CASPER SECURE™
SERVER EDITION 3.0

USER GUIDE

Future Systems SOLUTIONS

Copyright and Trademark Information

Table of Contents

Introduction

Casper Secure™ Server Edition is the only disk cloning solution designed specifically for Windows® server based platforms encrypted with PGP® Whole Disk Encryption or Windows BitLocker® Drive Encryption. Whether you need to upgrade a server with a new disk to increase speed or storage capacity, replace a failed disk, or maintain an instantly bootable backup replacement for a server, Casper Secure Server Edition is designed to make the process extraordinarily easy.

Casper Secure Server Edition features:

- **Quick and Easy Encrypted System Disk Upgrades and Replacements**. Casper Secure makes it faster and easier than ever to upgrade or replace a PGP whole disk encrypted or BitLocker encrypted disk or hardware RAID array in a server. Because all data is maintained in its original encrypted state, Casper Secure completely eliminates the unnecessary downtime incurred by other solutions that require you to perform a separate, time-consuming re-encryption step, which means a typical encrypted disk replacement that used to take two or more days to complete now can be completed in less than a couple of hours with Casper Secure. It supports all SCSI, SATA, ATA/IDE, and hardware RAID configurations, including solid state devices and sold state arrays.

- **Fast, Completely Encrypted System Backups**. Casper Secure creates a complete, instantly bootable, backup replacement for a Windows server system disk or hardware RAID array encrypted with PGP Whole Disk Encryption or Windows BitLocker Drive Encryption. Unlike traditional backup and disk imaging solutions, which can produce only an unencrypted backup of a PGP whole disk encrypted or BitLocker encrypted server, Casper Secure creates a backup that persists all of the encrypted data in its original encrypted state. This not only makes rapid recovery possible, it ensures your server backups remain 100% compliant with all data security directives regarding data at rest. In addition, exclusive SmartClone™ technology enables Casper Secure to maintain a complete backup replacement disk or array in the same amount of time required by most traditional backup programs to perform a partial or incremental *unencrypted* backup of an encrypted disk.

- **Rapid Recovery**. In the event of a hard disk or RAID array failure, a backup created by Casper Secure can be used as an immediate and permanent replacement for the failed hard disk or array. No special rescue disks or arduous data restoration processes are required to facilitate recovery, and most importantly, no lengthy re-encryption process is required.

- **Convenience**. Casper Secure enables complete system backups to be performed at any time without leaving Windows, so there is never a need to restart or interrupt the operation of a server to create a backup. In addition, features such as integrated scheduling, SmartWrites™, and SmartAlert™ technology permit backups to be performed completely unattended and in the background without interfering with the normal operation of the server for true “set it and forget it” operation.

NOTE: This User Guide is intended to provide you with an overview of the basic operations of Casper Secure Drive Backup. For additional assistance, please refer to the detailed help files included within the program.

System Requirements

- Windows Server 2008 and 2008 R2, Windows Server 2003, Windows Home Server, and Windows 2000 and 2000 Advanced Server

  NOTE: Casper Secure Server Edition is not designed for use with Windows Server for Itanium-Based Systems or Windows NT. Background copying not supported on Windows 2000 and 2000 Advanced Server.

- PGP Desktop version 9.6x or later, or BitLocker Drive Encryption feature enabled
- 100MB available disk space
- 128MB RAM (512MB or more recommended)
- Backup device (additional internal or external hard disk drive or RAID array)

Getting Help

The Casper Secure help includes troubleshooting information. To access help when running Casper Secure, select **Contents** from the **Help** menu, or press **F1**.

Additional support for Casper Secure is available on the Future Systems Solutions Web site at http://support.fssdev.com.

Installing Casper Secure Server Edition

The installation process takes just a few minutes and an automated wizard will guide you through the process. The instructions below outline in detail the steps for installing Casper Secure Server Edition.

Running the Casper Secure Server Edition Setup Program

1. Start the Casper Secure Server Edition Setup program.

   The **Welcome to the Casper Secure 3.0 Server Edition Setup Wizard** dialog will appear.

2. At the Welcome to the Casper Secure 3.0 Server Edition Setup Wizard dialog, click **Next**.

   The **Read the Future Systems Solutions, Inc. License Terms** dialog will appear. In order to proceed with the installation of Casper Secure Server Edition, you must agree to the terms of the license that is displayed.

3. Read the License Agreement, select **I accept the terms of this agreement**, and then click **Next**.

   The **Choose the installation you want** dialog will appear.

4. Click **Install Now**.

   The Casper files are added to your system.

5. Click **Run Casper Secure 3.0 Server Edition** to begin using Casper Secure Server Edition.

Using Casper Secure Server Edition

Casper Secure Server Edition makes it easy to upgrade or maintain a backup of a Windows server system disk device, as well as other hard disks used on a server.

When cloning a disk device such as a standalone hard disk or hard disk RAID array, Casper Secure creates a snapshot, representing a single point-in-time view of the disk device, and then clones it to another disk device. The result is disk device that can be used as an immediate and complete replacement for the original disk device.

Casper SmartSense™ technology will begin the process of upgrading or creating a backup of a Windows server system disk automatically when you attach a new hard disk to the server. If the new disk is installed internally, or if Casper SmartSense is unable to detect the new disk, you can manually launch Casper Secure SmartStart™ to begin the process. For more information about using Casper Secure SmartStart to upgrade or maintain a backup of a Windows system disk device, please refer to the **Casper Secure SmartStart Guide**.

To upgrade or maintain a backup for another disk deice on a server, or customize the upgrade or backup process of the system disk device, Casper Secure's Copy Drive wizard will guide you as outlined in this user guide.

Starting Casper Secure

1. Click the **Start** button.
2. Click **All Programs**.
3. Point to the **Casper Secure 3.0 Server Edition** menu.
4. Click **Casper Secure Server Edition**.

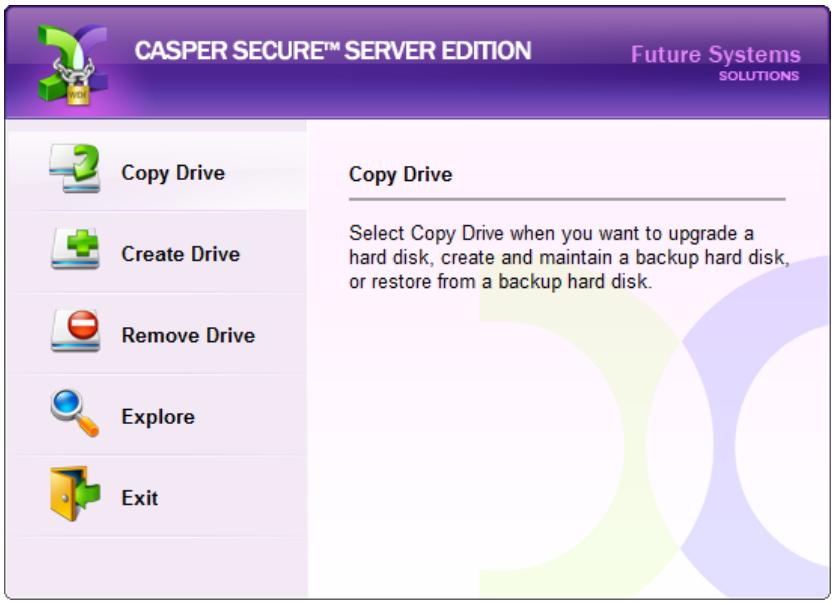
Upgrading a Hard Disk

The procedure for upgrading or replacing a hard disk in a server is basically the same whether you are upgrading a single hard disk or a RAID array configured through a hardware RAID controller. The new hard disk or RAID array must be temporarily installed or configured as a secondary disk device in the computer or attached as an external disk using an external USB, Firewire, or eSATA hard disk enclosure or bridge adapter.

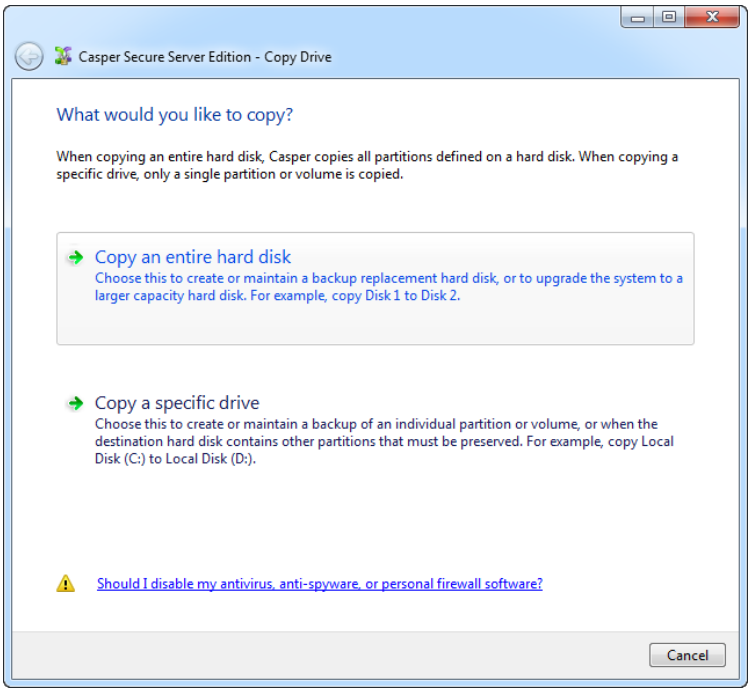
Example 1: Upgrading a Hard Disk

Assuming the new disk device is currently installed or attached to the system, the following procedure illustrates how Casper may be used to clone the original system disk device to the new disk device in order to complete the upgrade.

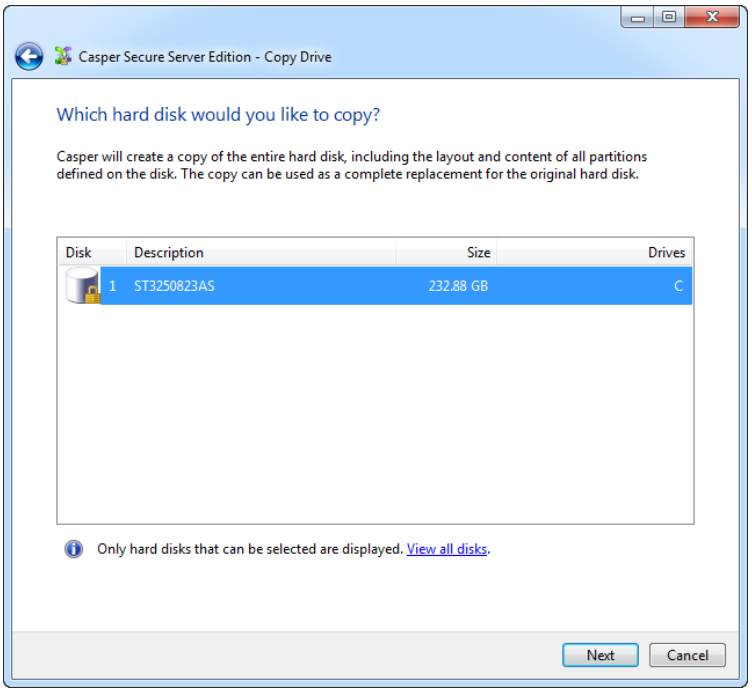
1. Select **Copy Drive**.



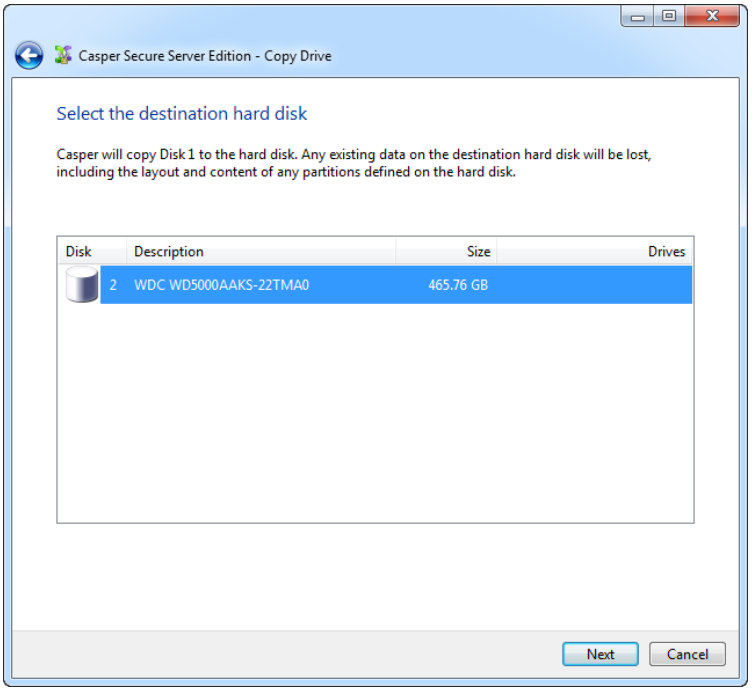
2. Select **Copy an entire hard disk**.



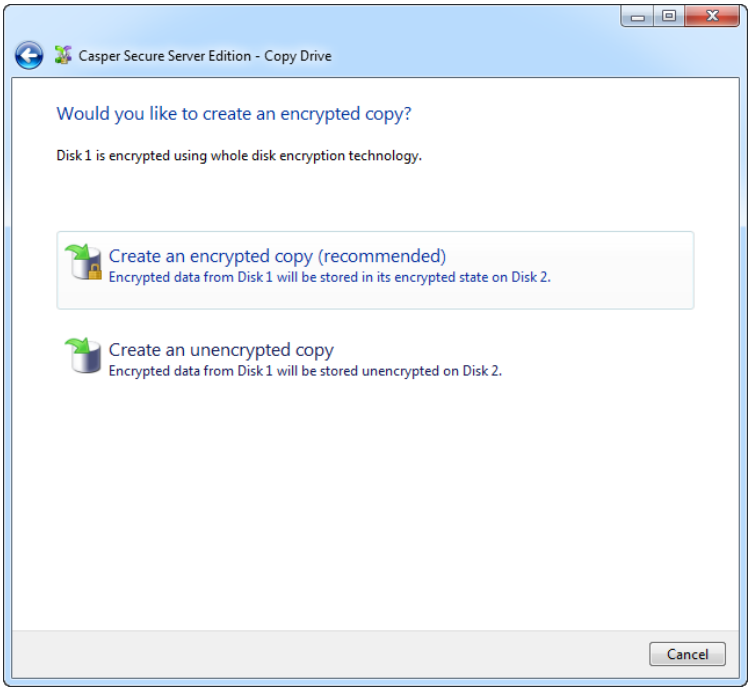
3. Select the disk device to be upgraded as the hard disk to copy, and click **Next**.



