Server preserves the case of file names but is case insensitive when comparing file names. Therefore, the server cannot have two files with the same name.

For example, a file saved as "FOO", another saved as "Foo", and a third saved as "foo" are considered the same file to the server.

A network share on a Snap Server is equivalent to an exported file system on an NFS server. NFS users can mount Snap Server shares and access their content directly or mount a subdirectory of a share. They can use dynamic mounting (with auto-mount) or static mounting (with automatic remount when the server restarts after being shut down). To perform a static mount, you must be logged into your UNIX system as root. Mount a Snap Server exported file system with the following commands:

```
mount snap_server:/share_name /local_dir
```

where *snap_server* is the Snap Server name or IP address, *share_name* is the name of the exported file system, and *local_dir* is the local directory to which the file system is mounted. Note the space inserted after the mount name. Below are two examples of a mount:

```
mount snap30286:/share1 /workdir
```

or

```
mount 192.168.1.1:/share1 /workdir
```

The Snap Server uses mount points (network shares) to control access. Files and directories (folders) accessible through the mount point have the access rights of the network share combined with any file and folder security.

You can configure Snap Server users and grant them rights for selected network shares. (Snap Server user names, such as ROOT and GUEST, are not case-sensitive.) You can then associate user accounts from one or more UNIX systems to a Snap Server user.

To configure NFS users first click **Users** on the Security menu and then click **New** to create a new, local user. (For more information about local users, see "Defining Snap Server Users" on page 21.) Select the user you created and then click **NFS**. On the NFS Settings for User page, click **New**. On the New NFS Settings for User page,

enter the user ID (UID), IP address, and Address Mask. Click **OK** to apply your changes. For more information, refer to the online help.

Macintosh Networks

The server operates like an AppleShare 6.0 file server. The interoperability with Windows clients is equivalent to that of a Windows NT 4.0 server with Services for Macintosh enabled.

If you use Microsoft networking, you can enable domain support for Macintosh networking users by configuring the Snap Server to use Microsoft domain security (see "Defining Snap Server Users" on page 21). In this configuration, you do not need to set up Macintosh networking users (and groups) as local Snap Server users.

Security settings for folders cannot be changed from a user computer using native Macintosh tools; any changes made will have no effect.

The Snap Server supports cross-platform access to application-specific files, thus allowing Macintosh-based and Windows-based applications to interoperate transparently. The Snap Server keeps the resource forks in a hidden folder. To maintain compatibility with Apple programs, it is best to copy, delete, or move these shared files using a Macintosh computer. (If working on a Windows computer, copy, delete, or move the entire folder containing the shared files.)

Novell Networks

The Snap Server operates in a manner similar to a Novell NetWare 3.12 file server.

The Snap Server is preconfigured to operate with other NetWare servers on a Novell network. If you want to use the Snap Server as the only server for a network of Windows computers, use Microsoft Windows networking instead.

You can link the Snap Server security to that of another NetWare server, meaning that all of the users (and groups) on the existing NetWare server are automatically accepted as remote users (or groups). (See "Defining Snap Server Users" on page 21.) The external NetWare server used for this purpose must be a 3.x server or have both bindery emulation and IPX support enabled. NDS users can take advantage of this feature to connect to the Snap Server using bindery authentication.

A network share on a Snap Server is equivalent to a volume on a NetWare server.

Operating the Snap Server as a Web Server

In addition to providing administration functions through the Web, the Snap Server can also operate as a Web server, providing Web access to files and folders.

The Snap Server supports direct read-only Web access to its files using the HTTP protocol. The Snap Server is not intended for use as an all-purpose Web server, as it does not support PERL or Java scripting, animations, streaming video, or anything that would require a special application or service running on the server.

Place all HTML files you want displayed under the webroot$ share. To access these files as Web pages, type in the URL in your web browser. For example:

```
http://snap_server/Index.html
```

where *snap_server* is the Snap Server's name or IP address, and *Index.html* is the name of the file you want to access.

