BlackArmor® NAS 440/420
User Guide

BlackArmor® NAS 440/420 User Guide

Seagate Technology LLC
920 Disc Drive
Scotts Valley CA 95066 U.S.A.

Open Source and License Source Information

For information about the open source and licenses used with Seagate products, please see the Seagate Web site at www.seagate.com/support

Contents

1. Preface

- About This Guide
- Kit Contents
- System Requirements
- Finding More Information

About This Guide

This *User Guide* provides all the information you need to successfully set up and use your Seagate BlackArmor® NAS 440/420 (BlackArmor server).

This guide contains complete setup instructions, as well as reference information about the components and features of your BlackArmor server. It also provides an overview of how you can get the most out of your BlackArmor server as your needs grow and change over time.

Note: Step-by-step instructions for using the BlackArmor software tools are included in the online Help provided with the software.

Some of the topics in this guide apply to BlackArmor *administrators* only—users that have access to the administrative features of your BlackArmor server. Administrators-only information is clearly identified.

Kit Contents

Your BlackArmor server kit includes:

- BlackArmor server
- Power adapter
- Ethernet cable
- Installation CD, including software, product documentation, and warranty information
- *BlackArmor Quick Start Guide*

System Requirements

Any computer that will be used to access your BlackArmor server must meet these requirements:

- A Microsoft Windows® or Apple Macintosh® computer running one of these operating systems:
  - Windows XP or Windows Vista®, with the latest Service Pack installed
  - Mac OS X 10.4.11 or later
- Ethernet card
- Supported Web browsers:
  - Microsoft Internet Explorer 6, 7 or 8 (Windows only)
  - Apple Safari 3, 4 or newer (Windows or Mac)
  - Mozilla Firefox 2, 3 or newer (Windows or Mac)

Additionally, you need:

- Local area network (LAN) or wireless LAN (WLAN)
- Network switch or router, with at least one available Ethernet port
- Internet connection (for remote access to server and software and firmware updates)

Finding More Information

For more information about your BlackArmor server, see:

- BlackArmor Quick Start Guide (printed)
- BlackArmor Manager Help
- BlackArmor Discovery Help
- BlackArmor Backup User Guide
- BlackArmor Backup Help
- Readme file

For more information, please refer to the Seagate Web site at www.seagate.com.

2. All About the Seagate BlackArmor® NAS 440/420

- Introduction
- About the BlackArmor Server
- What You Can Do With the BlackArmor Server
- The Difference Between a BlackArmor Administrator and User
- How to Get Started

Introduction

This chapter introduces the components and features of your BlackArmor® NAS 440/420 (BlackArmor server), describes what the BlackArmor server can be used for, and introduces the difference between BlackArmor administrators and general BlackArmor users.

This chapter also provides tips for setting up and getting the most out of your BlackArmor server. (To find out if you're an administrator or user, see "The Difference Between a BlackArmor Administrator and User" on page 12.)

About the BlackArmor Server

The BlackArmor server is a file server, a device that is used for storing and sharing all types of computer files on a local network. The BlackArmor server contains four Serial ATA (SATA) disk drives and has built-in data protection to help keep your data safe from disk drive failures and other catastrophes.

The BlackArmor server comes with software to help you back up, store, protect, and share your files.

The BlackArmor server is typically used by small business owners and people with home offices who want to store and protect the computer files that are important to them—client files, business records, financial information, and so on—and make them available to other people on their local network or over the Internet.

Main Components of the BlackArmor Server Kit

The BlackArmor server kit has four main components:

- **The BlackArmor Server**—Hardware that includes the disk drives that store and protect your files.
- **BlackArmor Discovery**—Software that finds and connects your BlackArmor server to your computer.

- **BlackArmor Manager**—A tool embedded in the server that helps you set up, modify, and monitor your BlackArmor server from your computer (or even remotely) using a Web browser.
- **BlackArmor Backup**—Software that helps you back up files, applications, and even operating systems to your BlackArmor server. You can also restore your system and data using this software. See the *BlackArmor Backup User Guide* for details.

Features of the BlackArmor Server

Note: The features described in this section are shown in the graphics on page 11.

The BlackArmor server includes:

- Four Serial ATA (SATA) disk drives that are *hot-swappable* (easily removable and replaceable). The disk drives are enclosed by the server door.
- Two Ethernet, or *LAN*, ports that let you access the server from your local network or over the Internet.

The server's two LAN ports can be configured for *link aggregation*, which means you can connect both LAN ports to your network at the same time for failover protection: the other link (port) takes over if one link fails. See page 38.

Alternatively, you can use one LAN port to connect to your network and the other LAN port to set up archive backup, where an exact copy of the data on your BlackArmor server is created and maintained on a second BlackArmor server. See page 37.

- Four USB ports that let you back up data directly to or from a portable USB drive, connect a USB printer that everyone on your local network can use, or connect an Uninterruptable Power Supply (UPS).
- LEDs representing the ports, disk drives, and server that indicate activity and status. See page 40.
- LCD screen that displays current server settings and status information, including messages that appear when an *event* (a problem or change in setting) occurs on the server. Buttons beside the screen help you scroll up and down through the available information. See page 39.

When the LEDs indicate a change in setting or status, information about this change appears on the LCD screen.

- A Reset button that lets you reset your BlackArmor server user name and password to their original settings.

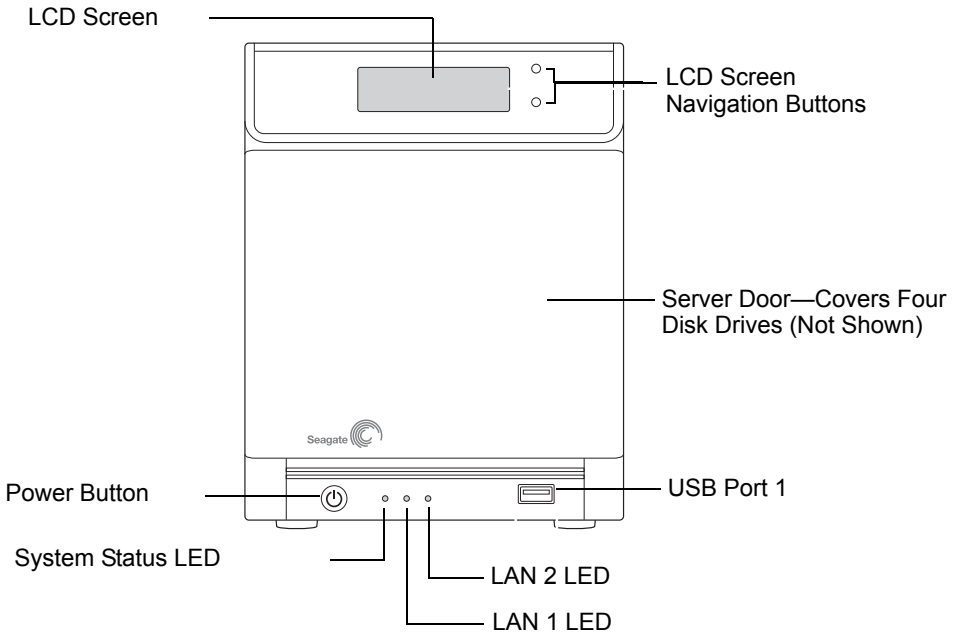


Figure 1: Front of BlackArmor Server

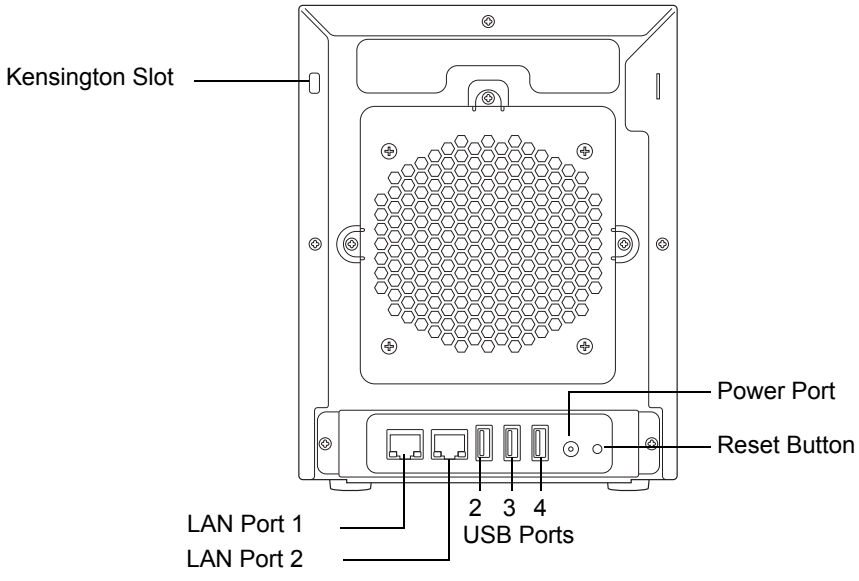


Figure 2: Back of BlackArmor Server

What You Can Do With the BlackArmor Server

In general, you can use your BlackArmor server to:

- Create a central storage place for the files you want to share with other people on your local network or over the Internet.
- Create and maintain automatic backup copies of all your files—even your operating systems.
- Share your files—contracts, business presentations, progress reports, and so on—with other people on your local network or with business clients over the Internet.
- Recover quickly from a computer disaster, such as the unintentional deletion of important files, the failure of a disk drive, the loss or theft of your computer.
- Access your BlackArmor server over the Internet from anywhere in the world to download files that you need where you are, or upload files that you want to secure or share while you're out of the office.
- Share a USB printer with other people on your local network.
- Create a media server so that everyone on your local network can enjoy downloaded photos, videos, and music.
- Enable the iTunes® service on the server so that users can stream music directly to a network computer with iTunes installed.

The Difference Between a BlackArmor Administrator and User

In addition to the features that can be used by everyone, such as file sharing, your BlackArmor server has behind-the-scenes, administrative features that should be accessed by only one or two people who are referred to in this guide as BlackArmor *administrators*.

Everyone who accesses the BlackArmor server is referred to in this guide as a BlackArmor *user*.

About BlackArmor Administrators

BlackArmor administrators have full access to all features and settings on the BlackArmor server, and to all files stored on it. A BlackArmor administrator can:

- Change any server setting
- Create and modify user accounts and group accounts
- Set up and modify folders (or *shares*)
- Update the server's firmware
- Replace a failed disk drive

- Reset the server's name and password to the original settings

About BlackArmor Users

All BlackArmor users, including administrators, can:

- Change their login password
- Save and share files on the BlackArmor server
- Back up files to the BlackArmor server
- Access the BlackArmor server over the Web, using Seagate Global Access
- Download large Web files directly to the BlackArmor server
- Access music, video, and photos (if the BlackArmor server is set up as a media server)
- Share a USB printer that's connected to the BlackArmor server (if any)

Note: The administrator can also create a user account that has administrative privileges. See the BlackArmor Manager help for instructions.

How to Get Started

This section describes the getting-started tasks for BlackArmor administrators and users.