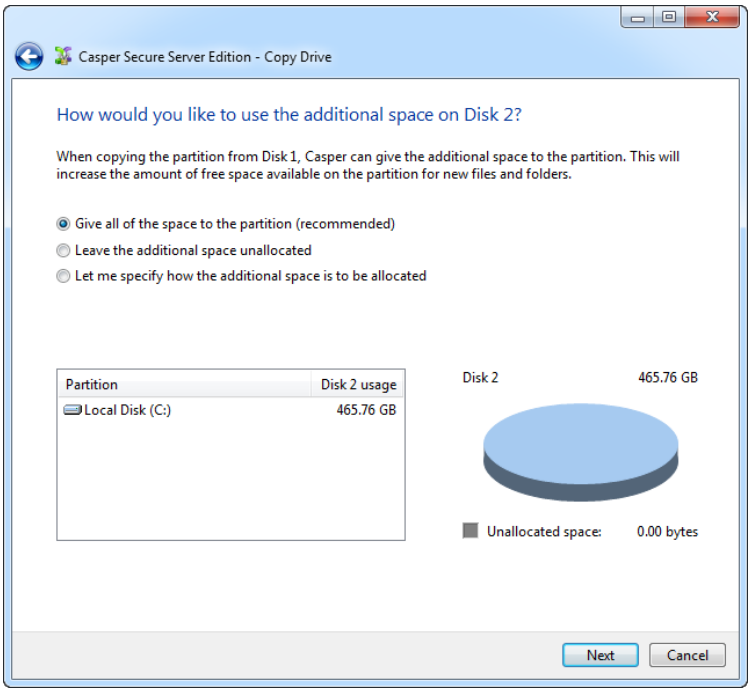
4. Select the new disk device as the destination, and click **Next**.



5. If the source disk device is encrypted using PGP whole disk encryption or BitLocker drive encryption, Casper Secure will offer the option of creating an unencrypted copy unless prohibited by administrative policy settings. Click **Create an encrypted copy**.

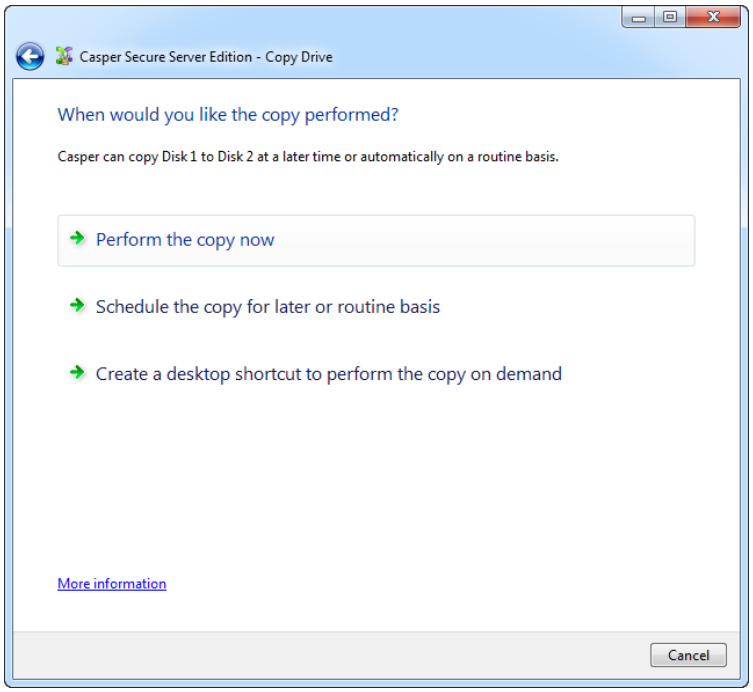


6. When prompted to specify how the additional space on the new disk device is to be used, retain the default selection and click **Next**.

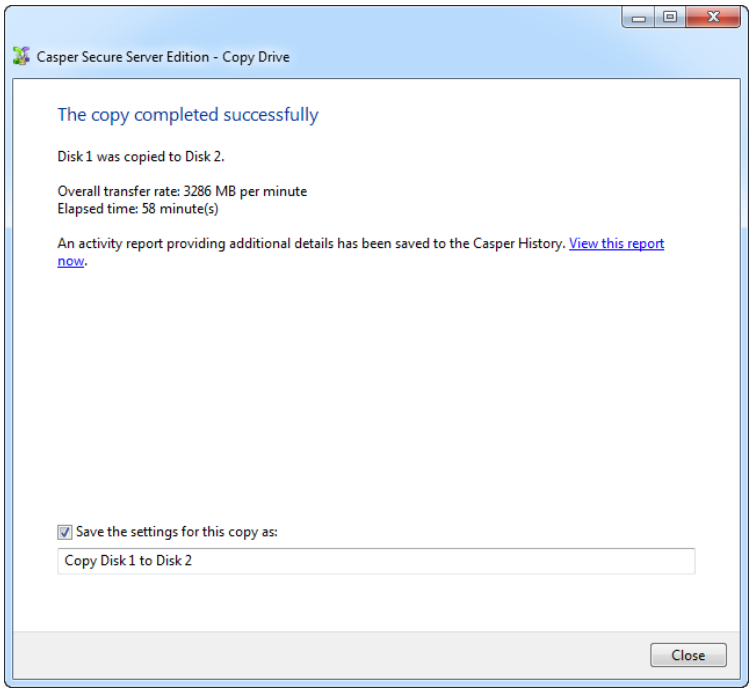


When the destination disk device is larger than the source, the default option will be *Give all of the space to the partition*, or *Proportionally distribute the space to all partitions* when there is more than one partition defined on the source disk device. For additional help with making a selection, press **F1**.

7. Click **Perform the copy now** to begin the copy.



8. When Casper Secure has completed the cloning process, click **Close**.



9. Shutdown and power-off the computer.
10. Reconfigure the computer to replace the original hard disk or RAID array with the new disk device.

Creating and Maintaining a Bootable System Backup

Using Casper Secure to create and maintain a bootable backup replacement disk for a Windows server requires a hard disk or secondary RAID array large enough to accommodate all of the data on the current system disk device.

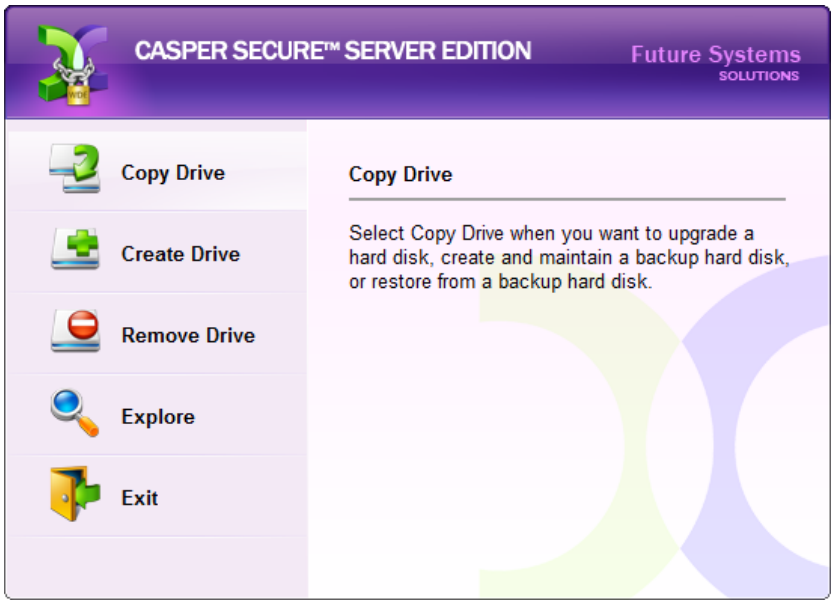
The following examples illustrate several ways to create and maintain a bootable system backup. The first example, **Creating a Backup**, demonstrates how to manually create a backup by cloning one hard disk to another. The second example, **Updating a Backup**, shows how to manually update a backup. The third example, **Scheduling a Routine Backup**, illustrates how to create a copy schedule to maintain the backup automatically. The fourth example, **Using Casper SmartSense to Maintain an External Backup**, shows how to configure Casper Secure to perform a backup automatically whenever you attach an external backup drive. The fifth example, **Using 1-Click Cloning to Maintain a Backup**, shows how to create a 1-Click Cloning desktop shortcut to maintain a backup on demand.

NOTE: For a hard disk attached as an external USB device, booting from the backup hard disk may require the selection of additional BIOS options to completely enable booting. By default, some BIOS implementations disable USB boot support, or have it configured for floppy or ZIP drive emulation rather than hard disk drive (HDD) emulation. If the computer's BIOS does not support booting from external USB hard disk type devices, the backup hard disk must be removed from its external enclosure and installed as a replacement for the internal hard disk in order to boot from it. Alternatively, a restore may be performed by using the Casper Secure Startup Disk to copy the external backup hard disk to the computer's internal disk device.

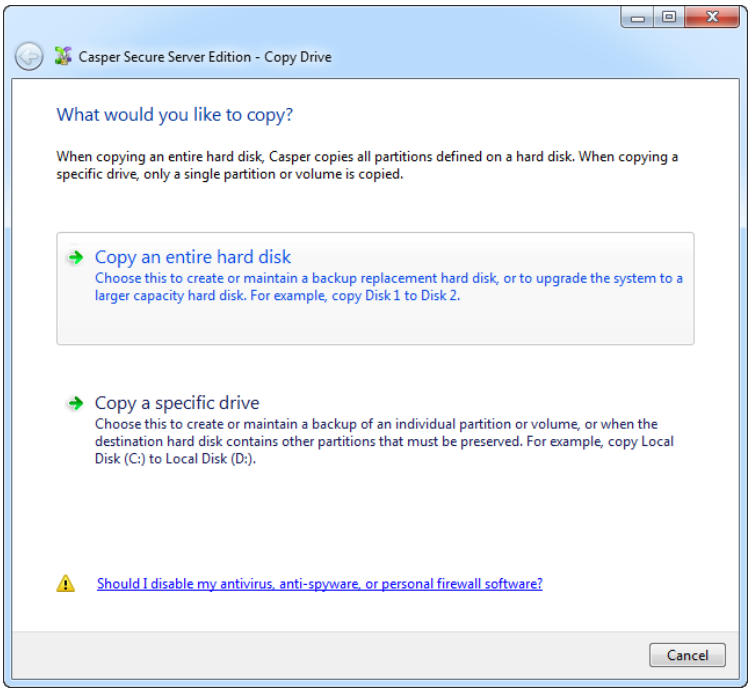
Example 2: Creating a Backup

Assuming the backup disk device is currently installed or attached to the system, the following procedure illustrates how to clone the system disk device to the backup disk device.

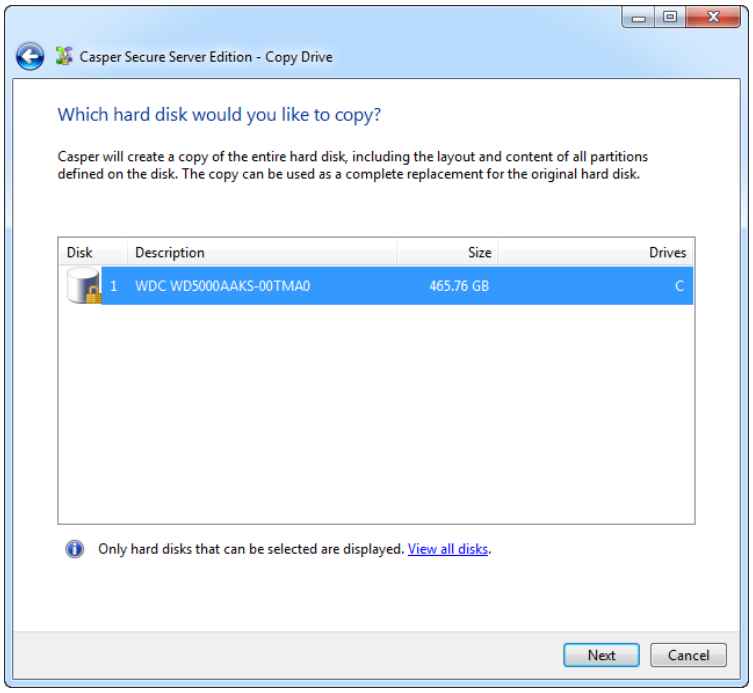
1. Select **Copy Drive**.



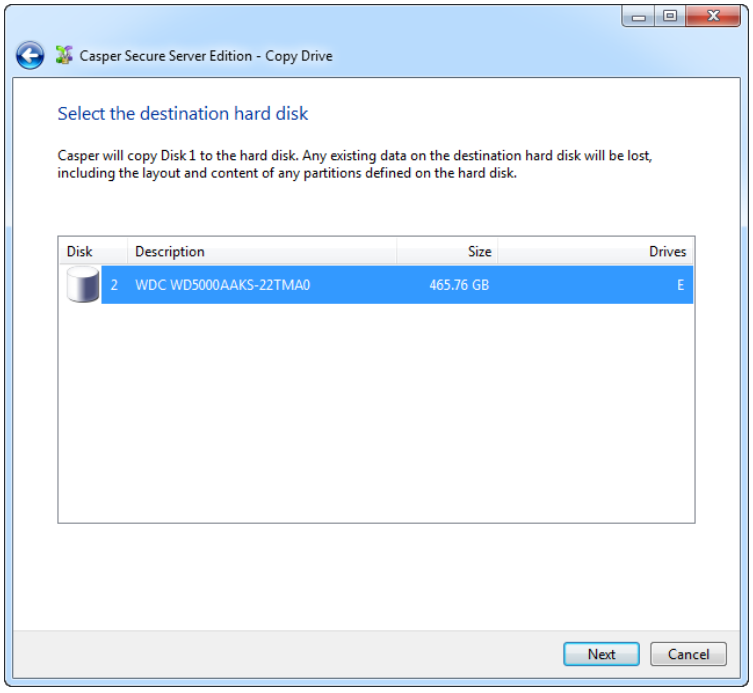
2. Select **Copy an entire hard disk**.



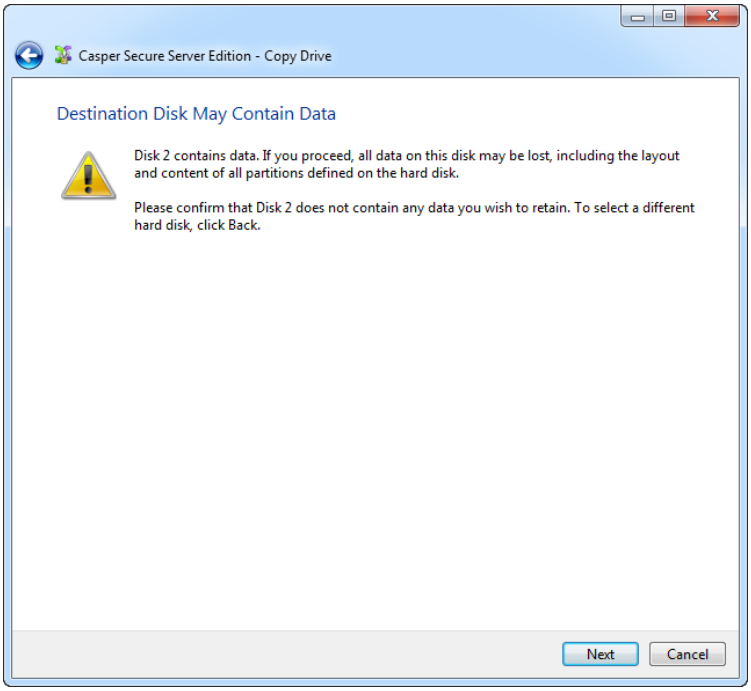
3. Select the disk device to backup as the hard disk to copy, and click **Next**.