To access a Snap Server share (see "Defining Users" on page 11), enter the following address in a Web browser's Address or Location box:

```
http://snap_server/share1
```

where *snap_server* is the Snap Server's name or IP address and *share1* is the name of the share. Your share should look similar to the ones below.

```
http://snap30286/share1
```

or

```
http://192.168.1.1/share1
```

By default, when you connect to a share from the Web, you see a list of files and folders contained in that share. How your browser displays a file depends on the file type and browser settings. To set up a Web "home" page for a share, create an HTML file named index.html and store it in the root of the share.

You can enable or disable Web access to network shares. From the Administration menu, click **Network Settings**, **Web**, and then **Enable or Disable Web**. When Web access is disabled, only administrators can access shares from the Web. When Web access is enabled, access is based on the security settings you defined. See "Setting Up Security" on page 21.

Tip You can use the Web settings to customize the server's Home page.

Operating the Snap Server as an FTP Server

Your Snap Server can also be used as an FTP server, allowing users to access the server's files and directories via FTP clients.

To access a Snap Server share (see "Assigning User Access to Network Shares" on page 24), enter the following address in a Web browser's or FTP program's Address or Location box:

`ftp://snap_server/share_name`

where *snap_server* is the Snap Server's name or IP address and *share_name* is the desired share.

It should look similar to the examples below.

`ftp://snap30123/share1`

or

`ftp://192.168.1.1/share1`

You now have standard FTP access to all files and directories within the share.

You can enable or disable FTP access to network shares. From the Administration menu, click **Network Settings**, **FTP**, and then **Enable FTP Server**. When FTP access is enabled, access is based on the security settings you defined. See "Setting Up Security" on page 21.

Managing the Snap Server with SNMP

Your Snap Server can be managed using SNMP.

SNMP is enabled by default. To disable SNMP access:

1. Go to the server's Home page and open the Administration menu.
2. Select **Network Settings** and then select **SNMP**.
3. Clear the SNMP access check box.

UPS Support

Your Snap Server can be used with uninterruptible power supplies (UPS). Snap Servers communicate with the UPS via the network, not via a serial cable.

You can configure the Snap Server to automatically shut down upon receiving a low battery message from your network-based uninterruptible power supply (UPS). Currently, only APC® brand UPS devices are supported.

To enable automated shutdown on low battery:

1. From the Web Administration Tool, select **Server Settings** and then select **UPS Support**. The page changes to show you available UPS settings.
2. Select **Enable UPS Support**.
3. Enter the IP address and administrator information for the primary UPS device.
4. If using a second device, enter the information for the secondary device.
5. Define the UPS device to use when determining that a shutdown is needed.
6. Click **OK** to complete the configuration.

Chapter 5

Troubleshooting

This chapter contains answers to several frequently asked questions. For more troubleshooting tips, visit the Snap Appliance Web site at http://www.snapappliance.com/support.

Question:	Answer:
Can I use standard UNIX file security on my Snap Server?	Yes. Snap OS v3.0 or greater supports standard UNIX-type file security. For details, check the Technical Reference.
Do Snap Servers support Novell NetWare 5 TCP/IP-only clients?	Your Snap Server only supports Novell networking clients that use IPX. There are two possible workarounds for this limitation: • Install the Microsoft Networking Client and its version of TCP/IP. • Install a NetWare client that supports IPX communications.
Can I use a third-party utility to defragment Snap Server hard disks?	No. Snap Servers use a variation of the Fast File System (FFS) which is highly efficient in preventing file fragmentation when hard disks are not filled to greater than 90% of their capacity.

