CASPER SECURE™

SERVER EDITION

USER GUIDE

v6.0

Future Systems SOLUTIONS

Copyright and Trademark Information

Information in this document is subject to change without notice. Federal law prohibits unauthorized use, duplication, and distribution of any part of this document in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Future Systems Solutions.

Future Systems Solutions may have patents, trademarks, copyrights, or other intellectual property rights covering subject matter in this document.

Copyright © 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

Casper, the Casper logo, Casper Secure, the Casper Secure logo, Drive2Drive, SmartClone, SmartWrite, AccuClone, SmartAlert, SmartSense, SmartStart, SmartRestore, 1-Click SmartStart, and 1-Click Cloning are trademarks or registered trademarks of Future Systems Solutions, Inc. BitLocker, Microsoft, Windows, and Windows Vista are trademarks or registered trademarks of Microsoft Corporation. Symantec and PGP are trademarks or registered trademarks of Symantec Corporation. Other brand and product names may be trademarks or registered trademarks of their respective holders.

Table of Contents

Introduction **5**

Getting Started **7**

System Requirements **7**

Installing Casper Secure **8**

Starting Casper Secure **8**

Getting Help **8**

Using Casper Secure **9**

Bootable Backups **9**

Restore-Point Backups **10**

Choosing a Backup Type **11**

Comparison of Bootable Backups and Restore-Point Backups **11**

Creating and Maintaining a Bootable System Backup **12**

Example 1: Creating a Bootable Backup **13**

Example 2: Updating a Bootable Backup **19**

Example 3: Automating a Bootable Backup **22**

Example 4: Automating a Bootable Backup to a Portable Device **25**

Configuring a SmartSense Backup 25

Starting a SmartSense Backup 28

Example 5: Performing a Bootable Backup On-Demand **29**

Creating a Desktop Shortcut for a Bootable Backup 29

Performing a Bootable Backup On-Demand 31

Creating and Maintaining a Restore-Point System Backup **32**

Example 6: Creating a Restore-Point Backup **33**

Example 7: Updating a Restore-Point Backup **37**

Example 8: Automating a Restore-Point Backup **40**

Example 9: Automating a Restore-Point Backup to a Portable Device **43**

Configuring a SmartSense Backup 43

Starting a SmartSense Backup 46

Example 10: Performing a Restore-Point Backup On-Demand **47**

Creating a Desktop Shortcut for a Restore-Point Backup 47

Performing a Restore-Point Backup On-Demand 49

Testing a System Disk Backup **50**

Testing a Bootable Backup **50**

Testing a Restore-Point Backup **50**

© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

Testing with Bootable Image Recovery 50
Testing within a Virtual Machine 51
Example 11: Testing the Latest Restore-Point within a VM 52
Example 12: Testing a Specific Restore-Point within a VM 54

Recovering from a System Disk Failure 57
Booting from a backup 57
Restoring from a backup 57
System Recovery Options at a Glance 57
Booting from a System Backup 58
Booting from a backup hard disk 58
Booting from a restore-point 59
Restoring a System Backup 60
Example 13: Manually Restoring a Restore-Point Backup 61
Example 14: Manually Restoring a Bootable Backup 68

Retrieving Specific Files and Folders from a Backup 73
Example 15: Accessing the Contents of a Bootable Backup 74
Example 16: Accessing the Contents of a Restore-Point Backup 77

Upgrading a Hard Disk 82
Example 17: Upgrading a Hard Disk 82

© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved. January 2025

Introduction

Casper Secure™ Server Edition is a disk cloning, imaging and backup solution designed specifically for Windows® servers using full drive encryption technologies for security and compliance. Whether you need to upgrade an encrypted server with a new disk to increase speed or storage capacity, replace a failed disk, or maintain an instantly bootable backup for rapid recovery, Casper Secure Server Edition is designed to make the process extraordinarily fast and easy while ensuring 100% compliance with all data security protocols and requirements.

Casper Secure Server Edition offers you these unique advantages:

- **Designed Specifically for Windows™ BitLocker™ and Symantec™ (PGP™) Drive Encryption Technologies** — Casper Secure completely eliminates the unnecessary downtime and security and compliance risks associated with other backup and recovery products. *With Casper Secure, data is never placed in an exposed or unencrypted state — all data remains in its original encrypted state during and after backup and recovery.*
- **Fast, Complete Encrypted Backups** — Casper Secure creates a complete, fully-encrypted backup of an encrypted drive with all encrypted data in its *original* encrypted state. Everything remains encrypted throughout the process, so you can avoid the arduous and lengthy decryption and encryption steps that are required with other drive imaging and backup solutions.
- **Rapid, Fully-Encrypted Recovery** — Casper Secure completely eliminates the separate data restoration and re-encryption steps required by other drive imaging and backup solutions. Whether you need to recover a single file or a server's entire system drive, recovery could not be faster or easier. You have complete and immediate access to all of the data on the backup; there are no additional passwords or exotic procedures to follow.
- **Bootable Backups Provide Instant Recovery** — Casper Secure can turn virtually any drive into an instantly bootable encrypted backup drive that can be used to boot and run the server in an emergency. If server's encrypted system drive should fail, simply restart the server to a Casper Secure Bootable Backup or remove the failed drive and replace it with the Casper Secure Bootable Backup. Either way, the server can be up and running again in minutes, eliminating a day or more of unnecessary downtime.
- **Restore-Point Backups Provide Selectable Point-In-Time Recovery** — A Casper Secure Restore-Point Backup stores a complete image of the servers encrypted system drive that you can be used to restore selected files and folders or the server's entire system drive to a previous point in time. Multiple Casper Restore-Point Backups can be stored on a single backup drive and can be restored directly to their original encrypted state without ever putting data at risk or requiring a separate, time-consuming data re-encryption step. SmartRestore™ technology makes recovery as easy as booting to a Casper Restore-Point Backup drive.
- **Ensures Compliance with Existing Security Directives** — Since all data remains in its original encrypted state during and after backup and recovery, Casper Secure maintains 100% compliance with all enterprise-wide data security directives and HIPAA requirements and completely eliminates the security and compliance risks associated with other backup and recovery solutions. With Casper Secure there are no new passwords to manage or

© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

separate security protocols or encryption technologies to vet, and more importantly, there are never any security gaps created during or after backup or recovery.

- **Reliability Assured with Verifiable Recovery** — Advanced data verification technology ensures data has not been compromised during the imaging process by faulty RAM, a defective cable, failing disk or bad controller interface. In addition, all Casper Secure system backups are immediately bootable. You can even quickly boot and test a system image backup in a VM for added peace-of-mind at any time.
- **Quick and Easy System Drive Upgrades and Replacements** — Casper Secure can quickly clone an encrypted drive or hardware RAID array to another without requiring a laborious, time consuming and unsecure backup, restore, and re-encryption process. Casper Secure supports all SAS, SCSI, SATA, ATA/IDE, and hardware RAID configurations, including solid state devices and sold state arrays, and it will automatically resize partitions during the cloning process to ensure rapid migration and full use of the larger disks and arrays.

© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

Getting Started

This User Guide is intended to provide you with an overview of the basic operations of Casper Secure. Additional information regarding Casper can be found in the help file or in one of the following supplementary guides:

Casper Secure SmartStart™ Guide: This guide provides an overview of Casper SmartStart. You should refer to this guide when you want to maintain a complete backup for a server's system disk or when you want to replace the server's system disk with a new disk to increase speed or storage capacity.

Casper Secure SmartRestore™ Guide: This guide provides an overview of Casper SmartRestore. You should refer to this guide when you need to restore a backup.

Casper Secure Startup Disk Creator Guide: This guide provides instructions for creating a Casper Secure Startup Disk, which may be required to restore a backup to the server's system drive.

System Requirements

- Windows Server 2025, Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, Windows 10, Windows 8.x, Windows 7, or Windows Vista[1]
- Windows BitLocker Drive Encryption[2], Symantec Endpoint Encryption (SEE), Symantec Encryption Desktop (SED) version 10.x, or PGP Desktop version 9.6x or later[3]
- 500MB available disk space
- 512MB RAM (1GB or more recommended)
- Backup device (additional internal or external hard disk drive)

[1] Casper Secure Server Edition is not designed for use with Windows Server for Itanium-based systems or Windows NT. Disk image file backups are supported only when running on Windows Server 2008 and later or when booting and running from the Casper Secure Server Edition Startup Disk. The VHDX image file format is supported only when running on Windows Server 2012 and later or when booting and running from a Casper Secure Server Edition Startup Disk created with the Windows 8.x ADK or later. Bootable image recovery is supported only on Windows Server 2008 and later with unencrypted images. Testing a restore-point backup within a virtual machine is supported only when running on Windows Server 2012 and later. Booting from a USB connected hard disk requires a computer with BIOS or UEFI firmware support for booting from USB hard disk drive (USB-HDD) devices. Not all computers support booting and running from USB hard disk type devices. Some computers equipped with both USB 3.0 and USB 2.0 ports will support booting only when the device is connected to a USB 2.0 port.

[2] Windows BitLocker Drive Encryption is currently supported only for drives using software encryption that have been formatted with the NTFS file system. BitLocker hardware encrypted drives and BitLocker encrypted drives that are formatted with the FAT file system can be copied only in their unencrypted state.

[3] Encrypted cloning and imaging is currently supported only for drives encrypted with software-based drive encryption. Self-encrypting drives (SED), including Opal compliant and Windows BitLocker eDrive compliant drives, may be copied in their encrypted state only when software encrypted.

© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved. January 2025

Installing Casper Secure

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.

1. Start the **Casper Secure Server Edition Setup** program
2. Read the **License terms and conditions** and then check **I agree to the License terms and conditions**
3. Click **Install**
4. Click **Finish** to close the Casper Secure Setup Program

Starting Casper Secure

In Windows Server 2016 and later, follow this procedure:

1. Click the **Start** button.
2. Click **Casper Secure 6.0 Server Edition**.

In Windows Server 2012, select **Casper Secure 6.0 Server Edition** from the Windows **All Apps** screen. In Windows Server 2008 R2 and earlier versions, follow this procedure

1. Click the **Start** button.
2. Click **All Programs**.
3. Click **Casper Secure 6.0 Server Edition**.

Getting Help

For additional assistance, including troubleshooting information, please refer to the online help included with the program. To access help when running Casper Secure, select the **Help** menu or press **F1**.

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

© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved. January 2025

Using Casper Secure

Casper 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 you use Casper to clone a disk, Casper creates a snapshot, representing a single point-in-time view of the disk, and then copies it to another disk. The result is another disk that can be used as an immediate and complete replacement for the original disk.

When you use Casper to create an image of a disk, Casper creates a snapshot of the disk and then copies it to a file. The result is a file representing a point-in-time image of the disk, which can be used later to restore the disk to the same state it was in when the image was created.

Casper SmartSense™ technology will begin the process of upgrading or creating a backup of the system disk automatically when you attach a new 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 SmartStart™ to begin the process. For more information about using Casper SmartStart to upgrade or maintain a backup of a Windows server system disk, please refer to the **Casper SmartStart Guide**.

To upgrade or maintain a backup for another disk on the server, or customize the upgrade or backup process of the system disk, you should refer to this Casper User Guide or the Casper Help file included with the Casper program. See **Getting Help** for more information.

You can use Casper to maintain bootable backups and restore-point backups for a server. Both provide unique recovery capabilities that you should consider before proceeding.

Bootable Backups

A bootable backup represents a separate backup device that you can use to temporarily boot and run the server in an emergency or that you can use as an immediate and permanent replacement for the server's system disk device. A bootable backup is sometimes referred to as a clone backup because it maintains a duplicate copy ("clone") of the system disk device.

Bootable backups provide the advantage of instant recovery because a separate data restoration process is unnecessary. Recovery is simply a matter of restarting the server from the bootable backup. For example, if the server's system disk device fails or becomes corrupted, you can permanently replace it with the bootable backup or temporarily change the server's boot sequence to designate your bootable backup as the preferred boot device.

Bootable backups also provide you with immediate access to all of the files and data. For example, you can use Windows File Explorer to retrieve a specific file or folder directly from the backup without having to separately mount the backup or extract files or folders from the backup.

Because a bootable backup represents a single, point-in-time copy of the Windows system disk device, it provides you with the ability to recover only a single point-in-time. For example, the backup will contain only those files and folders that were present on the server's system disk device when the backup was created or last updated. Each time you update a bootable backup, the prior contents of the backup are replaced with the current contents of the system disk device.

Using two or more separate disk devices to maintain additional bootable backups in a backup rotation is necessary when additional point-in-time backups are desired. This practice is also

© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved. January 2025

recommended to provide redundancy from backup corruption, which can occur when a bootable backup is interrupted during an update.

When relying strictly on a bootable backup to protect a server, it is good practice to rotate the backup disk device between each successive backup. For example, if you update the bootable backup weekly, you might use two separate disks to maintain two independent bootable backups for the server. On the first week, you would back up the server to the first backup disk. On the second week, you would back up the server to the second backup disk. On the third week, you would back up the server to the first backup disk again, and so on. In this way, should a problem develop with one of the backups, you can still fall back to the older backup to recover.

Using Casper to create and maintain a bootable backup for a server requires another disk device large enough to accommodate all of the data on the server's current system disk device. A second internal hard disk, or one mounted in a removable (mobile) drive bay is ideal. If the server supports booting from eSATA or USB hard disk type devices, using an external hard disk for the backup is also a good option.

Restore-Point Backups

A restore-point backup represents a collection of separate backups stored on a single storage device that you can use to temporarily boot and run the server in an emergency, restore selected files and folders, or restore the server's system disk device to a previous point in time. A restore-point backup is also known as an image backup because it consists of one or more image files, each corresponding to the state of the system disk device at the time the image was created.

Because multiple restore-points may be maintained on a single backup device, restore-point backups provide additional recovery options that are not available when using a bootable backup. For example, if the server's system disk fails or becomes corrupted, you can restore the system disk device to any one of the restore-points you have created. Likewise, when only a specific file or folder needs to be restored, you can choose a specific restore-point from which to retrieve the file or folder.

Unlike a bootable backup, a restore-point backup will not overwrite or replace any other data stored on the backup device. For example, the backup device for a restore-point backup can be almost any disk, including a disk that already contains other data such as documents, separate database backups, etc.

Using Casper to create and maintain a restore-point backup for a server requires a storage device with free space that is at least several times greater than the amount of used space on the server's system disk device. An external USB or eSATA connected storage device with the prerequisite amount of free space is often ideal for maintaining restore-point backups. While the exact amount of free space depends on several factors, usually about three times the amount of used space on the server's system disk device is enough free space for Casper to create and maintain multiple restore-points for a restore-point backup. For example, if 150GB represents the current amount of used space on the system disk device, using a storage device with approximately 450GB of free space is generally sufficient to maintain a restore-point backup with a good variety of restore-points.

As with a bootable backup, when relying strictly on restore-point backups to protect a server, it is good practice to rotate the backup device between successive backups. This will help to ensure a viable backup exists in the event one of your backup devices suffers an untimely mechanical failure or data corruption, which might otherwise prevent you from restoring a backup.

© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved. January 2025

Unlike a bootable backup, recovery using a restore-point backup requires a separate restoration step. For example, you must first boot the server from the restore-point backup, the Casper Startup and Recovery Environment or a Casper Secure Startup Disk to perform the restore. When bootable image recovery has been configured for the backup device, you can temporarily boot the server directly from the restore-point backup and perform the restore. Alternatively, when the Casper Startup and Recovery Environment has been added to the backup device, you can boot the server directly from the backup device to perform the restore. In most instances, Casper's SmartRestore™ technology will fully automate the restoration process for you. To create and use a separate Casper Secure Startup Disk, please see the **Casper Secure Startup Disk Creator Guide**.

Choosing a Backup Type

For the greatest level of protection, maintaining a combination of bootable backups and restore-point backups on multiple devices in rotation is ideal. When this is not possible, the type of backup you choose to maintain will depend greatly on your specific situation and recovery needs. For a server whereby minimizing downtime is of utmost importance this may mean that maintaining two or more bootable backup disk devices in rotation might be preferable to a restore-point backup.

Comparison of Bootable Backups and Restore-Point Backups

	Casper Bootable Backup	Casper Restore-Point Backup
Contains a complete backup of the server's system disk?	Yes	Yes
Can be used to temporarily boot and run server if necessary?	Yes	Yes[4]
Can be used to permanently boot and run server?	Yes	No
Can be used to recover just one or more files?	Yes	Yes
Provides multiple restore points?	No	Yes
Type of storage device required	Dedicated internal or external hard disk device	Internal or external storage device
Other data can be stored on the backup storage device?	No. Backup completely replaces existing content of storage device.	Yes. Backups can coexist with other new and existing files and folders on storage device.
Size of storage device required	Large enough to accommodate all of the data currently on Windows system disk	Free space equal to three times the amount of used space on current Windows system disk

[4] Due to limitations with Windows native boot functionality, only unencrypted restore-point backups may be booted through bootable image recovery at this time.

© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

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 server's current system disk device.

A second internal hard disk or one mounted in a removable (mobile) drive bay is ideal. If the server supports booting from eSATA or USB hard disk type devices, using an external hard disk for the backup is also ideal.

The following examples illustrate various ways to create and maintain a bootable backup of a server's system disk device.

Example 1: Creating a Bootable Backup. This example demonstrates how to initialize a new disk or secondary RAID array for use as a complete backup replacement for the server's system disk device.

Example 2: Updating a Bootable Backup. This example shows how to manually update an existing bootable backup of the server's system disk device.

Example 3: Automating a Bootable Backup. This example illustrates how to fully automate a bootable backup.

Example 4: Automating a Bootable Backup to a Portable Device. This example shows how to automate a bootable backup maintained on a portable disk such as a USB, Firewire, or eSATA connected disk.

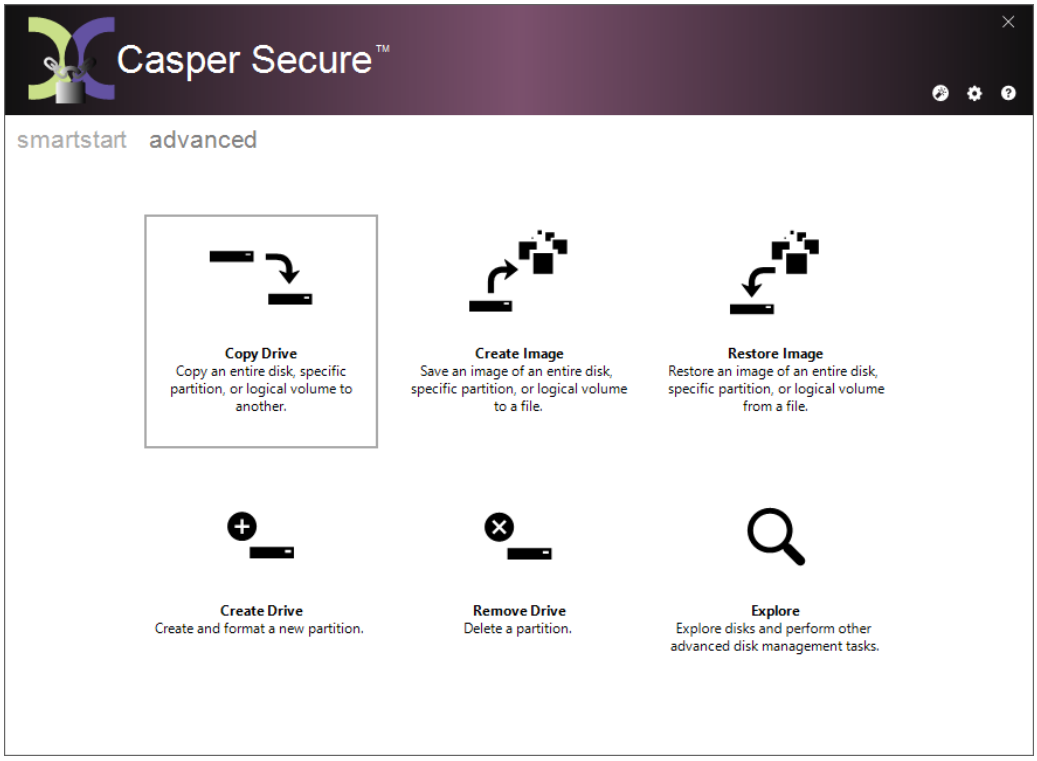
Example 5: Performing a Bootable Backup On-Demand. This example demonstrates how to create a desktop shortcut to maintain a bootable backup on-demand.

© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved. January 2025

Example 1: Creating a Bootable Backup

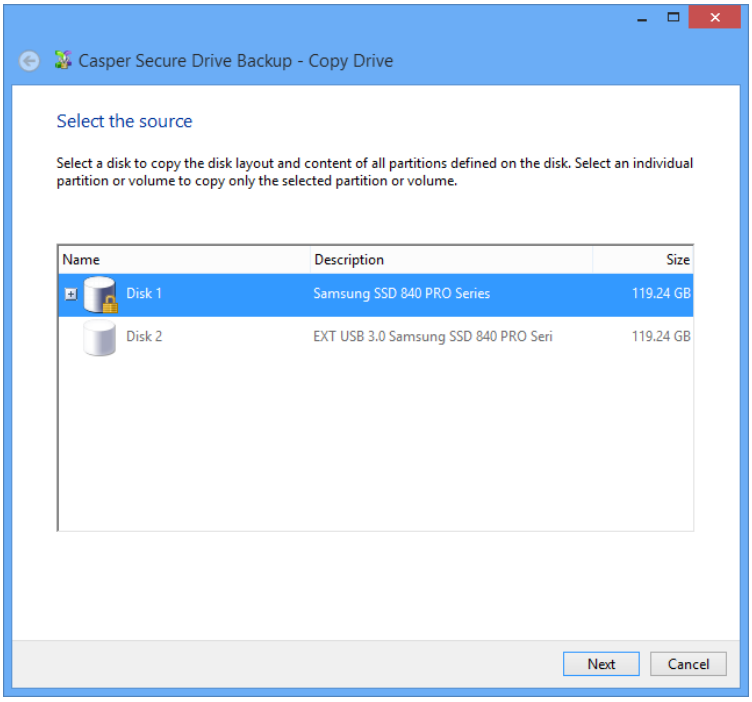
Assuming the backup disk device is currently installed or attached to the server, the following procedure illustrates how to clone the server's system disk device to the backup device to produce a bootable backup.

1. From the Casper console select the **Advanced** tab and then click **Copy Drive**.

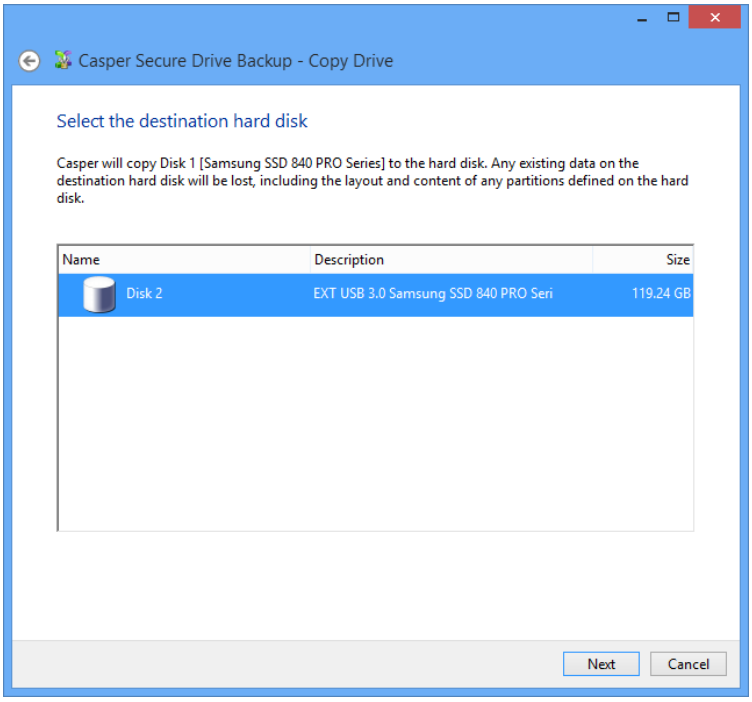


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

2. Select the disk device to backup (e.g., the hard disk or RAID array on which Windows Server is installed) as the source and click **Next**.

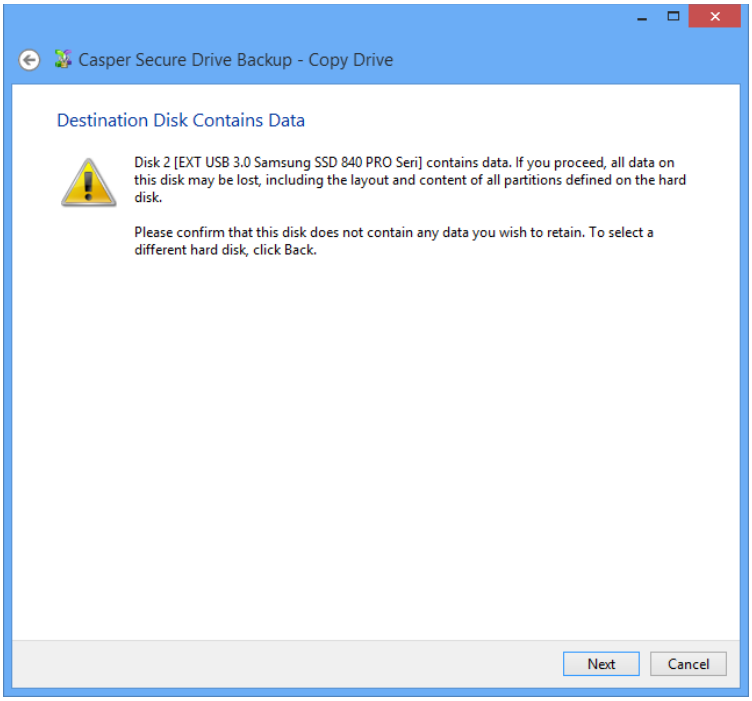


3. Select the backup disk device as the destination and click **Next**.

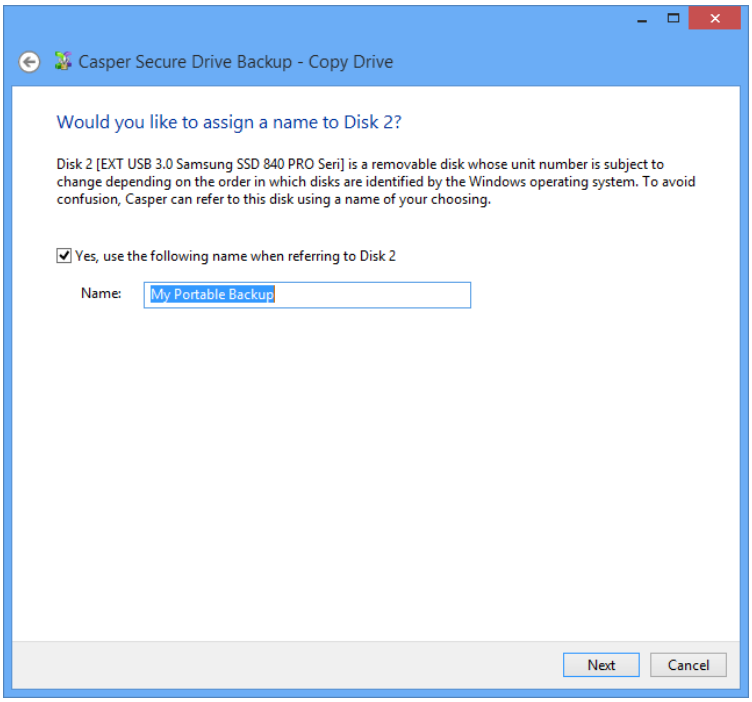


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

4. If the selected destination device defines a partition or contains data, Casper 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.