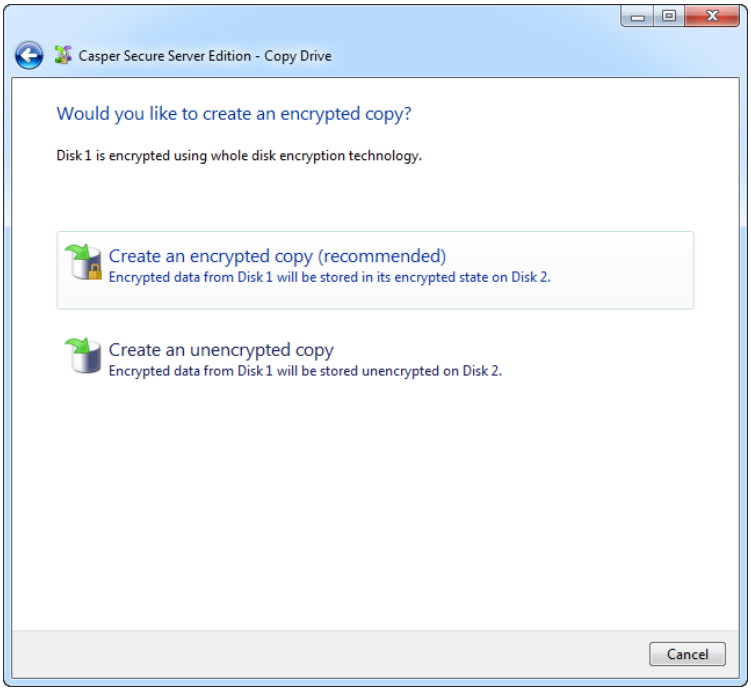
4. Select the backup disk device as the destination, and click **Next**.



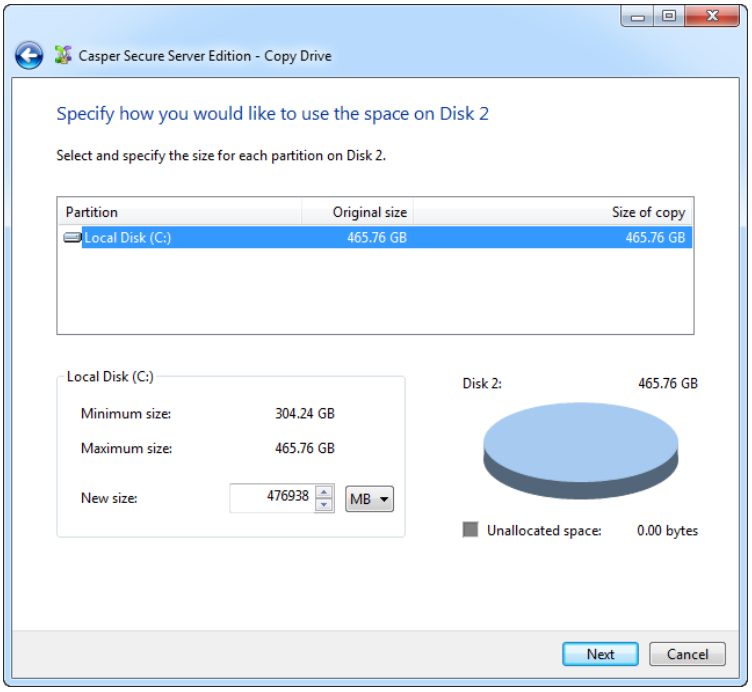
5. If the selected destination disk device defines a partition or contains data, Casper Secure will warn you that the contents will be overwritten. Confirm you have selected the correct disk device to receive the backup, and click **Next** to proceed.



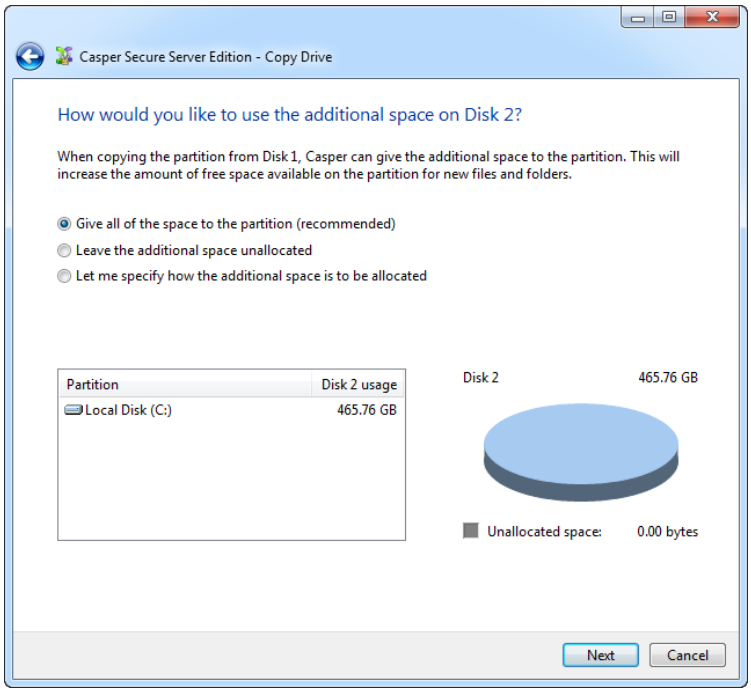
6. If the source disk device is encrypted using PGP whole disk encryption or BitLocker drive encryption, Casper Secure will offer the option of creating an unencrypted copy unless prohibited by administrative policy settings. Click **Create an encrypted copy**.



7. When prompted to specify how the space on the backup disk device is to be used, retain the default selection and click **Next**. If the destination disk device is the same size or smaller than the source disk device, Casper Secure will ask you to manually configure how the space is to be used.

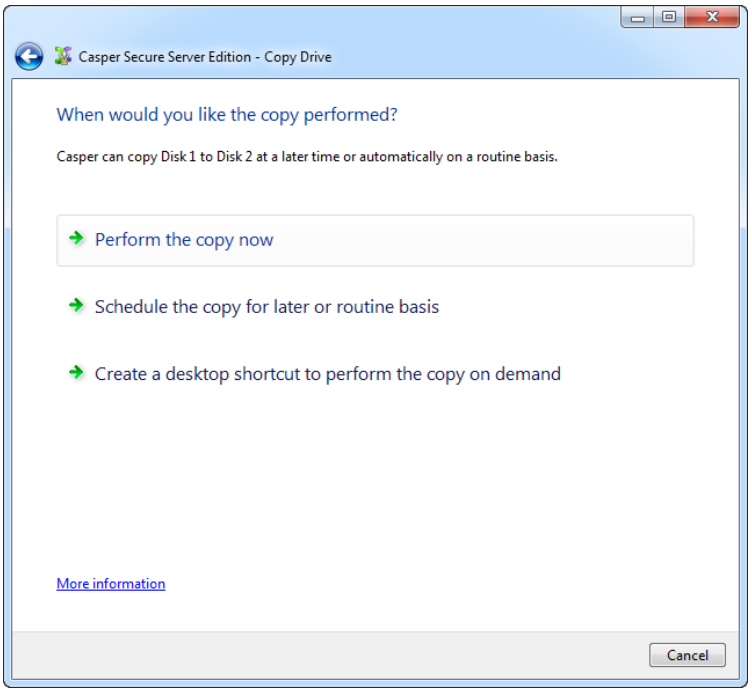


When the destination disk device is larger than the source, the default option will be *Give all of the space to the partition*, or *Proportionally distribute the space to all partitions* when there is more than one partition defined on the source disk device.

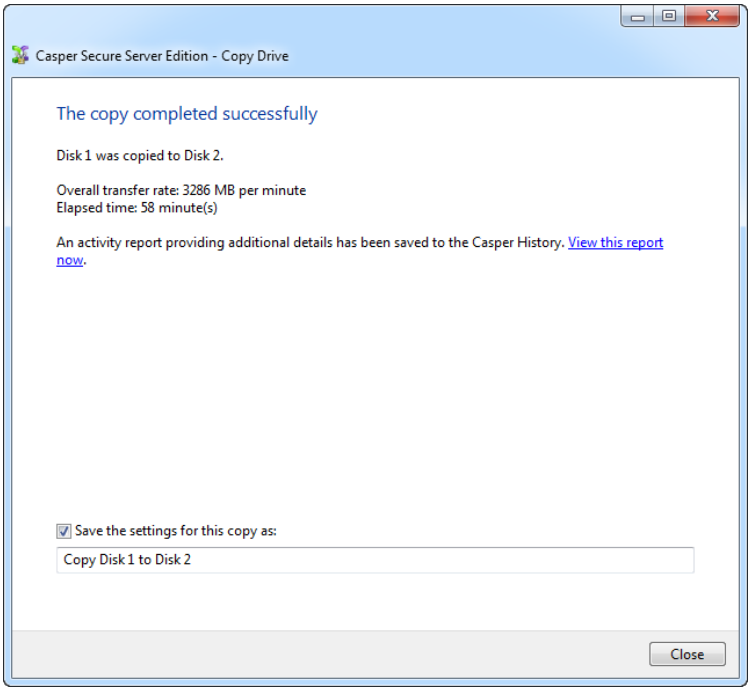


Simply clicking **Next** to accept the default selection or value is generally best. For additional help with making a selection, press **F1**.

8. Click **Perform the copy now** to begin the copy.



9. When Casper Secure has completed the cloning process, click **Close**.

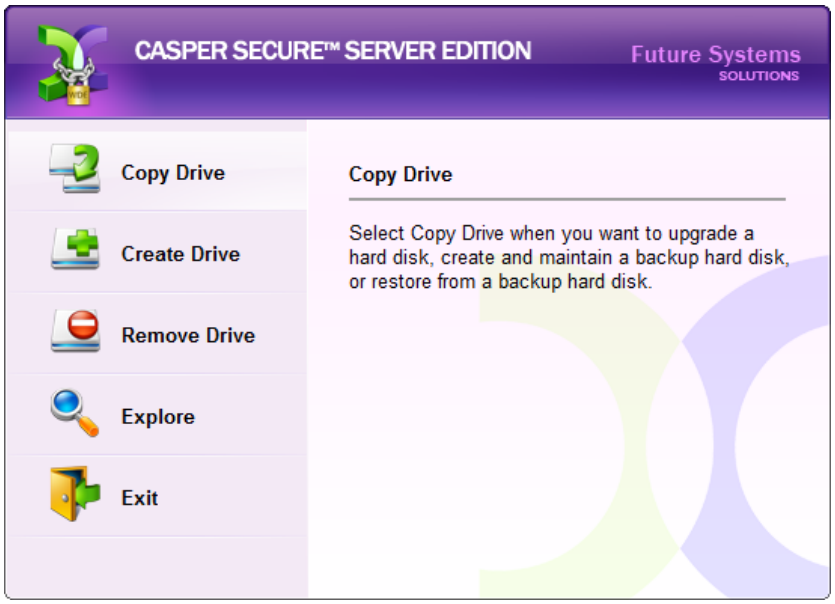


Example 3: Updating a Backup

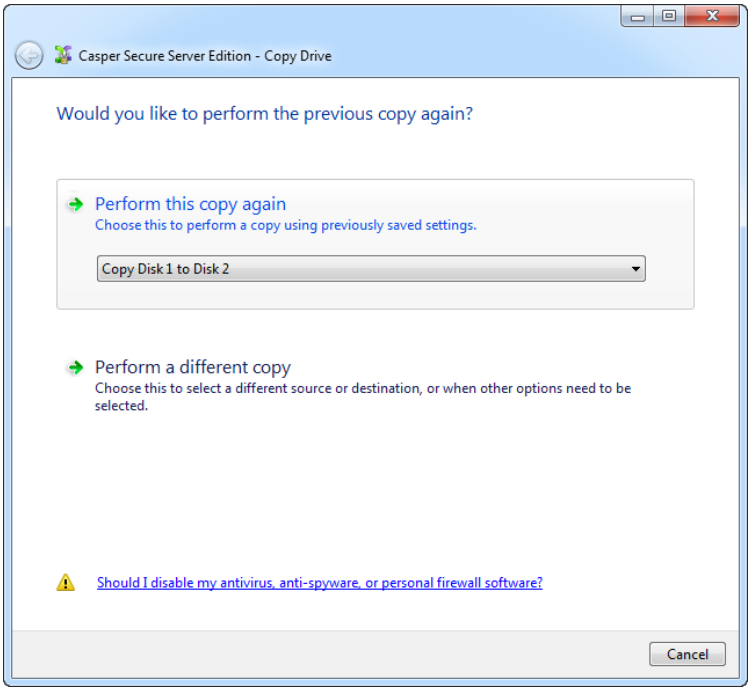
You can manually update a backup by repeating the procedure used to create the backup. When the settings for the copy have been saved as shown in the final step of the preceding example, you can use Casper's SmartStart functionality to jumpstart the process. Assuming the backup hard disk is currently installed or attached to the system, the following two procedures illustrate how a prior copy may be quickly repeated.

Repeating a Copy via *Perform this copy again*

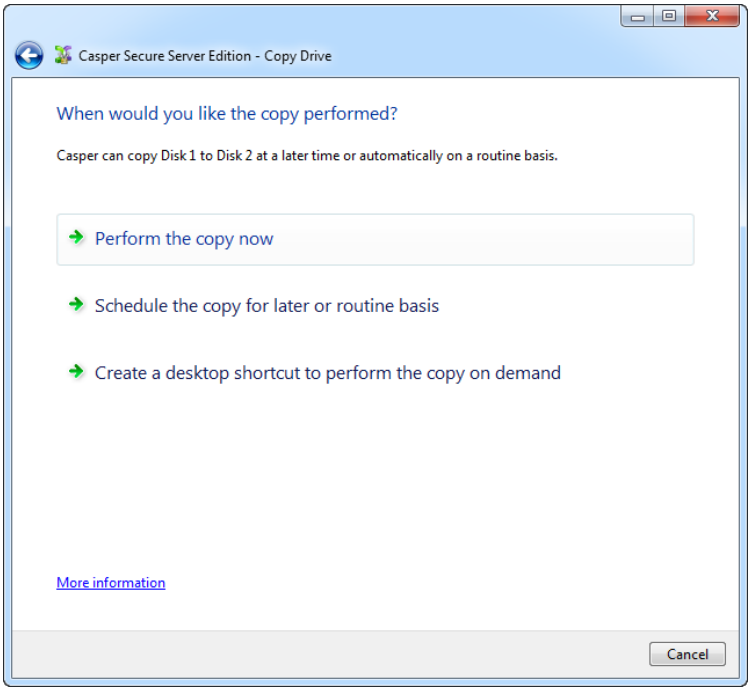
1. Select **Copy Drive**.



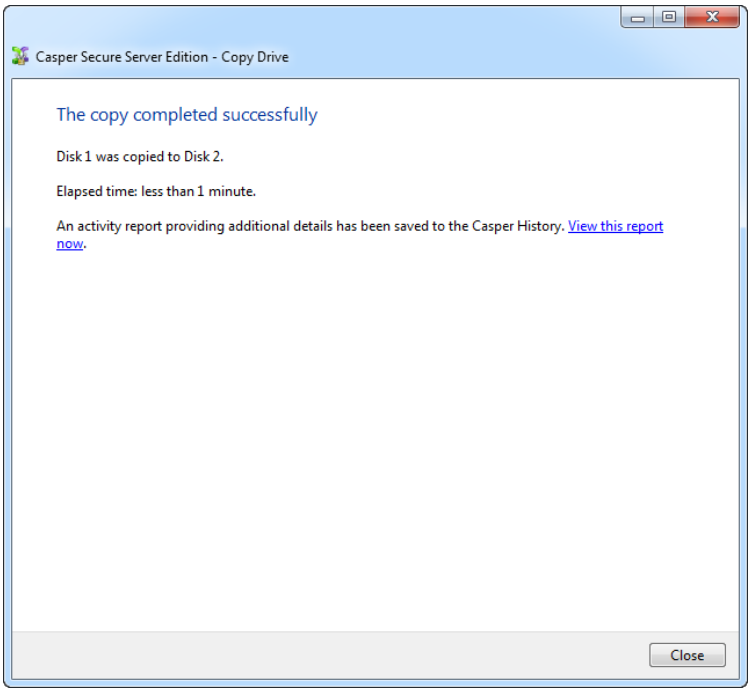
2. Select the previous copy to be repeated from the list provided and click **Perform this copy again**.