BlackArmor Administrators Start Here

To get started with your BlackArmor server:

1. Install the BlackArmor server and software (see page 16).
2. Connect to the server using BlackArmor Discovery (see page 17).
3. Complete the initial setup of the server using BlackArmor Manager (see page 18.)
4. Create customized folders, or shares, for storing saved files (see page 18).
5. Create individual user accounts for everyone who will be accessing your BlackArmor server and assign each user access to the folder shares you created, as required (see page 19).
6. Provide user account information to each BlackArmor user (see page 20).
7. *(Optional)* Make your BlackArmor server accessible over the Web by enabling Global Access in BlackArmor Manager (see page 21).
8. *(Optional)* Make a USB printer available to everyone on your local network by connecting it to your BlackArmor server (see page 22).
9. *(Optional)* Connect an Uninterruptable Power Supply to your BlackArmor server to maintain power to the server in the event of a power failure. (see page 43).

10. *(Optional)* Turn your BlackArmor server into a media server so that BlackArmor users can access music, photos and videos (see page 22).
11. Continue with BlackArmor Users Start Here in the next section to begin using your BlackArmor server to save, protect, and share your own files.

BlackArmor Users Start Here

To get started with your BlackArmor server:

1. Ensure that you have these items from the BlackArmor administrator:

- The BlackArmor Discovery software
- The BlackArmor Backup software
- Your BlackArmor log in name and password
- The names of the folder share(s) that you can access
- A description of any access limitations you have (for instance, read-only access to a particular folder share)
- A copy of the BlackArmor NAS 440/420 User Guide

2. Install the BlackArmor software (see page 16).

You don't need to install BlackArmor Backup if you are already using other software for regular file backups.

3. Connect to the server and the folder shares you have access to using BlackArmor Discovery (see page 17).
4. Share your files by saving them to shares that can be accessed by other people on your local network or over the Web.
5. *(Optional)* Create a full backup of your important files, or set up recurring backups, using BlackArmor Backup (see page 50).
6. *(Optional)* If a USB printer has been connected to the BlackArmor server, add it to your list of available printers, following your operating system's instructions.

3. Getting Started with Your BlackArmor® Server

- Introduction
- Setup Steps for Administrators
- Getting Started as a BlackArmor User

Introduction

This chapter provides step-by-step instructions for installing and setting up your BlackArmor® server and software.

If you are not a BlackArmor administrator, skip to page 24.

Note: For an overview of the setup steps, see “How to Get Started” on page 13.

This illustration shows the layout and location of a typical BlackArmor server and software setup.

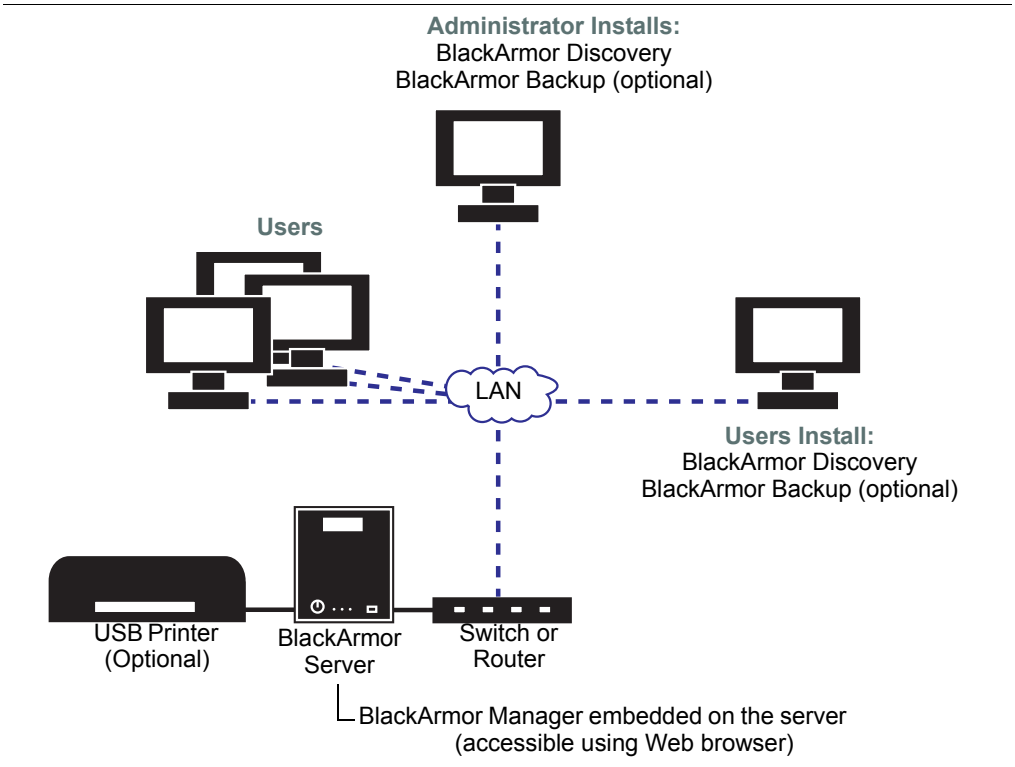


Figure 3: Typical BlackArmor Setup and Installation

Setup Steps for Administrators

If you are not a BlackArmor administrator, skip to page 24.

Installing the BlackArmor Server and Software

Before you begin:

- Ensure that your computer meets the requirements listed on page 8.
- Ensure that you have a solid, flat, stable surface for the server to sit on in an area with reliable ventilation. Ensure that the server's vents will not be covered or blocked and that the server is not placed near a heat source. Ensure that the server won't be in an area where liquids may be spilled on it.
- Ensure that you have help lifting the server if you are uncomfortable lifting objects of moderate weight.

To install the BlackArmor server and software:

1. Use the Ethernet cable included in the kit to connect the BlackArmor server to a switch or router on your local network. Connect the Ethernet cable to port 1, as shown below.

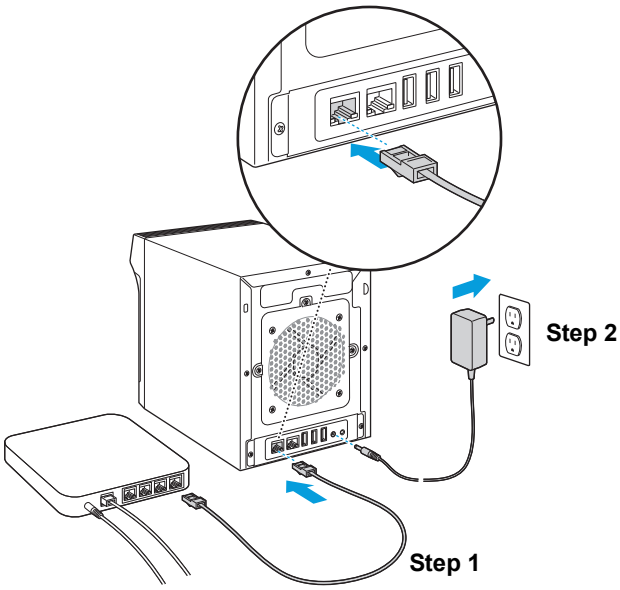


Figure 4: Connect power and network cables

If you have a second Ethernet cable and want to connect both LAN ports to the switch or router, connect it now. See page 38 for more information.

2. Use the power adapter included in the kit to connect the BlackArmor server to a grounded power outlet.

The server powers on automatically and the LED lights on the front panel of the server illuminate. The LCD screen shows the start-up progress.

3. Insert the installation CD into your computer.

The installation wizard opens automatically. Install both BlackArmor Discovery *and* BlackArmor Backup unless you are already using another backup software program.

4. Click **Next**.
5. Click **Next** to accept the default installation location; or, click **Browse** to select a custom location, then click **Next**.
6. Click **Next** to accept the default program folder name; or, enter a custom name, then click **Next**.

BlackArmor Discovery is installed.

7. Click **Finish**.

Connecting to the Server

To connect to your BlackArmor server:

1. Double-click the BlackArmor Discovery icon on your desktop (Windows) or in your Applications folder (Mac).

When BlackArmor Discovery opens, it automatically searches for all BlackArmor servers on your network and displays them in a list.

2. Select your new BlackArmor server.
3. (Windows) Click **View Drive Details** then click **Manage**. (Mac) Click **Manage Server**.

BlackArmor Manager opens.

> **Note:** BlackArmor Discovery remains open, unless you choose to close it. If you do close it, you can open it again at any time by double-clicking the icon on your desktop (Windows) or in your Applications folder (Mac).

4. Log in using the default settings. (The user name and password are case-sensitive.)

user name: **admin**

password: **admin**

> **Note:** Your BlackArmor server comes with other default settings to help you get started storing, sharing, and protecting your files right away. For more information, see page 29.

Completing the Initial Setup

The first time you log in to your BlackArmor server, the setup wizard opens. To complete the setup:

1. Click **Next** to begin the initial setup of the BlackArmor server.
2. Read the Seagate BlackArmor license agreement, then click **I Agree**.
3. Customize your server's basic settings:

- Enter a name for your BlackArmor server. To make the server easy to identify on your local network, give it a unique and easy-to-remember name. The name can be up to 16 alphanumeric characters long and can include hyphens. Spaces are not allowed.
- Enter a description for the server, using the location, content, or other feature of the server that will help you differentiate it from other servers on your local network.

4. Select the time zone that represents the location of your server, then set the current date and time.
5. Click **Next**.
6. Enter and re-enter the new administrator password, then click **Next**.

Seagate highly recommends customizing the administrator password to protect your BlackArmor server and its contents. Passwords can be up to 16 alpha-numeric characters long and are case-sensitive.

Good password example: **LEag29ue**

Bad password example: **blackarmor**

7. Select the network mode you want, then click **Next**.

By default, the BlackArmor server's network mode is set to DHCP.

Unless you are part of a large corporation with an IT department, Seagate highly recommends using the DHCP network mode.

8. Click **Next** to complete the setup.
9. Review the contents of the setup summary. Click **Back** to make any necessary changes, or click **Finish** to complete the setup.

Creating Custom Shares

Your BlackArmor server comes with two preconfigured shares: Download and Public. If these two shares meet your current needs, skip to "Creating User Accounts" on page 19.

You can also create your own custom shares using the BlackArmor Manager Web interface. You might want to do this if you want to store files by category, such as client files, project files, or financial archive files; or if you want to store files by business team, such as marketing, accounting, or sales.

To create custom shares:

1. In the menu bar, select **Storage**, click **Shares**, then click the **Add** icon.
2. Enter a name for the new share.

To make the share easy to recognize on the server, give it a name that's descriptive and easy to remember.

3. Enter a description of the share.
4. Select the share's owner from the drop-down list of all user accounts. (See Creating User Accounts to create individual user accounts.)
5. Select the types of protocols you want the share to support (see page 34).
6. Select the volume in which to create the share, if there is more than one volume on your server.
7. You can protect files on the share from being accidentally deleted by adding a recycle bin to the share. Deleted files can be recovered from the recycle bin, if necessary.

To add a recycle bin, beside **Recycle Bin Service**, click **Enable**.

8. You can set the share to download specific types of files into default folders—for instance, all music files into Music.

To automatically sort downloaded files, beside **Drag&Sort Service**, click **Enable**. See "Special Features of Shares" on page 34 for information about this service.