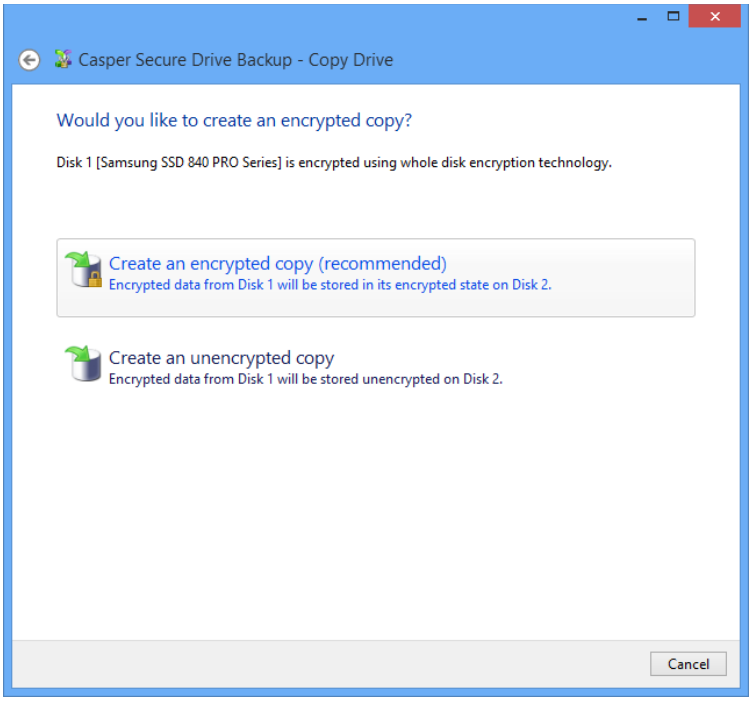


5. When selecting an external hard disk as the destination, Casper will prompt you to assign a name to the disk. A name is optional. If you use multiple external hard disks, a name can make it easier to identify which external hard disk is being used for a Casper backup. Click **Next** to proceed.

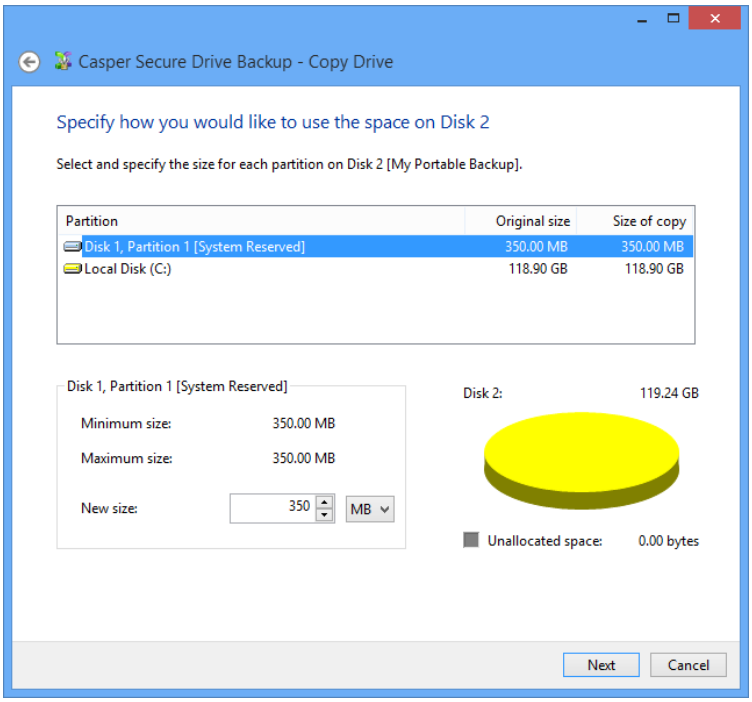


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

6. If the source device is encrypted using a supported drive encryption technology, Casper will offer the option of creating an unencrypted copy unless prohibited by administrative policy settings. Click **Create an encrypted copy**

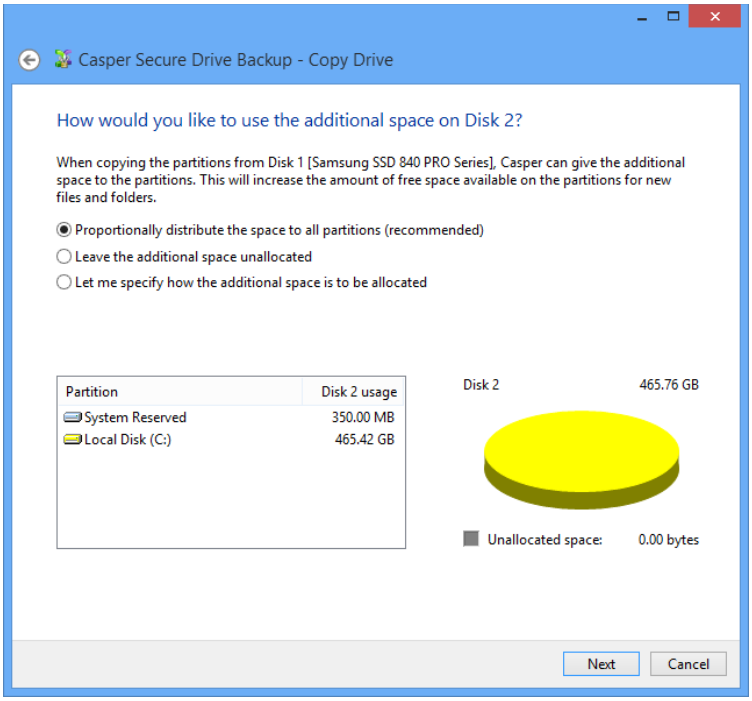


7. When prompted to specify how the space on the backup disk device is to be used, retain the default selection and click **Next**. If the destination device is the same size or smaller than the source device, Casper will ask you to manually configure how the space is to be used.



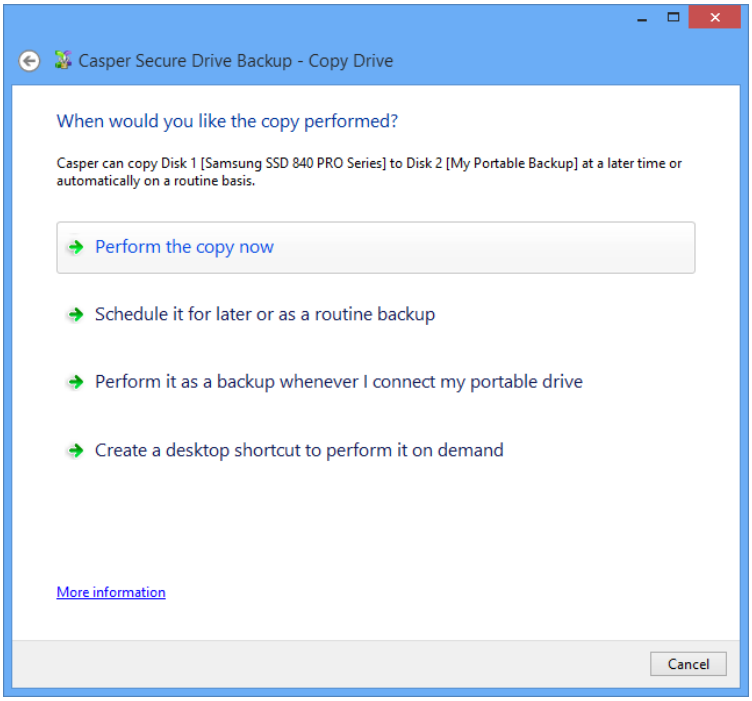
© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved. January 2025

When the destination 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* if there is more than one partition defined on the source device.



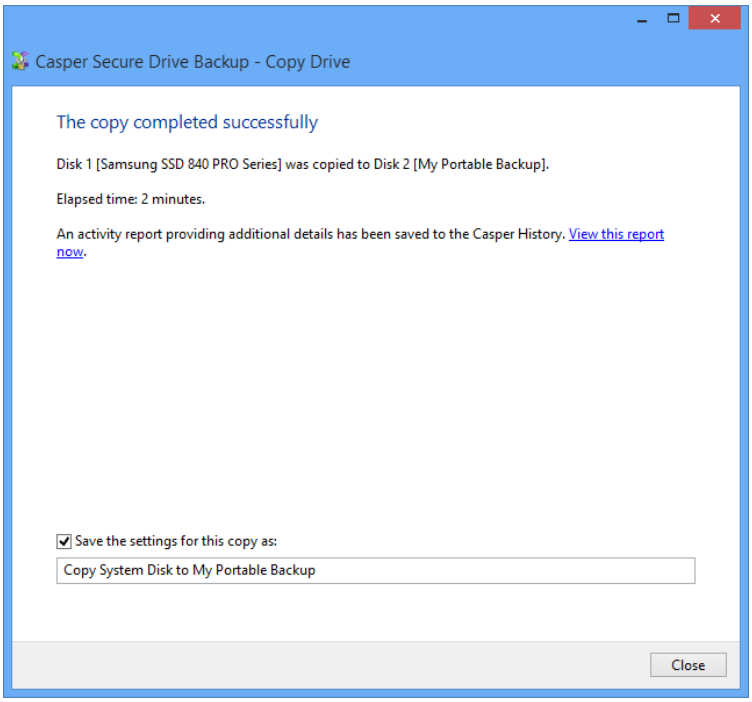
Simply clicking **Next** to accept the default selection or value is generally best. For additional help with making a selection, press **F1**.

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



© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

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

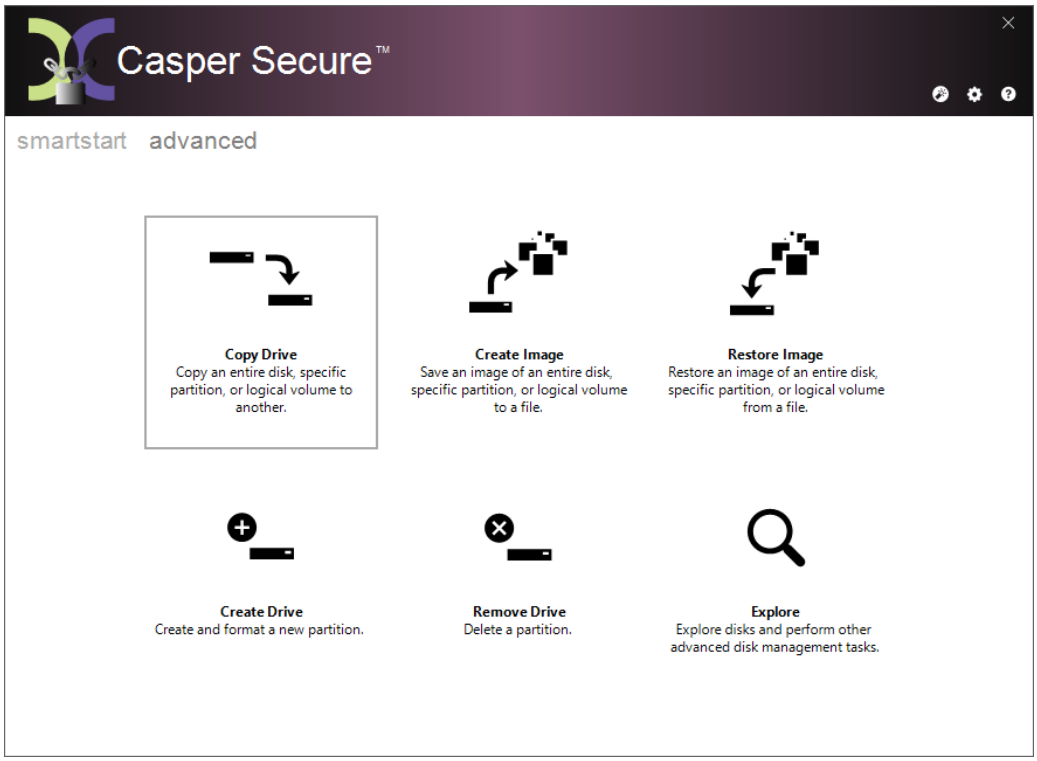


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

Example 2: Updating a Bootable Backup

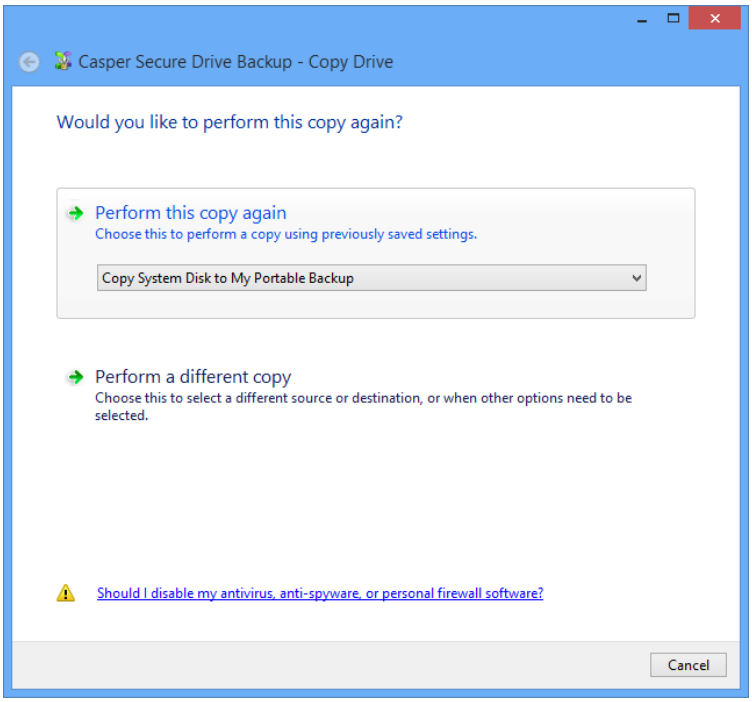
You can manually update a bootable backup by repeating the procedure used to create the backup. When the settings for the copy have been saved as shown in the final step of the preceding example, Casper makes this process even easier. Assuming the backup hard disk is currently installed or attached to the system, the following procedure illustrates how a prior copy may be quickly repeated to update an existing bootable backup.

1. From the Casper console select the **Advanced** tab and then click **Copy Drive**.

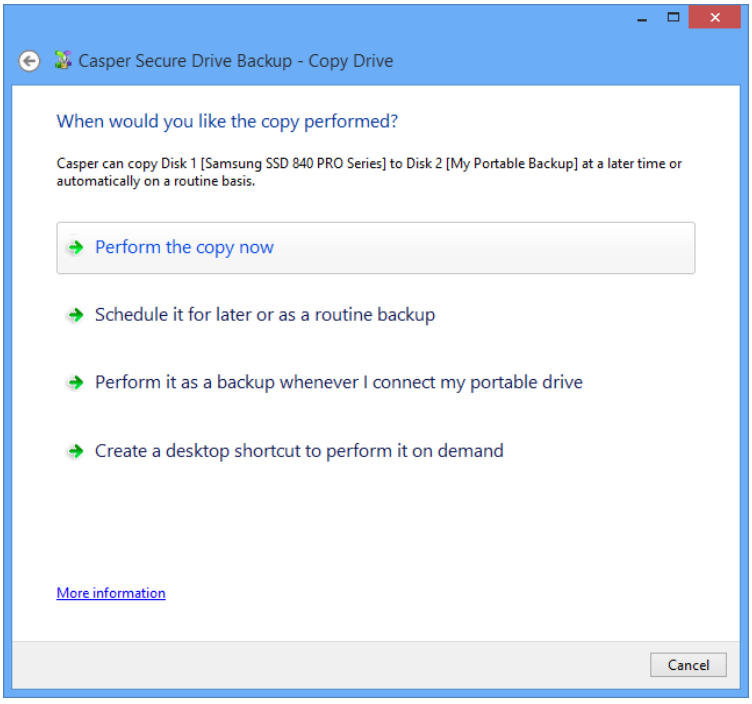


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

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

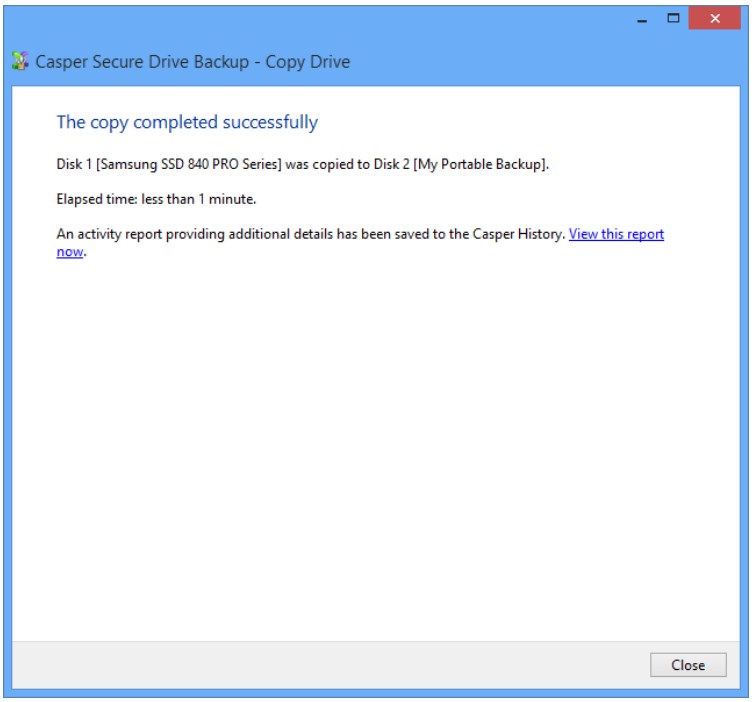


3. Click **Perform the copy now** to begin the cloning process.



© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

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

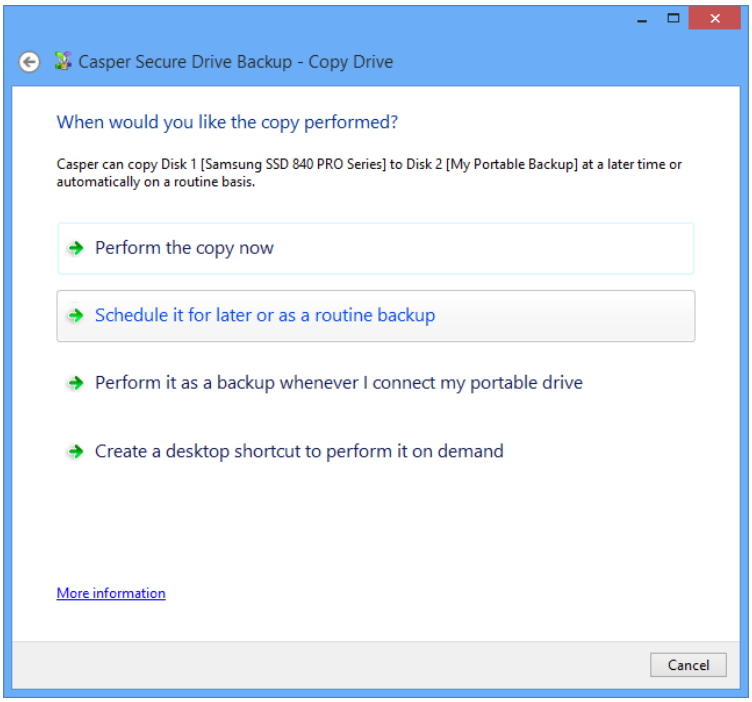


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

Example 3: Automating a Bootable Backup

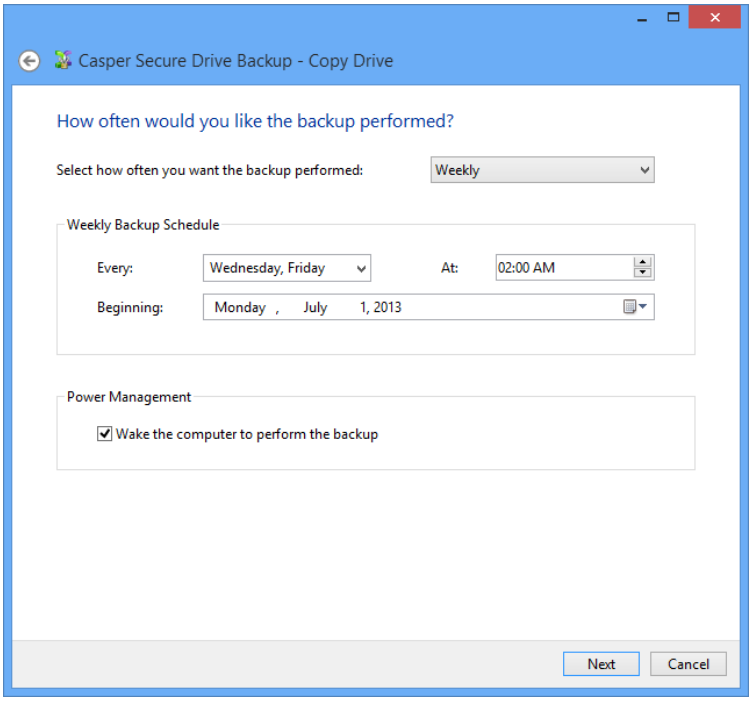
You can fully automate the process of creating and maintaining a bootable backup for a server by scheduling Casper to run on a routine basis. The procedure outlined below is the same whether you are performing an initial backup as demonstrated in Example 1 or updating an existing backup as demonstrated in Example 2.

1. When prompted by the Copy Drive wizard, click **Schedule it for later or as a routine backup**.

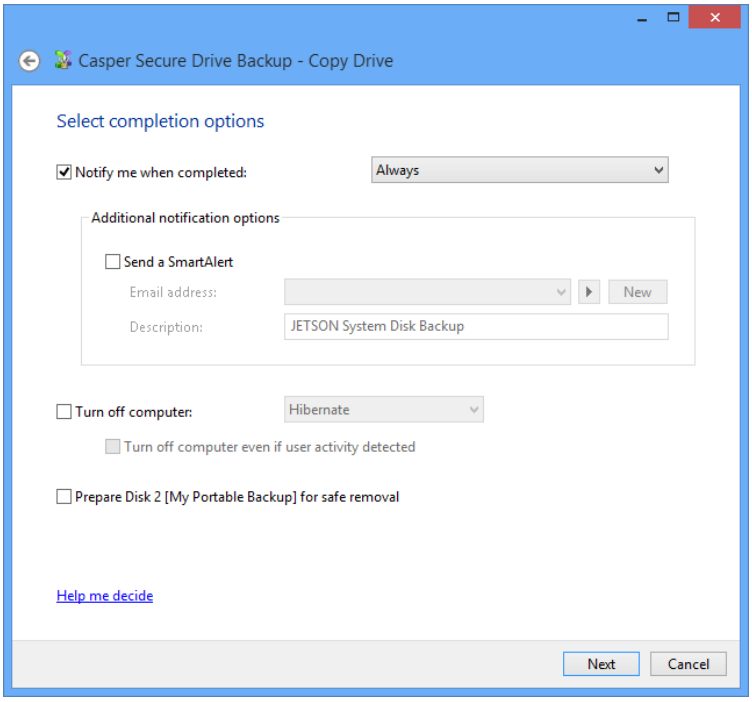


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

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

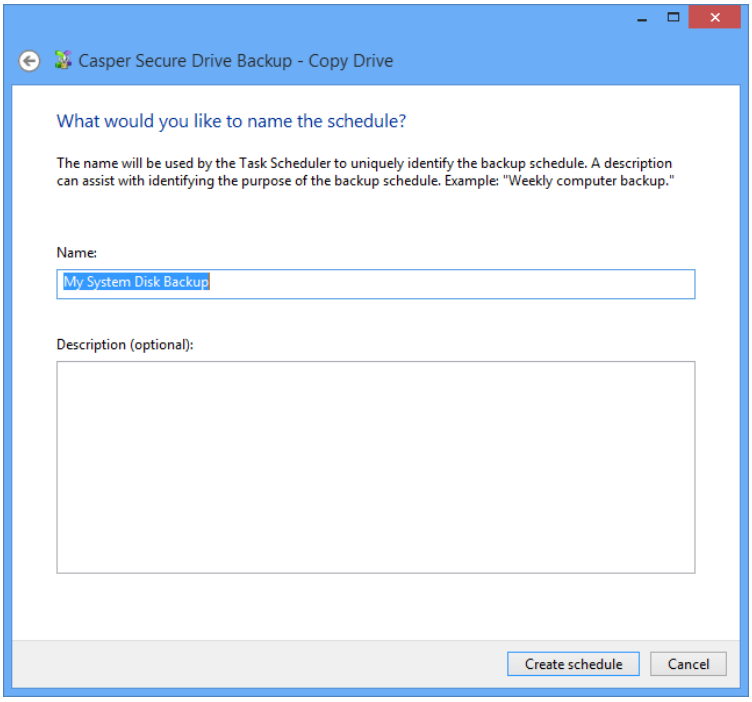


3. Select the desired completion options and click **Next**.

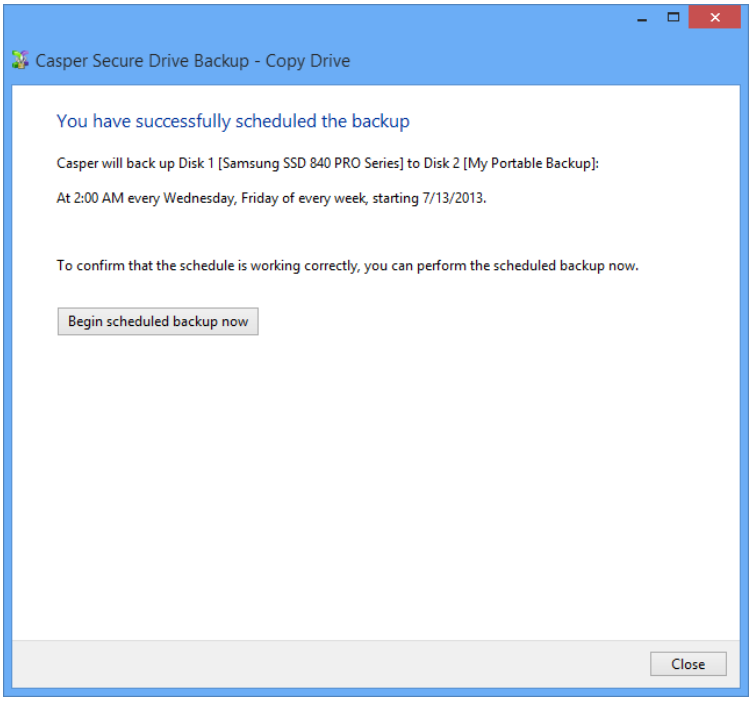


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

4. Enter a name for the schedule, or retain the name suggested by Casper, and then click **Create schedule** to add the copy schedule to the server's Scheduled Tasks.