3. Click **Perform the copy now** to begin the copy.

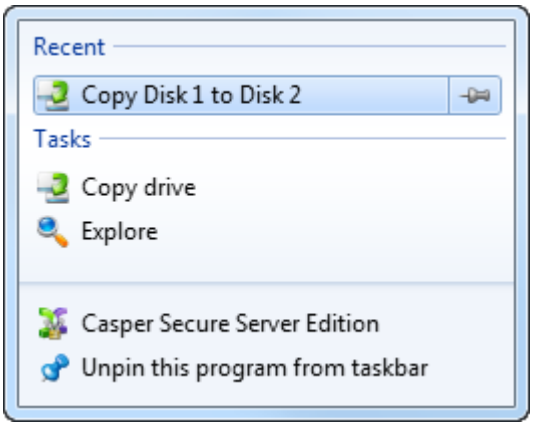


4. When Casper Secure has completed the cloning process, click **Close**.

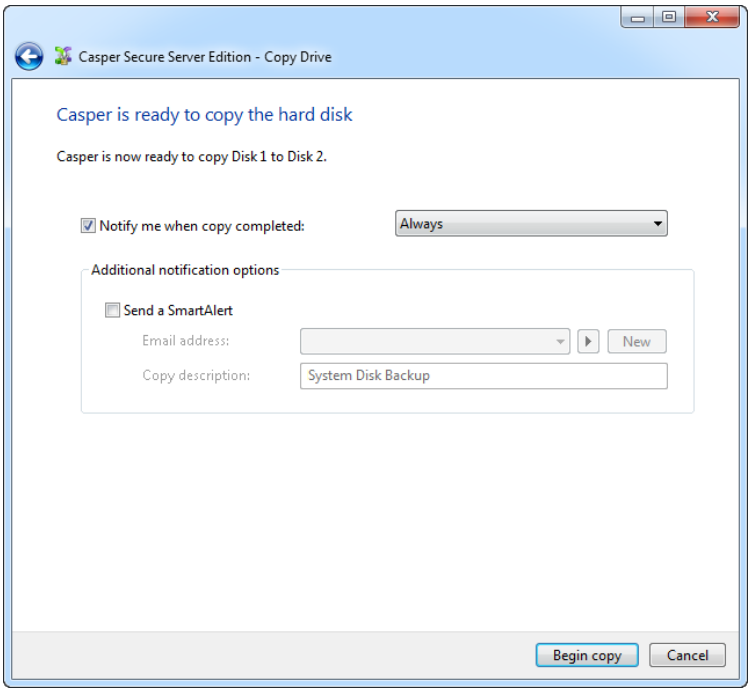


Repeating a Copy via the Casper Secure Taskbar Icon (Windows 2008)

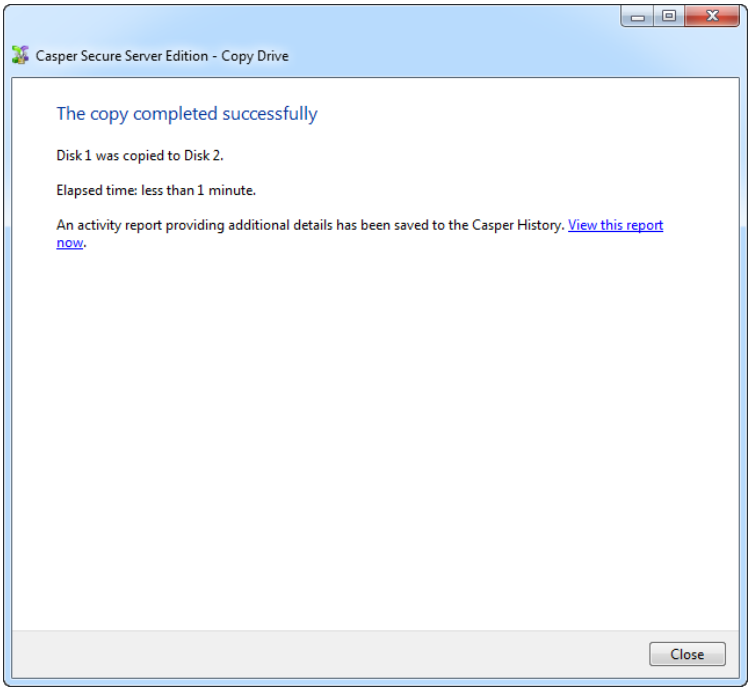
1. Right-click the Casper Secure icon appearing on the Windows 2008 taskbar to display the icon's taskbar menu.
2. Click the copy to be repeated from the **Recent** list.



3. Click **Begin copy** to begin the copy.



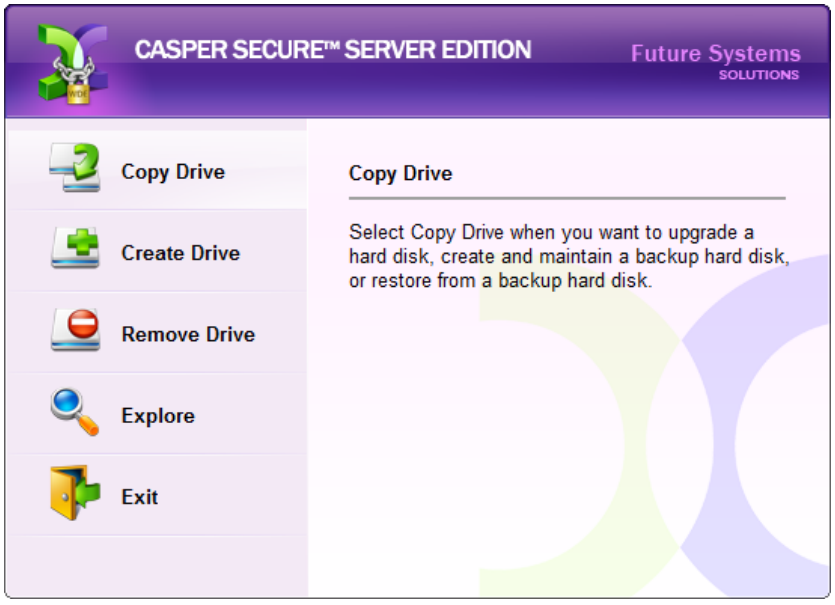
4. When Casper Secure has completed the cloning process, click **Close**.



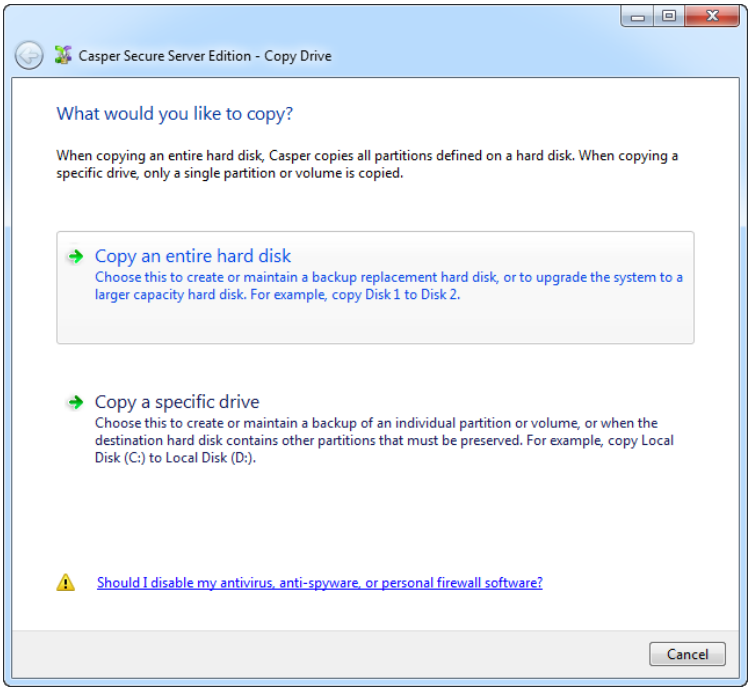
Example 4: Automating a Routine Backup

You can fully automate the process of creating and maintaining a backup replacement disk device for a server by scheduling Casper Secure to run on a routine basis. Assuming the backup disk device is currently installed or attached to the system, the following procedure shows how to schedule a copy to be performed on a routine basis.

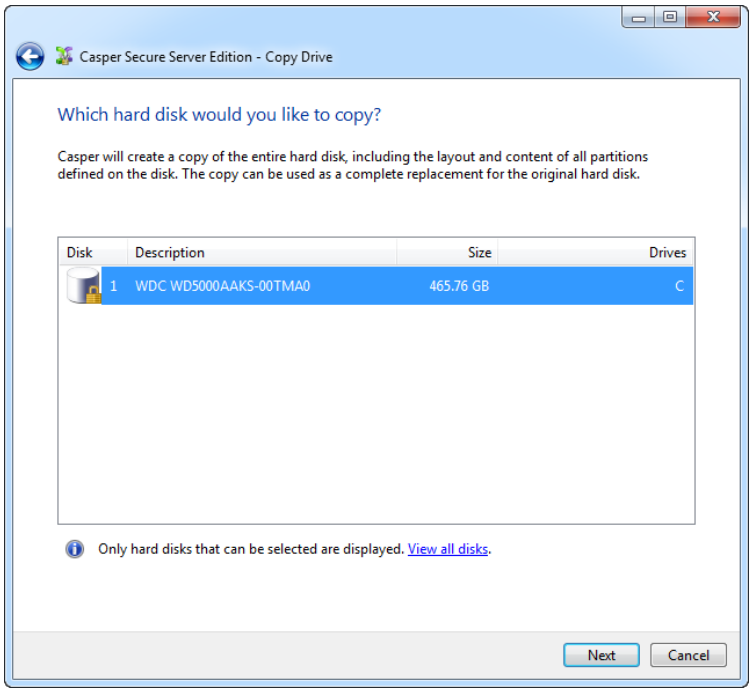
1. Select **Copy Drive**.



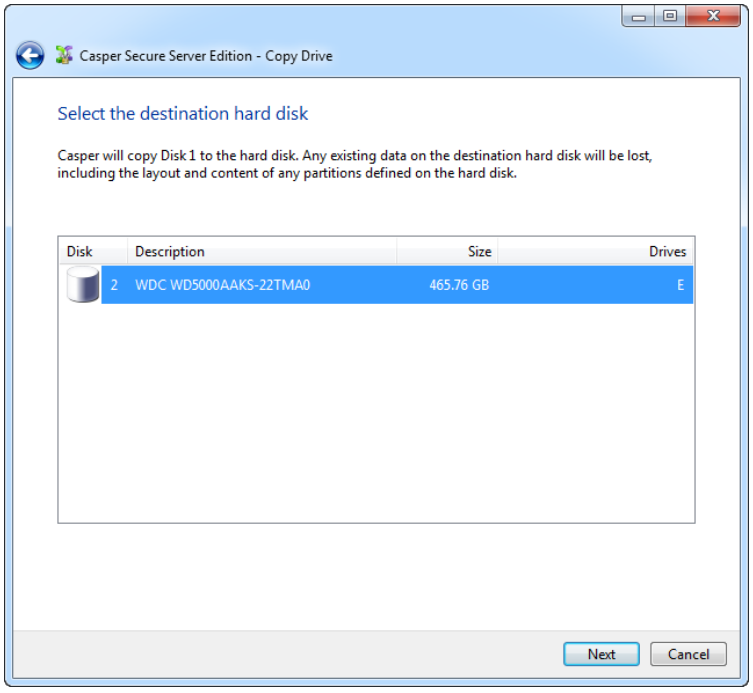
2. Select **Copy an entire hard disk**.



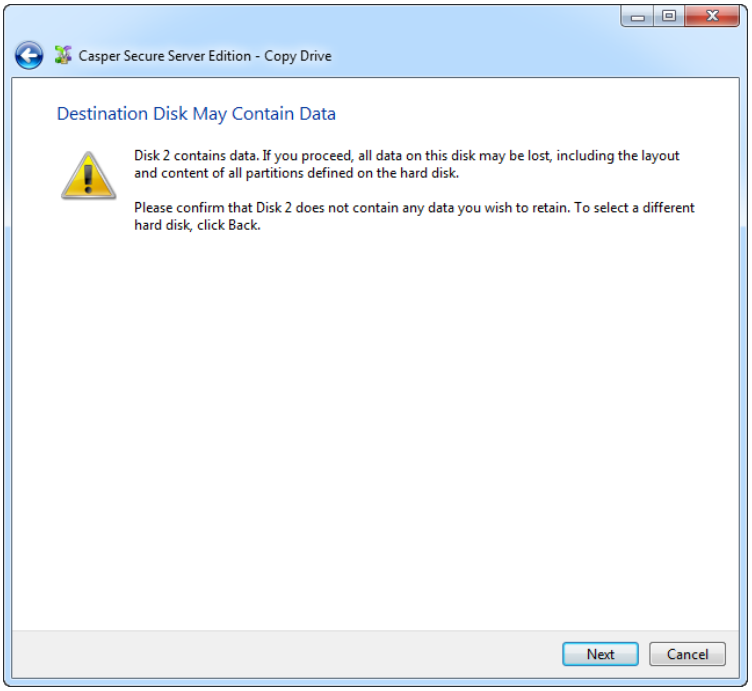
3. Select the disk device to backup as the hard disk to copy, and click **Next**.



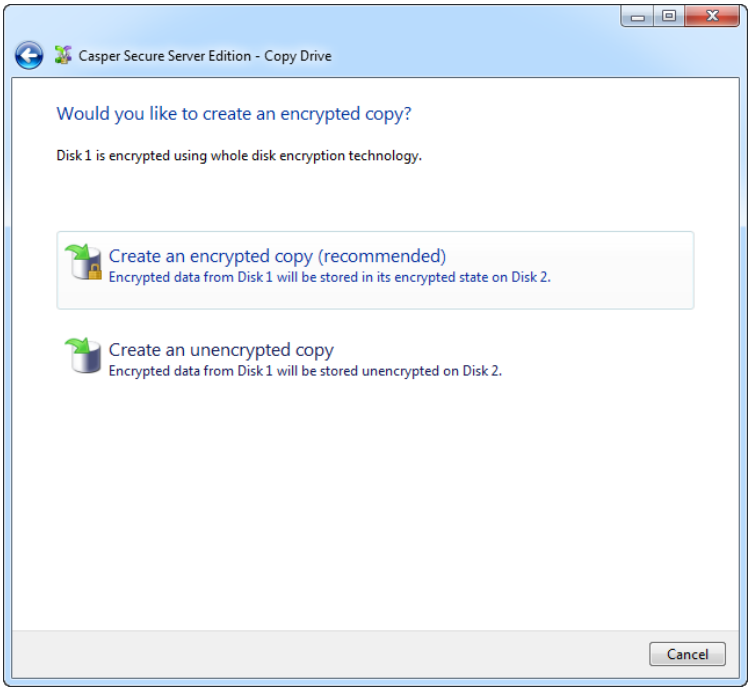
4. Select the backup disk device as the destination, and click **Next**.