9. You can use your BlackArmor server to share digital photos, videos and music with people on your local network. To set up this service, beside **Media Service**, click **Enable**.
10. Click the check box for **Share Access** to go to the page on which you set up and customize user and group access to this new share. See the BlackArmor Manager online Help for more information.
11. Click **Submit**.

The share is created.

Creating User Accounts

Your BlackArmor server comes with one administrator account only. Your next step is to use BlackArmor Manager to create individual user accounts.

Part of creating user accounts is assigning each user access to the default shares or the new shares you create.

To create a user account:

1. In the menu bar, select **Access**, then click **Users**.
2. Click the **Add** icon.

3. Customize the account as required:

- **User Name**: Name user enters when logging in
- **Admin Rights**: Sets the user as a BlackArmor administrator
- **Full Name**: User's name
- **Password** and **Confirm Password**: Up to 15 alphanumeric characters that user enters when logging in
- **Group**: Group of users to which this account belongs, if any
- **Create User Private Share**: Whether or not BlackArmor Manager should create a new private share for this account
- **Volume**: Which volume (if there is more than one) the private share should be created in
- **Services**: Which type(s) of file service should be supported by the private share

4. Click **Submit**.

The new account appears in the list of user accounts.

Note: You can make it faster and easier to manage access to shares by sorting users into user groups. User groups allow you to modify share access for individuals or entire groups from a single window. See page 36 for more information.

Distributing BlackArmor User Information

Once you have created user accounts, provide these items to each BlackArmor user so they can get started using your BlackArmor server:

- The BlackArmor Discovery software
- The BlackArmor Backup software (optional)
- The user's BlackArmor log in name and password
- The names of the shares that the user has access to, and the limitations of their access—read-only, for instance—if any
- A copy of this guide and the section the user should read to get started with the BlackArmor server ("BlackArmor Users Start Here" on page 14)

You can create copies of the software for each BlackArmor user from the supplied CD or download what you need from www.seagate.com/support

Making BlackArmor Accessible Using Seagate Global Access

Note: This step is optional. Only BlackArmor administrators can enable global access for the server.

You can choose to make the BlackArmor server's files and folders accessible over the Web by enabling Global Access in BlackArmor Manager.

Seagate Global Access is a service that you can use to view, download, share, and work with the files stored on your BlackArmor server from anywhere in the world. You can also use Global Access to upload files to your BlackArmor server.

To access the BlackArmor server over the Web:

- The administrator must enable Global Access on the server using BlackArmor Manager. This allows the server to be accessed remotely.
- Each user, including the administrator, must have a Global Access account to use this feature. Anyone who wants to access the BlackArmor server over the Web must have their own Global Access account. (Accounts are free.)

Enabling Global Access to the Server (administrator task)

1. In the menu bar, select **Access**, then click **Global Access**.
2. Click the **Enable** check box.
3. Click **Submit**.

Access is now enabled to the server. Users must also create a Seagate Global Access Account and enable Global Access to access the server's files over the Web. See "Creating a Seagate Global Access Account" on page 25.

Enabling Global Access as a User

Once Global Access is enabled on the server by the administrator, each user must also enable access for their user account.

You must have a Seagate Global Access account to enable global access. You can create an account from the Global Access page, described below. See "Creating a Seagate Global Access Account" on page 25 for detailed instructions.

1. Log in to the server with your BlackArmor user account.
2. In the Menu bar, click **Global Access**. (If your user account has administrative privileges, select **Access** then click **Global Access**.)
3. Click the **Enable** check box.
4. If you have not created a Global Access Account, click **Create an Account**. Otherwise, go to step 5.

A new Web browser window appears. Follow the on-screen instructions to create a new account.

5. Enter the email address and password for your Seagate Global Access account.

6. Click **Submit**.

See the Global Access user documentation for help granting other people access to your private share.

Signing in to Your Seagate Global Access Account

1. Log in to the server with your user account.
2. In the Menu bar, select **Global Access**.
3. If not entered, enter your Seagate Global Access email address and password.
4. Click **Sign In to Your Account**.

See the Global Access user documentation for help granting other people access to your private share.

Connecting a USB Printer to Your BlackArmor Server

Note: This step is optional. Only BlackArmor administrators can set up a printer.

You can make a USB printer available on your local network by connecting it to your server.

To connect a printer:

1. Ensure that the printer is powered off.
2. Use a high-quality USB cable to connect the printer to one of the USB ports on the back of your BlackArmor server.
3. Power on the printer and install the driver on your computer (if you haven't already), following the manufacturer's instructions.
4. Have other people on your local network add the USB printer to their list of available printers, following the instructions for their operating system.

The printer is now available to all BlackArmor users. The Printer Manager is in the BlackArmor Manager's Network menu. See the online help for more information.

Setting Your BlackArmor as a Media Server

Note: This step is optional. Only BlackArmor administrators can enable the media server feature.

You can use your BlackArmor server to share digital photos, videos and music with people on your local network. The media folders in which you place your files (Our Music, Our Pictures and Our Videos) are available once you enable the Drag&Sort feature using BlackArmor Manager. See the BlackArmor Manager online help for more information.

To set up your BlackArmor server as a media server:

1. In the menu bar, select **Media**, then click **Media Service**.
2. Beside **Service**, select **Enable**.
3. Set the default sorting method for media files, if required, then click **Submit**.

Your BlackArmor server can also function as an iTunes server so that BlackArmor users can stream music directly to a network computer with iTunes installed, or to an iPod® connected to a network computer.

4. Set a recurring time for the server to check for new music. You can set the time from every five minutes to once a day.
5. Click **Submit** to save the settings.

The media service is enabled.

Creating Media and Music Folders

Follow these steps if you need to create the Media Server folders:

1. Start BlackArmor Discovery.
2. Select the server:

- (Windows) Select the server and then click **View Drive Details**.
- (Mac) Select the server in the upper table of the Discovery window and then click **Mount Share** with the Public share selected in the lower table.

3. Select the Public share and then click **View** (Windows) or double-click the mounted share (Mac).

The share opens.

4. Create the following folders, exactly as shown: “Our Music”, “Our Pictures”, Our Videos”.

You can now place your files to share in the appropriate folders.

Next Steps for Administrators

Before continuing, you should familiarize yourself with the features of your BlackArmor server and software by reviewing this guide.

Your BlackArmor server is preconfigured with settings that are appropriate for typical use, so that you can get started storing, sharing, and protecting your files right away (see page 29). You can customize your BlackArmor server as required, using BlackArmor Manager.

After the initial setup, you can:

- Set up group accounts to make it easier to manage access permissions (see page 36).
- Set up the server’s volumes and RAID configurations (see page 31).
- Set up an on-going archive backup process with a second server on your network (see page 37).
- Store all your photos, videos, and music files to the server and use it as a media server so that media players on your network can access your files (see page 38).
- Monitor the server locally or remotely (see page 39).

The remainder of this guide introduces the server's features and provides some recommendations to help you create a storage system that meets your needs.

Note: Don't forget that you are also a BlackArmor user. To begin storing, backing up, and sharing your files, continue with Getting Started as a BlackArmor User.

Getting Started as a BlackArmor User

Follow the steps in this section to get started with your BlackArmor server.

1. Ensure that you have these items from the BlackArmor administrator:
   - The BlackArmor Discovery software
   - Your BlackArmor log in name and password
   - The BlackArmor Backup software (optional)
   - The names of the share(s) that you can access
   - A description of any access limitations you have (for instance, read-only access to a particular share)
   - A copy of the BlackArmor NAS 440/420 User Guide
2. Install the BlackArmor software.

   Install both BlackArmor Discovery *and* BlackArmor Backup unless you are already using another backup software program.
3. Connect to the BlackArmor server and the shares you have access to using BlackArmor Discovery.
   - (Windows) Double-click the BlackArmor Discovery icon on your desktop.
   - (Mac) Double-click the BlackArmor Discovery icon in your Applications folder.

   When BlackArmor Discovery opens, it automatically searches for all BlackArmor servers on your network and displays them in a list.
4. Select your new BlackArmor server.

   A list of shares on the server appears (Mac). Click **Manager Server**.
   - (Windows) Click **View Drive Details**. A list of shares on the server appears.
5. Use the up and down arrows to scroll through the list of shares and then do one or more of the following:
   - To access the server using BlackArmor Manager, click **Manage** and then enter your assigned user name and password. Contact your administrator if you do not have this information.
   - To view shares, select the share and then click **View**.

- To map a share, select the share you want, then click **Map**.
  - If prompted, log in using your BlackArmor user name and password. The share is mounted and its icon appears on your Desktop (Mac).
  - (Windows) Select a drive letter from the drop-down menu, then click **Yes**. The drive letter is assigned to the share. The share appears in Windows Explorer with that drive letter.
- If you have access to more than one share, continue to find and map additional shares as needed.

Note: You can mount/map as many public and private shares as you need to. However, to mount/map more than one *private* share, each private share must have the same log on credentials.

6. Save your files to shares that can be accessed by other people on your local network or over the Web.

Optional Steps

- *(Optional)* Create a full backup of your important files, or set up recurring backups, using BlackArmor Backup (see page 50).
- *(Optional)* If a USB printer has been connected to the BlackArmor server, add it to your list of available printers, following your computer's operating system instructions.
- *(Optional)* If your BlackArmor administrator has enabled the Media Service on the server and you have access to the share where the music files are stored, install iTunes on your computer and begin streaming music, following the iTunes instructions.
- *(Optional)* If your BlackArmor administrator has enabled Global Access on the server, sign up for a free Global Access account so you can access your BlackArmor server files over the Web. See "Creating a Seagate Global Access Account" on page 25.

Creating a Seagate Global Access Account

Seagate Global Access is a service that you can use to view, download, share, and work with the files stored on your BlackArmor server from anywhere in the world, share files stored on a private share, or share your files with anyone outside of your network.

To create a Seagate Global Access account:

1. Go to the Seagate Global Access Web site at *http://globalaccess.seagate.com*
2. The Seagate Global Access Sign In page opens. Click the link to begin.
3. On the Seagate Global Access Sign In page, enter your email address below **Don't have an account?** and then click **Send**.
4. The page refreshes to indicate that Seagate has sent you an email.

Global Access sends an invitation to join to the email address you entered; the email contains a link to a Web page where you can open a Global Access account. Follow the on-screen instructions to open the account and log in to Global Access.

Click the **Help** button on the Global Access Web site for instructions on using Seagate Global Access.

4. Getting the Most from Your BlackArmor® Server

- Introduction
- Your Role as a BlackArmor Administrator
- Your BlackArmor Server's Default Settings
- Managing BlackArmor Volumes, Shares and Storage
- Managing BlackArmor Users
- Protecting Your BlackArmor Files with Network Backups
- Setting up Aggregation Failover
- Setting Your BlackArmor Server as a Media Server
- Monitoring Your BlackArmor Server
- Changing the BlackArmor Server's Advanced Settings
- Maintaining Your BlackArmor Server

Introduction

This chapter describes the features of your BlackArmor® server and software, and provides tips to BlackArmor administrators using them.