5. Click **Close** to return to the Casper console.



© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved. January 2025

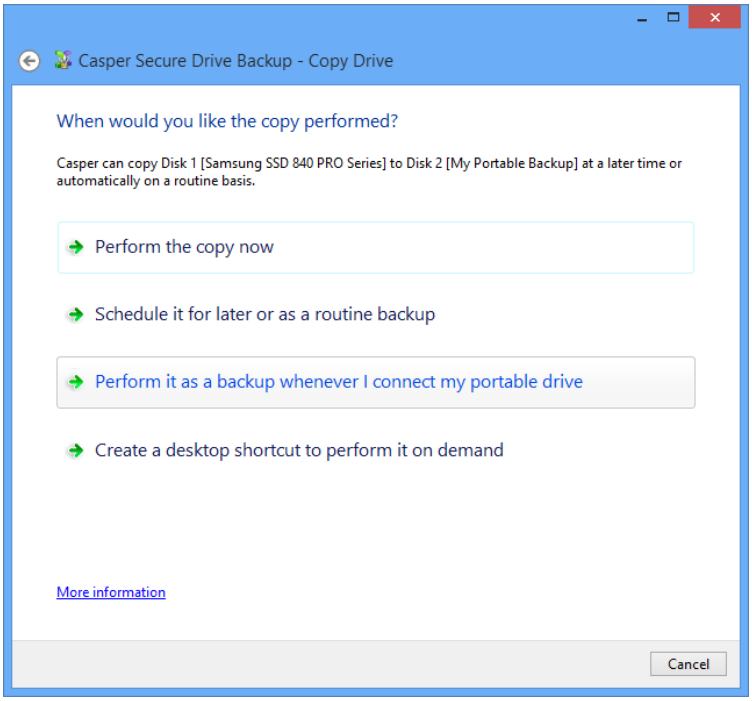
Example 4: Automating a Bootable Backup to a Portable Device

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

Configuring a SmartSense Backup

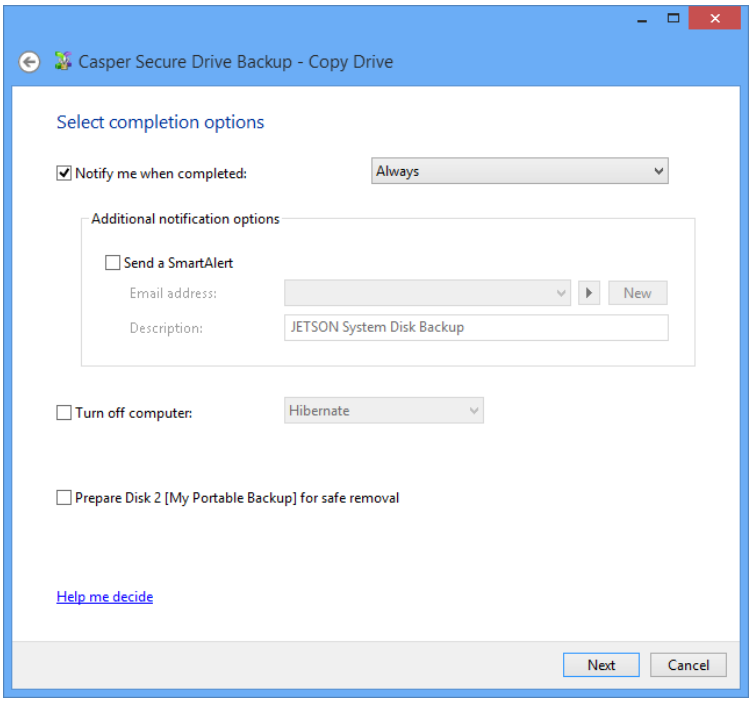
The procedure outlined below is the same whether you are performing an initial backup as demonstrated in Example 1 or updating an existing backup as demonstrated in Example 2.

1. When prompted by the Copy Drive wizard, click **Perform it as a backup whenever I connect my portable drive**.

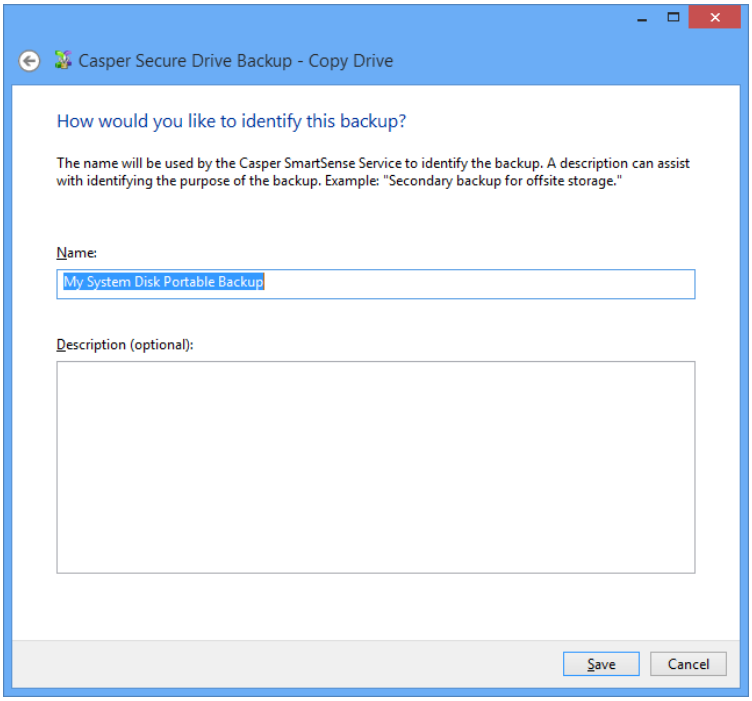


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

2. Select the desired completion options and click **Next**.

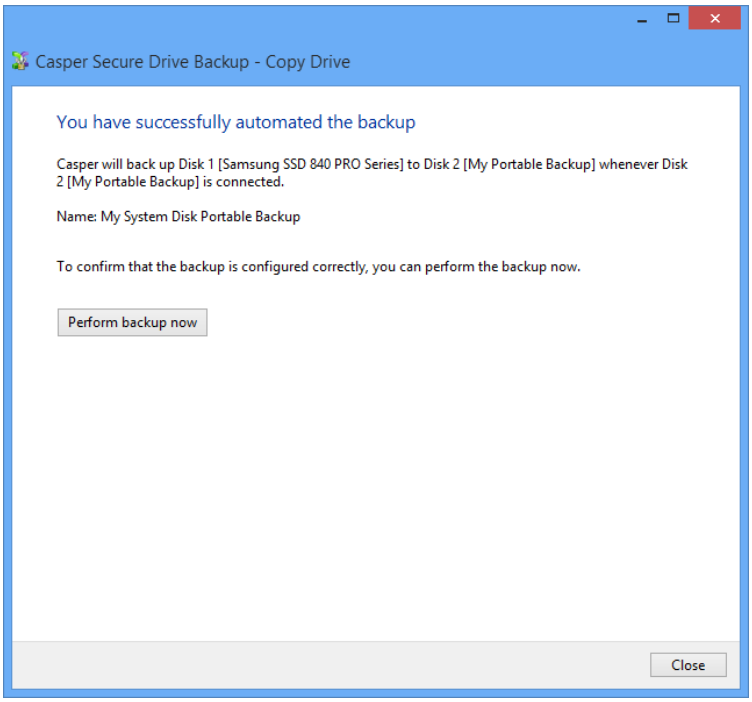


3. Enter a name to uniquely identify the backup, or retain the name suggested by Casper, and then click **Save** to register the backup with the Casper SmartSense Service.



© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

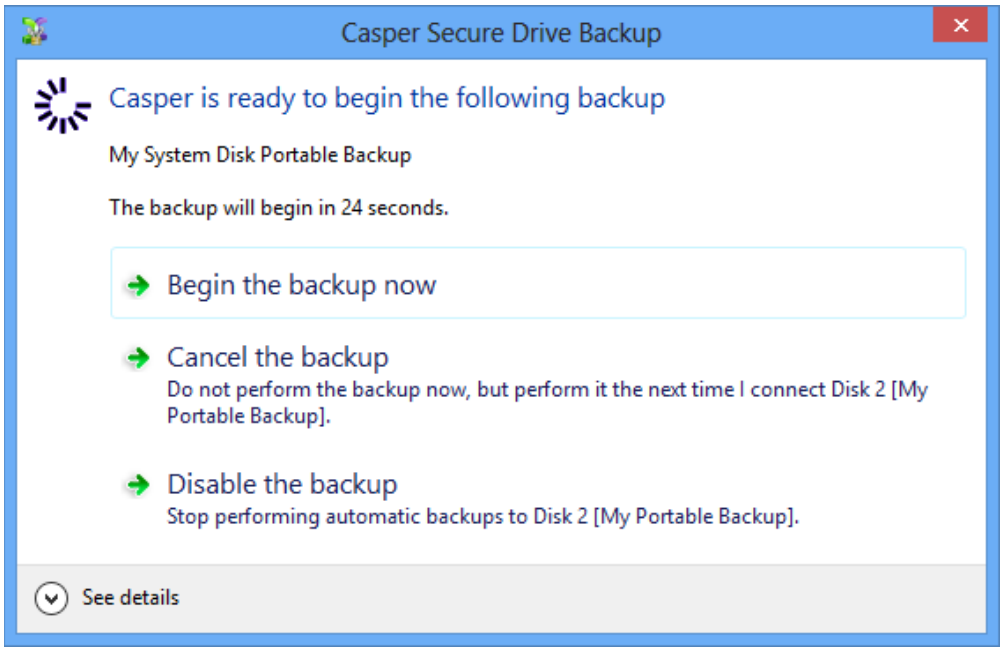
4. Click **Close** to return to the Casper console.



© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

Starting a SmartSense Backup

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



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.

© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

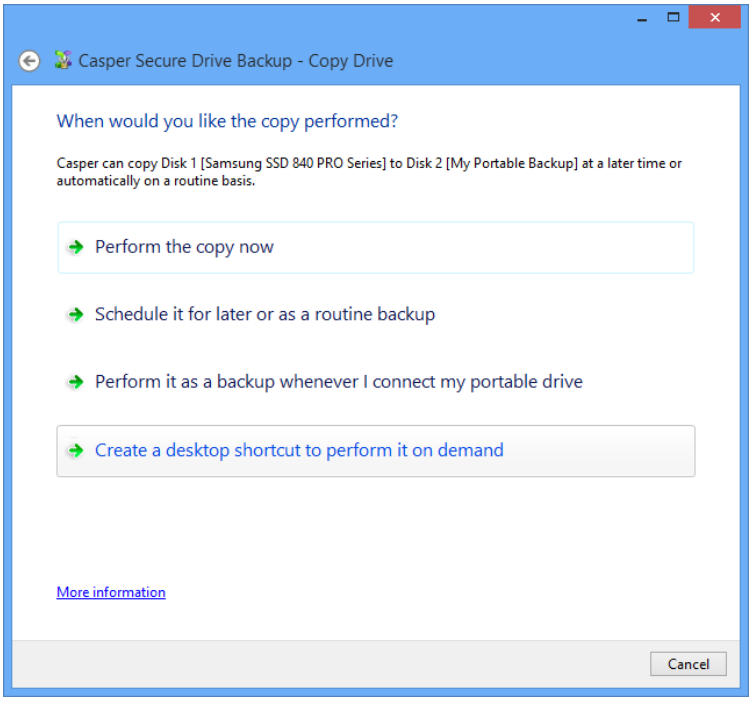
Example 5: Performing a Bootable Backup On-Demand

You can create a desktop shortcut to perform a bootable backup on-demand.

Creating a Desktop Shortcut for a Bootable Backup

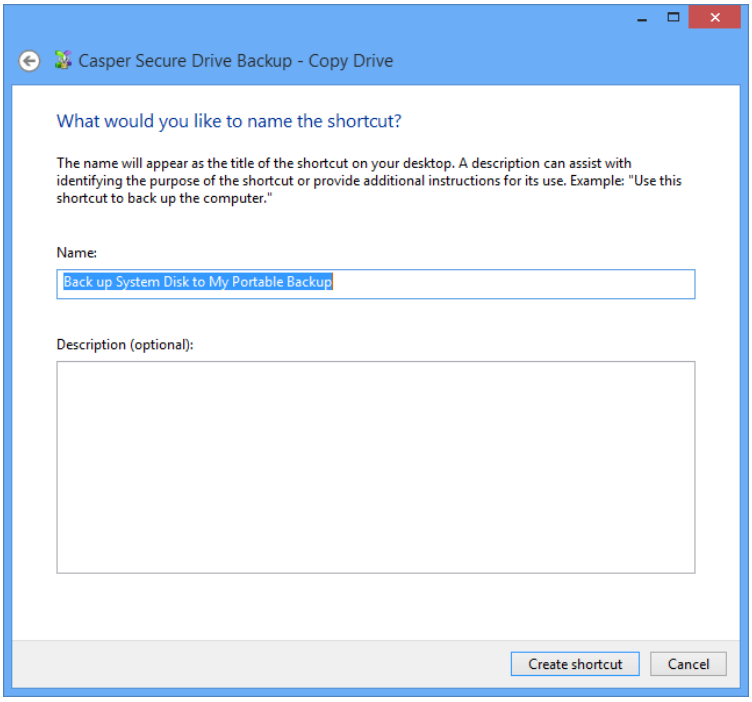
The procedure outlined below is the same whether you are performing an initial backup as demonstrated in Example 1 or updating an existing backup as demonstrated in Example 2.

1. When prompted by the Copy Drive wizard, click **Create a desktop shortcut to perform it on demand**.

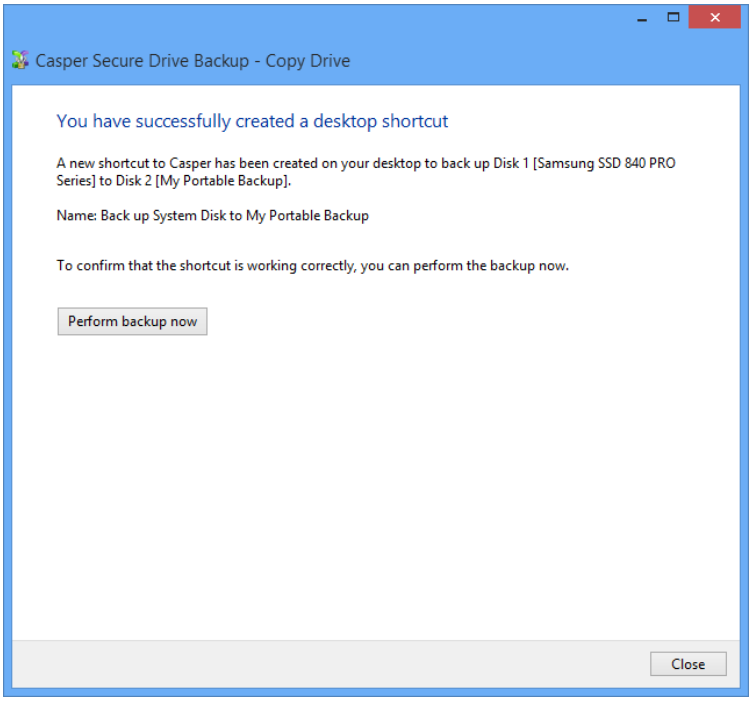


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

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



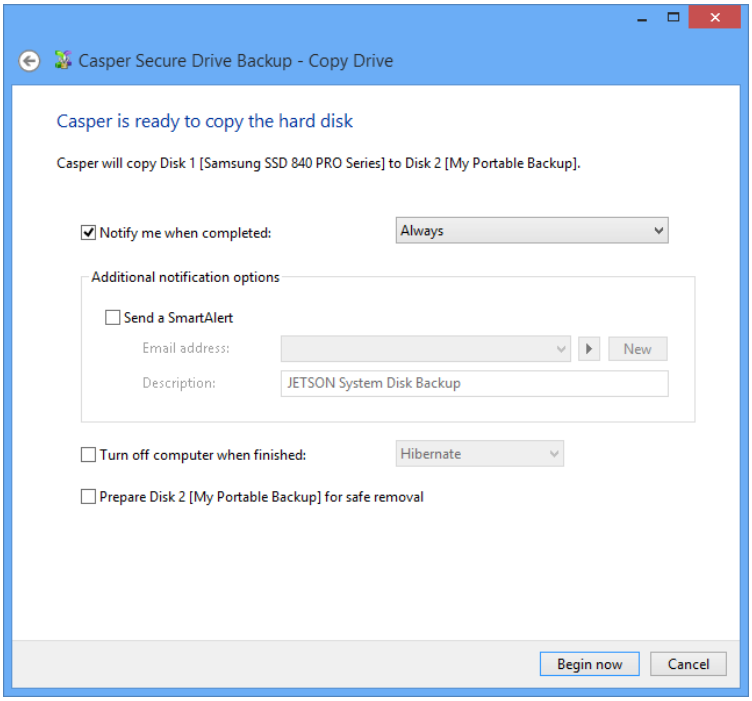
3. Click **Close** to return to the Casper console.



© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved. January 2025

Performing a Bootable Backup On-Demand

After creating a desktop shortcut, you can use the Casper shortcut appearing on the desktop to begin the backup. Click **Begin now** to start the backup.



© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

Creating and Maintaining a Restore-Point System Backup

Using Casper Secure to create and maintain a restore-point backup for a Windows server requires a storage device with free space that is at least several times greater than the amount of used space on the server's system disk device. An external USB or eSATA connected storage device with the requisite amount of free space is often ideal for maintaining restore-point backups. While the exact amount of free space depends on several factors, usually about three times the amount of used space on the server's system disk device is enough free space for Casper to create and maintain multiple restore-points for a restore-point backup. For example, if 150GB represents the current amount of used space on the server's system disk, using a storage device with approximately 450GB of free space is generally sufficient to maintain a restore-point backup with a good variety of restore-points.

The following examples illustrate various ways to create and maintain a restore-point backup of a server's system disk device.

Example 6: Creating a Restore-Point Backup. This example demonstrates how to create a restore-point backup for the server's system disk device.

Example 7: Updating a Restore-Point Backup. This example shows how to manually update an existing restore-point backup by creating a new restore point.

Example 8: Automating a Restore-Point Backup. This example illustrates how to fully automate a restore-point backup.

Example 9: Automating a Restore-Point Backup to a Portable Device. This example shows how to automate a restore-point backup maintained on a portable device such as a USB, Firewire, or eSATA connected disk.

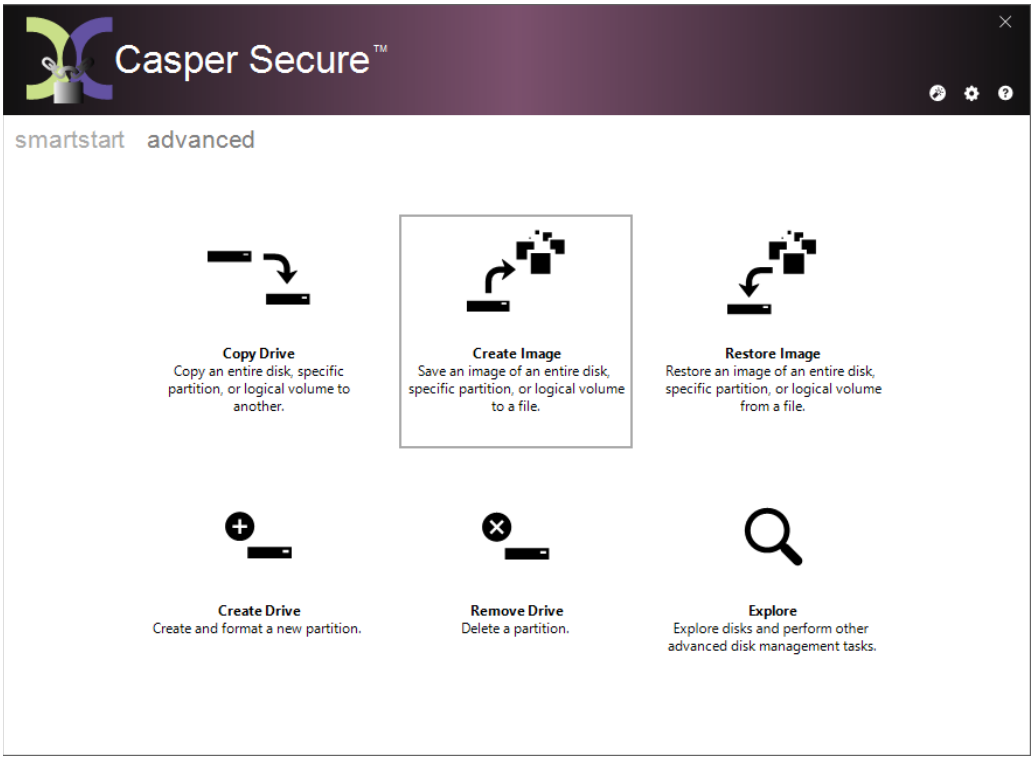
Example 10: Performing a Restore-Point Backup On-Demand. This example demonstrates how to create a desktop shortcut to maintain a restore-point backup on-demand.

© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved. January 2025

Example 6: Creating a Restore-Point Backup

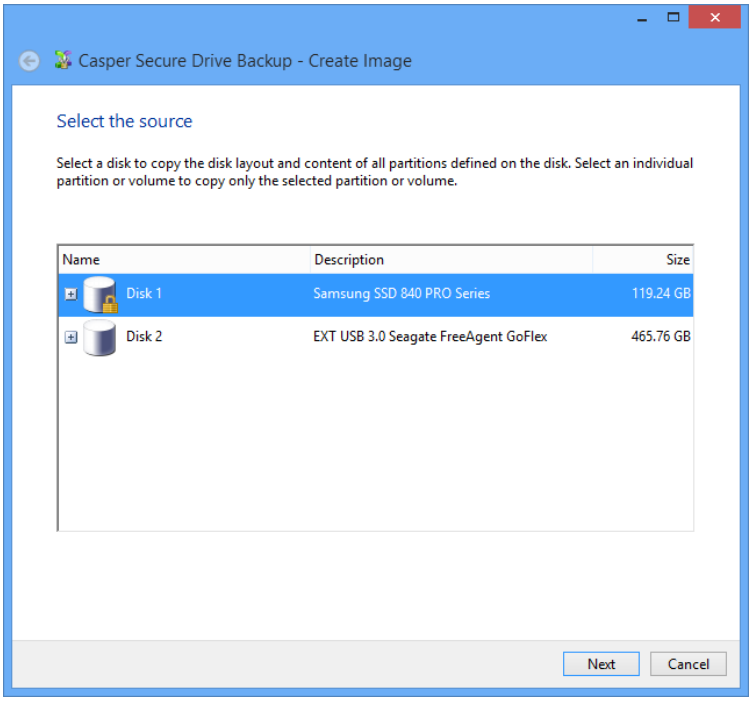
Assuming the backup device is currently installed or attached to the system, the following procedure illustrates how to create an image of the server's system disk device to produce a restore-point backup.

1. Select **Create Image**.

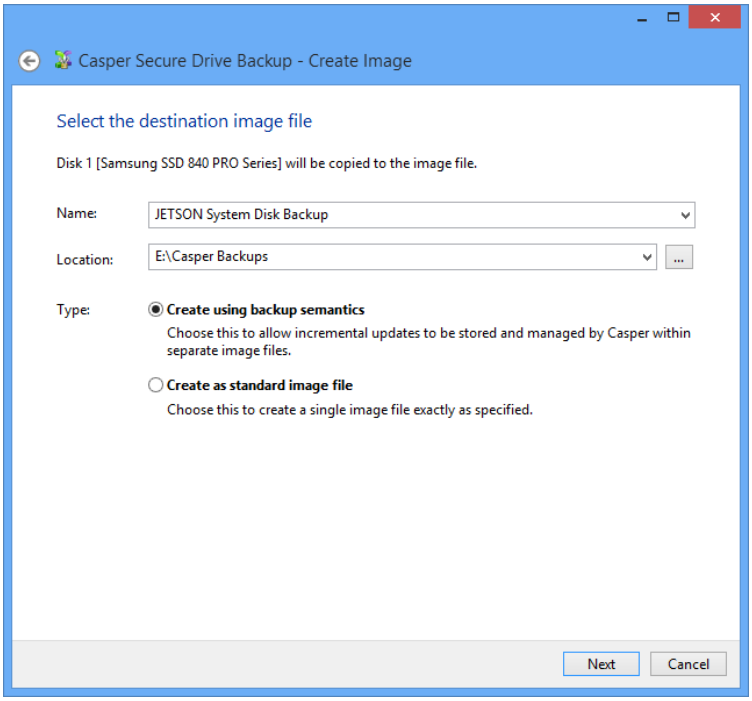


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

2. Select the disk device to backup (e.g., the hard disk or RAID array on which Windows Server is installed) as the source and click **Next**.

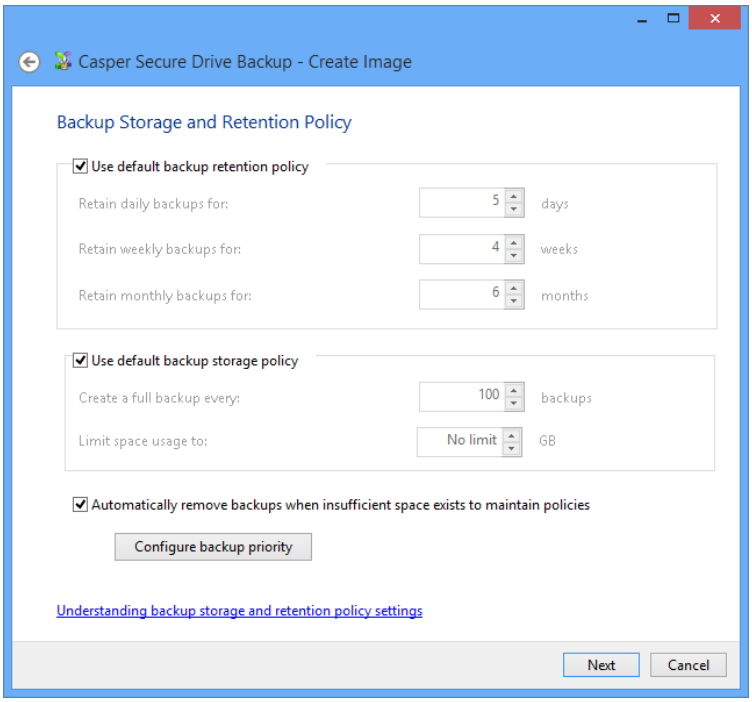


3. Enter a name for the restore-point backup, or retain the name suggested by Casper, and then select the location where the image file(s) will be stored. To allow future restore-points to be managed by Casper, choose **Create using backup semantics** and click **Next**. For additional help, press **F1**.

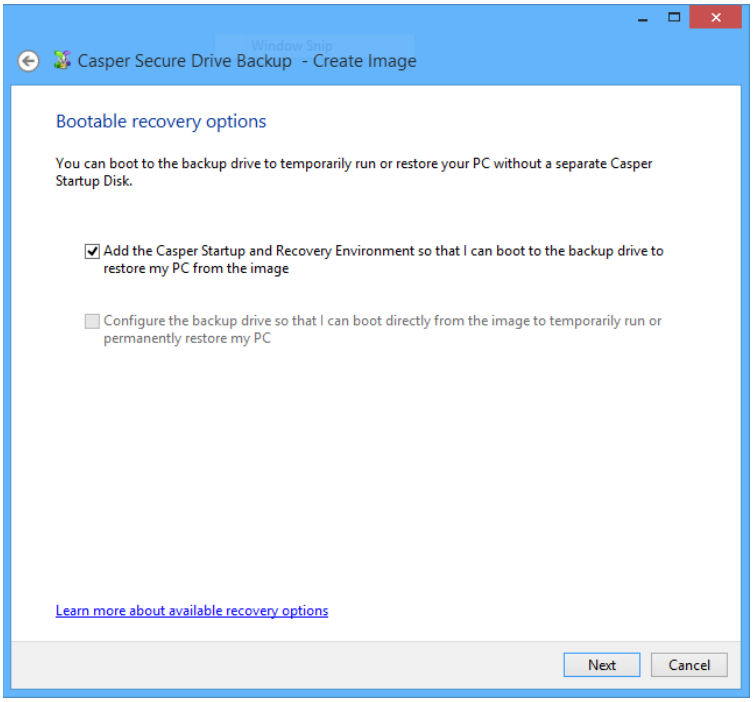


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

4. When using backup semantics, Casper will prompt you to specify the storage and retention policy for the backup. This policy governs how restore-points are created and managed. It also defines what happens when additional storage space is needed to create a new restore-point. Click **Next** to proceed.