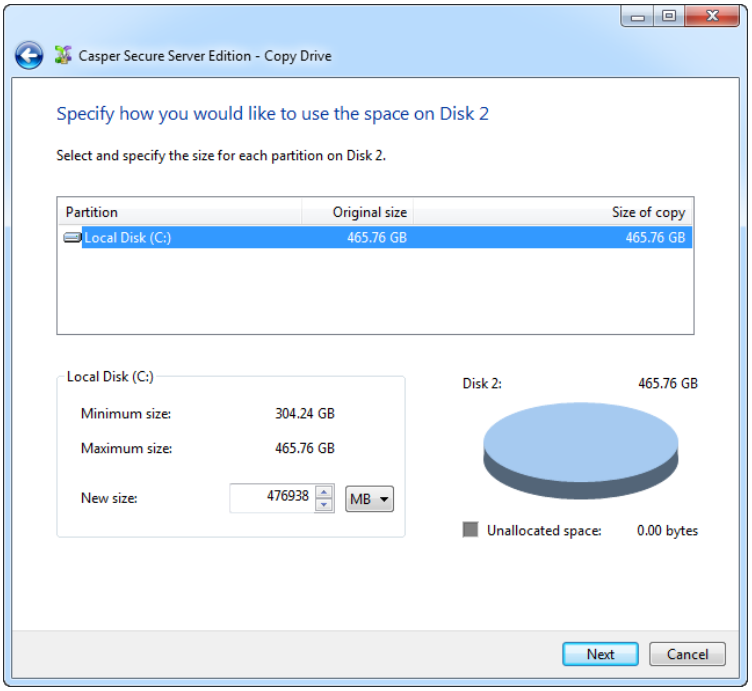
5. If the selected destination disk device defines a partition or contains data, Casper Secure will warn you that the contents will be overwritten. Confirm you have selected the correct disk device to receive the backup, and click **Next** to proceed.



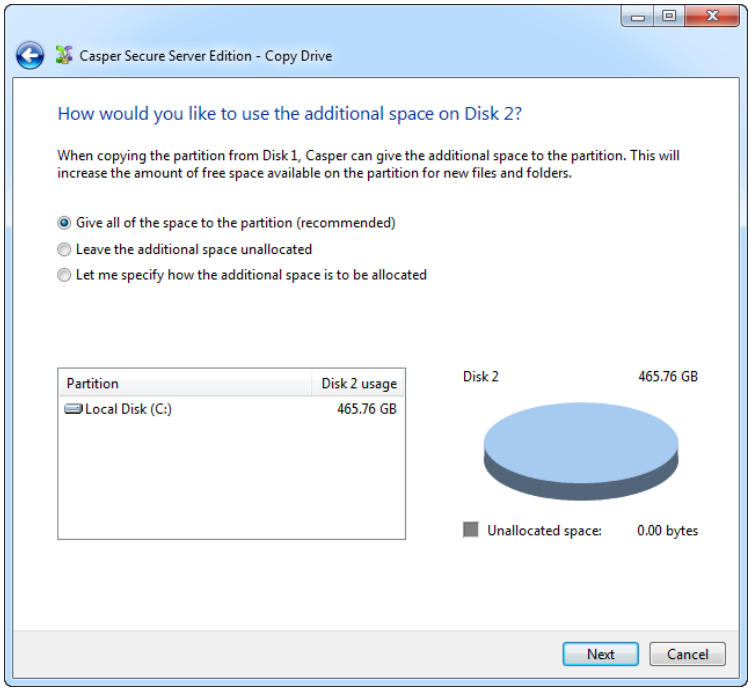
6. If the source disk device is encrypted using PGP whole disk encryption or BitLocker drive encryption, Casper Secure will offer the option of creating an unencrypted copy unless prohibited by administrative policy settings. Click **Create an encrypted copy**.



7. When prompted to specify how the space on the backup disk device is to be used, retain the default selection and click **Next**. If the destination disk device is the same size or smaller than the source disk device, Casper Secure will ask you to manually configure how the space is to be used.

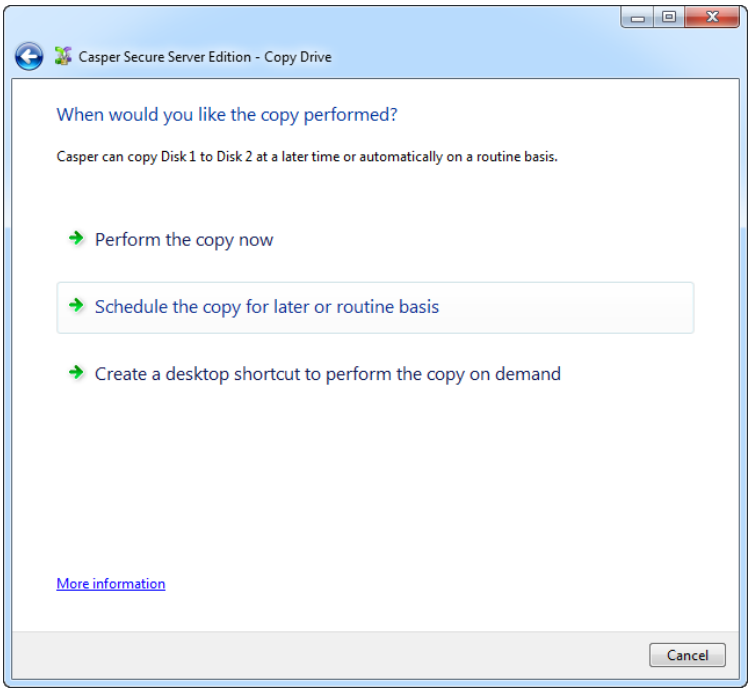


When the destination disk device is larger than the source, the default option will be *Give all of the space to the partition*, or *Proportionally distribute the space to all partitions* when there is more than one partition defined on the source disk device.

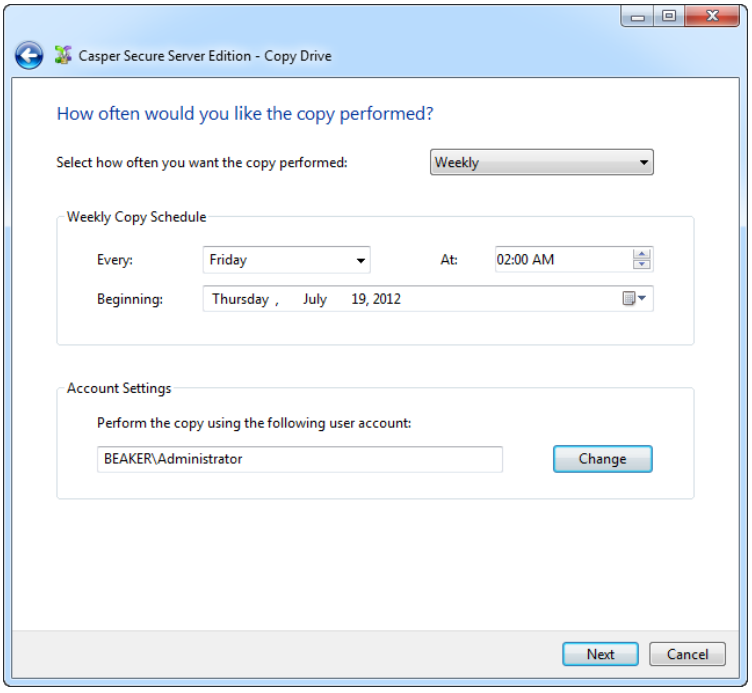


Simply clicking **Next** to accept the default selection or value is generally best. For additional help with making a selection, press **F1**.

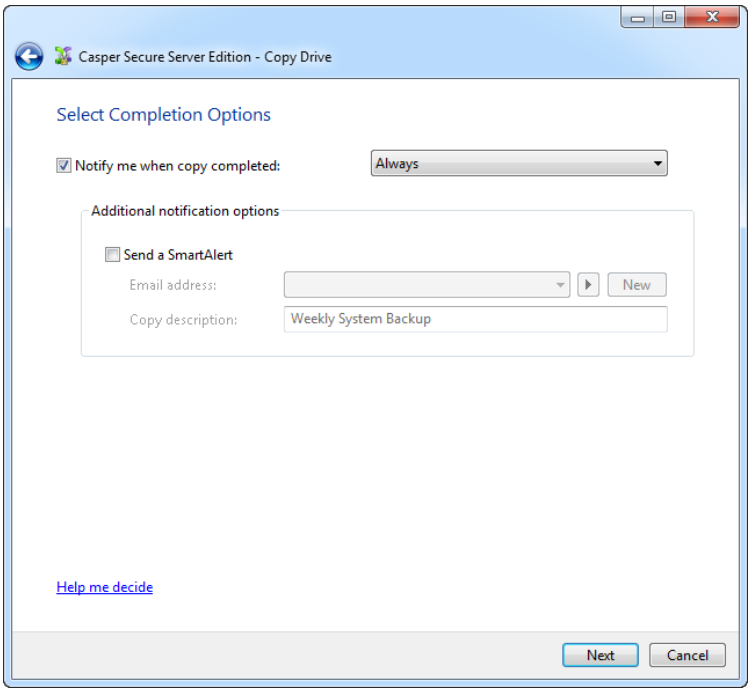
8. Click **Schedule the copy for later or routine basis**.



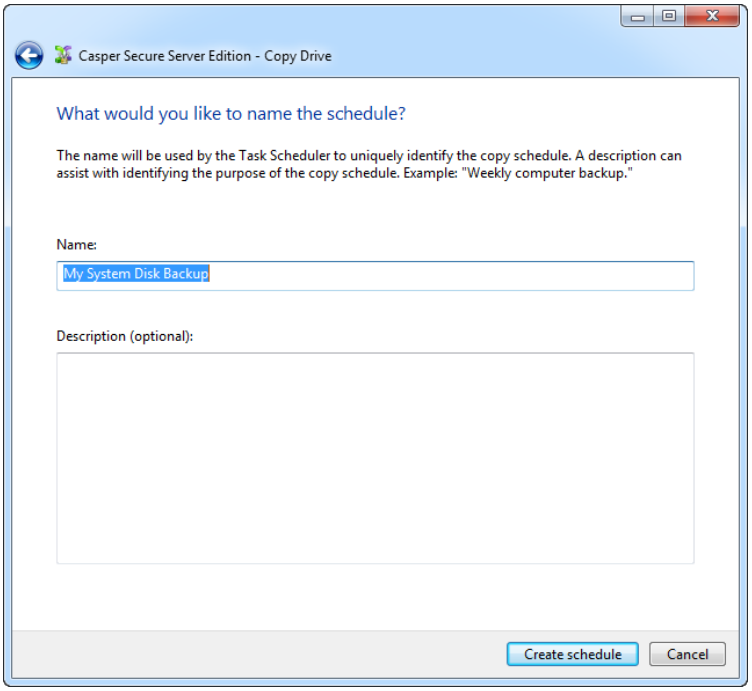
9. Select the schedule you would like Casper Secure to follow to maintain the backup, and click **Next**. For help with the schedule, press **F1**.



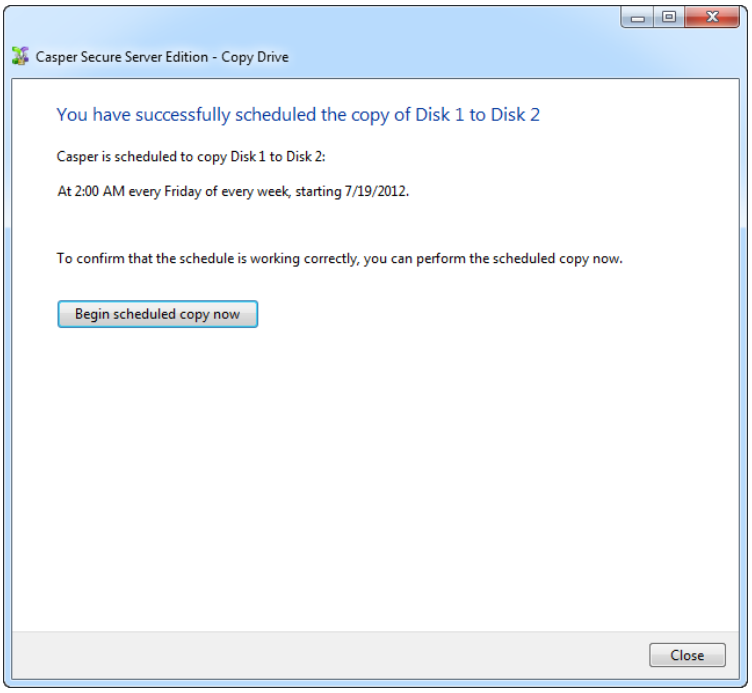
10. Select the desired completion options, and click **Next**.



11. Enter a name for the schedule, or retain the name suggested by Casper Secire, and then click **Create schedule** to add the backup schedule to your Windows Scheduled Tasks.



12. Click **Close** to return to the Casper Secure console.



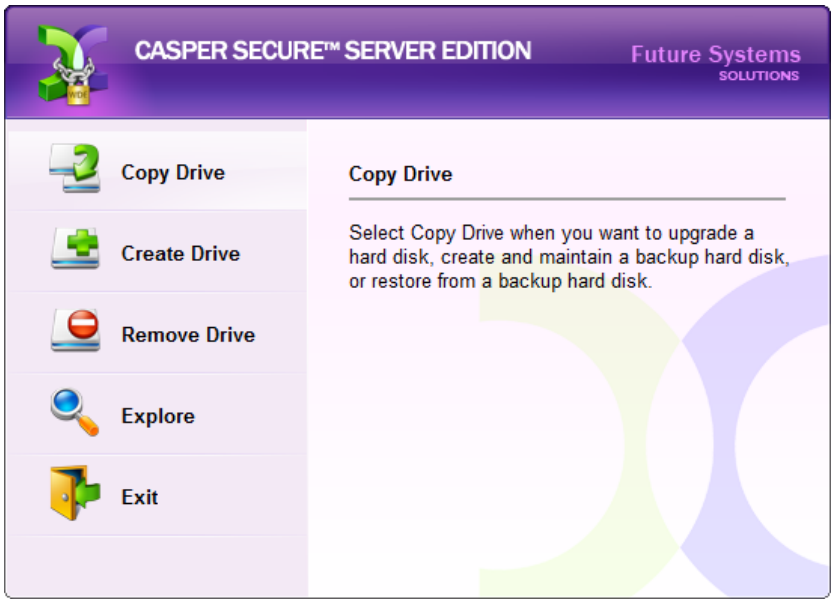
Example 5: Automating an External Backup

When using a portable drive such as an external USB or Firewire drive for a backup, you can configure Casper Secure to automatically perform a backup whenever you attach the backup drive.