Some of the features of the BlackArmor server are more suitable for administrators who consider themselves experienced or advanced computer users. Topics about those features are clearly marked.

Note: The topics in this chapter refer to tasks that only BlackArmor administrators can do. If you're not a BlackArmor administrator, skip to Chapter 5 "Tips for BlackArmor® Users" on page 47.

Your Role as a BlackArmor Administrator

BlackArmor administrators have full access to all features and settings on the BlackArmor server, and to all files stored on it.

Your role as a BlackArmor administrator is to:

- Manage the storage space available on your BlackArmor server by creating and modifying volumes and shares (see page 30).
- Control access to the server by creating and managing BlackArmor user accounts (see page 36).
- Keep your BlackArmor server running smoothly by monitoring the health of the server and its disk drives (see page 39).
- Keep your BlackArmor server running smoothly by updating its firmware when new versions become available (see page 44).

As a BlackArmor administrator, you can also take advantage of these features to get the most out of your BlackArmor server:

- Create group accounts to make it faster and easier to manage access to shares. User groups allow you to modify share access for individuals or entire groups from a single window (see page 36).
- Protect the files stored on your BlackArmor server by setting up recurring archive backups of the complete contents of the server (see page 37).
- Set up *link aggregation*, where you connect both LAN ports to your network at the same time in case one link fails (see page 38).
- Set up the BlackArmor server as a media server, so that BlackArmor users can stream music directly to a network computer or media player with iTunes installed (see page 38).
- Conserve energy—and lower your power bill—by setting the disk drives in your BlackArmor server to *spin down* (stop spinning) and enter a standby mode when they're not in use (see page 42).
- Connect your BlackArmor server to a UPS, which will provide enough power for you to save whatever files you're working on and properly power off the server in the event of a power failure (see page 43).
- *(Advanced)* Ensure that incoming network traffic reaches its destination by using BlackArmor Manager to set up Dynamic DNS (see page 42).

The remainder of this chapter describes your BlackArmor server's default settings, then describes how to change them and use other server features to build the data storage solution that fits your needs.

Your BlackArmor Server's Default Settings

Your BlackArmor server is preconfigured with settings that are appropriate for typical use, so that you can get started storing, sharing, and protecting your files right away:

- **User accounts**—The BlackArmor server includes one preconfigured user account for the administrator, which can be modified with a custom password during the initial setup (see page 18). You can also add as many new user accounts as you need using BlackArmor Manager (see page 36).
- **Shares**—The BlackArmor server includes two preconfigured shares: Download and Public. You can modify the features of each share to suit your needs, or add new public or private shares using BlackArmor Manager (see page 33).
- **RAID protection**—The BlackArmor server is preconfigured with RAID 5 protection when using four drives. RAID 5 stands for Redundant Array of Independent Disks level 5, and is a technology that builds redundancy into your storage system to help keep your data safe from disk drive failures and other catastrophes.

You can use a different level of RAID protection, if you want to. In addition to RAID 5, both RAID 1 and RAID 10 provide data protection. However, RAID 5 is highly recommended as it provides the best level of protection available on your BlackArmor server. Additionally, Seagate recommends that only users familiar and comfortable with RAID technology make changes to the server's RAID protection.

For more information, see page 31.

- **Network settings**—Although you do *not* have to connect both LAN ports to your network to use your BlackArmor server, the server will support two simultaneous LAN connections so that it can transfer data at a faster rate. For more information, see page 38.

The server is also preconfigured with DHCP as its network mode. DHCP is recommended. *DHCP* stands for Dynamic Host Configuration Protocol, and is basically a method of assigning IP addresses automatically to all the systems on a network. (Static mode requires that all IP addresses be assigned and changed manually.)

Unless you are part of a large corporation with an IT department, Seagate highly recommends using the DHCP network mode.

- **Administrator password**—The server's default login information is:

  user name: admin

  password: admin

You are prompted to change the administrator password during the initial server setup. If you didn't, or want to change it again, open BlackArmor Manager (see page 17). You can change the administrator password by selecting **Admin Password** from the System menu. For step-by-step instructions for updating the password, refer to the BlackArmor Manager online Help.

You may need to use the default user name and password again in the future, if the server is ever reset to its initial configuration.

- **Global Access setting**—The BlackArmor server is not preconfigured to be accessed over the Web. Enable Seagate Global Access if you want to be able to access the files on your BlackArmor server from anywhere in the world, or share your files with anyone outside of your network, like business clients or friends (see page 21).
- **Downloader settings**—The BlackArmor server is preconfigured to allow large Web file downloads at any time, using the BlackArmor Manager Downloader tool. You can limit the size and number of simultaneous Web downloads and limit Web downloads to specific days and times using BlackArmor Manager (see page 35).
- **Media Server settings**—The BlackArmor server is not preconfigured as a media server. You can use BlackArmor Manager to turn the server into a media server for sharing of digital photos, videos and music with people on your local network, as well as enable the iTunes service so that BlackArmor users can stream music directly to a network computer with iTunes installed (see page 22).

Managing BlackArmor Volumes, Shares and Storage

This section discusses:

- Understanding Volumes and Shares
- Working with Volumes
- Working with Shares
- Setting Storage Space Limits for BlackArmor Users
- Setting Grace Time for Exceeded Quotas
- Controlling Web File Downloads to the BlackArmor Server

Understanding Volumes and Shares

By default, your BlackArmor server is configured with one volume and two shares: Download and Public. A *volume* is storage space that can be made up of one or more disk drives, or of only part of a single disk drive. A *share* is a folder. Shares are created within volumes.

The default volume and shares are appropriate for typical use, so that you can get started storing, sharing, and protecting your files right away. However, as a BlackArmor administrator, you can also use BlackArmor Manager to create more volumes and shares on your BlackArmor server if you want to divide the total storage space into smaller amounts that you can allocate for different uses.

For instance, you could create three volumes to hold different types of information:

- Volume A: Business Files
- Volume B: Backup File Storage

- Volume C: Media Files

You could then create one or more folders (shares) in each volume to suit your needs:

- Volume A: Business Files
  - Share 1: Client Files
  - Share 2: Financial Files
  - Share 3: Human Resources Files
- Volume B: Backup File Storage
  - Share 1: Daily Backups
  - Share 2: Month-end Backups
- Volume C: Media Files
  - Share 1: Music Files
  - Share 2: Photo Files
  - Share 3: Video Files

Working with Volumes

By default, the available storage space in your BlackArmor server is configured into one volume that's protected by RAID 5.

Understanding RAID

RAID stands for Redundant Array of Independent Disks and is a technology that builds redundancy into your storage system to help keep your data safe from disk drive failures and other catastrophes.

RAID comes in many levels, which vary according to the amount of protection they provide (and how they provide it), and the number of disk drives they support.

By default, your BlackArmor server is preconfigured with RAID 5, which not only stores your data safely but also builds in redundant information called *parity*, which is data that's used to reconstruct your files if one of the disk drives in the server fails.

You can choose to use a different level of RAID protection for your volumes—your BlackArmor server supports RAID levels 0, 1, 5, 10, and JBOD (which stands for Just a Bunch of Disks). However, RAID 5 is highly recommended as it provides the best level of protection available on your BlackArmor server.

This table explains the different levels of RAID supported by your BlackArmor server.

Table 1: Supported RAID Levels for Volumes

RAID Level of Volume	Number of Disk Drives Required	Description
RAID 0 (Also known as striping)	2 – 4	A volume where data is distributed evenly (striped) across the disk drives in equal-sized sections. A striped volume does not maintain redundant data, and so *offers no data protection*.
RAID 1 (Also known as mirroring)	2	A volume where one disk drive is a mirror of the other (the same data is stored on each disk drive). Provides data protection.
RAID 5	3 – 4	A volume with RAID 5 uses data striping and parity data to provide redundancy. (Parity is extra information that's used to re-create data if a disk drive fails. In volumes with RAID 5, parity data is striped evenly across the disk drives with the stored data.)
RAID 10	4	A volume with RAID 10 is built from two or more equal-sized RAID 0 volumes. Data in a volume with RAID 10 is both striped and mirrored.
Span (Also known as a JBOD[a])	1 – 4	A group of disk drives in a server, *not protected by RAID*.

a.'Just a Bunch of Disks'.

Seagate recommends that only users familiar and comfortable with RAID technology make changes to the server's RAID protection.

Creating New Volumes

As a BlackArmor administrator, you can create all the shares you want in the default volume, or you can create more volumes using BlackArmor Manager. When you create a volume, you can specify:

- The size of the volume
- The disk drive(s) you want to use
- The level of RAID protection it should have (see page 31)

You can use the same disk drives in multiple volumes providing there is available space on those drives. For instance, you could use half the space on disk drives 1, 2, and 3 to create Volume A, and the other half of the space on the same disk drives to create Volume B.

To create a new volume, open BlackArmor Manager (see page 17). Volumes are in the Storage menu. For more information on volumes, including deleting and modifying volumes, see the online Help.

Working with Shares

Shares on the BlackArmor server can be either public (open to everyone, with some restrictions) or private (restricted to selected user accounts).

As a BlackArmor administrator, you can create, modify, or delete shares at any time, as required. However, when you delete a share, you lose all the files stored in that share. Use caution when deleting shares from your BlackArmor server.

Private Shares

A private share is associated with one user account, and only BlackArmor users with permission can access that share. Private shares are password protected. (As a BlackArmor administrator, you can turn a private share into a public share by modifying the share's settings in BlackArmor Manager.)

You can limit share access by:

- Granting access to specified BlackArmor users only.
- Limiting some BlackArmor users to read-only access. *Read-only* access means that a BlackArmor user can view files on the share, but can't edit those files or upload files to the share.
- Granting any BlackArmor user full access to the share, which allows the user to save and back up files to the share, edit files on the share, and download any files from the share to a computer or to a USB drive connected to the server (see page 50).

The owner of the share can also grant other people access to some or all of the files on the share by using Global Access. See page 25.

Note: To mount/map more than one *private* share at a time, each private share must have the same log on credentials.

Private shares are created as part of a BlackArmor user's account. To create a private share, open BlackArmor Manager (see page 17). User accounts are in the Access menu.

To modify a share's permission settings, open BlackArmor Manager (see page 17). Share permissions are in the Access menu.

For step-by-step instructions for using BlackArmor Manager, refer to the online Help.

Public Shares

Public shares are not restricted, and BlackArmor users can mount/map as many public shares as they need to.

To create a public share, open BlackArmor Manager (see page 17). Shares are in the Storage menu. For step-by-step instructions for using BlackArmor Manager, refer to the online Help.

Special Features of Shares

These features are available on any share. You can enable or disable them, as required for the purpose of the share:

- **File Protocol Support**—Files are shared between computers on a network using standard file protocols. You can set a share to support any or all of these protocols:
  - **CIFS (**Common Internet File System)—Lets people with different computers running Windows operating systems share files without having to install special software.
  - **FTP** (File Transfer Protocol)—Provides secure file sharing over the Internet between your BlackArmor server and other computers.
  - **NFS** (Network File System)—Provides file sharing with computers running Linux or UNIX operating systems, or computers running NFS client software.
- **Recycle Bin Service**—You can protect the files on a share by enabling the BlackArmor Manager Recycle Bin. When the Recycle Bin is enabled on a share, BlackArmor Manager saves files deleted from the share so that they may be retrieved if you need them back.
- **Drag&Sort Service**—You can set a share to automatically download media files to a specific location on BlackArmor users' computers, based on the type of files being downloaded. For instance, downloaded music files would automatically be placed in a folder called Music.