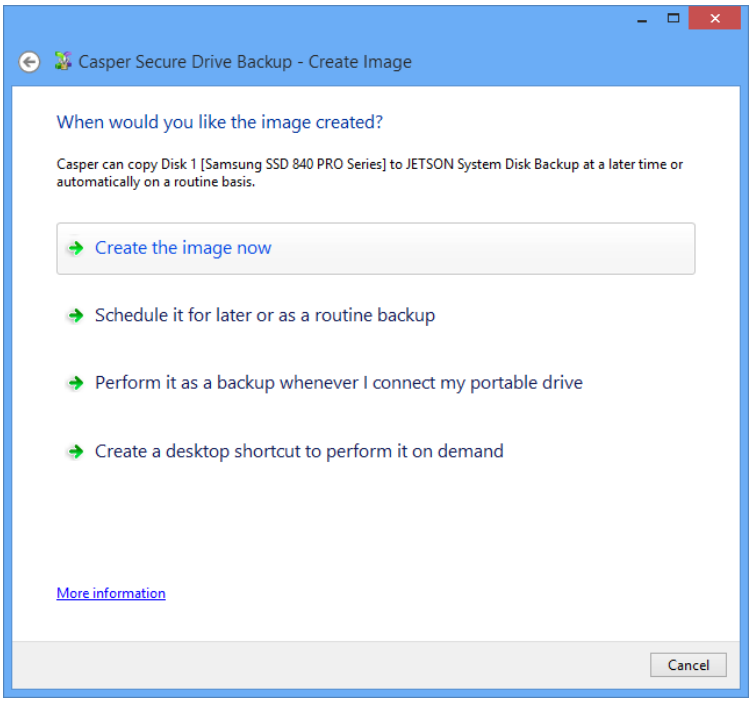


5. When creating a restore-point backup for the server's system disk on a bootable device, Casper will offer to add the Casper Startup and Recovery Environment. This option eliminates the need to create and use a separate Casper Secure Startup Disk to restore the image. Click **Next**.

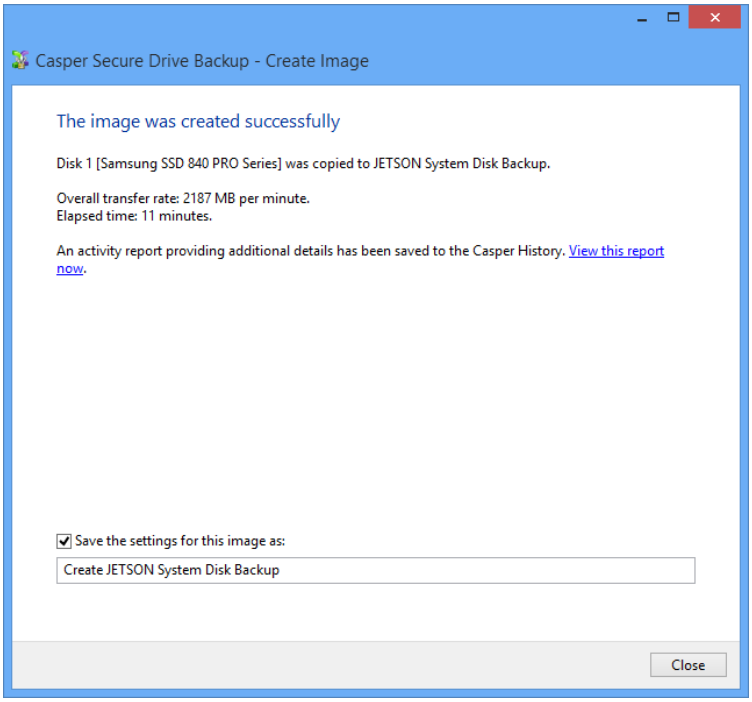


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

6. Click **Create the image now** to begin the imaging process.



7. When Casper has completed the imaging process, click **Close**.

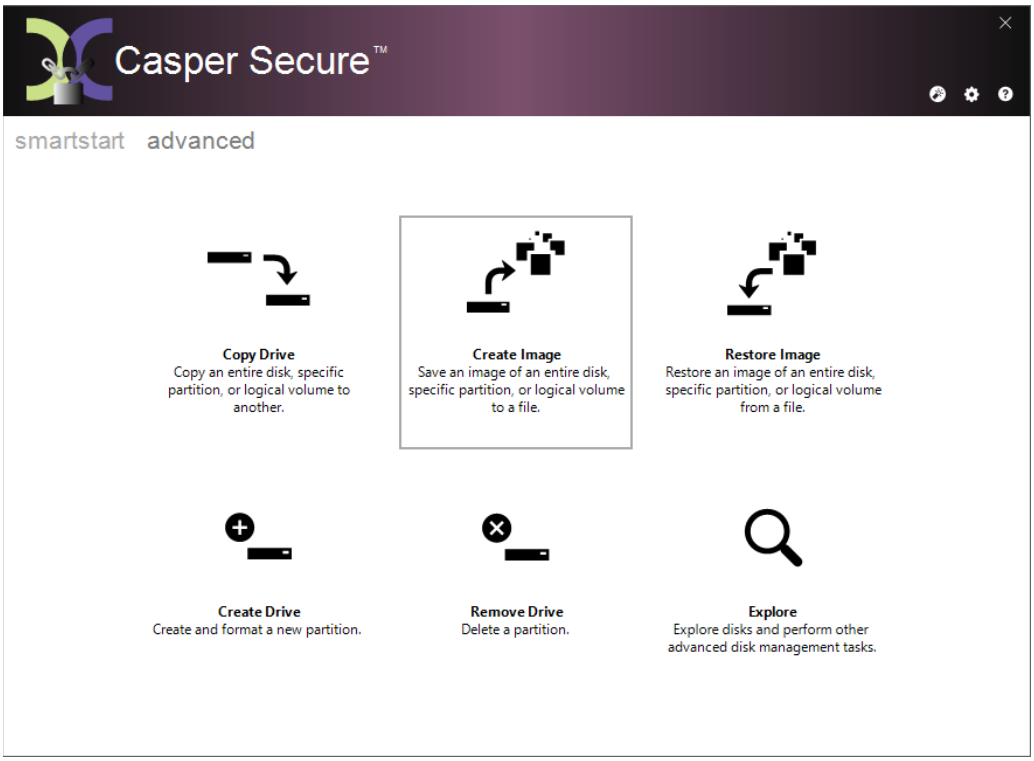


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

Example 7: Updating a Restore-Point Backup

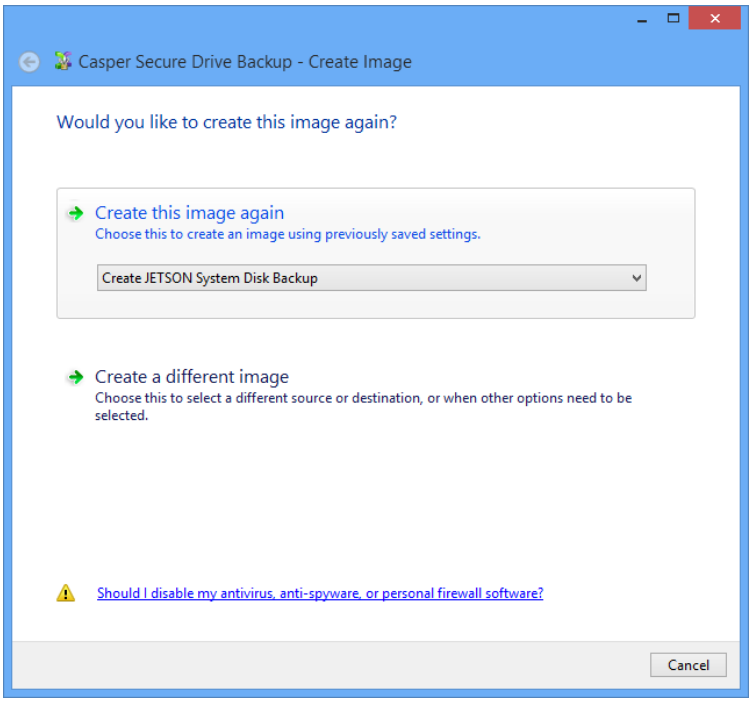
You can manually update a restore-point backup with a new restore-point by repeating the procedure used to create the initial restore-point backup. When the settings for the image have been saved as shown in the final step of the preceding example, Casper makes this process even easier. Assuming the backup device is currently installed or attached to the system, the following two procedures illustrate how to quickly create the image again to produce a new restore-point.

1. Select **Create Image**.

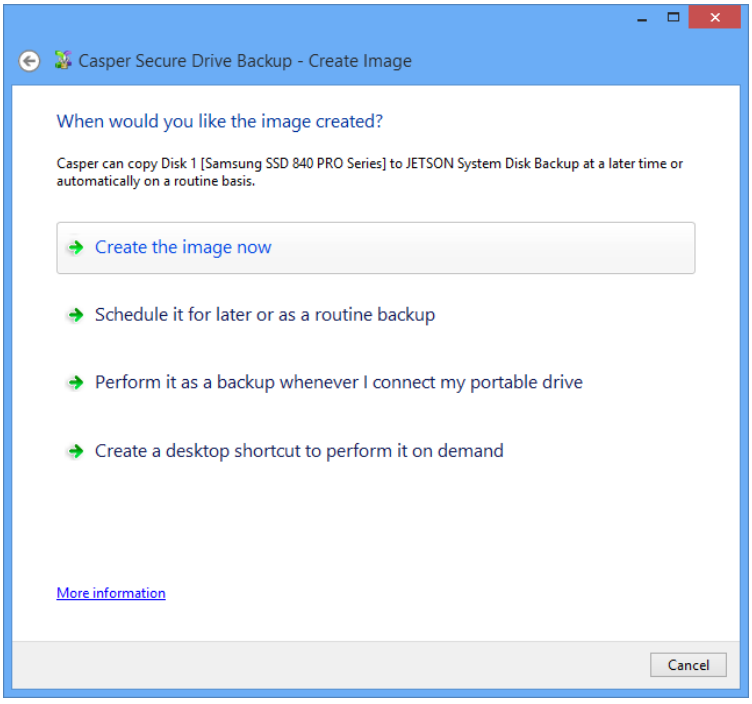


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

2. Select the image from the list provided and click **Create this image again**.

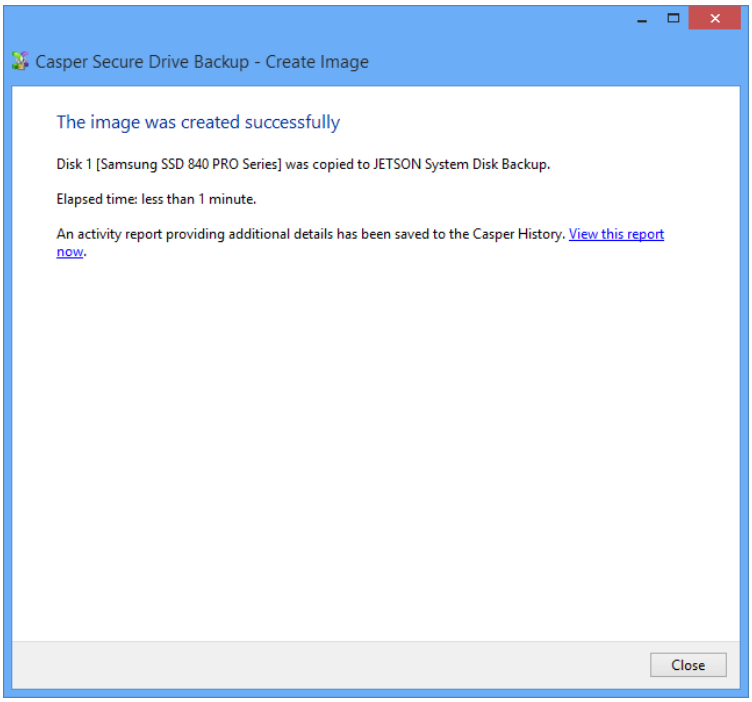


3. Click **Create the image now** to begin the imaging process.



© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved. January 2025

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

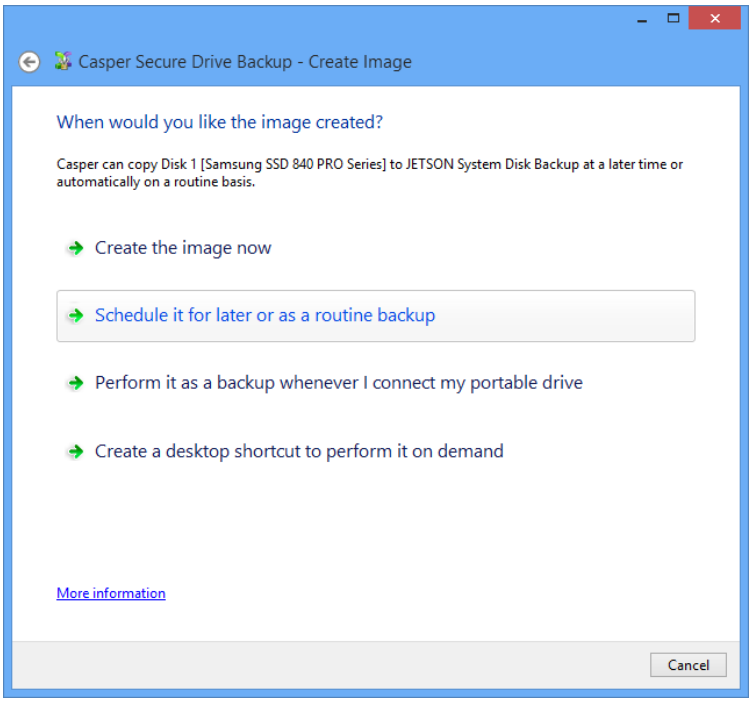


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

Example 8: Automating a Restore-Point Backup

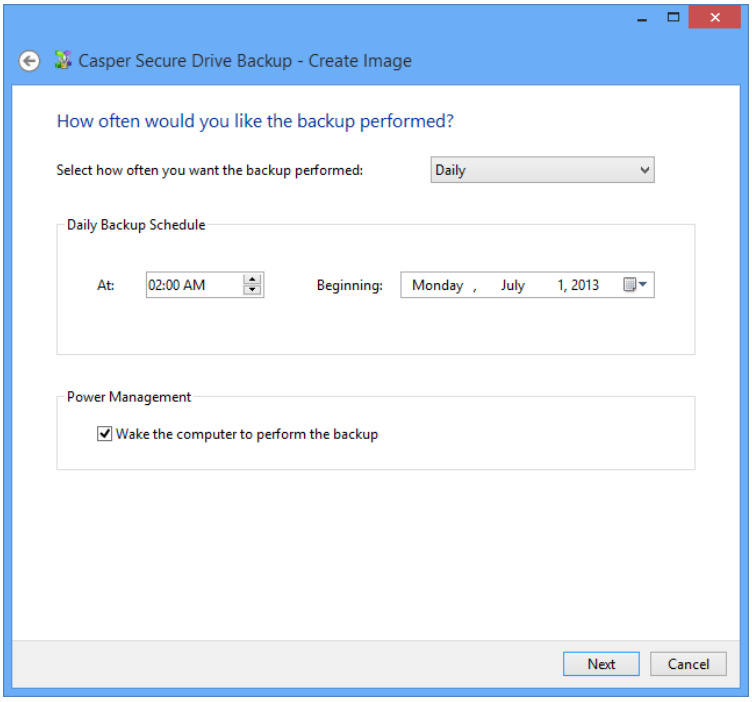
You can fully automate the process of creating and maintaining a restore-point backup for a server by scheduling Casper to run on a routine basis. The procedure outlined below is the same whether you are performing an initial backup as demonstrated in Example 6 or updating an existing backup as demonstrated in Example 7.

1. When prompted by the Create Image wizard, click **Schedule it for later or as a routine backup**.

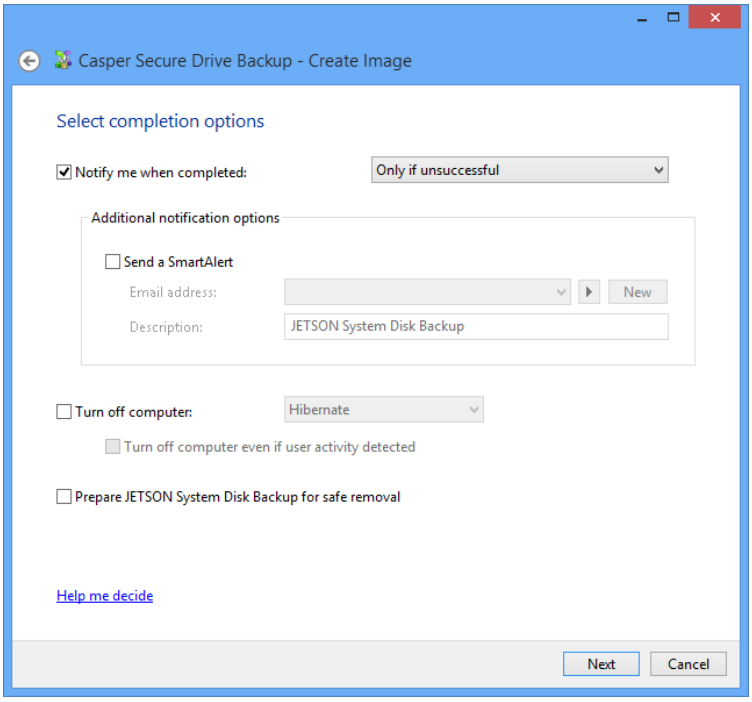


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

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

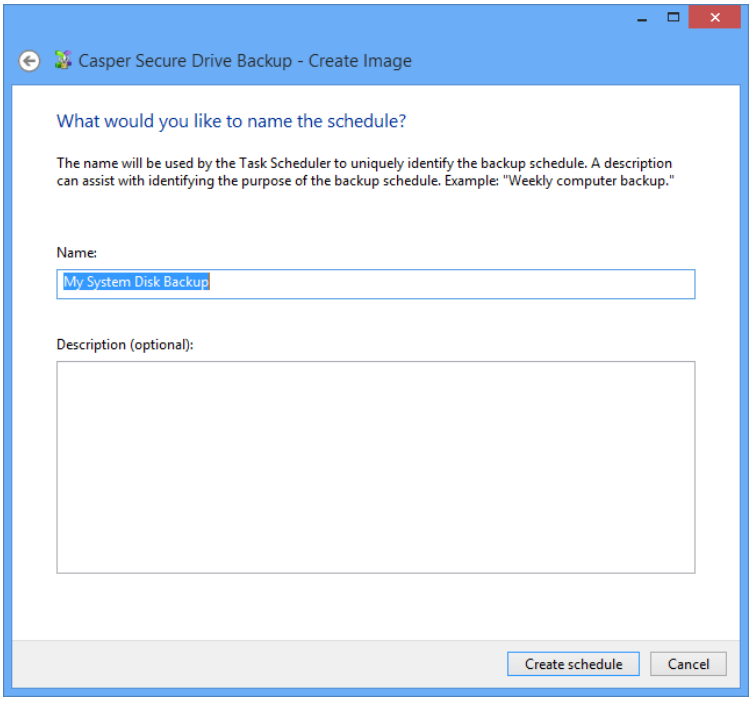


3. Select the desired completion options and click **Next**.

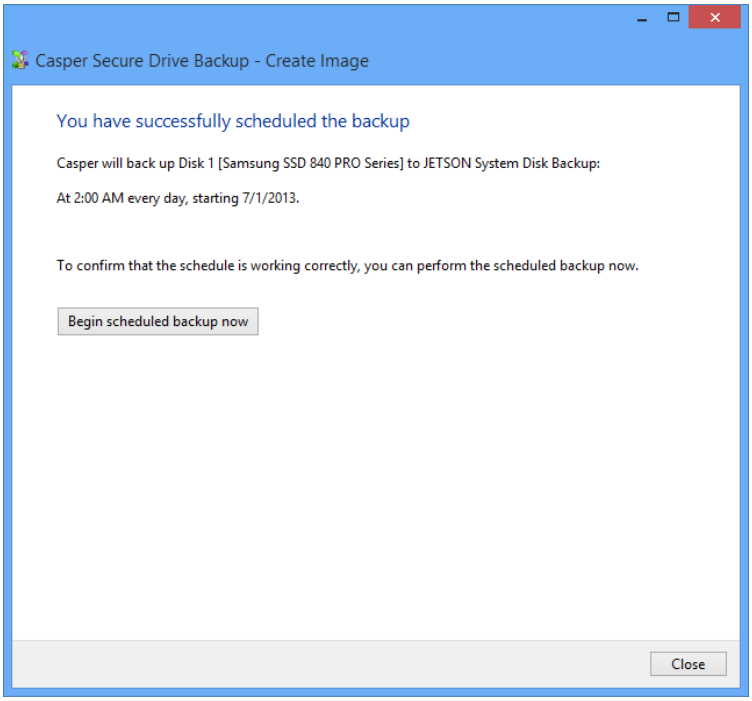


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

4. Enter a name for the schedule, or retain the name suggested by Casper, and then click **Create schedule** to add the copy schedule to the server's Scheduled Tasks.



5. Click **Close** to return to the Casper console.



© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved. January 2025

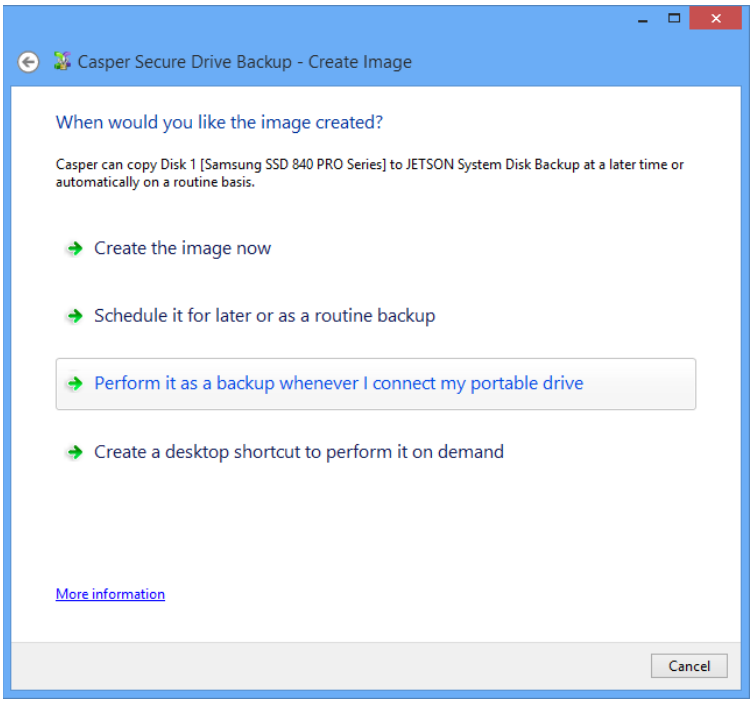
Example 9: Automating a Restore-Point Backup to a Portable Device

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

Configuring a SmartSense Backup

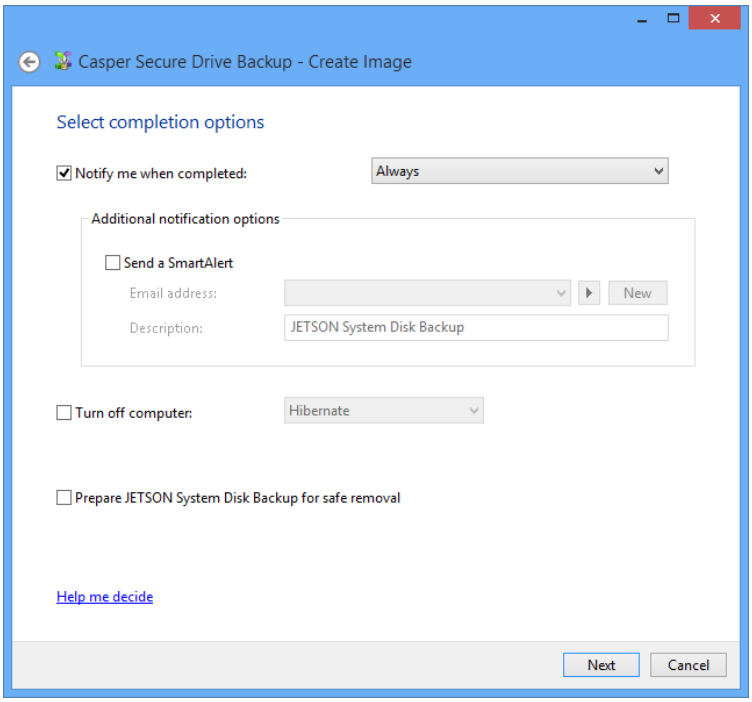
The procedure outlined below is the same whether you are performing an initial backup as demonstrated in Example 6 or updating an existing backup as demonstrated in Example 7.

1. When prompted by the Create Image wizard, click **Perform it as a backup whenever I connect my portable drive**.

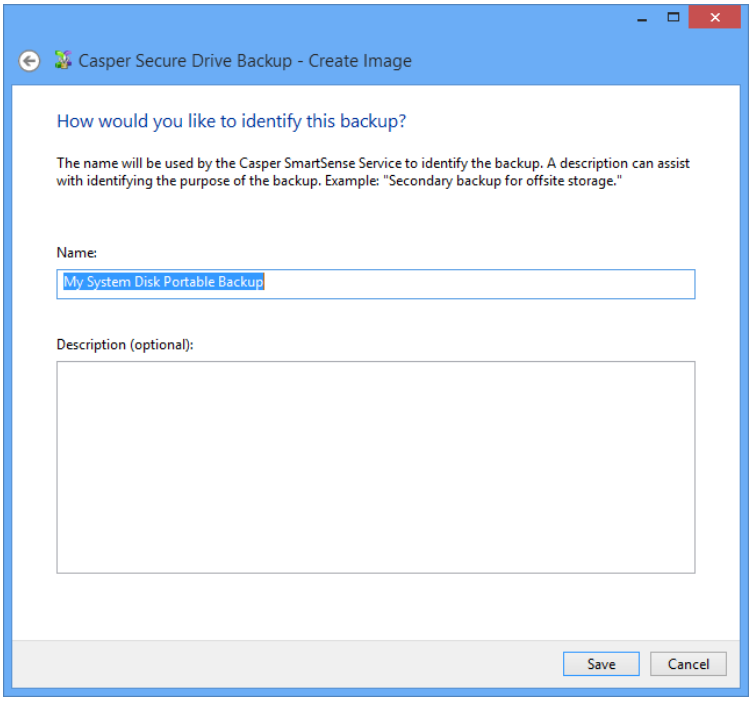


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

2. Select the desired completion options and click **Next**.

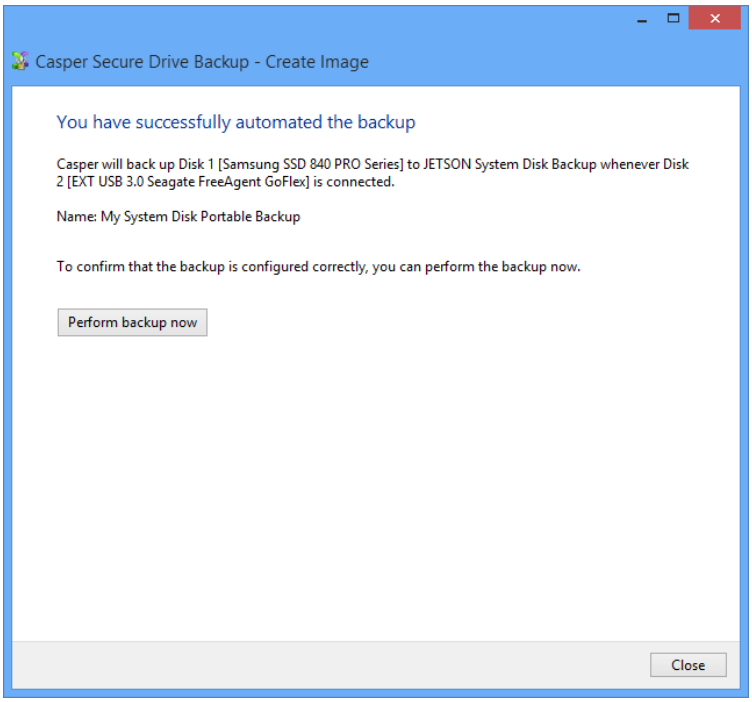


3. Enter a name to uniquely identify the backup, or retain the name suggested by Casper, and then click **Save** to register the backup with the Casper SmartSense Service.



© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

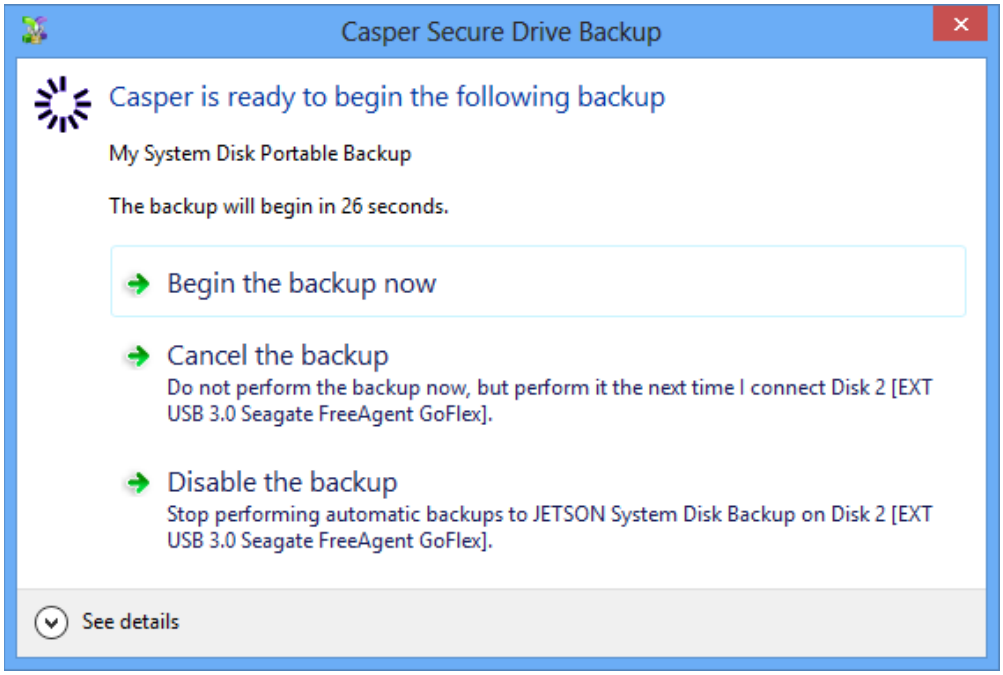
4. Click **Close** to return to the Casper console.



© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

Starting a SmartSense Backup

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



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.

© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

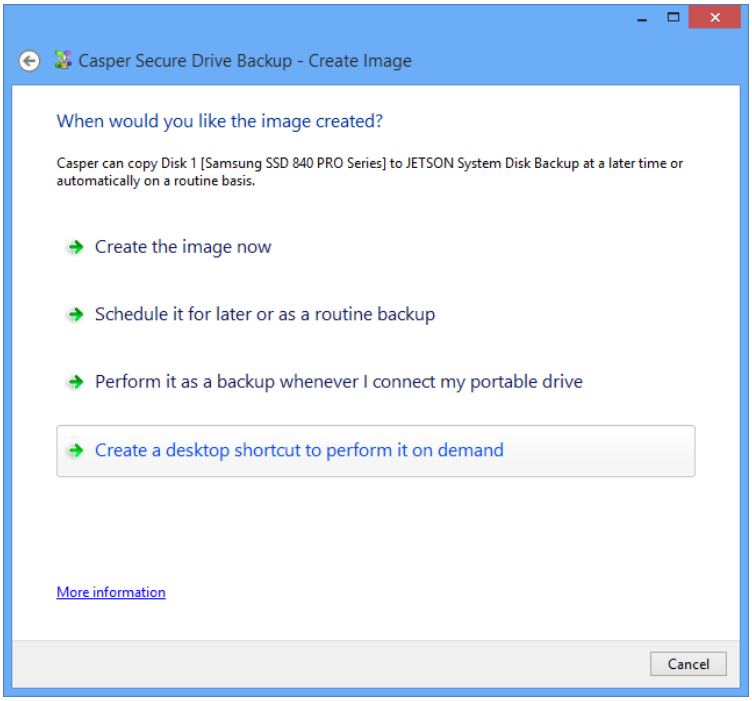
Example 10: Performing a Restore-Point Backup On-Demand

You can create a desktop shortcut to perform a bootable backup on-demand.

Creating a Desktop Shortcut for a Restore-Point Backup

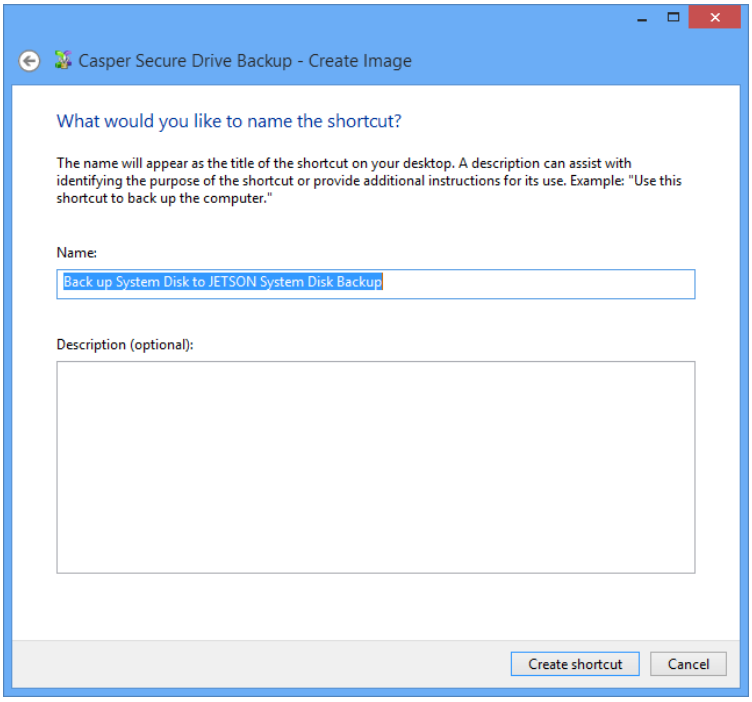
The procedure outlined below is the same whether you are performing an initial backup as demonstrated in Example 6 or updating an existing backup as demonstrated in Example 7.

1. When prompted by the Create Image wizard, click **Create a desktop shortcut to perform it on demand**.

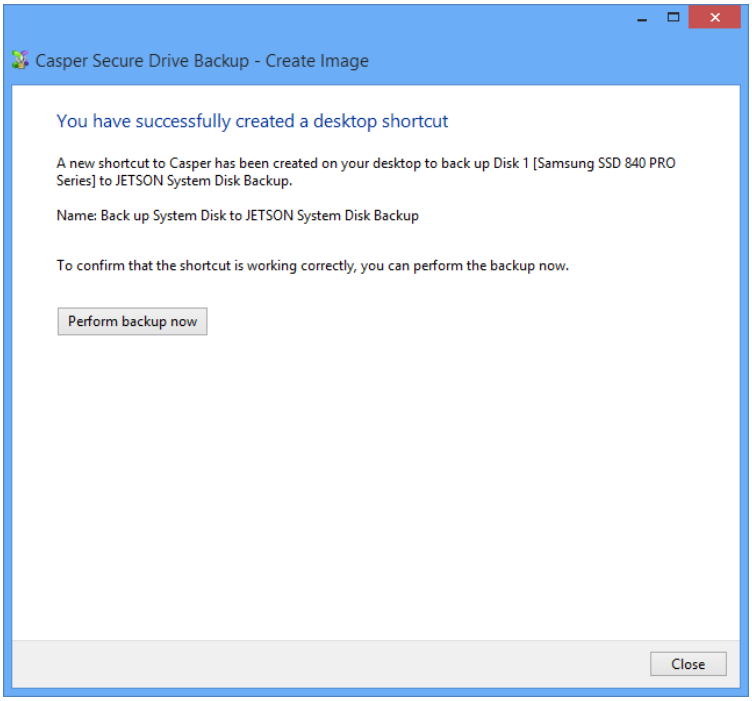


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

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



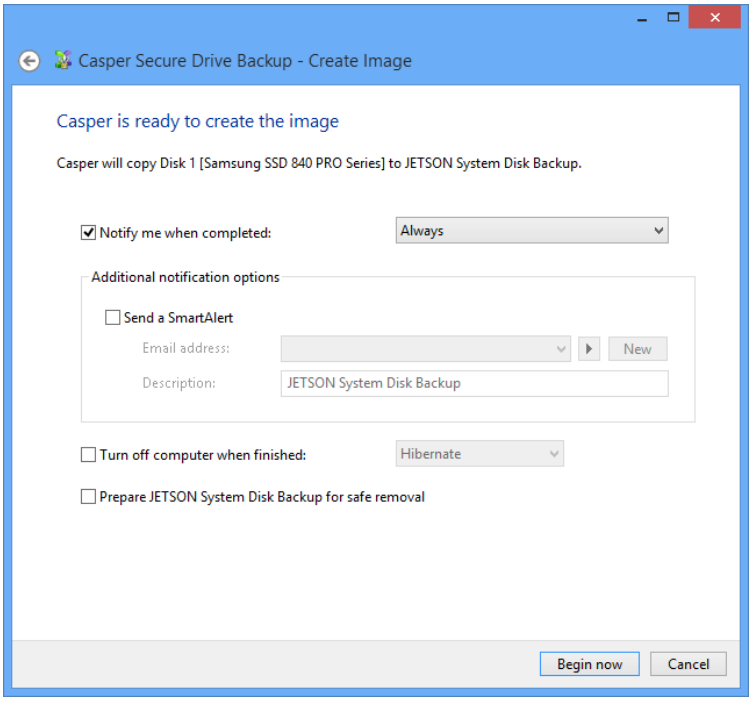
3. Click **Close** to return to the Casper console.



© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

Performing a Restore-Point Backup On-Demand

After creating a desktop shortcut, you can use the Casper shortcut appearing on the desktop to begin the backup. Click **Begin now** to start the backup.



© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

Testing a System Disk Backup

Having confidence in a backup is important. After all, a backup is useless if it cannot be used to facilitate recovery within a crisis. Casper performs rigorous testing during the creation of a backup to ensure a backup is not corrupted by faulty hardware or errant software. Once a backup has been created, periodic testing should be performed as part of a server's regular scheduled maintenance plan to ensure the backup is not rendered corrupt after-the-fact.

Testing a Bootable Backup

You can test a bootable backup by temporarily reconfiguring the server to boot from the backup disk device. See **Booting from a System Backup** for more information.

When booting directly to the backup, it will take on the identity of the original Windows system disk device, and the original system disk device, if left attached, will take on the identity of the backup. For example, if the server's system disk device normally boots and appears as Local Disk (C:) and the backup appears as Local Disk (F:), the backup will boot and appear as Local Disk (C:) and the original system disk device will appear as Local Disk (F:). All of the server's programs, settings, and data will run and appear just as they did on the original Windows system disk device when the backup was created.

Once you are satisfied that the server is operating as expected from the backup, you can resume normal operation of the server by restarting from the original Windows system disk device.

Testing a Restore-Point Backup

There are two ways to test a restore-point backup of the server's Windows system disk device. If you created the restore-point backup with bootable image recovery enabled, you can temporarily boot the server directly from the restore-point.[5] If Windows Hyper-V is available on the server, you can temporarily boot and test the backup within a virtual machine.

Testing with Bootable Image Recovery *(Unencrypted Images Only)* [5]

You can test a restore-point backup with bootable image recovery by temporarily reconfiguring the server to boot from the backup disk device and then selecting the desired restore-point from which to boot. See **Booting from a System Backup** for more information.

When booting to the backup, it will take on the identity of the original Windows system disk device, and the original system disk device, if left attached, will take on the identity of the backup. For example, if the server's system disk device normally boots and appears as Local Disk (C:) and the backup appears as Local Disk (F:), the backup will boot and appear as Local Disk (C:) and the original system disk device will appear as Local Disk (F:). All of the server's programs, settings, and data will run and appear just as they did on the original Windows system disk device when the backup was created.

Once you are satisfied that the server is operating as expected from the backup, you can resume normal operation of the server by restarting from the original Windows system disk device.

[5] Due to limitations with Windows native boot functionality, only unencrypted restore-point backups may be booted through bootable image recovery at this time.

© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved. January 2025

Testing within a Virtual Machine

If Windows Hyper-V functionality is available, you can quickly test a restore-point backup within a temporary Hyper-V virtual machine (VM) without restarting the server.

By default, the temporary VM is created without network access. This will ensure the restore-point backup running within the temporary virtual machine does not interfere with operation of the live server. You can enable network access by adding a network switch to the VM in Casper Settings, Test Boot, Virtual Machine Settings.

Changes made to files contained in the restore-point backup while running within the VM will be lost when the virtual machine connection window is closed.

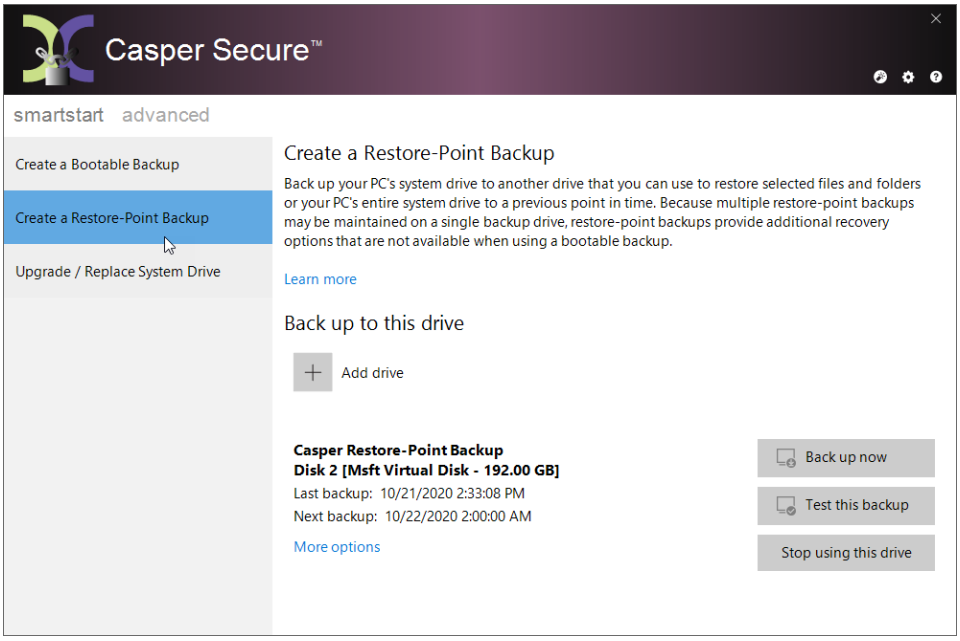
Nested VMs are not supported. You cannot test a restore-point backup within a temporary VM while Casper is running within a VM.

© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

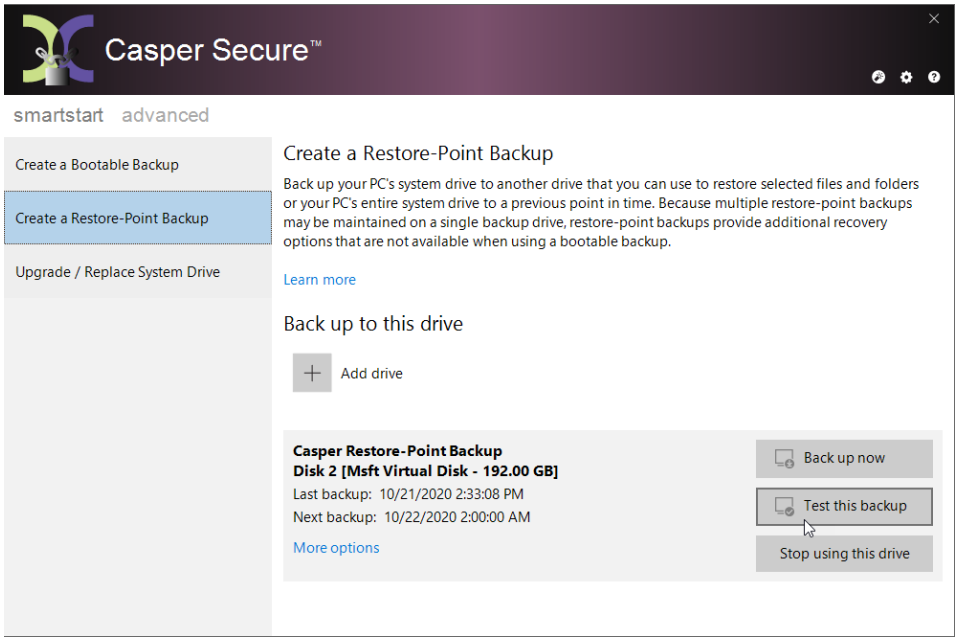
Example 11: Testing the Latest Restore-Point within a VM

If you created a restore-point backup using Casper SmartStart and the hard disk containing the backup is currently installed or attached to the server, the following procedure illustrates how to boot and test the latest restore-point within a Windows Virtual Machine.

1. From the Casper console, select the **SmartStart** tab and then click **Create a Restore-Point Backup** to display your existing restore-point backups.

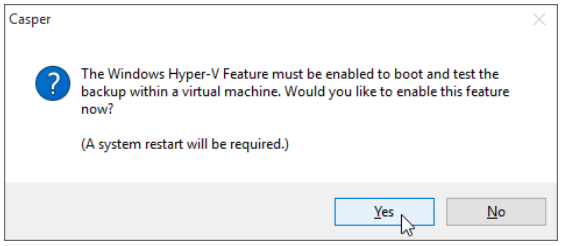


2. Select **Test this backup**.

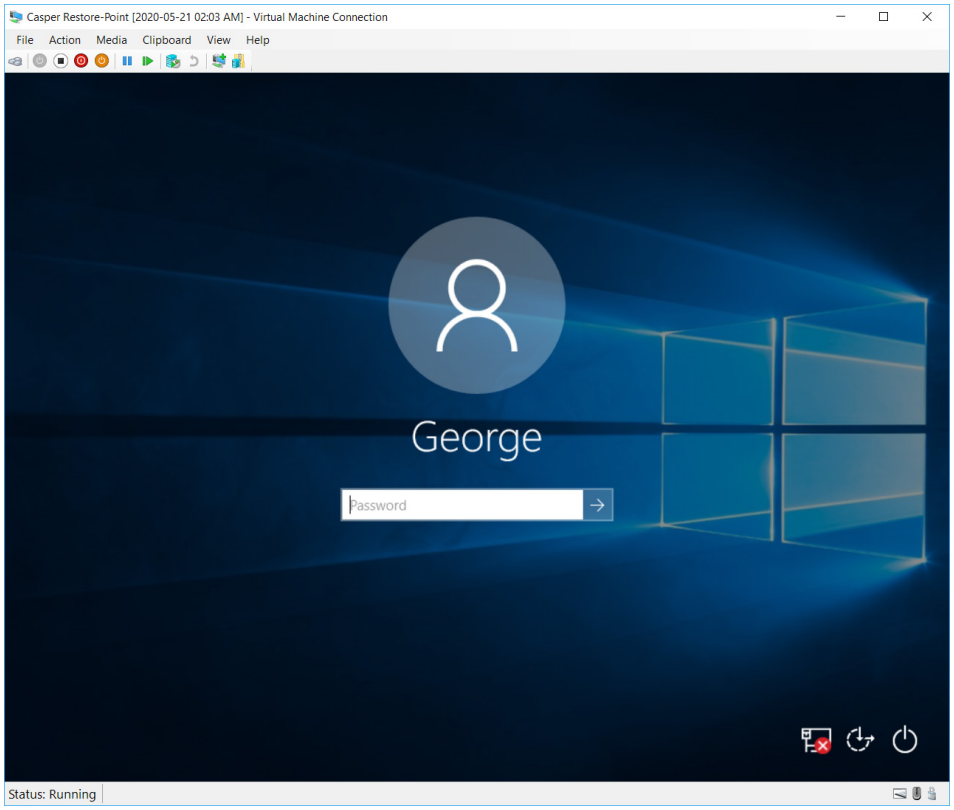


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

If the Hyper-V feature is not currently enabled, Casper will offer to enable it for you.



3. Once the temporary virtual machine has been configured it will boot to the latest restore-point backup image. This process can take several minutes.



When you have finished testing, simply close the virtual machine connection window to shut down and destroy the temporary virtual machine.

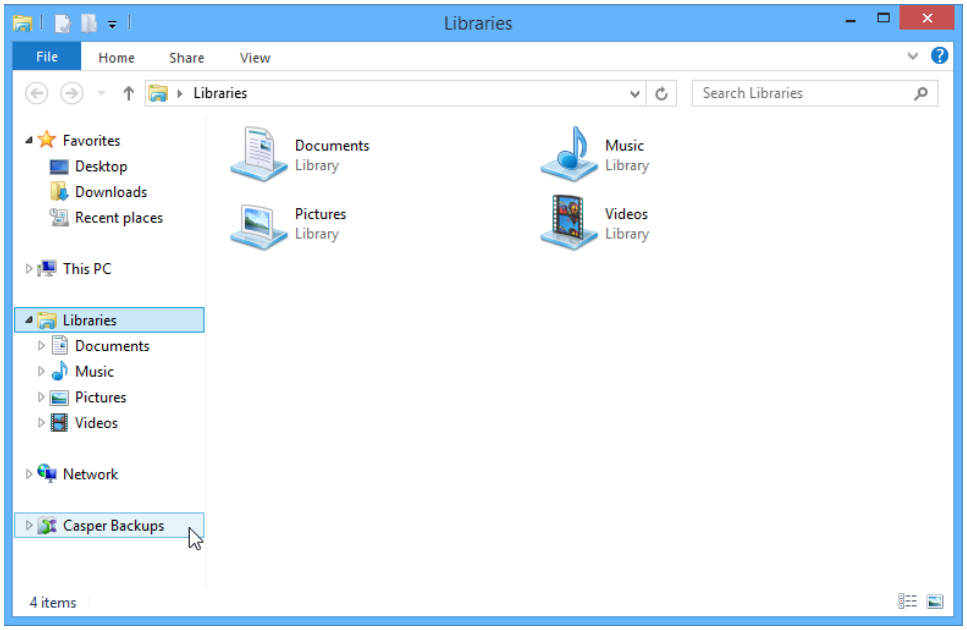
When testing a restore-point backup of a BitLocker encrypted system drive within a virtual machine, Casper will configure the temporary virtual machine to automatically unlock the BitLocker encrypted image. When testing a restore-point backup of a system drive encrypted with a different encryption technology, you must provide the requisite preboot authentication credentials.

© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

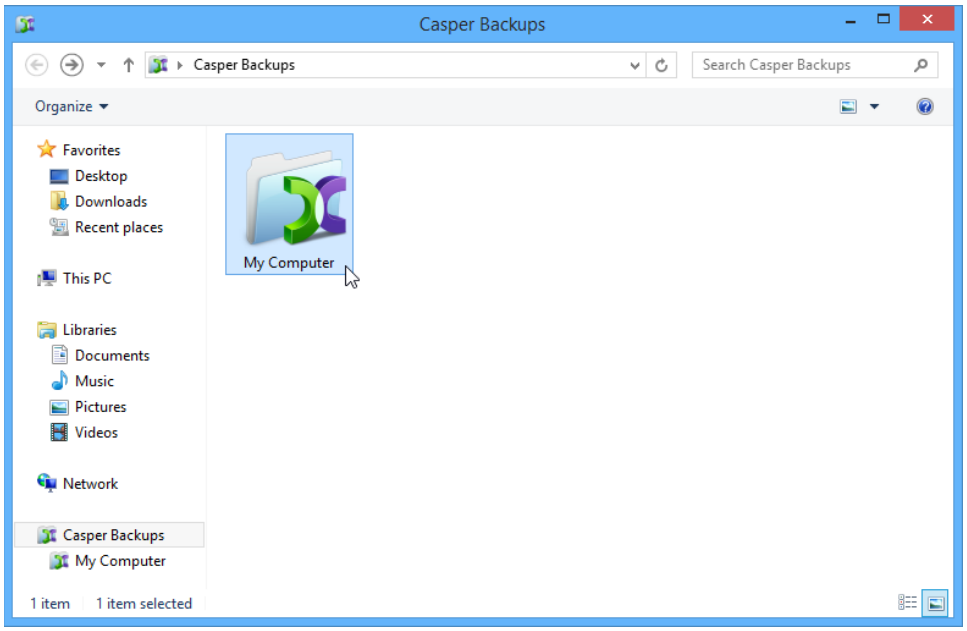
Example 12: Testing a Specific Restore-Point within a VM

If you created a restore-point backup of the Windows system disk device with bootable image recovery enabled and the disk device containing the backup is currently installed or attached to the server, the following procedure illustrates how to boot and test a selected restore-point within a Windows Virtual Machine.

1. Open the **Casper Backups** folder. On Windows Server 2012 or later, start **Windows File Explorer** and then click **Casper Backups**. On Windows Server 2008 and earlier, open **Windows Explorer** and click **Casper Backups**.