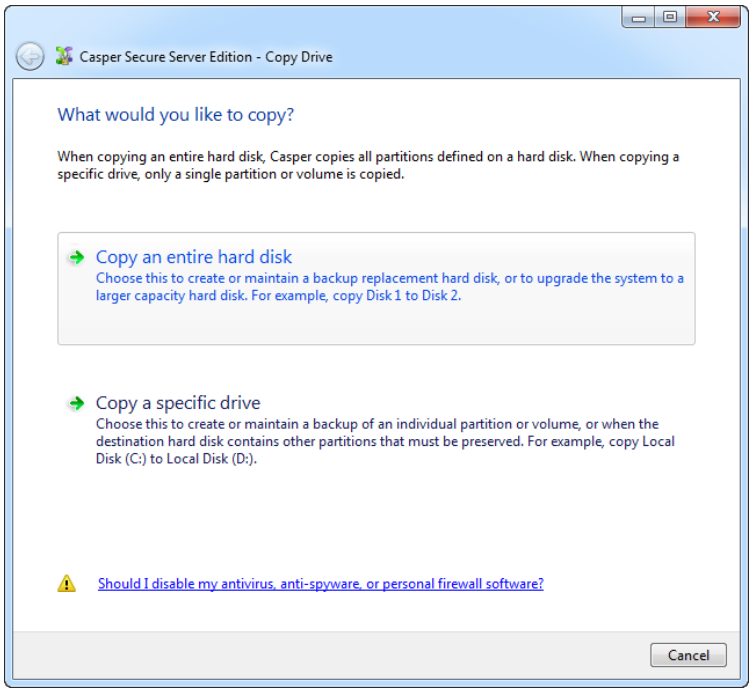
Configuring a SmartSense Backup

Assuming the external backup drive is currently attached to the system, the following procedure shows how to register the drive with the Casper SmartSense Service so that the backup will be started automatically whenever you attach the external backup drive.

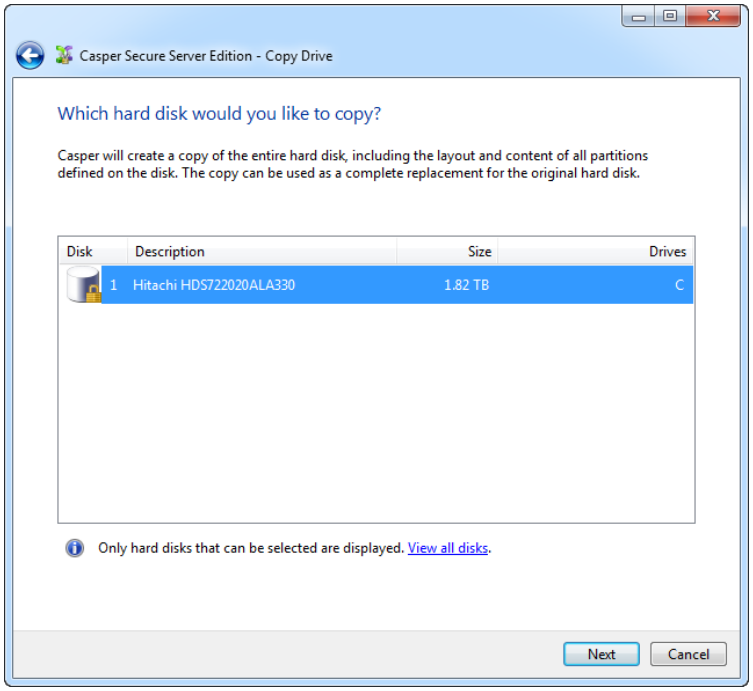
1. Select **Copy Drive**.



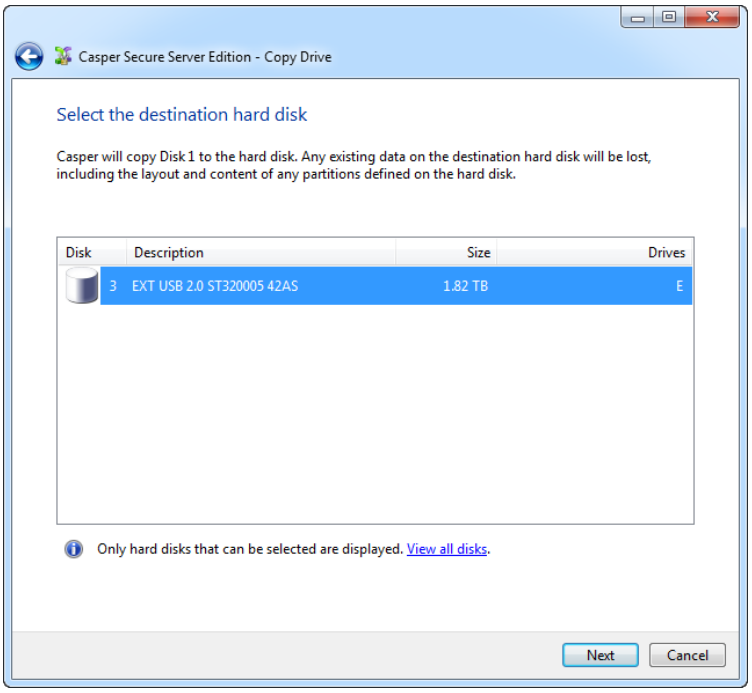
2. Select **Copy an entire hard disk**.



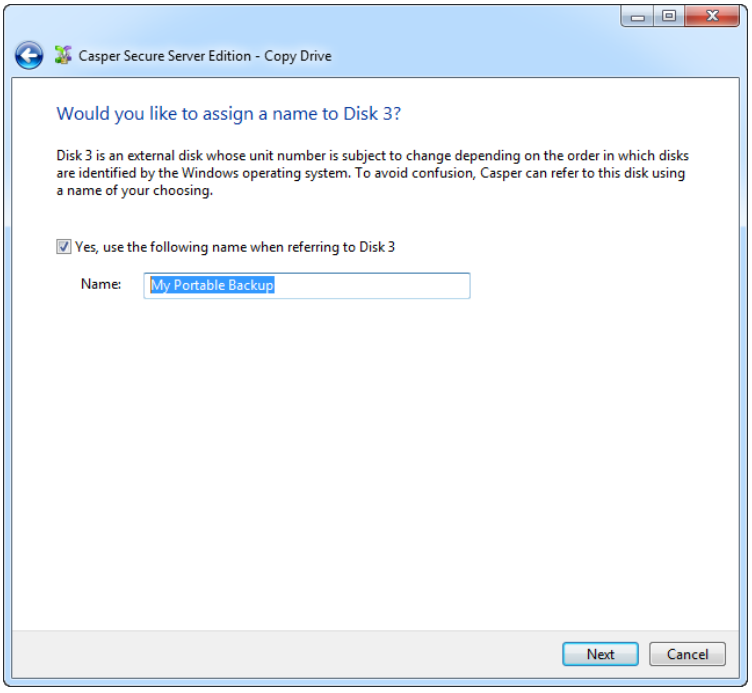
3. Select the disk device to backup as the hard disk to copy, and click **Next**.



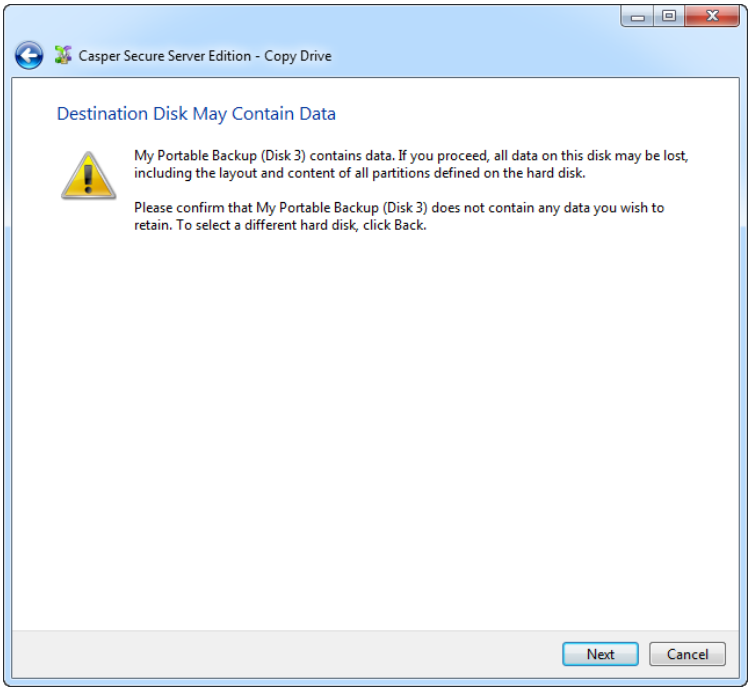
4. Select the external backup disk as the destination, and click **Next**.



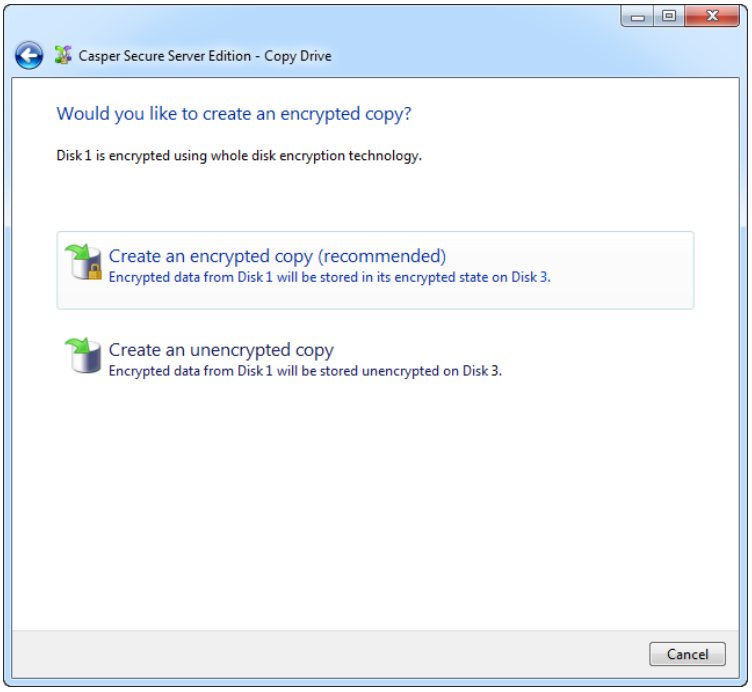
5. When selecting an external hard disk as the destination, Casper Secure will prompt you to assign a name to the disk. A name is optional. If you use multiple external hard disks, a name can make it easier to identify which external hard disk is being used for a Casper Secure backup. Click **Next** to proceed.



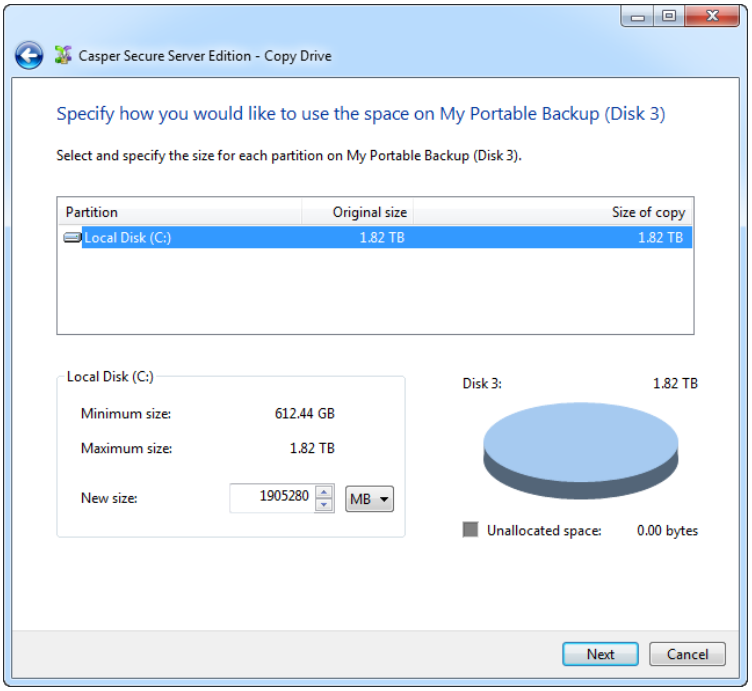
6. If the selected destination disk defines a partition or contains data, Casper Secure will warn you that the contents will be overwritten. Confirm you have selected the correct disk to receive the backup, and click **Next** to proceed.



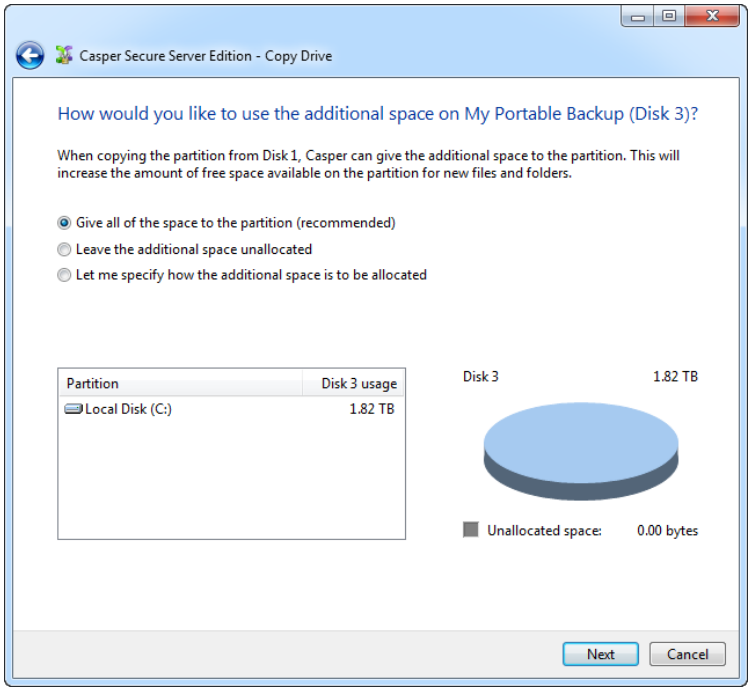
7. If the source disk device is encrypted using PGP whole disk encryption or BitLocker drive encryption, Casper Secure will offer the option of creating an unencrypted copy unless prohibited by administrative policy settings. Click **Create an encrypted copy**.



8. When prompted to specify how the space on the backup disk is to be used, retain the default selection and click **Next**. If the destination disk is the same size or smaller than the source disk device, Casper Secure will ask you to manually configure how the space is to be used.

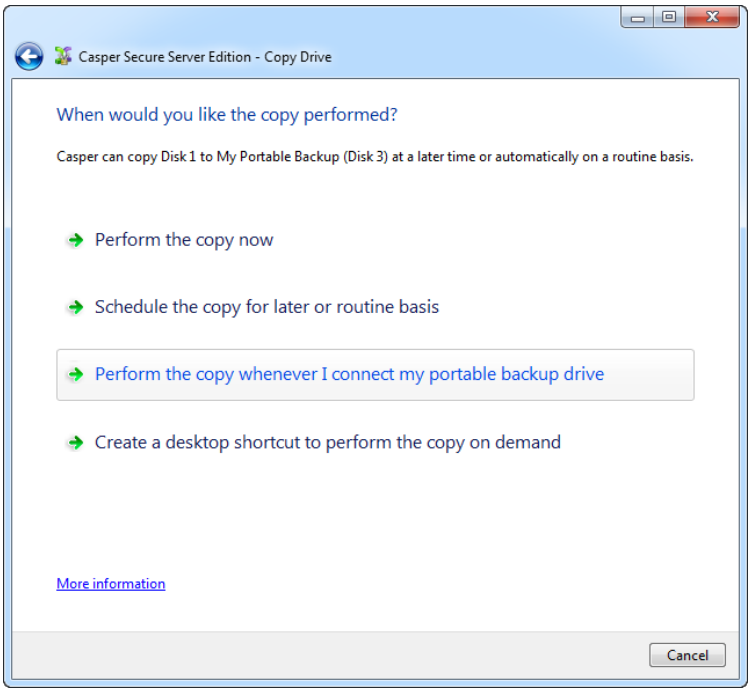


When the destination hard disk is larger than the source, the default option will be *Give all of the space to the partition*, or *Proportionally distribute the space to all partitions* when there is more than one partition defined on the source disk.