To enable or disable any of these special features, open BlackArmor Manager (see page 17). Shares are in the Storage menu. For step-by-step instructions for using BlackArmor Manager, refer to the online Help.

Setting Storage Space Limits for BlackArmor Users

By default, your BlackArmor server imposes no limits on a user's storage space (except for the volume size set up for the user).

However, as a BlackArmor administrator, you can set storage space limits on any user account or share. You can also set different limits for each user account, for each share that a user has access to, or set limits on some user accounts but not on others.

If a BlackArmor user fills allocated storage space, older or unneeded files must be removed by a BlackArmor administrator to make room for additional files.

To set storage space limits for BlackArmor users, open BlackArmor Manager (see page 17). Storage space limits are set per Volume on the Quota page, which is in the Storage menu. For step-by-step instructions for using BlackArmor Manager, refer to the online Help.

Setting Grace Time for Exceeded Quotas

As a BlackArmor administrator, you can set a grace time limit, which allows a quota to exceed its storage limitations for a period of time. If the quota is reached, you can temporarily allow an additional 100 megabytes (MB) of storage space to be used. You might do this to ensure users have time to identify what files to keep or to preserve usable storage space.

Once the grace date is reached, no additional files can be added until space is made available.

To set the grace time for stored files, open BlackArmor Manager (see page 17). The grace time limit is set on the Quota page, which is in the Storage menu. See the BlackArmor Manager online Help for more information.

Controlling Web File Downloads to the BlackArmor Server

BlackArmor Manager includes a special tool for downloading large files directly to the server from FTP and other sites on the Web. This tool is called the Downloader, and it allows BlackArmor administrators to manage when large Web downloads take place so that the server isn't overwhelmed.

The Downloader places Web download jobs in a queue, and jobs take place automatically in the order in which they appear in the queue. If a job isn't first in line, it won't start right away. As a BlackArmor administrator, you can adjust the queue to re-prioritize download jobs.

You can also impose limits on when Web download jobs can take place and how many can take place simultaneously (never more than three). You can limit Web downloads to evenings, weekends, or other slow times in the week.

Consider how much bandwidth your BlackArmor server has and how much of it you want consumed by lengthy downloads, then set limits to prevent multiple large files from being downloaded simultaneously or during peak times when your BlackArmor server is busy with other tasks.

To adjust the Downloader settings for your BlackArmor server, or to check the Downloader queue and re-prioritize existing jobs, open BlackArmor Manager (see page 17). Downloader Management is in the Storage menu. For step-by-step instructions for using BlackArmor Manager, refer to the online Help.

Managing BlackArmor Users

This section describes the features of a user account and provides an overview of how to set up new accounts using BlackArmor Manager. For step-by-step instructions for using BlackArmor Manager, refer to the online Help.

Working with User Accounts

Everyone who will be using your BlackArmor server needs a unique user account. However, a user account is not required if a folder is made public for access by others. As a BlackArmor administrator, you can customize each user account as required to suit the needs of that BlackArmor user. (See “Creating User Accounts” on page 19 for more information.)

You can:

- Give a user BlackArmor administrator privileges
- Add the user to a group account (see the next section)
- Create a private share for the user

After a user account has been created, it can be modified or deleted at any time.

To create, modify, or delete a user account, open BlackArmor Manager (see page 17). User accounts are in the Access menu. For step-by-step instructions for using BlackArmor Manager, refer to the online Help.

Creating and Modifying User Groups

You can make it faster and easier to manage share access by sorting BlackArmor users into groups. Group accounts make it faster and easier to assign access to shares by allowing you to set access levels for individuals or entire user groups from a single screen.

Create user groups in BlackArmor Manager by creating the group account and adding users to it. Assign BlackArmor users to groups based on common access needs.

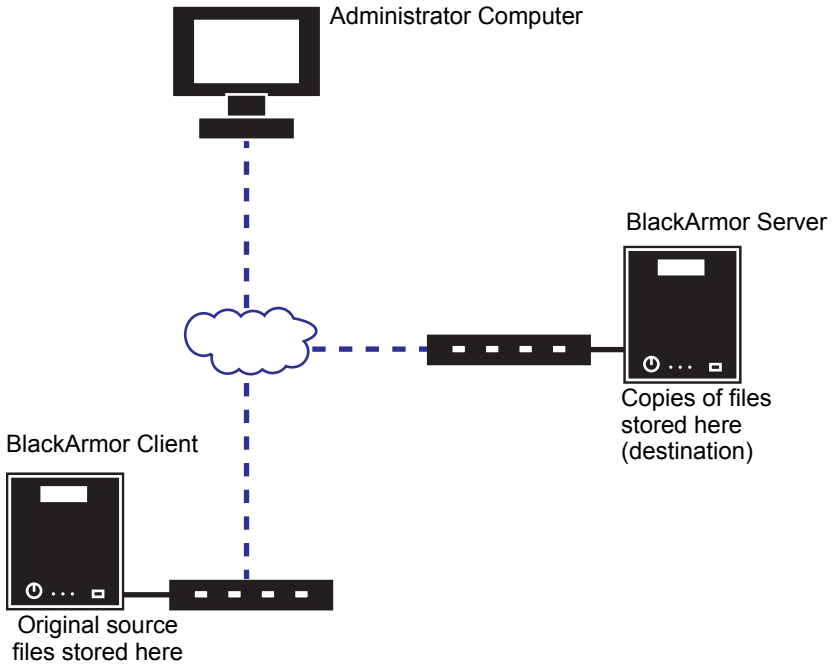
When you are modifying access permissions for the shares on your BlackArmor server, you can assign a group to a selected access level instead of assigning each individual separately.

To create, modify, or delete a user group, open BlackArmor Manager (see page 17). Groups are in the Access menu. For step-by-step instructions for using BlackArmor Manager, refer to the online Help.

Protecting Your BlackArmor Files with Network Backups

Your BlackArmor server has two LAN ports, one of which must be used to connect the server to your local network (port 1 by default). The server's two LAN ports can be configured for *link aggregation*, which means you can connect both LAN ports to your network at the same time for failover protection: the other link (port) takes over if one link fails. See page 38.

Or, you can set up NAS to NAS backup, where a permanent link is created between your BlackArmor server and another server on your network, and automatic and continuous backups of your BlackArmor server take place. These continuous backups provide the best protection against data or device loss, especially if the second server is located in a different building or part of the city (or country) than your BlackArmor server.



Use BlackArmor Manager to set up the network connection between the two servers—the BlackArmor Client (where your BlackArmor users' files are stored) and the BlackArmor Server (where the copies, or replicas, of the files are stored)—and begin the initial backup. You can then use BlackArmor Manager to schedule recurring backups.

To back up from your BlackArmor® server to another server on your network, you first need to enable the Backup Service.

1. Open BlackArmor Manager (see page 19).
2. In the menu bar, select **Storage**, then click **Backup Manager**.
3. In the **Storage** menu on the left side of the window, click **Server Setting**.
4. Click the check box beside **Backup Service**.

The authentication information displays. This information is used when restoring backed up files.

5. Enter an authentication name and password for all aliases.
6. Select the storage volume.
7. Enter an alias name, then click **Add new alias**.
8. Click **Submit**.

The settings are saved.

9. See the BlackArmor Manager online help for more information about the types of backup tasks you can set up.

Setting up Aggregation Failover

The server's two LAN ports can be configured for *link aggregation*, which means you can connect both LAN ports to your network at the same time for failover protection: the other link (port) takes over if one link fails. See page 38.

To set up link aggregation, connect both of your BlackArmor server's LAN ports to the network switch or router, using two Ethernet cables. Then, open BlackArmor Manager (see page 17) and select **Aggregation** as the LAN setting. LAN settings are in the Network menu. For step-by-step instructions for using BlackArmor Manager, refer to the online Help.

Setting Your BlackArmor Server as a Media Server

You can store photos, videos, and music on your BlackArmor server so that they can be accessed by anyone.

You can use BlackArmor Manager to turn the server into a media server, and set it to download media files into default folders automatically. For instance, if a user was downloading music files, they would download into the user's Music folder automatically.

You can also turn your BlackArmor server into an iTunes server so that a BlackArmor user can stream music directly to a network computer with iTunes installed, or to an iPod connected to a network computer.

To set up your BlackArmor server as a media server, open BlackArmor Manager (see page 17) and go to the Media menu. For step-by-step instructions for using BlackArmor Manager, refer to the online Help.

Monitoring Your BlackArmor Server

BlackArmor Manager and the BlackArmor server itself provide many ways to monitor the server's activity and status:

- Monitoring Status with the Server's LCD Screen
- Monitoring Status with the Server's LEDs
- Using Email Alerts to Monitor Server Status
- Checking Disk Drive Status Using SMART

Monitoring Status with the Server's LCD Screen

Your BlackArmor server has an LCD screen on the front that displays current server setting and status information.

Use the LCD screen navigation buttons beside the screen to scroll up and down through the information. Press and hold the button for the selected information to view more detail.

When an "event" occurs on the server—for instance, if you change a setting on the server, or if an error (such as the loss of a network connection or the failure of a disk drive) occurs—basic details about the event appear on the LCD screen. If an error has occurred, details about the error remain on the screen until the problem has been fixed.

Monitoring Status with the Server's LEDs

Your BlackArmor server has eight LEDs to help you monitor the status of its components. (See the illustration on page 10 for help locating the LEDs.)

Table 2: Front and Rear Panel LEDs

LED	State and Color	Indication
Power	Solid Blue	Server is powered on
	Off	Server is powered off
System Status	Solid Blue	Server is ready for use
	Solid Amber	Server has a system error
LAN Port 1	Off	Port has no network connection
	Solid Blue	Port has network connection
	Blinking Blue	Network connection is busy
LAN Port 2	Off	Port has no network connection
	Solid Blue	Port has network connection
	Blinking Blue	Network connection is busy

Table 2: Front and Rear Panel LEDs

LED	State and Color	Indication
Disk Drive 1	Solid Blue	Disk drive is installed and operating properly
	Solid Amber	Disk drive has been removed or has failed
Disk Drive 2	Solid Blue	Disk drive is installed and operating properly
	Solid Amber	Disk drive has been removed or has failed
Disk Drive 3	Solid Blue	Disk drive is installed and operating properly
	Solid Amber	Disk drive has been removed or has failed
Disk Drive 4	Solid Blue	Disk drive is installed and operating properly
	Solid Amber	Disk drive has been removed or has failed

Using the LEDs to Monitor the Server

1. The System Status LED will indicate when there's a problem. When it's blue, the server and its components are working properly.

If the System Status LED turns amber, a problem has occurred.

2. Check the LAN port LEDs on the back of the server and the disk drive LEDs behind the door to locate the source of the problem.
3. If one or both LAN port LEDs have gone off, you may have lost your network connection. If a disk drive LED is amber in color, that disk drive may have failed (or been removed).