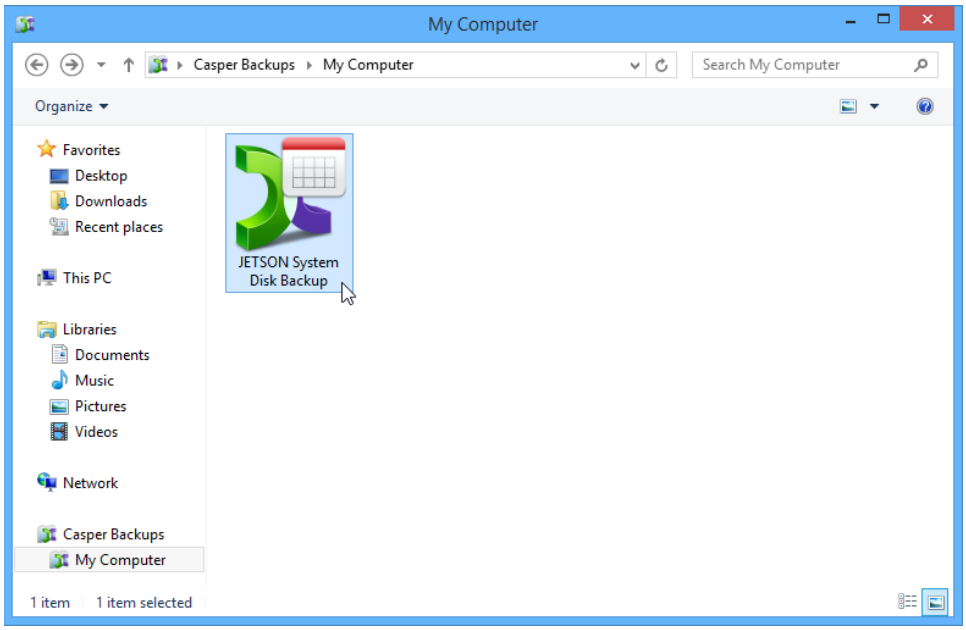


2. Double-click the **My Computer** folder to browse all of the restore-point backups discovered for the server.

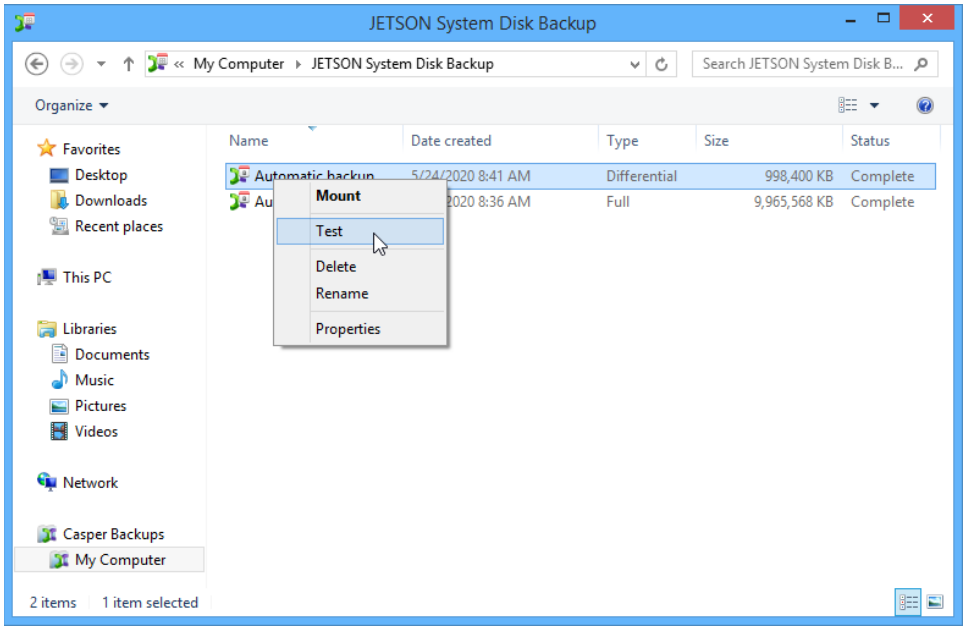


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

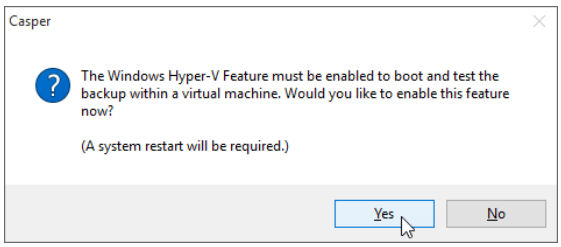
3. Double-click the backup containing the restore-point you want to boot and test.



4. Right-click on the desired restore-point and then click **Test**.

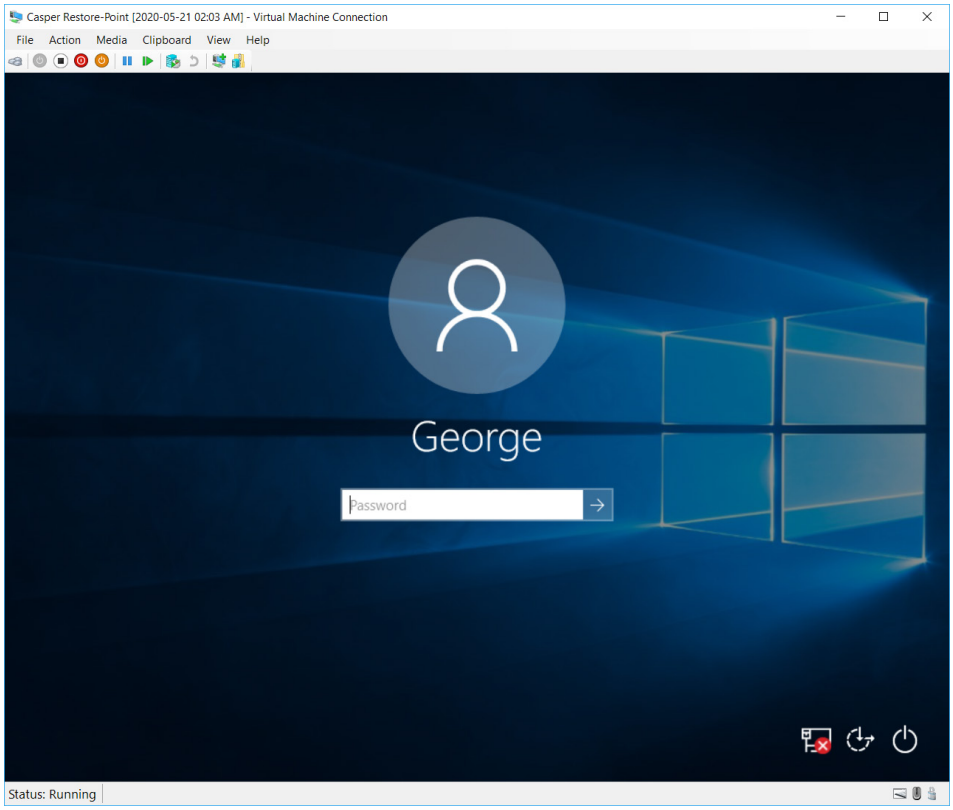


If the Hyper-V feature is not currently enabled, Casper will offer to enable it for you.



© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved. January 2025

5. Once the temporary virtual machine has been configured it will boot to the selected restore-point backup image. This process can take several minutes.



When you have finished testing, simply close the virtual machine connection window to shut down and destroy the temporary virtual machine.

When testing a restore-point backup of a BitLocker encrypted system drive within a virtual machine, Casper will configure the temporary virtual machine to automatically unlock the BitLocker encrypted image. When testing a restore-point backup of a non-system drive or a system drive encrypted with a different encryption technology, you must provide the requisite preboot authentication credentials.

© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

Recovering from a System Disk Failure

If you have used Casper Secure to create a backup of the server's Windows system disk device, and the device fails or its contents become corrupted, you can restore the server to working order by using the Casper backup.

Booting from a backup

If you have a bootable backup, or a restore-point backup created with bootable image recovery enabled, you can get the server running again in just a few minutes.

For a bootable backup simply reconfigure the server to boot from the backup disk device. For a restore-point backup, first reconfigure the server to boot from the backup disk device that contains the restore-point backup and then select the desired restore-point from which to boot.[6]

For details, please see **Booting from a System Backup**.

Restoring from a backup

If you are unable to boot directly from a backup, you can restore the server's Windows system disk from a backup. Restoration may be made to either the original Windows system disk device or a replacement disk device (e.g., when the original device is no longer operable).

If you have a restore-point backup and the Casper Startup and Recovery Environment was added to the backup disk, you can boot the server directly from the backup disk device to perform a restore. If you are unable to boot the server from the backup disk device, you can use a Casper Secure Startup Disk to manually restore a backup.

For details, please see **Restoring a System Backup**.

System Recovery Options at a Glance

Casper Bootable Backup Recovery Options	Casper Restore-Point Backup Recovery Options
Boot server from backup disk device to temporarily run server or restore backup.	If bootable image recovery was enabled, boot server directly from selected restore-point to temporarily run server or restore selected backup.[6]
Permanently replace existing system disk device with backup disk device.	If Casper Startup and Recovery Environment was added to backup disk device, boot server from backup disk device and restore selected backup.
Boot server from Casper Startup Disk and restore backup from backup disk device.	Boot server from Casper Startup Disk and restore selected backup from backup disk device.

[6] Due to limitations with Windows native boot functionality, only unencrypted restore-point backups may be booted through bootable image recovery at this time.

© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

Booting from a System Backup

If you have a bootable backup, you can run the server directly from the backup simply by reconfiguring the server to boot from the backup disk device. Similarly, if you have a restore-point backup created with bootable image recovery enabled, you can run the server directly from the backup by first reconfiguring the server to boot from the backup disk device that contains the restore-point backup and then selecting the desired restore-point from which to boot.

When booting directly to a backup, the backup will take on the identity of the original Windows system disk device. For example, if the server's system disk device normally boots and appears as Local Disk (C:), the backup will boot and appear as Local Disk (C:) whenever the server has been configured to boot and run from it. In addition, all of the programs, settings, and data will run and appear just as they did on the original Windows system disk device when your backup was created.

Booting from a backup hard disk

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 boot priority setting in the server's BIOS or EFI Firmware to designate the backup disk device as the preferred boot device. The exact process depends on the manufacture of the server, but typically pressing F12 or F2 when starting the server will allow you to change the boot device order or temporarily select a specific device from which to boot the server.

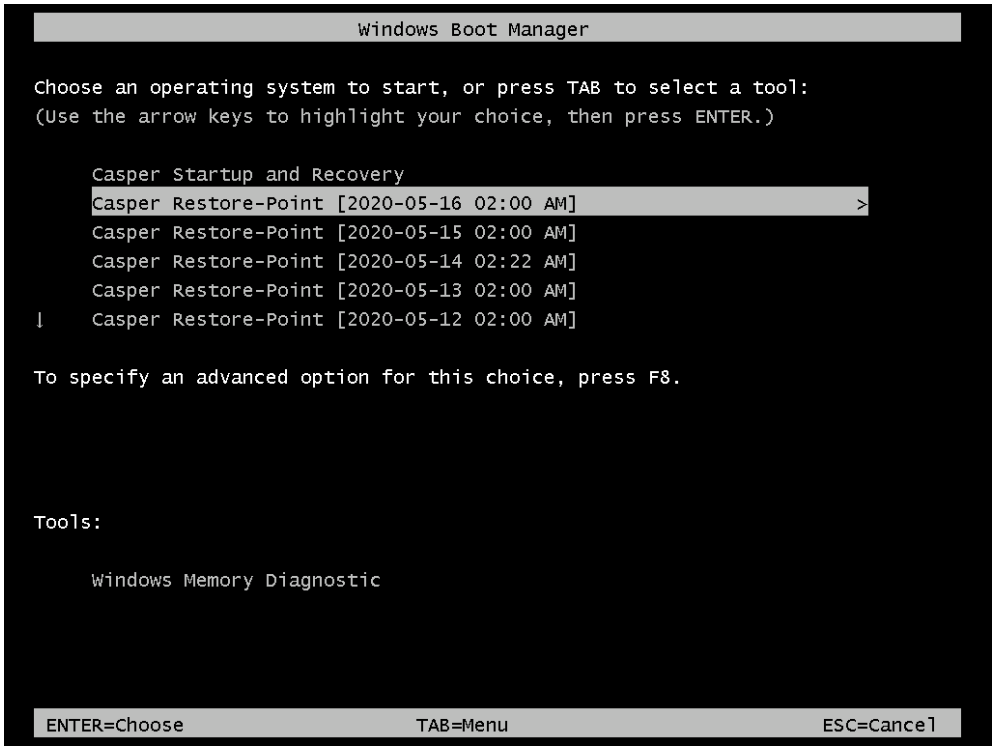
If the server's BIOS or EFI Firmware does not offer an option to select the designated backup disk device as the preferred boot device, or if the original system disk device fails completely, the backup disk device must be reconfigured to replace the original system disk device.

For a backup hard disk attached as an external USB device, booting from the backup hard disk may require the selection of additional BIOS or EFI Firmware 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 server's BIOS or EFI Firmware does not support booting from external USB hard disk type devices, a bootable backup hard disk must be removed from its external enclosure and installed as a replacement for the internal 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 or restore-point to the server's internal disk device.

© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

Booting from a restore-point[7]

When starting the server from the backup disk device that contains the restore-point backup, you can choose the specific restore-point from which to boot.



[7] Due to limitations with Windows native boot functionality, only unencrypted restore-point backups may be booted through bootable image recovery at this time.

© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

Restoring a System Backup

If you created a restore-point backup, or if you are unable to boot the server to the bootable backup, a system backup can be restored by booting the server to the Casper Startup and Recovery Environment.

If the Casper Startup and Recovery Environment was added to the backup disk device, you can boot the server directly from the backup disk device to perform the restore. When restoring a bootable backup, or when the Casper Startup and Recovery Environment is not present on the backup disk device, a Casper Secure Startup Disk can be used to boot the server to perform the restore. For more information on creating and using a Casper Secure Startup Disk, please see the **Casper Secure Startup Disk Creator Guide**.

Booting a server from the Casper Startup and Recovery Environment may take several minutes. Once it has completed the boot process, Casper SmartRestore™ will attempt to automatically identify the backup and prompt you to begin the restore. If SmartRestore is unable to locate the backup, the Casper console will display. For more information on using Casper SmartRestore to perform a restore, please see the **Casper Secure SmartRestore Guide**.

The following examples illustrate how to manually restore a system backup when Casper SmartRestore is unable to locate the backup.

Example 13: Manually Restoring a Restore-Point Backup. This example shows how to manually restore a backup using the **Restore Image** wizard.

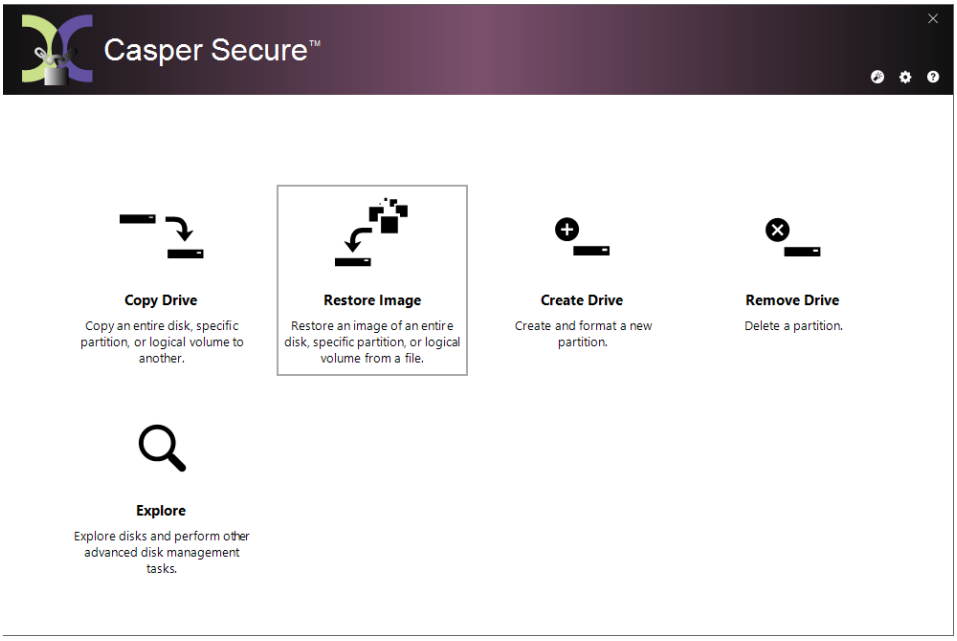
Example 14: Manually Restoring a Bootable Backup. This example demonstrates how to manually restore a bootable backup using the **Copy Drive** wizard.

© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved. January 2025

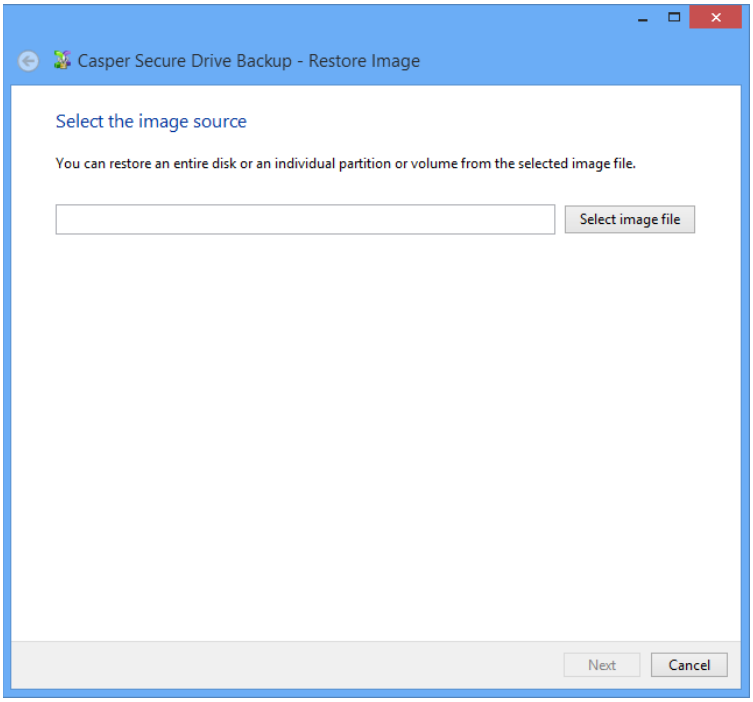
Example 13: Manually Restoring a Restore-Point Backup

Assuming the server is presently booted to the Casper Startup and Recovery Environment and SmartRestore was unable to locate the backup, the following procedure illustrates how to manually restore an image of the server's system disk device to either the original system disk device or a replacement disk device.

1. Select **Restore Image**.

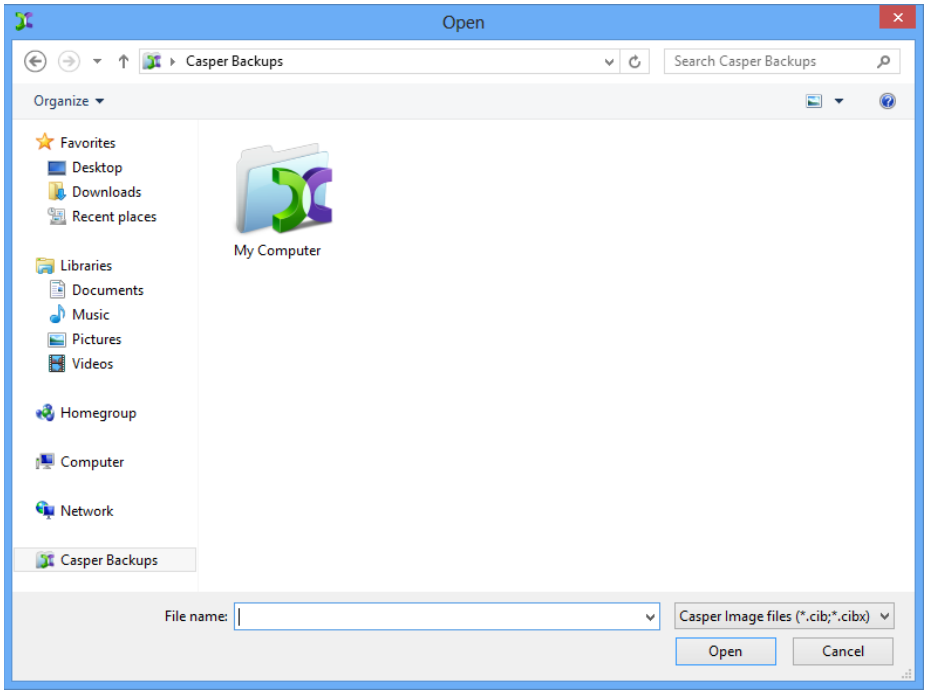


2. Click **Select image file**.



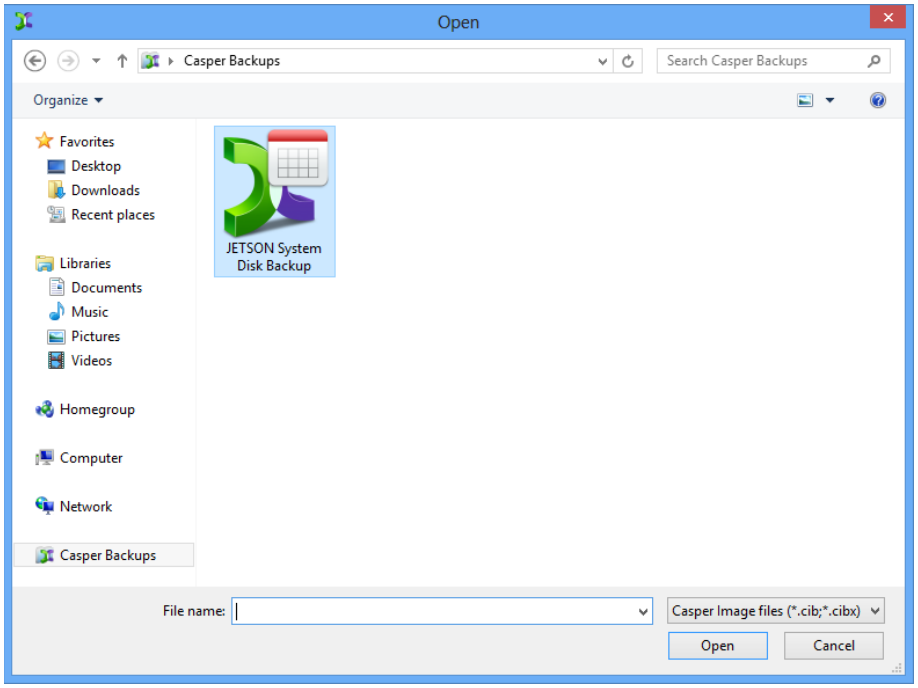
© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

3. In the Open dialog, navigate to the folder that contains the backup you want to restore. By default, the **Casper Backups** folder will be selected. This special folder provides direct access to all of the restore-point backups that were discovered. Double-click the **My Computer** folder to see all of the restore-point system backups that were located for the server.