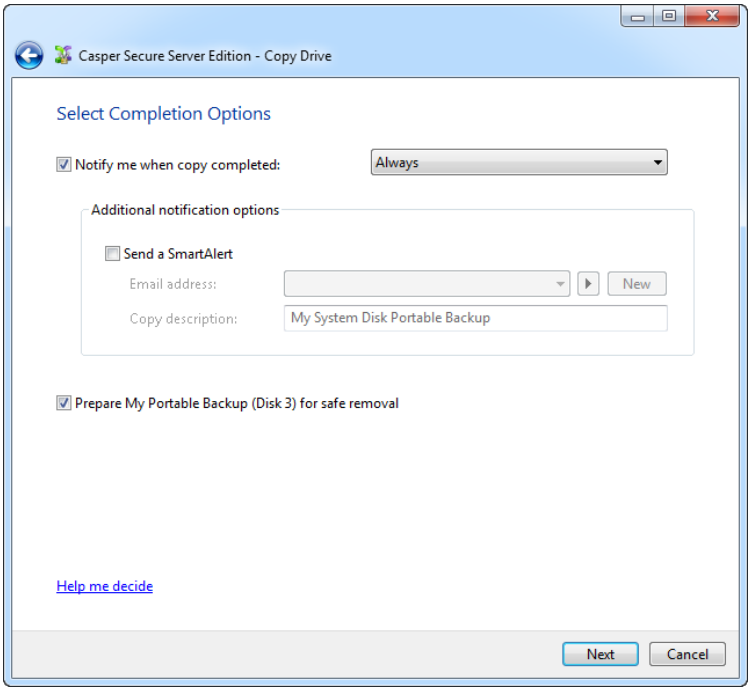


Simply clicking **Next** to accept the default selection or value is generally best. For additional help with making a selection, press **F1**.

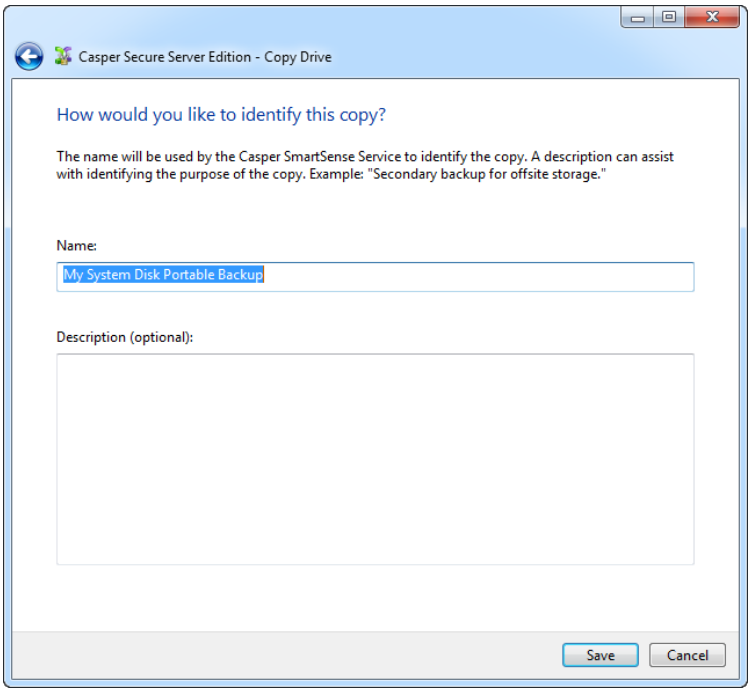
9. Click **Perform the copy whenever I connect my portable backup drive**.



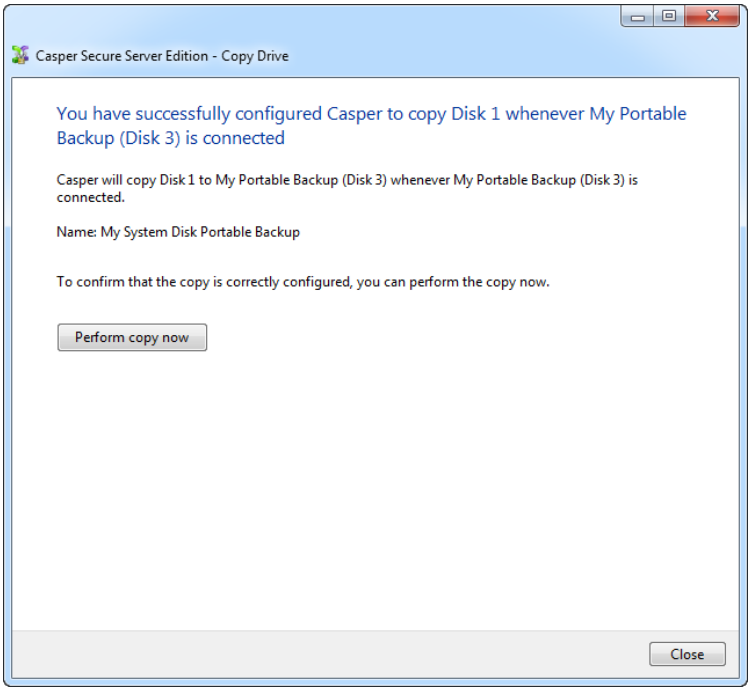
10. Select the desired completion options, and click **Next**.



11. Enter a name to uniquely identify the backup, or retain the name suggested by Casper Secure, and then click **Save** to register the backup with the Casper SmartSense Service.

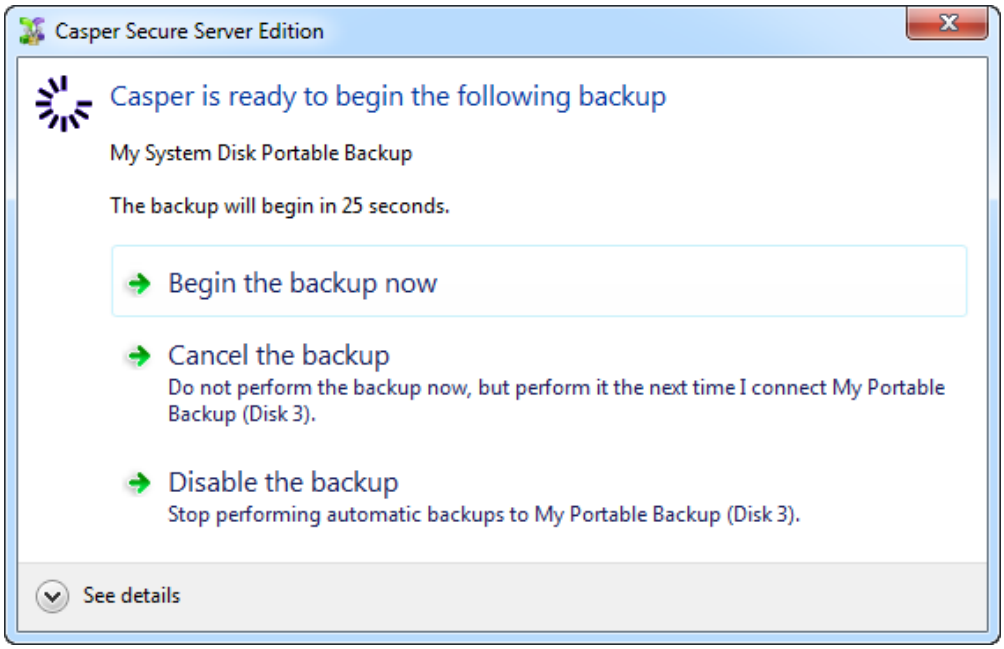


12. Click **Close** to return to the Casper Secure console.



Starting a SmartSense Backup

Once your portable backup drive has been registered with the Casper SmartSense Service, the backup can be started by simply attaching the portable drive to the computer.



The backup will start automatically after a short delay. You can begin the backup immediately by selecting **Begin the backup now**. Click **Cancel the backup** to skip the backup, or **Disable the backup** to skip the current backup and prevent future backups from beginning automatically.

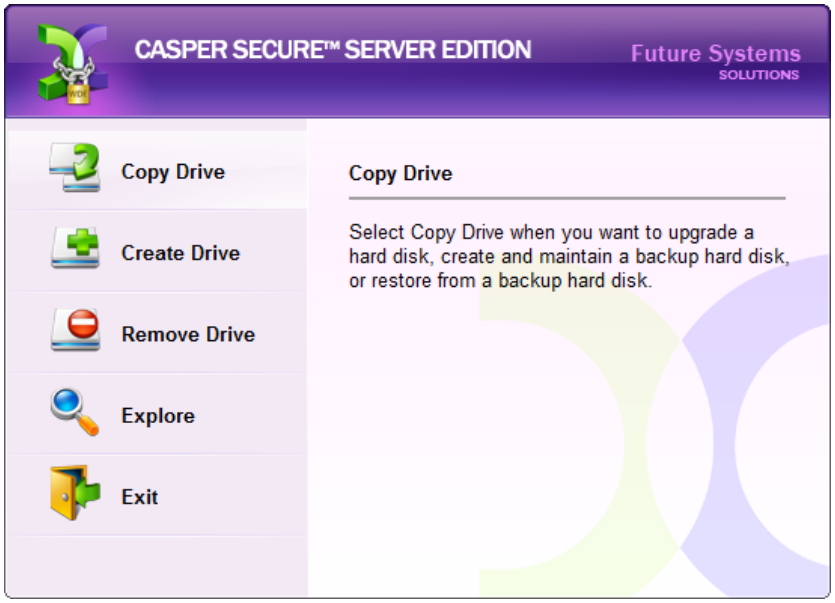
Example 6: Performing a Routine Backup On-Demand

You can create a 1-Click Cloning desktop shortcut to perform a routine backup on-demand.

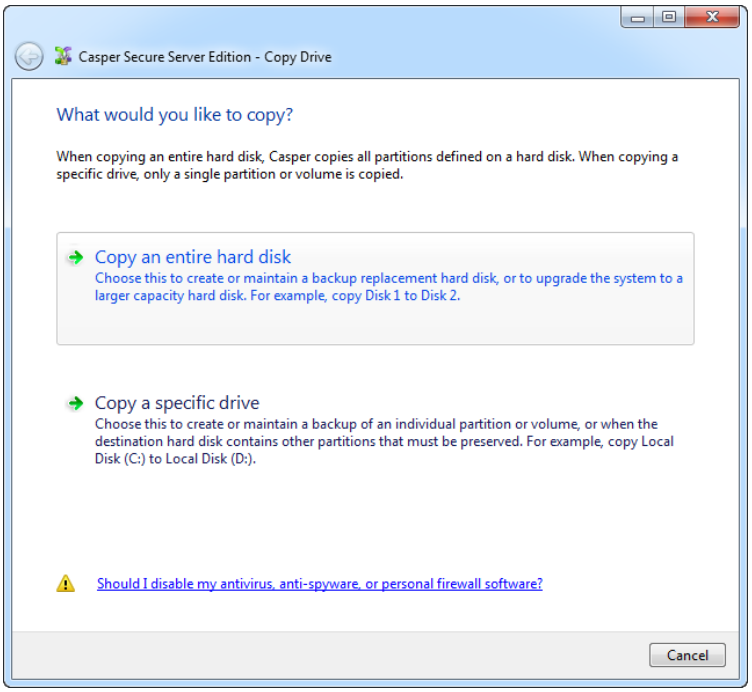
Creating a 1-Click Cloning Shortcut

Assuming the backup disk device is currently installed or attached to the system, the following procedure shows how to create a 1-Click Cloning Shortcut to perform a backup on-demand.

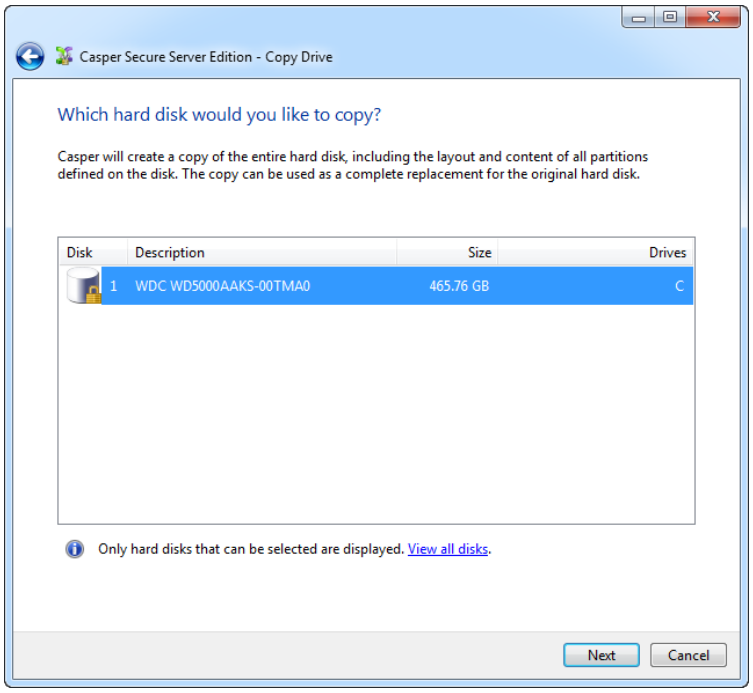
1. Select **Copy Drive**.



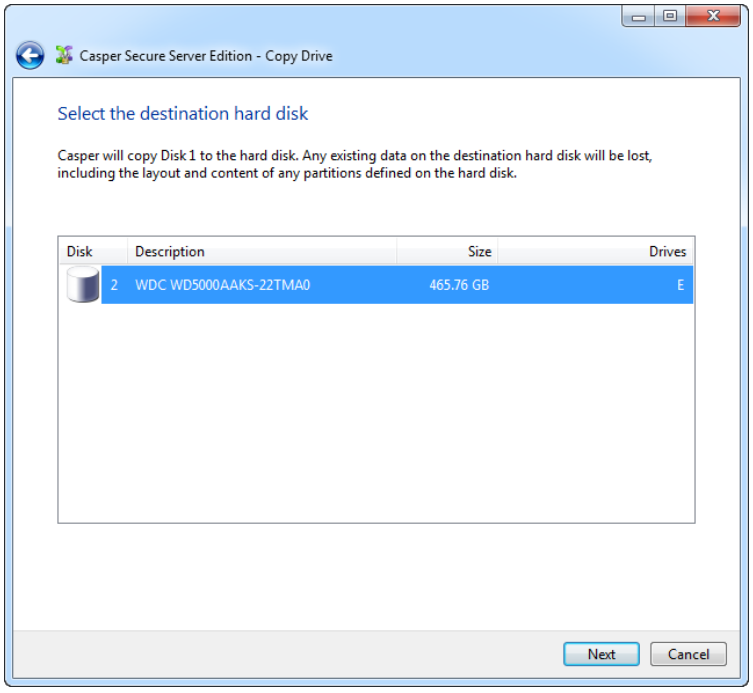
2. Select **Copy an entire hard disk**.