See Chapter 6 "Solving Problems" on page 53 for help solving the problem.

Using Email Alerts to Monitor Server Status

Note: Only BlackArmor administrators can set up email alerts.

You can use BlackArmor Manager to notify you by email when the status of the server changes or when a server setting is modified. You can set BlackArmor Manager to send email alerts to up to five people. You must have a Seagate Global Access account to receive email messages.

To set up email alerts, open BlackArmor Manager (see page 17). Email alerts are in the System menu. For step-by-step instructions for using BlackArmor Manager, refer to the online Help.

Checking Disk Drive Status Using SMART

Note: Only BlackArmor administrators can complete a SMART diagnosis.

You can use BlackArmor Manager to perform SMART diagnoses on the server's disk drives.

SMART stands for Self-Monitoring Analysis and Reporting Technology, a technology built into disk drives that let them automatically monitor their own health and report on possible problems.

Running a SMART diagnosis on the server's disk drives on a regular basis can help prevent disk drive failure by catching potential problems early. Because only disk drives that support SMART can be tested with BlackArmor Manager, ensure that you always use SMART disk drives in the server.

To run a SMART diagnosis, open BlackArmor Manager (see page 17). SMART tests are in the System menu. For step-by-step instructions for using BlackArmor Manager, refer to the online Help.

Changing the BlackArmor Server's Advanced Settings

This section describes some of the server settings that you may want to modify to meet your current needs.

Note: Where noted, only people comfortable with advanced technology concepts should attempt to modify the server.

This section discusses:

- Dynamic Domain Name System (DNS) Settings
- File Protocol Settings
- Network Time Protocol (NTP) Settings
- Power Saving Settings
- Secure Socket Layer (SSL) Settings
- Uninterruptible Power Supply (UPS) Settings
- Web Access Protocol Settings
- Workgroup and Domain Settings

Dynamic Domain Name System (DNS) Settings

Note: Only people familiar with Dynamic DNS should try changing these settings.

Dynamic DNS is a way of maintaining the link between an unchanging domain name (like www.seagate.com) and the constantly changing IP address of a computer that uses DHCP instead of a static IP address. A DDNS service keeps track of changing IP addresses and forwards all network traffic for your domain name to whatever the current IP address is.

You can set up Dynamic DNS for your BlackArmor server using BlackArmor Manager. You must select one of the DNS service providers, then set a domain name for the server in BlackArmor Manager. See the Web site of the DNS service provider you choose for more information.

To set up DDNS, open BlackArmor Manager (see page 17). Dynamic DNS is in the Network menu. For step-by-step instructions for using BlackArmor Manager, refer to the online Help.

File Protocol Settings

Files are shared between computers on a network using standard file service rules. See "Special Features of Shares" on page 34 for information about the supported protocols.

Network Time Protocol (NTP) Settings

An NTP time server synchronizes the date and time on your BlackArmor server. NTP runs continually and adjusts the time on your BlackArmor server based on the NTP time server clock.

You can enable NTP service on your BlackArmor server by entering the Fully Qualified Domain Name (FQDN) or IP address of your NTP time server. To set up the NTP service, open BlackArmor Manager and then select **General Setup** from the System menu. See the online Help for more information.

Power Saving Settings

By default, the disk drives in your BlackArmor server spin constantly whenever the server is powered on; however, there are times, like evenings, weekends, and holidays, when your server may not be in use.

You can use the BlackArmor Manager Power Save feature to conserve energy—and lower your power bill—by setting the disk drives to *spin down* (stop spinning) and enter a standby mode when they're not in use. Enable power save from the System menu's **Advanced** page.

Secure Socket Layer (SSL) Settings

Note: Only people familiar with SSL should try adding SSL support to the BlackArmor server.

SSL (also known as Transport Layer Security) is a type of encryption used to protect data being sent over a network or the Internet. SSL uses a system of keys, like secret passwords, to send and receive files securely. See "Web Access Protocol Settings" on page 43 for more information.

You add SSL support to your BlackArmor server by entering an SSL certificate and key pair.

Uninterruptible Power Supply (UPS) Settings

An uninterruptible power supply is a power supply that has a battery in it that maintains power to a computer or server in the event of a power failure.

A UPS is intended to provide enough power for you to save whatever files you're working on and properly power off the computer or server; it's not meant to keep any system running for the duration of a power failure.

You can connect your BlackArmor server to a UPS and customize the UPS settings in BlackArmor Manager. You can specify when you want the UPS to power off the BlackArmor server if you are not present at the time. You can choose to have the server shut down when:

- The battery life of the UPS reaches 15% of full power or the battery has five minutes of life left, or less.

Or,

- A specified amount of time has passed since the power failure began. (You can specify the amount of time.)

Web Access Protocol Settings

By default, your BlackArmor server is set to the HTTP Web access protocol. HTTP stands for Hypertext Transfer Protocol and is the most common way that data and files are stored on the Internet.

You can set your BlackArmor server to use HTTPS (HTTP over Secure Socket Layer) if you have set SSL on the server. (See "Secure Socket Layer (SSL) Settings" on page 42.)

Workgroup and Domain Settings

By default, your BlackArmor server is set as a *workgroup*. A workgroup is a number of computers on a network that share resources. You can add any computer to the server's workgroup, or you can add the server to an existing workgroup.

Alternatively, you can set your BlackArmor server as a *domain* member. A domain is a group of computers administered as a single unit from a central location.

When you add the BlackArmor server as a domain member, it is centrally managed by a Windows domain controller, which provides another level of security when users attempt to access the server. Users within the domain receive their own unique accounts and must be authenticated to receive access.

The domain's administrator must authorize the BlackArmor server as a domain member. You must know the domain administrator's user name and password to add your server to a domain. See the BlackArmor Manager online help for instructions on adding the server as a domain member.

Maintaining Your BlackArmor Server

This section explains the basic things you may need to do to properly maintain your BlackArmor.

This section discusses:

Basic Hardware Safety and Maintenance

Follow these guidelines to keep your BlackArmor server operating properly. Failure to do so may result in slower performance or loss of data.

- Always shut down and restart the server using BlackArmor Manager (for instructions, refer to the BlackArmor Manager online Help) or by pressing the POWER button on the front. Don't just unplug it or shut it down from a power bar.
- Keep the server on a flat, level, stable horizontal surface. Keep it cool, keep it dry, and don't put anything on it or beside it that might block its vents and allow it to overheat.
- Clean the outside surfaces of the server with a damp cloth only (don't use cleansers of any kind), and unplug the server before you clean it to avoid possible electric shock.
- Don't try to open or remove the outer case that houses the server. It is okay to remove and replace disk drives, but don't try to do any other hardware maintenance yourself.
- Never remove more than one drive at a time. Failure to do so will result in data loss.
- Call for professional service if:
  - The server's power cord becomes damaged.
  - The server has liquid spilled onto it or is exposed to water.
  - The server has been dropped or if the outer case becomes damaged.
  - The server doesn't operate normally even though you're following all the operating instructions properly.

Keeping the Server's Firmware Current

Note: Only a BlackArmor administrator can update the server's firmware.

You should update your server's *firmware* (essentially, software that's built into the server) as new versions become available, to ensure that you have the most up-to-date features and functionality. You can find the new versions of BlackArmor firmware on the Seagate Web site at www.seagate.com.

You can choose between two update methods in BlackArmor Manager:

- **Automatic firmware updates**—BlackArmor Manager downloads new firmware versions, completes the update process, and restarts the server. You can start the update immediately or schedule the update for a more convenient time.

You can also set BlackArmor Manager to check regularly for new versions of the firmware, and either let you know when a new version is available or install the update automatically.

- **Manual firmware updates**—You must check the Seagate Web site at www.seagate.com for new firmware versions, download the firmware files, and start the update yourself.

Seagate recommends using automatic updates to ensure that your server is always running the latest, strongest version of the BlackArmor firmware.

Resetting Your BlackArmor Server

Follow these steps to reset the BlackArmor server's name, DHCP setting (network mode) and log in password.

Note: You will need a paperclip or other narrow device to perform this task.

1. Carefully access the back of the server.
2. Ensure that the server is powered on and connected to the LAN.
3. On the back of the server, find a single small opening. The reset button is inside the opening.
4. Insert the end of the paperclip into the opening, then press and hold the reset button. *Do not* release the button yet.
5. Hold the reset button until the disk drive LEDs on the front of the server light up, then turn amber (yellow). This takes several seconds.
6. Release the reset button.

The server reboots itself. Once the server has restarted and the LAN and disk drive LEDs are lit up, the reset is complete. The server is renamed to "BA-*MAC address*", where *MAC address* is the last six characters of the server's MAC address.

5. Tips for BlackArmor® Users

Introduction

This chapter provides tips and information that will help BlackArmor® users get the most out of the BlackArmor server.

BlackArmor users can:

- Store their files on the BlackArmor server and share them with others.
- Back up their files, applications, and even operating systems using BlackArmor Backup.
- Access their BlackArmor files over the Web using Global Access (if enabled).
- Download large Web files directly to the BlackArmor server using the BlackArmor Manager Downloader.
- Retrieve accidentally deleted files from the BlackArmor Manager Recycle Bin (if enabled).

Understanding Your BlackArmor User Account

This section describes the features and possible limitations of your BlackArmor user account.

Access Limitations

Shares on the BlackArmor server can be either public (open to everyone, with some restrictions) or private (restricted to selected user accounts).

See your BlackArmor administrator to find out what your access limitations are.

Private Shares

Private shares are password protected and restricted to use by people designated by your BlackArmor administrator.

Once the BlackArmor administrator creates a user account, you can limit access to a private share by:

- Limiting access to this share to specified BlackArmor users only.
- Limiting some BlackArmor users to read-only access. *Read-only* access means that you can view files on the share, but can't edit those files or upload your own files to the share.

You have full access to your private share, which allows you to save and back up your files to the share, edit files on the share, and download any files from the share to your computer or to a USB drive connected to the server (see page 50).

You can grant other people access to some or all of the files on your private share locally, or remotely, by using Global Access. See page 25 for more information and for instructions on setting up a Global Access account. Refer to the Global Access user documentation for help granting other people access to your private share.

Note: To mount/map more than one *private* share at a time, each private share must have the same log on credentials.

Public Shares

Public shares are not restricted, and you can mount/map as many public shares as you need to.

Storage Space Limitations

Your BlackArmor administrator can limit the amount of storage space you're allowed to use on a specific share.

You may have space limitations on one share but not on another; you may have more space to use on one share and less on another. Or, you may have no space limitations at all—except for the maximum storage space on the BlackArmor server itself.

See your BlackArmor administrator to find out if you have any storage space limitations, and what those limitations are.

If you fill your allocated storage space, either remove older or unneeded files to make more room, or see your BlackArmor administrator to have more storage space assigned to you.

Automatic Sorting for Media Files

Shares on your BlackArmor server may be set to automatically sort media files to a specific location on your computer, based on the type of files. For instance, when you download music files, they would automatically be placed in a folder called Our Music.