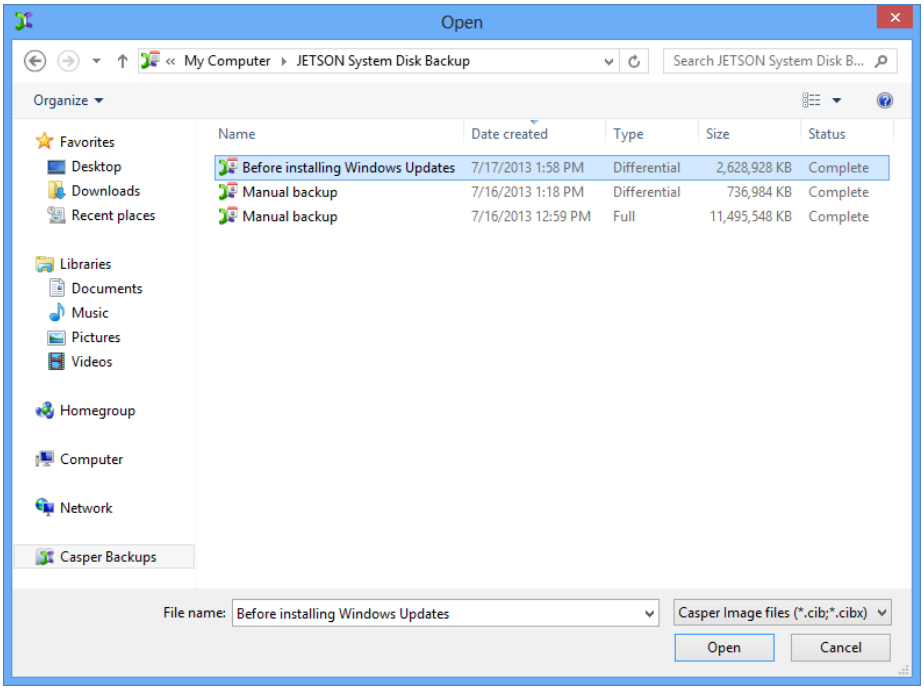


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

4. Select the backup you want to restore and click **Open**.

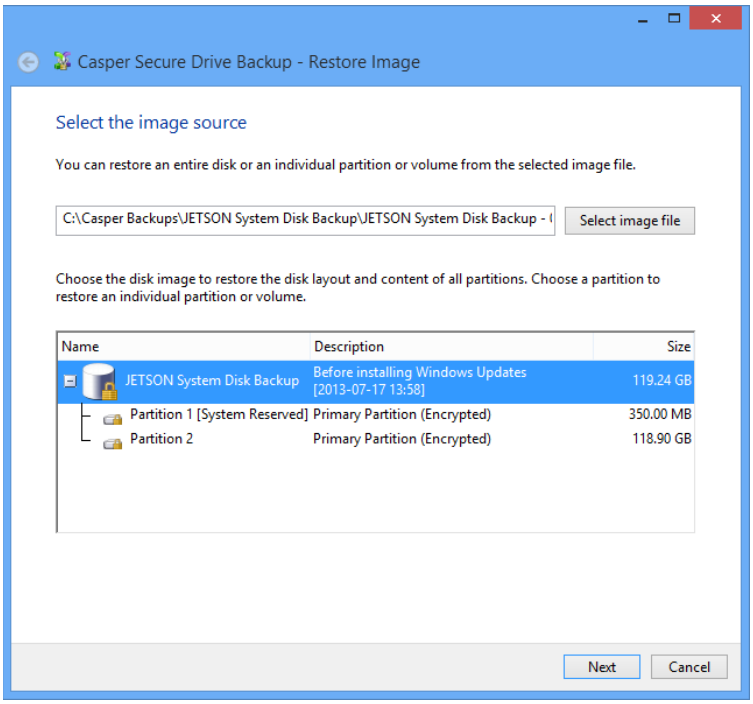


5. Select the image you want to restore and click **Open**.

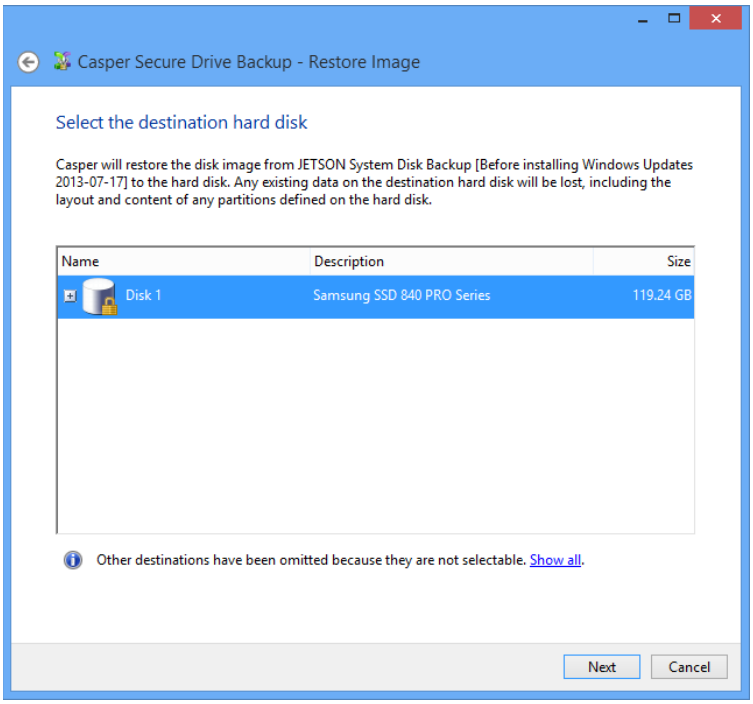


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

6. Once the selected image has loaded, click **Next**.

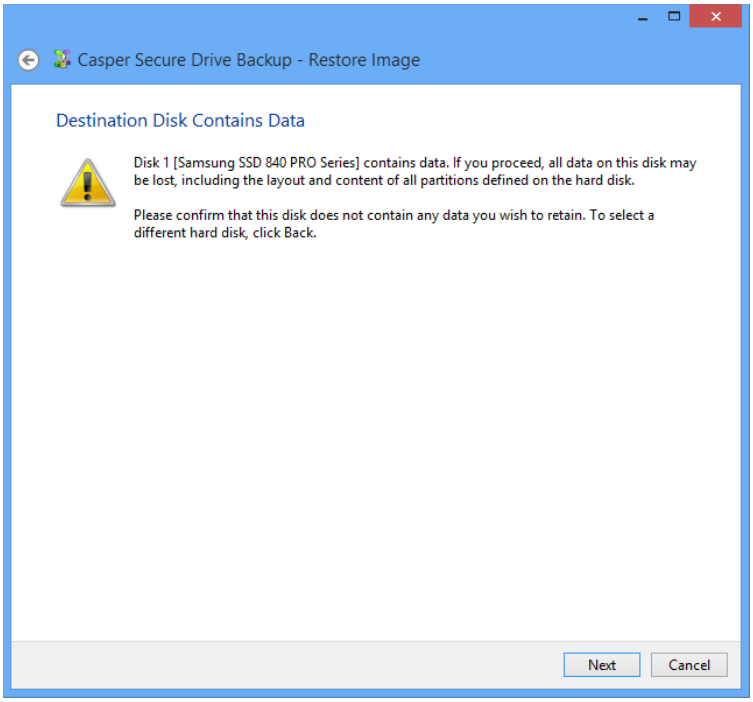


7. Select the disk device that will become the restored Windows system disk as the destination and then click **Next**.

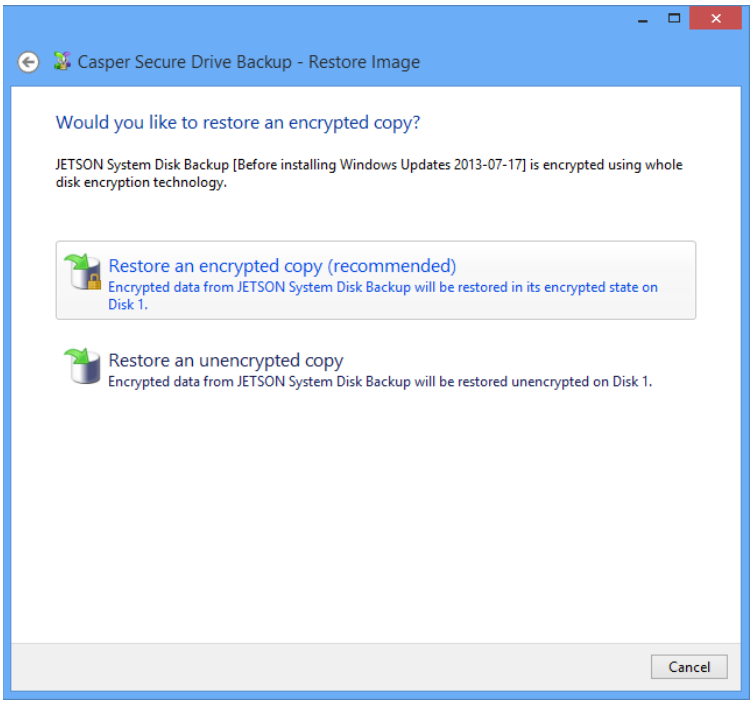


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

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

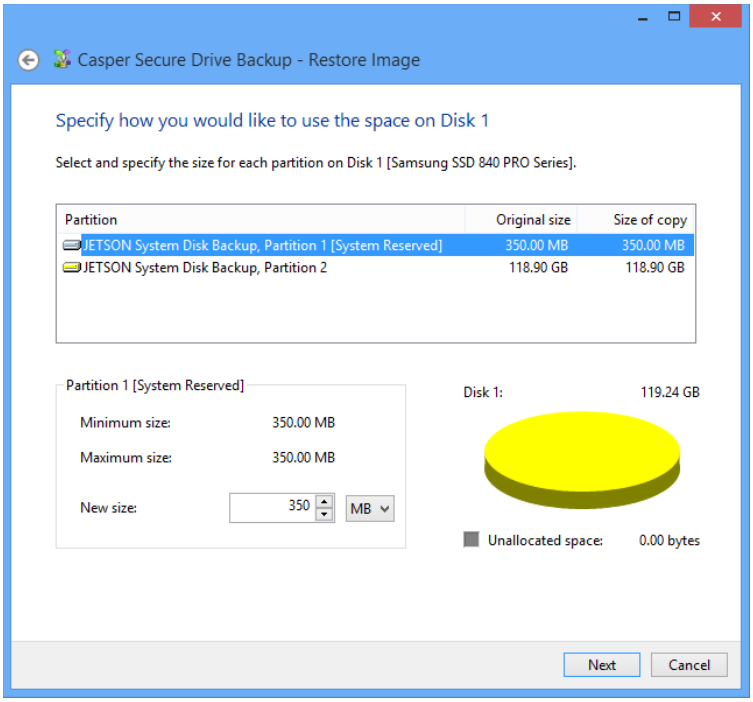


9. If the source image is encrypted using drive encryption technology, Casper will offer the option of restoring an unencrypted copy unless prohibited by administrative policy settings. Click **Restore an encrypted copy**

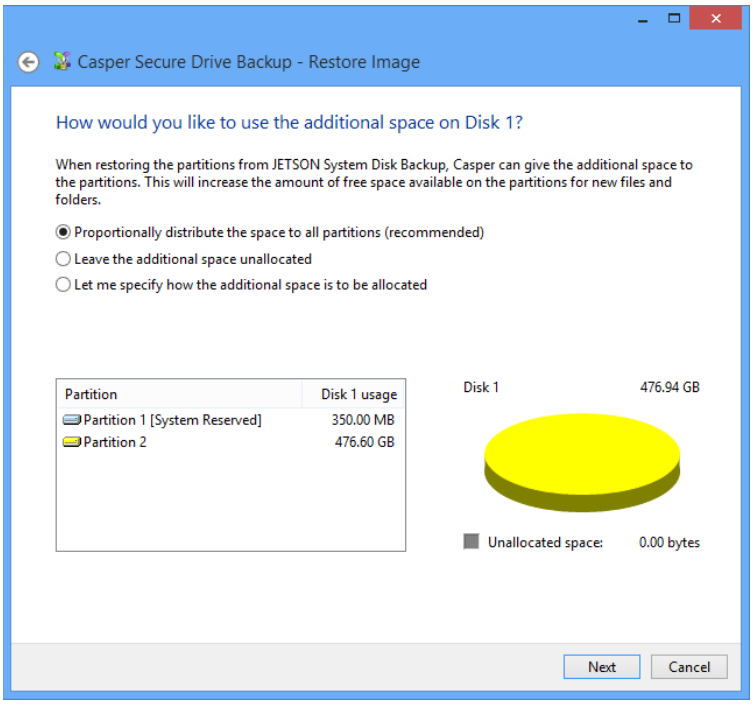


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved. January 2025

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



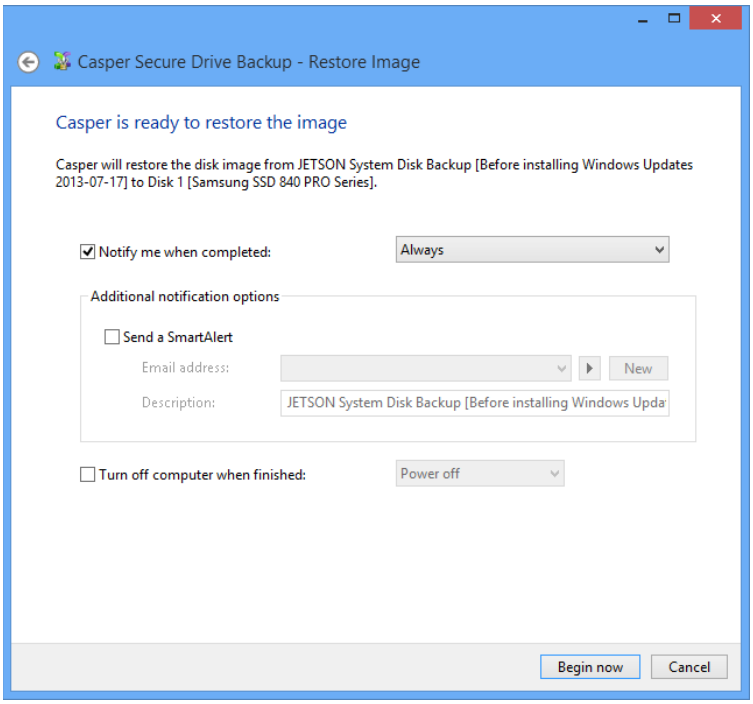
If restoring the image to a disk device that is larger than the original, the default option will be *Give all of the space to the partition* or *Proportionally distribute the space to all partitions* when there is more than one partition defined in the image.



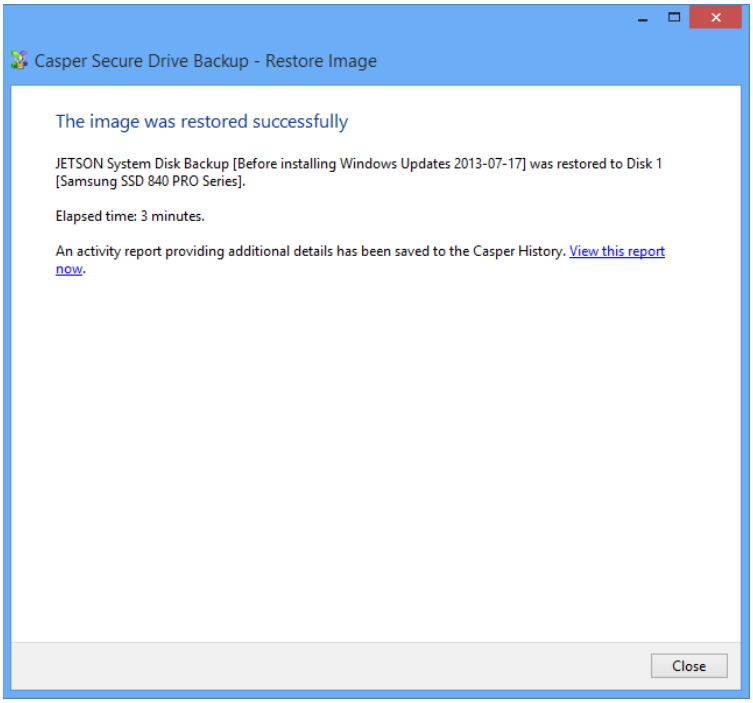
Simply clicking **Next** to accept the default selection or value is generally best.

© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

11. Click **Begin now** to begin the image restoration process.



12. When Casper has completed the restoration process, click **Close**.

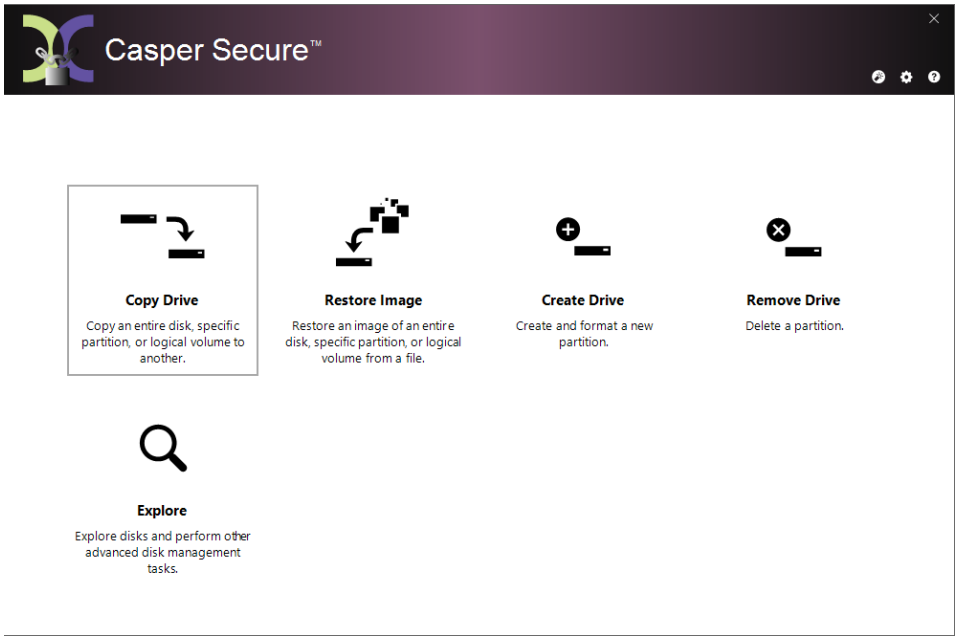


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

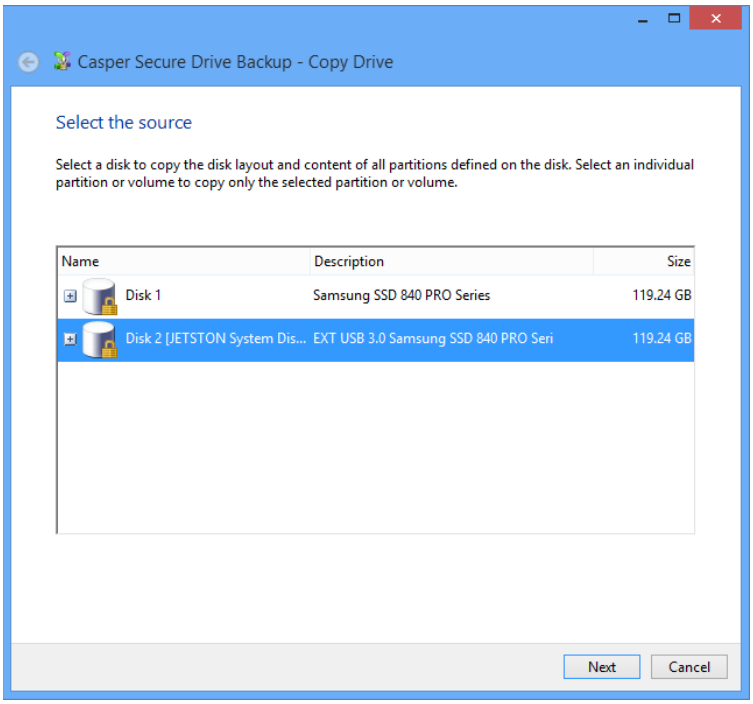
Example 14: Manually Restoring a Bootable Backup

Assuming the server is presently booted to the Casper Startup and Recovery Environment and SmartRestore was unable to locate the backup, the following procedure illustrates how to manually restore a bootable backup of the server's system disk device to either the original system disk device or a replacement disk device

1. Select **Copy Drive**.

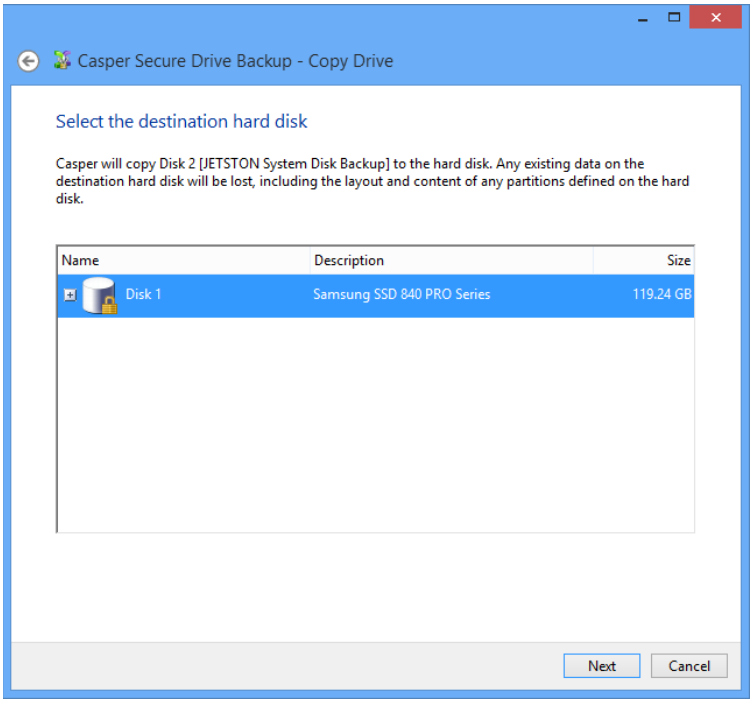


2. Select the disk device containing the bootable backup to restore as the source and click **Next**.

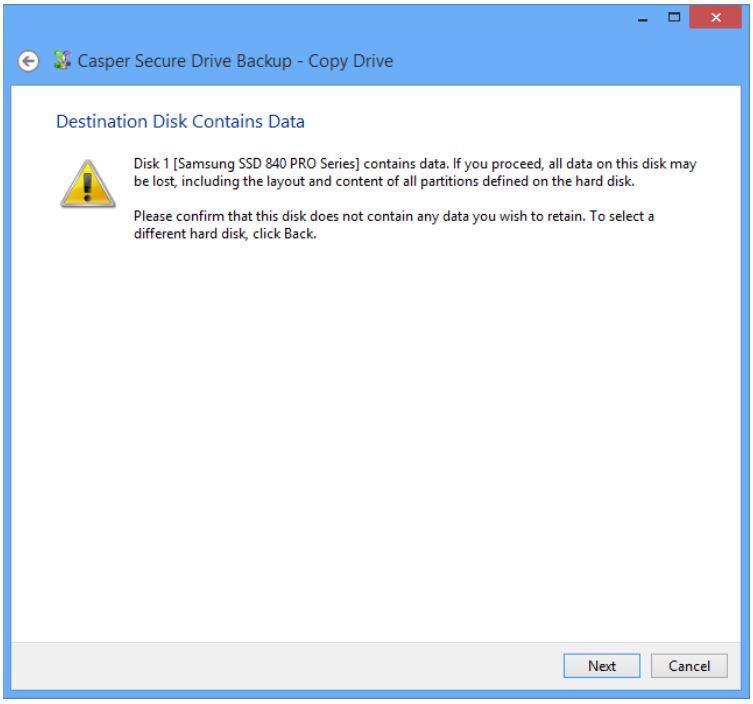


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

3. Select the disk device that will become the restored Windows system disk as the destination and then click **Next**.

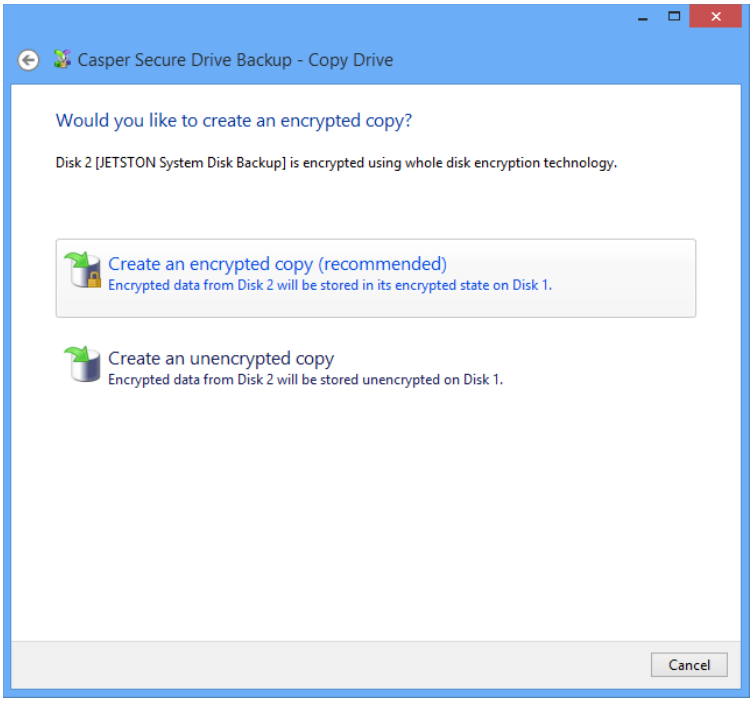


4. If the selected destination defines a partition or contains data, Casper will warn you that the contents will be overwritten. Confirm you have selected the correct disk device to receive the restored backup and click **Next** to proceed.

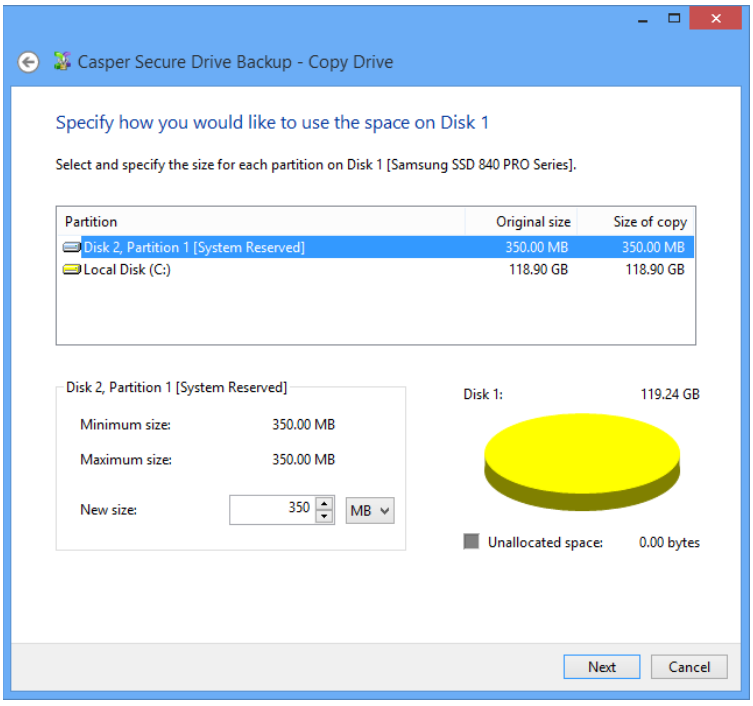


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved. January 2025

5. If the backup device is encrypted using drive encryption technology, Casper will offer the option of creating an unencrypted copy unless prohibited by administrative policy settings. Click **Create an encrypted copy**

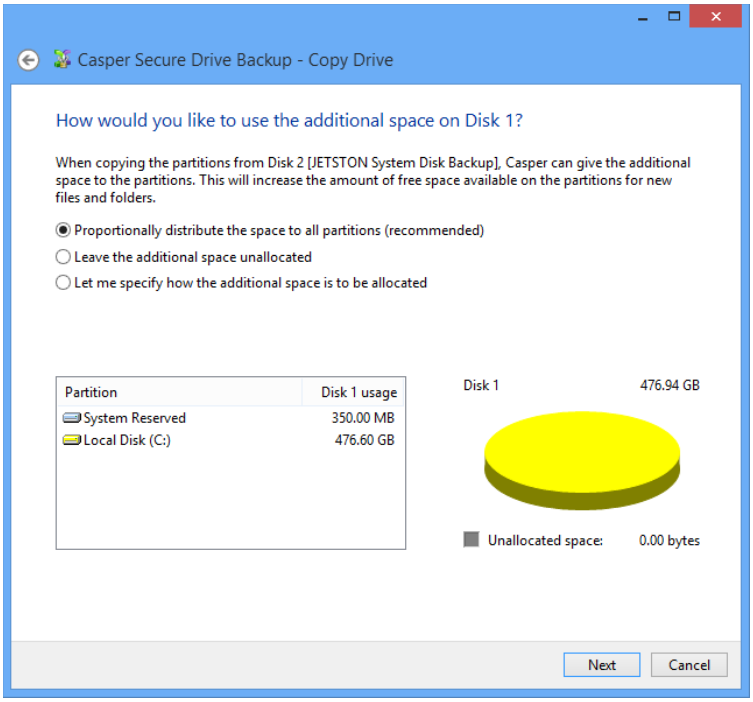


6. When prompted to specify how the space on the destination device is to be used, retain the default selection and click **Next**. If the destination is the same size or smaller than the backup source, Casper will ask you to manually configure how the space is to be used.



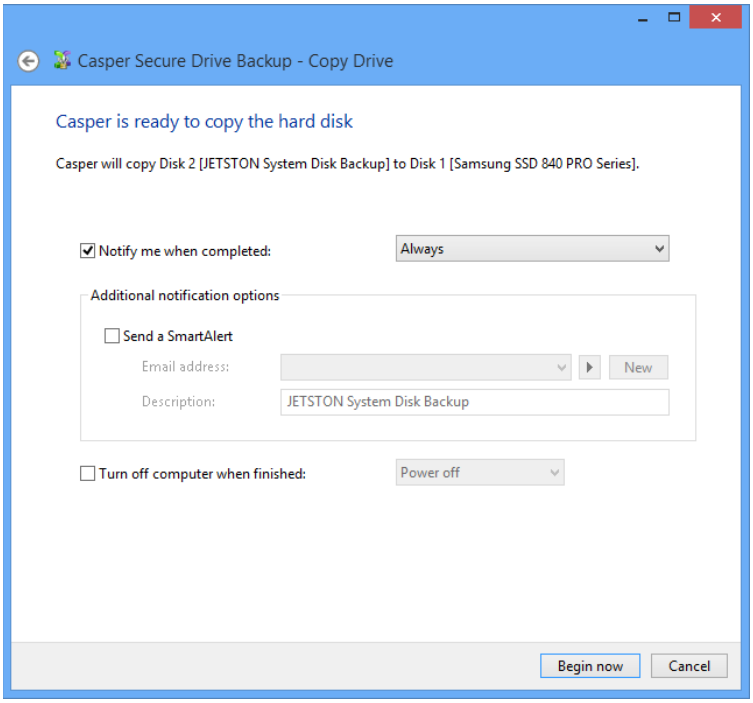
© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

When the destination is larger than the backup 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 backup source.



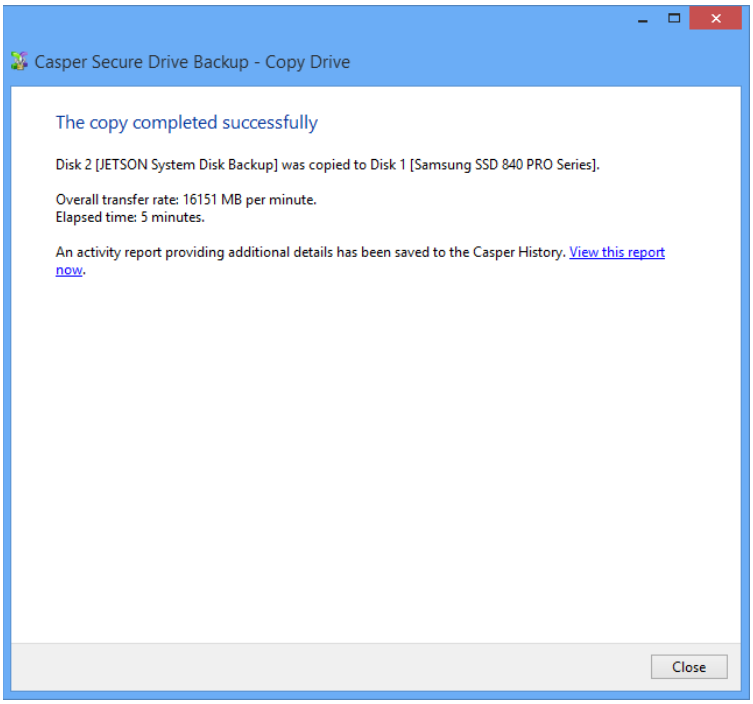
Simply clicking **Next** to accept the default selection or value is generally best.

7. Click **Begin now** to begin the cloning process.



© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

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



© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

Retrieving Specific Files and Folders from a Backup

You can retrieve a specific file or folder from a backup without booting to the backup or performing a restore. Because a bootable backup is a clone of the server's system disk device, it can be accessed in the same manner as the system disk device whenever it is connected to the server. Similarly, the contents of a restore-point backup can be accessed in the same manner as the server's system disk device whenever it has been mounted.

The following examples illustrate how to access the contents of a backup to retrieve specific files and folders without booting or restoring the entire backup.