Question:	Answer:
How can I back up a Snap Server?	The Snap Server can be backed up over the network from a workstation or remote server with a backup device such as a tape drive or hard drive connected to the workstation or remote server. We have tested the most popular server backup applications. Products that are known to work include: • Windows 95/ 98/NT/2000/Me/XP Native Backup • Computer Associates ARCserve/*IT* (Windows 2000 and NetWare 6.6) • Veritas Backup Exec (Windows version 8.6, and NetWare version 8.5) • Dantz™ Retrospect™ (Macintosh) See “Backing Up the Snap Server” on page 32 for details.
How can I back up my system settings?	On the Save Configuration page, accessible from Setup Settings, you can enable saving your system settings. You can perform this operation manually or set up automatic periodic saves. Select the frequency of saves. Make sure that your backup process includes the hidden OS_Private folder in the root of the file system.
How do I grant complete access to a few users on my network, but not others?	The simplest way is to use the browser-based security setup screen to enter the user names of the people you want to allow access to the Snap Server. Then either remove or password-protect the GUEST user account. Users defined in the Snap Server's security automatically become members of the EVERYONE group, which is granted complete access to all shares in the default configuration. By disabling or password protecting the GUEST account, you prevent connection by any user not defined to the Snap Server's security. See “Accessing the Snap Server with GUEST Privileges” on page 27.

Question:	Answer:
Why do I get “Access Denied” messages after configuring Microsoft Windows Domain Security?	The Snap Server authenticates the users as local Snap Server users first, before authenticating through the Windows domain. However, the Windows domain users/ groups are typically the ones who have been granted access to the shares. Decide whether to use the Microsoft Domain security (recommended) or the native Snap Server security, but do not combine the two. It is acceptable to leave the default local users (GUEST, ROOT, SUPERVISOR, and ADMINISTRATOR) and the default local groups: (EVERYONE and ADMIN), but do not add duplicate users and groups of those that are found on the domain controller.
How do I reset my server to factory defaults?	Connect to your server and select **Administration**, then **Server Settings**. Click **Factory Defaults**. Select from: • Reset IP Address only • Reset IP Address and Network Settings • Reset IP Address, Network Settings, and Shares • Reset IP Address, Network Settings, Shares, and File/ Folder Security. Select the desired settings and click **OK** to restore default settings.

Question:	Answer:
How do I reset Snap Server settings if I cannot connect to it? Resetting the Snap Server to its factory default settings does not change the existing disk configuration or erase any data stored on your disks. However, clearing all of the system settings will remove the File/Folder Security and Quotas.	To reset the server settings: **1** Turn the Snap Server off (as described on page 7) and wait for all of the lights to turn off. **2** Press and hold down the Reset button. While you are still pressing Reset, turn the Snap Server back on; wait until both the System and Disk lights start flashing in sync. (To press the Reset button, push a pencil point or similar object into the reset button.) **3** Release the Reset button. **4** To select the settings you want to clear and reset, 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. **5** Watch the Disk light and verify that 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 light should flash three times repeatedly to confirm the reset. If the number of flashes exceeds the number you intended, repeat steps 4 and 5 of this procedure. **6** When the light confirms the level of reset you intended, press and hold down the Reset button until both the System and Disk lights turn off, and then release the Reset button. The server then restarts, and resets the settings you cleared to the factory defaults.
Why does Windows sometimes inaccurately report free space?	Some Windows clients are unable to recognize free disk space in excess of 2GB. This problem only affects the display, it does not affect the available space or your ability to use it. Use a Web browser to determine how much free space is actually available. See “Using the Administration Menu” on page 30.
Why do I get “File is in use” errors in my AutoCAD users report?	AutoCAD users on Microsoft networks sometimes get an inaccurate error message indicating that a file is in use when this is not the case. This is due to the Microsoft Network client, and is not specific to the Snap Server. A patch to correct this problem is available from Autodesk, the makers of AutoCAD.

Snap Server Web Resources

For more information on your Snap Server, visit our Web site at http://www.snapappliance.com.

Numerics

A

B

C

D

E

F

G

H

I

J

S

T

U

V

W