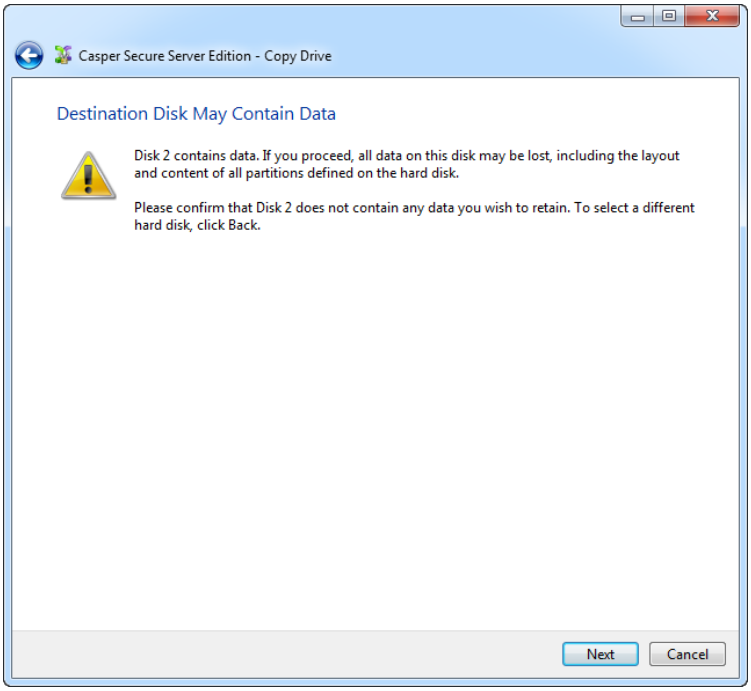
3. Select the disk device to backup as the hard disk to copy, and click **Next**.



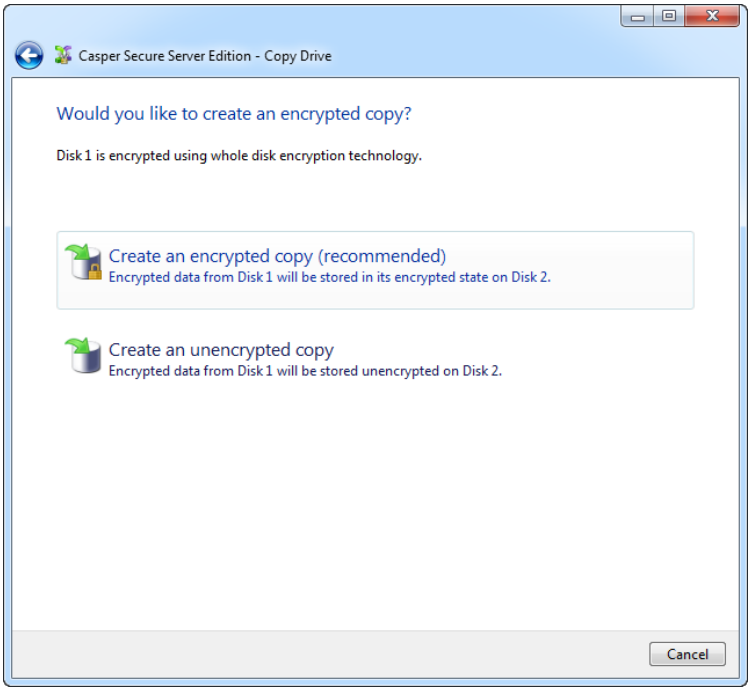
4. Select the backup disk device as the destination, and click **Next**.



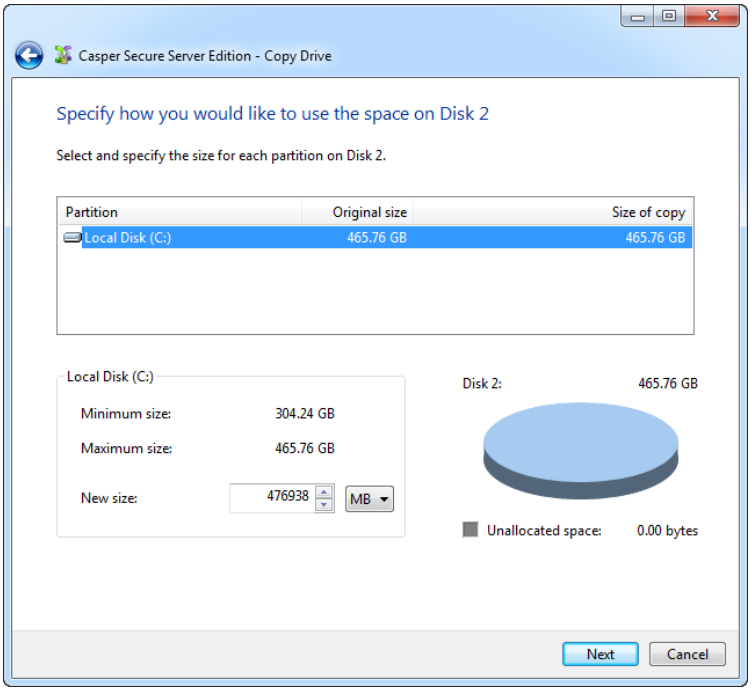
5. If the selected destination disk device defines a partition or contains data, Casper Secure will warn you that the contents will be overwritten. Confirm you have selected the correct disk device to receive the backup, and click **Next** to proceed.



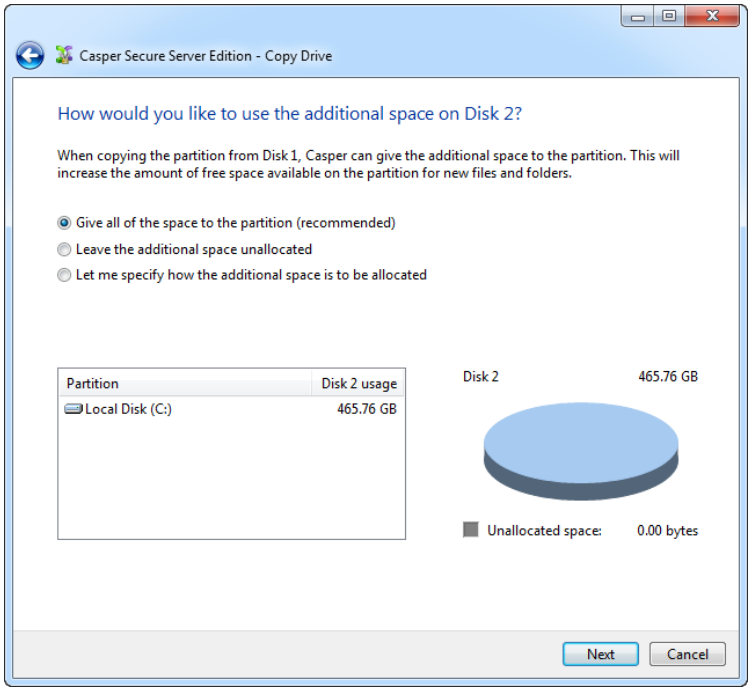
6. If the source disk device is encrypted using PGP whole disk encryption or BitLocker drive encryption, Casper Secure will offer the option of creating an unencrypted copy unless prohibited by administrative policy settings. Click **Create an encrypted copy**.



7. When prompted to specify how the space on the backup disk device is to be used, retain the default selection and click **Next**. If the destination disk device is the same size or smaller than the source disk device, Casper Secure will ask you to manually configure how the space is to be used.

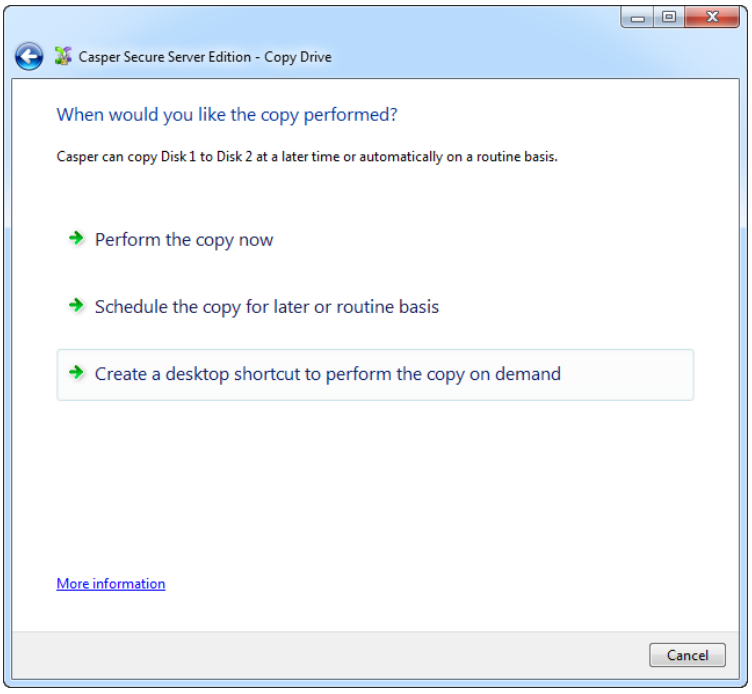


When the destination disk device is larger than the source, the default option will be *Give all of the space to the partition*, or *Proportionally distribute the space to all partitions* when there is more than one partition defined on the source disk device.

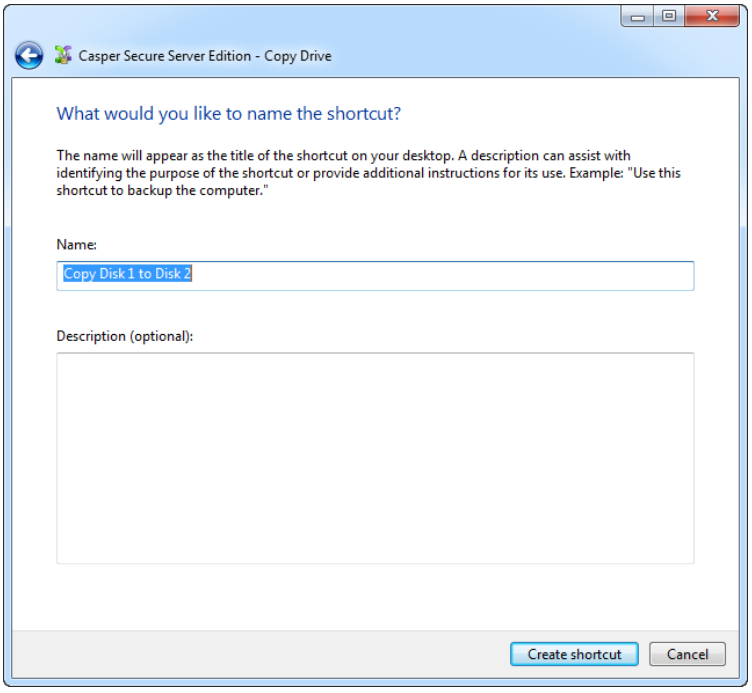


Simply clicking **Next** to accept the default selection or value is generally best. For additional help with making a selection, press **F1**.

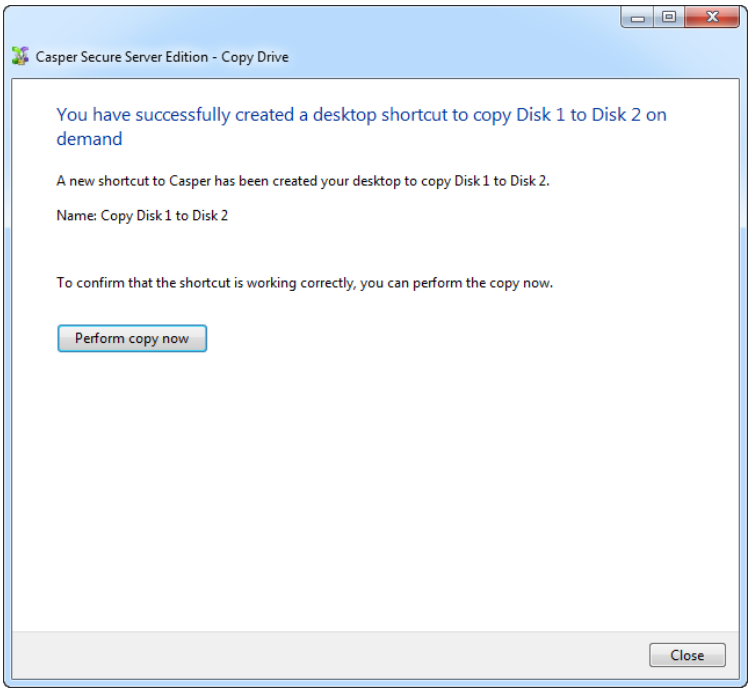
8. Click **Create a desktop shortcut to perform the copy on demand**.



9. Enter a name for the shortcut, or retain the name suggested by Casper Secure, and click **Create shortcut**.

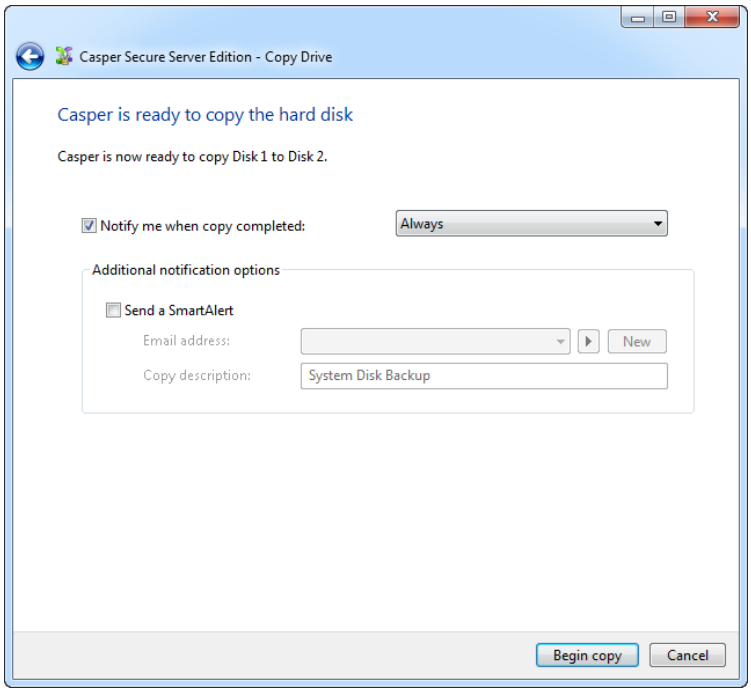


10. Click **Close** to return to the Casper Secure console.



Performing a 1-Click Cloning Backup

After creating a 1-Click Cloning shortcut, you can use the shortcut appearing on your desktop to begin the backup. Click **Begin copy** to start the backup.



Booting from a Backup Hard Disk

If you have used Casper Secure to create a backup of the server's system disk device, and this disk device fails or its contents become corrupted, you can boot the computer from the backup disk device.

When the backup disk device is installed as an internal hard disk or secondary RAID array, or when it is attached externally as an eSATA or USB device, booting from the backup disk device is accomplished by changing the computer's BIOS boot priority setting to designate the backup disk device as the preferred boot device. If the computer's BIOS does not offer an option to select the designated backup disk device as the preferred boot device, or if the original disk device fails completely, the backup disk device is reconfigured to replace the original disk device.

> **NOTE:** For a hard disk attached as an external USB device, booting from the backup hard disk may require the selection of additional BIOS options to completely enable booting. By default, some BIOS implementations disable USB boot support, or have it configured for floppy or ZIP drive emulation rather than hard disk drive (HDD) emulation. *If the computer's BIOS does not support booting from external USB hard disk type devices, the backup hard disk must be removed from its external enclosure and installed as a replacement for the internal system disk device in order to boot from it.* Alternatively, a restore may be performed by using the Casper Secure Startup Disk to copy the external backup hard disk to the computer's internal system disk device. For more information about creating and using the Casper Secure Startup Disk, please see the **Startup Disk Creator Guide**.