See your BlackArmor administrator to find out if the shares you can access have automatic download sorting (referred to in BlackArmor Manager as "Drag & Sort") enabled.

Grace Time Limits for Quotas

If there is a storage quota for your account, your BlackArmor administrator can set a grace time limit, which allows a quota to exceed its storage limitations for a period of time. Once the grace date is reached, no additional files can be added until space is made available.

See your BlackArmor administrator to find out if the server has any grace time limits for stored files.

File Protocol Support on Shares

Files are accessed by computers on a network using standard file protocols. See <Section Reference>Special Features of Shares for information about the supported protocols.

Accessing Shares and Files on the BlackArmor Server

After you have connected to the BlackArmor server, and mounted/mapped the shares you can access, you can immediately begin saving files to the server.

Note: You can mount/map as many public and private shares as you need to. However, to mount/map more than one *private* share, each private share must have the same log on credentials.

You can access the shares on your BlackArmor server:

- Locally, the way you would access any network drive on your computer (for instance, using Windows Explorer). See page 24 for help mounting/mapping shares to your computer.
- Remotely, over the Web, using Seagate Global Access (if your BlackArmor administrator has enabled Global Access on the BlackArmor server). For more information about Global Access, see page 25.

Once you have successfully accessed a share, you can view and download files from the share, and upload and back up files to that share, if you have permission (see page 47).

See your BlackArmor administrator for help getting access to the shares you need and understanding your viewing, downloading, and uploading permissions.

Backing Up Your Files

To protect your important files from loss, corruption, or accidental deletion, you should complete and maintain regular file backups using BlackArmor Backup.

You can also back up files by downloading them from your BlackArmor server to an external USB drive, or uploading them from a USB drive to the server.

Backing Up Files with BlackArmor Backup

BlackArmor Backup is a full backup software application with a wide range of features that let you customize a backup system to suit your needs.

You can use BlackArmor Backup to start a backup whenever you want. You can also use BlackArmor Backup to set up recurring backups that can take place at convenient times (for instance, overnight or on the weekends, when you aren't using your computer).

You can use BlackArmor Backup to protect all the files, applications, and even the operating system on your computer.

If you haven't already installed BlackArmor Backup, see page 24 for instructions.

For more information, refer to the *BlackArmor Backup User Guide* or online Help.

Backing Up Files Between Servers

Note: This task can be done by an administrator only.

You can use BlackArmor Manager to back up to and from your BlackArmor server and another backup server on your network. To complete a backup to another server, you will need the server's IP address and log in credentials.

The Backup Manager is in the BlackArmor Manager's Storage menu. For step-by-step instructions for backing up files between servers, refer to the BlackArmor Manager online Help.

Backing Up To or From an External USB Drive

Note: This task can be done by an administrator only.

You can use BlackArmor Manager to immediately back up your files (or schedule backups) *from* an external USB drive *to* the BlackArmor server, or *from* your BlackArmor server to an external USB drive.

To begin a backup to or from an external USB drive, insert the drive into an available USB port on the BlackArmor server (see page 11 for help locating the server's USB ports), then open BlackArmor Manager (see page 17). The Backup Manager is in the Storage menu.

For step-by-step instructions for backing up your files, refer to the BlackArmor Manager online Help.

Accessing Your BlackArmor Files Over the Web

If your BlackArmor administrator has enabled Global Access on the server, sign up for a free Global Access account so you can access your BlackArmor server files over the Web.

Seagate Global Access is a service that you can use to view, download, and work with the files stored on your BlackArmor server from anywhere in the world, share files stored on a private share, or share your files with anyone outside of your network.

With Global Access, you can:

- Download important business files or presentations from a client's office anywhere in the world.
- Share files with clients without requiring them to use an FTP application.
- Upload important files from your laptop so that you know they're safe while you continue to travel.
- Grant other people access to files on your private share.

To access your BlackArmor server over the Web:

- Ensure that Global Access is enabled on the BlackArmor server. See your BlackArmor administrator to find out more.
- Create a Global Access account. Anyone who wants to access the BlackArmor server over the Web must have their own Global Access account. (Accounts are free.)

See page 25 for instructions on setting up a Global Access account. Refer to the Global Access user documentation for help granting other people access to your private share.

Downloading Large Web Files to Your BlackArmor Server

BlackArmor Manager includes a special tool for downloading large files directly to the server from FTP and other sites on the Web. This tool is called the **Downloader**, and it allows your BlackArmor administrator to manage when large Web downloads take place so that the server isn't overwhelmed.

Downloader jobs may not begin immediately. Web downloads take place automatically in the order in which they appear in the Downloader queue (which can be adjusted by your BlackArmor administrator), so if your job isn't first in line, it won't start right away.

Additionally, your BlackArmor administrator can also impose limits on when Web download jobs can take place and how many can take place simultaneously (never more than three). BlackArmor administrators can limit Web downloads to evenings, weekends, or other quiet times in the week.

See your BlackArmor administrator to find out when you can download Web files using the Downloader, or to have your existing download job moved up in the Downloader queue.

Retrieving Deleted Files from the Recycle Bin

Shares on your BlackArmor server may be protected by the BlackArmor Manager Recycle Bin. When the Recycle Bin is enabled on a share, BlackArmor Manager saves files deleted from the share so that they may be retrieved if you need them back.

If you accidentally delete a file, open BlackArmor Manager (see page 17) and then click **Recycle Bin**. For step-by-step instructions for retrieving deleted files, refer to the BlackArmor Manager online Help.

6. Solving Problems

This chapter provides solutions to the most common problems you may encounter while setting up and using your BlackArmor® server:

- General Troubleshooting Tips
- Common Problems and Solutions
- Removing and Replacing a Disk Drive

General Troubleshooting Tips

If you have problems setting up or using your BlackArmor server, follow these suggestions:

- Ensure that the server is properly connected to your local network. Check that the Ethernet cable(s) are connected and functioning properly.
- Ensure that your network is functioning properly.
- Ensure that the server is properly connected to a power source and turned on. Check that all disk drives are functioning properly.
- Ensure that your computer meets the BlackArmor system requirements. See “System Requirements” on page 8 for more information.
- Ensure that your computer is running a supported Web browser. See “System Requirements” on page 8 for a list of supported browsers.
- Ensure that you are logging in with the correct administrator user name and password. (Remember that passwords are case-sensitive.)

Common Problems and Solutions

This section provides solutions to common problems that may occur in BlackArmor Manager.

I can’t connect to the server over the local network.

Check that the server is powered on and connected to the network. Ensure that you have used LAN Port 1 to connect the server to the network.

Check that the server is powered on and connected to the network.

Try connecting to the server from a different computer.

Try using a different Ethernet cable.

I can’t connect to the server over the Web.

Check that the server has Global Access enabled. See “Making BlackArmor Accessible Using Seagate Global Access” on page 22.

Enable Email Setup in BlackArmor Manager and then send a test email.

I can’t open BlackArmor Manager.

Check that the server is powered on and connected to the network. Run BlackArmor Discovery and try to reconnect with the server, then launch BlackArmor Manager.

I can’t log in to BlackArmor Manager.

Ensure that you are using a valid user name and password. Remember that user names and passwords are case-sensitive.

I can’t access a share.

Ensure that you have access to that share.

Ensure that you are using a valid user name and password. Remember that user names and passwords are case-sensitive.

The volume that contains the share may be degraded because of a disk drive error or failure. Check the status of your server’s disk drives; see “Monitoring Status with the Server’s LEDs” on page 39 for more information.

I can’t access a file on a share.

Ensure that you are allowed access to that file.

The volume that contains the share may be degraded because of a disk drive error or failure. Check the status of your server’s disk drives; see “Monitoring Status with the Server’s LEDs” on page 39 for more information.

I can’t store any more files on a share because its volume is full.

If you are a user, see your BlackArmor administrator.

If you are an administrator, consider removing some of the files currently stored on the server.

A firmware upgrade failed.

Try to upgrade the firmware manually. For further assistance, contact Seagate Support at www.seagate.com/support

I can’t get streaming music from the BlackArmor server.

Ensure that you have iTunes installed on your computer. Ensure that you are using a computer that’s connected to the local network. Ensure that you have access to the share where music files are stored.

A volume is in degraded mode.

A disk drive may have failed. For further assistance, contact Seagate Support at www.seagate.com/support

Removing and Replacing a Disk Drive

Follow these steps to replace a hard drive in the BlackArmor® NAS 440/420 server. You may also use these instructions to replace a damaged hard drive carrier.

Note: Only Seagate hard drives can be used for replacement. Failure to use Seagate replacement parts can and will forfeit the warranty period of the BlackArmor NAS 440/420.

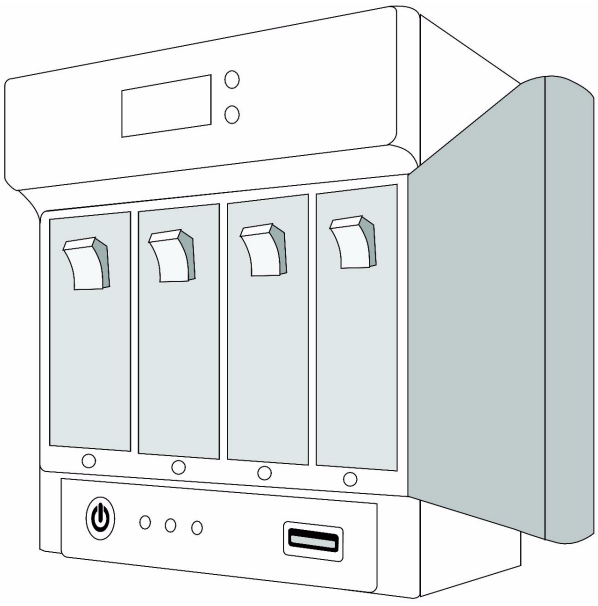
WARNING: ESD Precautions

Electrostatic discharge (ESD) can damage the processor, hard drives, main board, memory modules (RAM), and other BlackArmor components. Always observe the following precautions before replacing a hard drive:

- Do not remove a component from its protective packaging until you are ready to install it.
- Do not touch the component pins, leads, or circuitry.
- Wear a wrist grounding strap and attach it to a metal part of the system before handling components. If a wrist strap is not available, maintain contact with the system throughout any procedure requiring ESD protection.
- Keep the work area free of nonconductive materials, such as ordinary plastic assembly aids and foam packing.

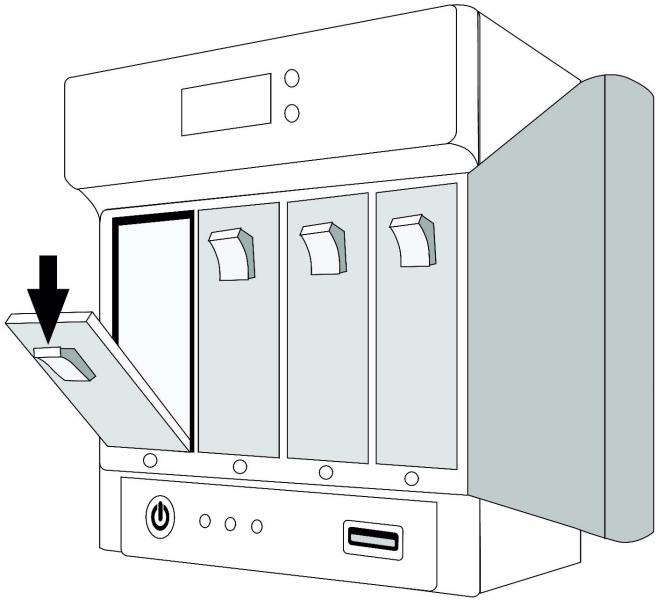
Removing a Hard Drive

1. Open the BlackArmor Manager Web interface.
2. In the menu bar, select **Storage**, and then click **Disk Manager**.
3. Beside the failed disk drive, click the **Safely Remove Disk** icon, and then click **OK**.
4. Open the front panel of the server.



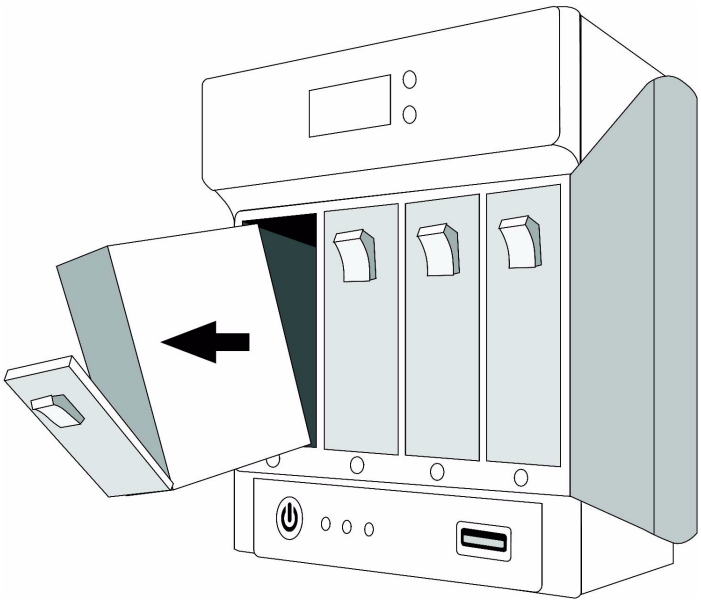
5. Locate the failed hard drive. Ensure that there is no activity on the drive by checking its LED—it should not be illuminated.

Warning: Never remove more than one drive at a time. Failure to do so will result in data loss.



6. Press down on the orange button to release the failed drive from the server. If the server is powered on, wait until the drive stops spinning (approximately one minute) before continuing.
7. Holding the handle, gently slide the hard drive partially out of the server until you can get a firm grip on the drive itself, and then remove the drive from the server. Because the hard drive is heavy, do not completely remove it or carry it by the plastic handle. Hold the drive firmly on the top and bottom.

Caution: The hard drive may be hot when removed.



8. Position (hold) the hard drive/carrier so that the drive label is facing up and the text is readable (not upside down).
9. Carefully bend the left side of the plastic carrier outward to release the failed drive from the carrier.
10. Remove the failed hard from the plastic carrier enclosure.

Replacing a Hard Drive

1. Place the new hard drive into the carrier, ensuring that the four pins hold the drive securely in place. If you are replacing a damaged hard drive carrier, place the drive removed from the damaged carrier into the replacement carrier.
2. Carefully slide the new drive into the server. Push firmly to install it completely, and then close the handle to lock the drive in place.

The hard drive's LED should turn green.

3. Close the front panel of the server.
4. In BlackArmor Manager, the drive's status changes to Foreign.
5. Click the **Claim Disk** icon, and then click **OK**. The drive's status changes to Good.
6. Click the **Recover** icon, and then click **OK**.

7. Technical Specifications

Network Connection

- 2 10/100/1000 Ethernet RJ-45 network connectors

USB Ports

- 4 USB 2.0 ports (1 at front, 3 at rear)

Power Supply

- 90W external power supply (full range AC input; 19V DC output)

Disk Drives

- 4 SATA II disk drives with tool-less carriers
- Hot-swappable

Physical Dimensions

- Height: 200 mm
- Width: 160 mm
- Depth: 210 mm

Power

- Power Rating: 100–240VAC, 50–60 Hz
- Input Voltage: 90–264VAC
- Steady AC Current: 1.5A (RMS) at 100VAC
- Input Frequency Range: 47–63Hz

Operating Environment

- 5 °C to 35 °C (41 °F to 95 °F)
- 20% to 80% humidity (noncondensing)

Nonoperating Environment

- -20 °C to +60 °C (-4 °F to 140 °F)
- 20% to 80% humidity (noncondensing)

8. Glossary

access level

Also known as permission level, the amount of access any person has to the BlackArmor® server. BlackArmor Manager has two permission levels: *administrator* and *user*.

administrator

A BlackArmor administrator is responsible for the BlackArmor server and all its settings. An administrator can set up or delete user accounts, group accounts, and shares; assign or remove access permissions; modify any setting on the server; and create other administrators. See also user.

archive backup

See Remote access can also refer to shutting down or resetting the server using BlackArmor Manager instead of physically pressing the Power button. See also local access..

CIFS

Common Internet File System. A file system that lets people with different computers running Windows operating systems share files without having to install special software.

domain

A group of computers administered as a single unit from a central location.

event

A problem or change in setting on the BlackArmor server. A change in the server's name or the failure of a disk drive are both server events.

external USB hard drive

See USB drive

firmware

Software that's built into hardware.

format

To format a disk drive is to prepare it for reading and writing data. Formatting erases background information from a disk drive, tests it, and prepares it for use. Formatting may destroy existing files on a disk drive. You must format a disk drive before you can use it.

FTP

File Transfer Protocol. A format for exchanging files over the Internet. FTP is commonly used to upload files to or download files from a server over the Internet.

group account

In BlackArmor Manager, a collection of user accounts grouped together to make it faster and easier to manage access to shares. All users in a group have the same level of access to any particular share. See also user account.

hot-swap

To remove and replace a disk drive without first powering off the server.

HTTP (Hypertext Transfer Protocol)

Rules for exchanging the most common form of documents (hypertext documents) over the Internet.

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer)

Rules for exchanging HTTP documents over encrypted connections.

JBOD

Just a Bunch of Drives. See span.

IP address

The identifier of a computer, server, or other device on a TCP/IP network. IP addresses are a sequence of four numbers separated by periods. (For example, 123.456.78.1.) Every device on your local network has a unique IP address.

link aggregation

A method of increasing the speed of a device's network connection by using more than one Ethernet port simultaneously to connect to the network.

If you connect both of your BlackArmor server's LAN ports to your network router or switch and set Aggregation in BlackArmor Manager, both connections work simultaneously and in parallel to move data more quickly—similar to filling a bucket using two hoses instead of one.

local access

Access to the server from a computer on your local network. Or, manual access to the server, which involves physical contact with the server or its cables. See also remote access.

mirror

A level of RAID protection also known as RAID 1. A mirror is built from two disk drives, where one disk drive is a mirror of the other (the same data is stored on each disk drive). Compared to independent disk drives, a mirrored volume provides faster performance, but has only 50% of the capacity.

NFS

Network File System. An application that lets all users on a network share files that are stored on different types of computers.

NTP (Network Time Protocol) server

Synchronizes the date and time of computers and servers on a network, based on Coordinated Universal Time (UTC).

parity

Data created in volumes with RAID 5 protection that's used to reconstruct files if one of the disk drives in the server fails. See also RAID 5.

private share

A folder that is accessible only to users with permission granted by the share's owner.

RAID

Redundant Array of Independent Disks. A technology that combines disk drives together for improved performance and fault tolerance (the ability to withstand the failure of a disk drive).

RAID 0

See stripe.

RAID 1

See mirror.

RAID 5

A level of RAID protection. A volume with RAID 5 is built from a minimum of three disk drives, and uses data striping and parity data to provide redundancy. (Parity is extra information that's used to re-create data if a disk drive fails. In volumes with RAID 5, parity data is striped evenly across the disk drives with the stored data.) Parity data provides data protection, and striping improves performance. See also stripe.

RAID 10

A level of RAID protection. A volume with RAID 10 is built from two or more equal-sized RAID 1 volumes. Data in a volume with RAID 10 is both striped and mirrored. Mirroring provides data protection, and striping improves performance. See also mirror, and stripe.

remote access

Access to the server from a computer that is not on your local network. For instance, accessing the server from a client's computer, over the Internet, is remote access.

Remote access can also refer to shutting down or resetting the server using BlackArmor Manager instead of physically pressing the Power button. See also local access.

RSA key

An encryption decoder that's part of SSL, a type of encryption used to protect data being sent over a network or the Internet. "RSA" stands for Rivest, Shamir, and Adelman, who invented the technology.

Seagate Global Access

A service that you can use to view, download, share, and work with the files stored on your BlackArmor server from anywhere in the world. You can also use Global Access to upload files to your BlackArmor server.

server

A computer or device on a network that manages resources. The BlackArmor server is a file server, a storage appliance that's dedicated to storing files; it can also be used as a print server, a device that manages one or more printers.

share

A folder on your BlackArmor server that stores and protects backup files, as well as other files that can be accessed by other people.

SMART

Self-Monitoring Analysis and Reporting Technology. Technology built into disk drives that let them automatically monitor their own health and report on possible problems. Not all disk drives have SMART support.

span

A group of disk drives collected in a server, not protected by RAID. Also known as JBOD. See also RAID.

spin down

Referring to disk drives, a term that means to stop spinning.

SSL certificate

Secure Socket Layer certificate, part of the SSL encryption method. SSL (also known as Transport Layer Security) is a type of encryption used to protect data being sent over a network or the Internet. SSL uses a system of keys, like secret passwords, to send and receive files securely.

stripe

Also known as RAID 0. A volume with striping includes two or more disk drives where data is distributed evenly (striped) across the disk drives in equal-sized sections. A striped volume does not maintain redundant data, and so *offers no data protection*.

However, compared to an equal-sized group of independent disks, a striped volume provides faster performance.

UPS

Uninterruptible Power Supply. A power supply that has a battery in it that maintains power to a computer or server in the event of a power failure. A UPS is intended to provide enough

power for you to save whatever files you're working on and properly power off the computer or server; it's not meant to keep any system running for the duration of a power failure.

USB

Universal Serial Bus. The interface between your computer and the USB devices you plug into it. Your computer communicates with USB devices through the USB interface.

USB drive

A portable disk drive that connects to a computer with a USB cable, instead of being installed inside the computer itself. Also known as a thumb drive, jump drive, flash drive, or external USB hard drive.

user

In BlackArmor Manager, a person who can save, back up, and share files using the BlackArmor server, but who can't modify user account, group account, share, or server settings.

user account

An account, with a user name and password, that a person uses to access the BlackArmor server. User accounts have access level permissions associated with them.

volume

Data storage space that can be made up of one or more disk drives, or of only part of a single disk drive.

Web access protocol

The rules for sending information over the Internet. Your BlackArmor server has two Web access protocol choices, HTTP and HTTPS.

workgroup

A collection of computers on a network that share resources.

Index