Example 15: Accessing the Contents of a Bootable Backup. This example shows how to browse a bootable backup using Windows File Explorer to retrieve a file located in the [*My*] *Documents* folder.

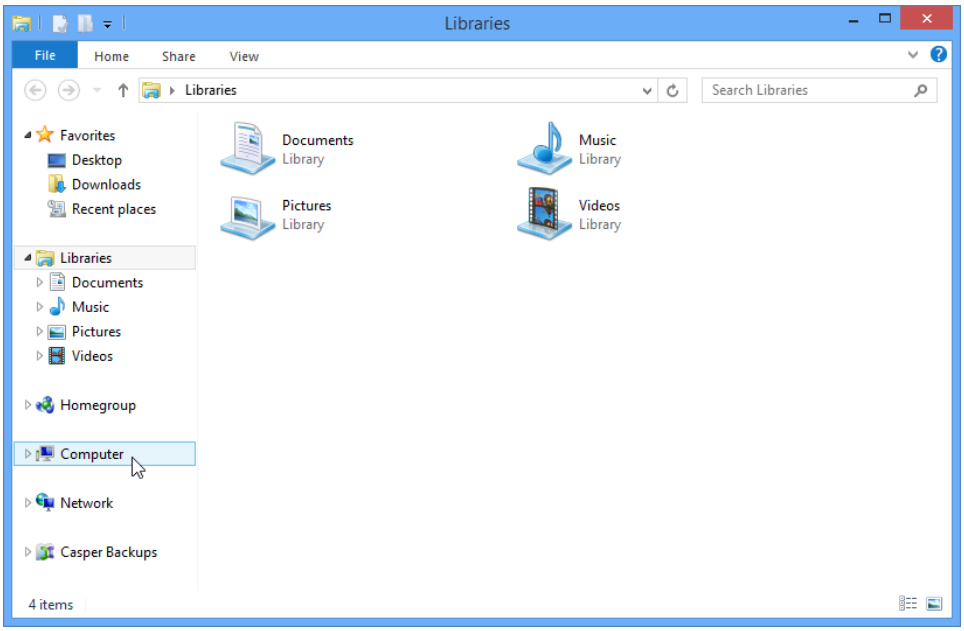
Example 16: Accessing the Contents of a Restore-Point Backup. This example demonstrates how to use Windows File Explorer to mount a specific restore-point within a restore-point backup and retrieve a file from the *Documents* folder of the backup.

© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

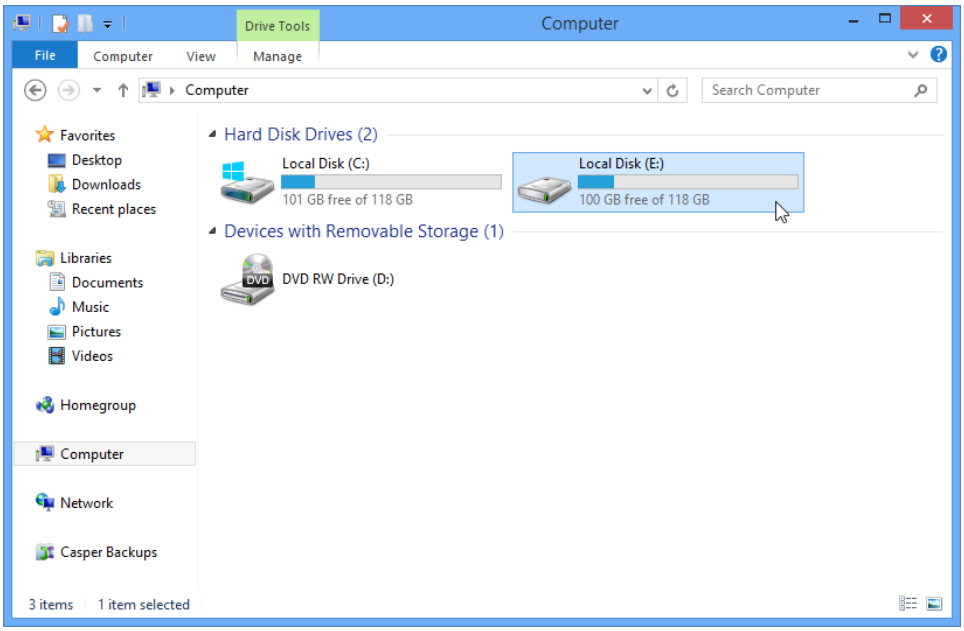
Example 15: Accessing the Contents of a Bootable Backup

Assuming the disk device containing the bootable backup is currently installed or attached to the server, the following procedure illustrates how to browse the contents of the backup to retrieve a specific file from the [*My*] *Documents* folder.

1. Open **This PC** or [**My**] **Computer**. On Windows Server 2012, start **Windows File Explorer** and then click **This PC**. On Windows Server 2008 and earlier, simply click [**My**] **Computer** on the *Start* menu.

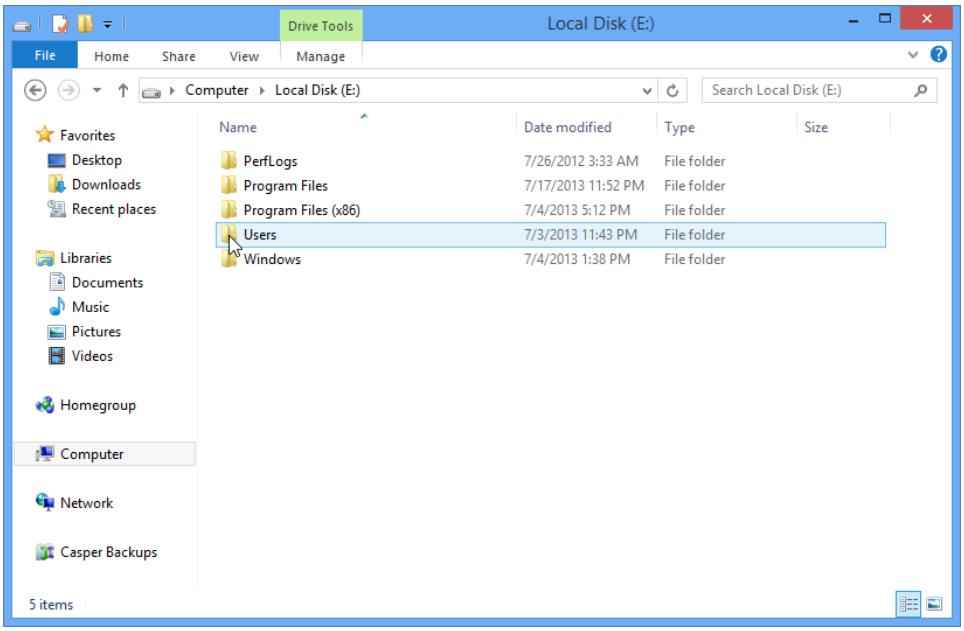


2. Double-click the drive containing your bootable backup. In this example, **Local Disk (E:)** represents the drive letter assigned by Windows to the backup drive.

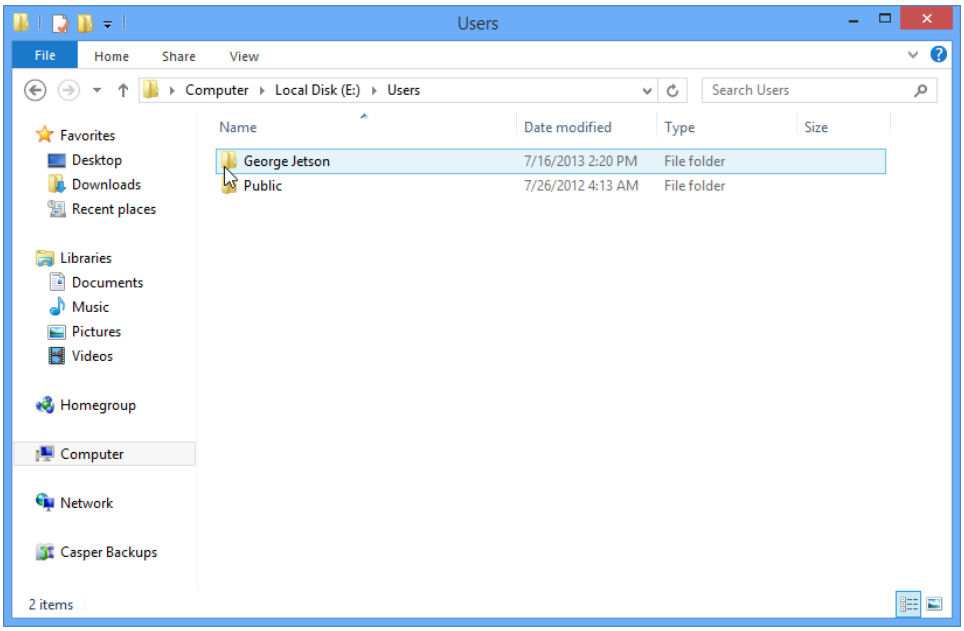


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

3. Double-click **Users** to open the Users folder.

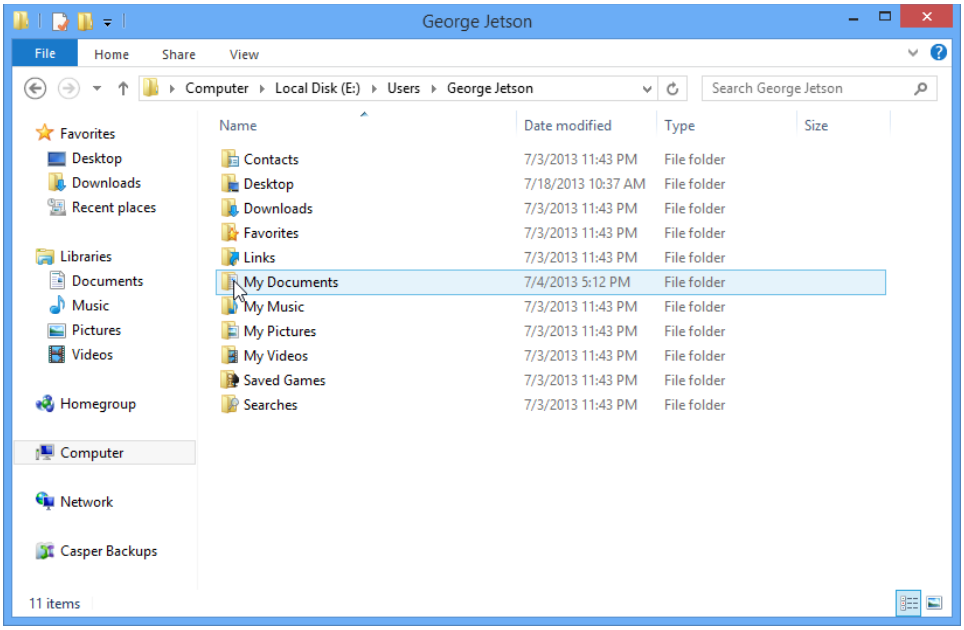


4. Double-click the folder that corresponds to the account name with which you normally log onto the computer. In this example, the user logs on as **George Jetson.**

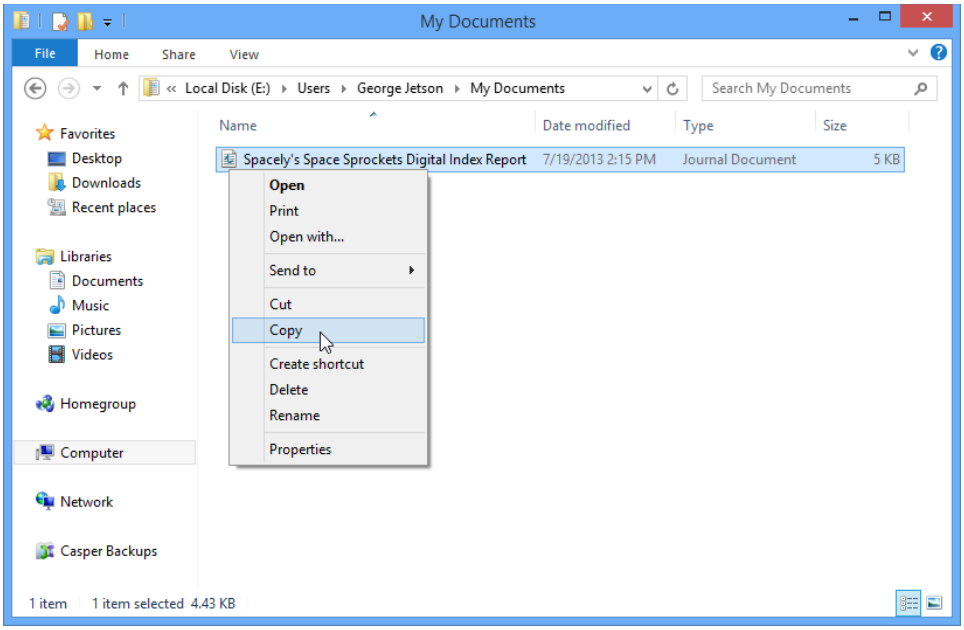


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

5. Double-click the [**My**] **Documents** folder to access the contents of the *Documents* folder. The contents of this folder will represent the original contents of the *Documents* folder appearing on the system drive when the backup was created.



6. Once you have located the desired file or folder, you can access or copy it as you would any other file on the original drive.

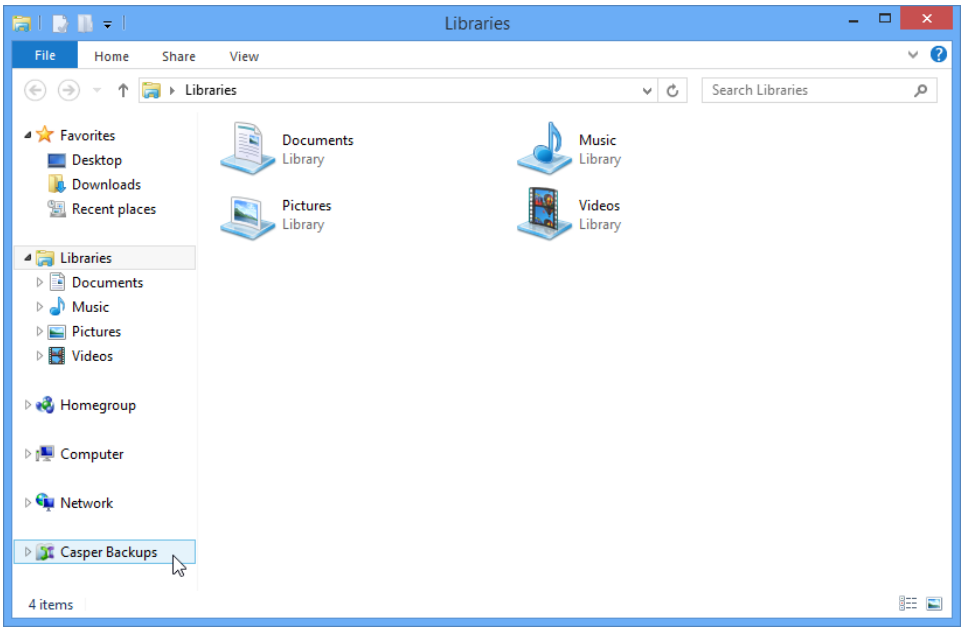


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

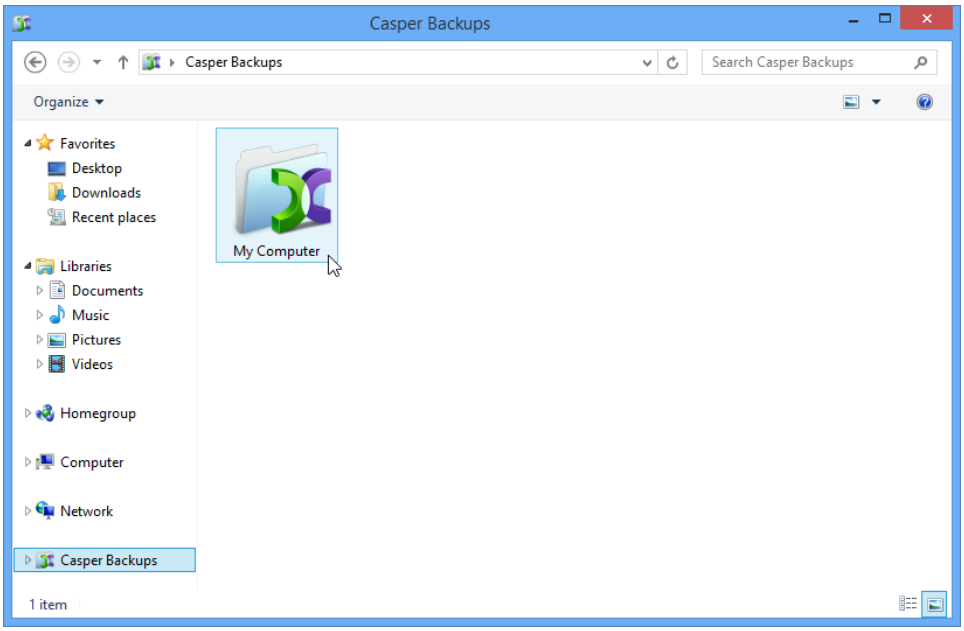
Example 16: Accessing the Contents of a Restore-Point Backup

Assuming the backup device containing the restore-point backup is currently installed or attached to the server, the following procedure illustrates how to mount a restore-point backup and retrieve a specific file from the *Documents* folder.

1. Open the **Casper Backups** folder. On Windows Server 2012, start **Windows File Explorer** and then click **Casper Backups**. On Windows Server 2008 and earlier, open **Windows Explorer** and click **Casper Backups**.

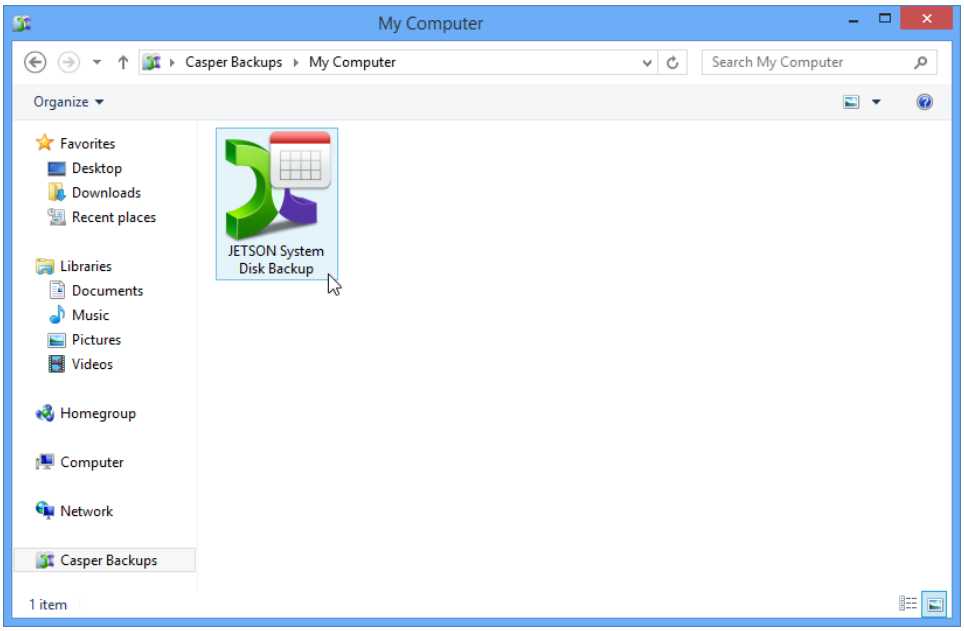


2. Double-click the **My Computer** folder to browse all of the restore-point backups discovered for the server.

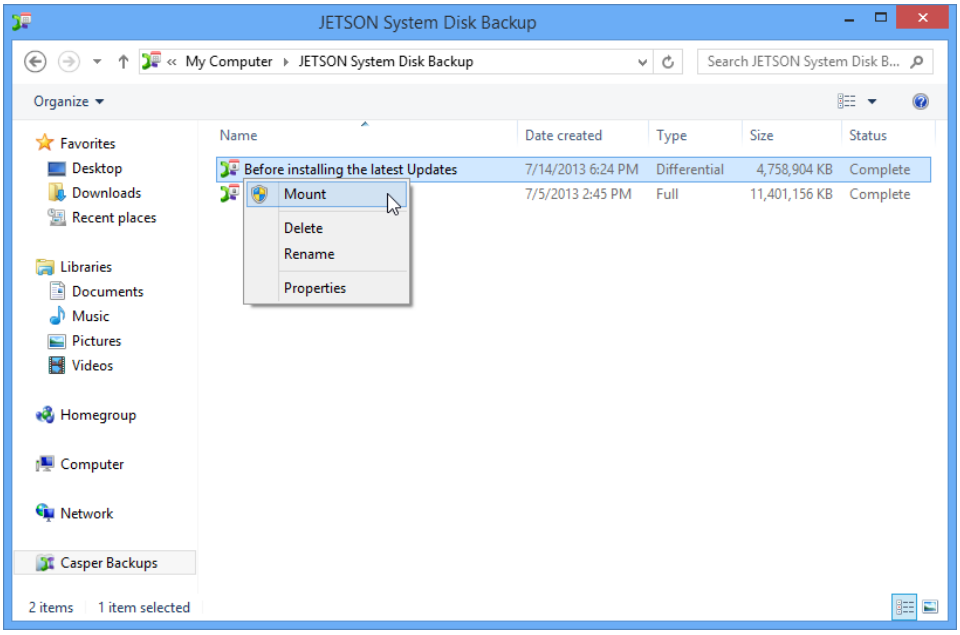


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

3. Double-click the backup containing the restore-point you want to access.

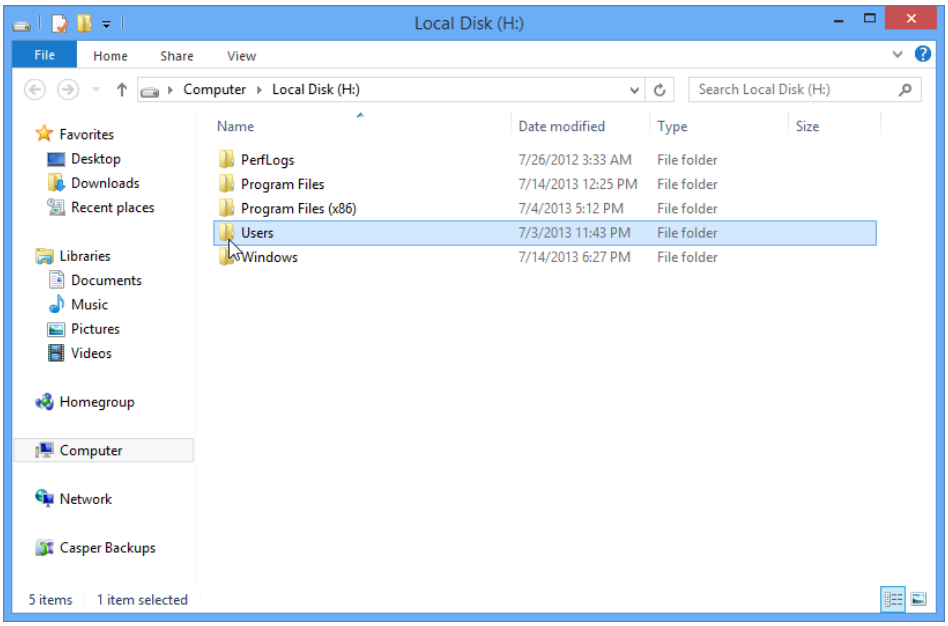


4. Right-click on the desired restore-point, and then click **Mount**.

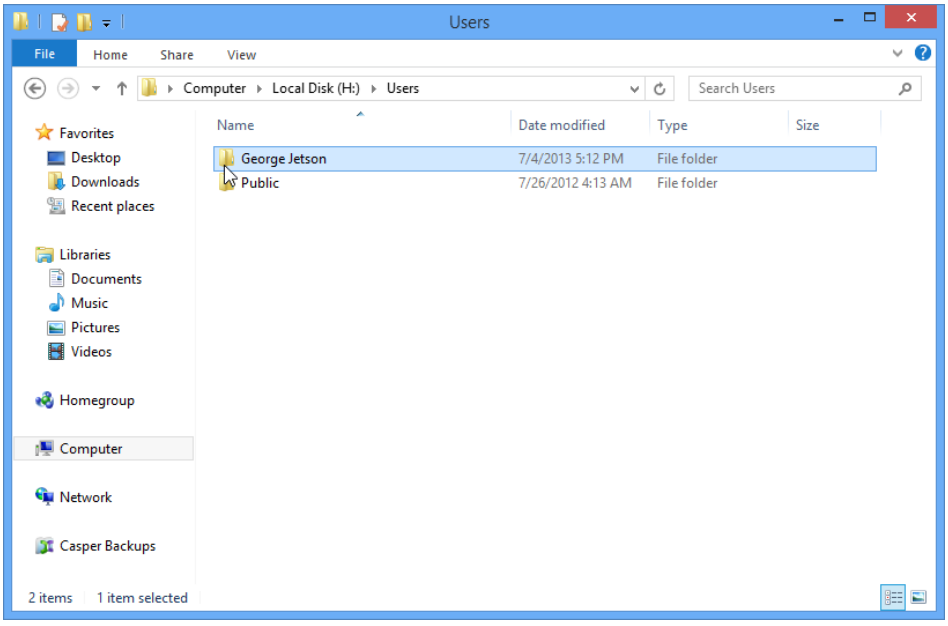


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

5. After the restore-point has been mounted and a drive letter has been assigned, a new Explorer window will open to reveal its contents. In this example, **Local Disk (H:)** was assigned to the restore-point when it was mounted. Double-click **Users** to open the Users folder.

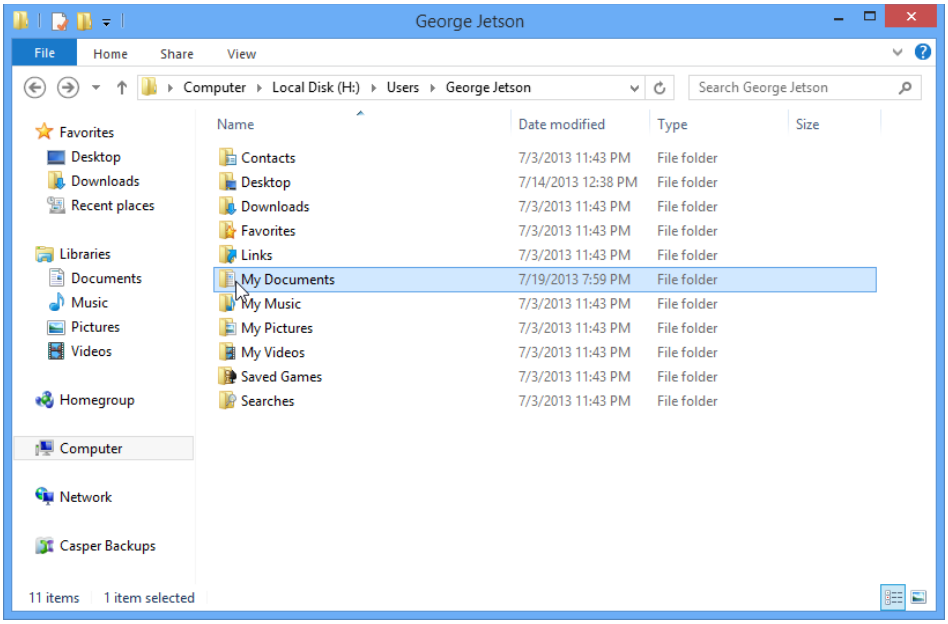


6. Double-click the folder that corresponds to the account name with which you normally log onto the computer. In this example, the user logs on as **George Jetson.**

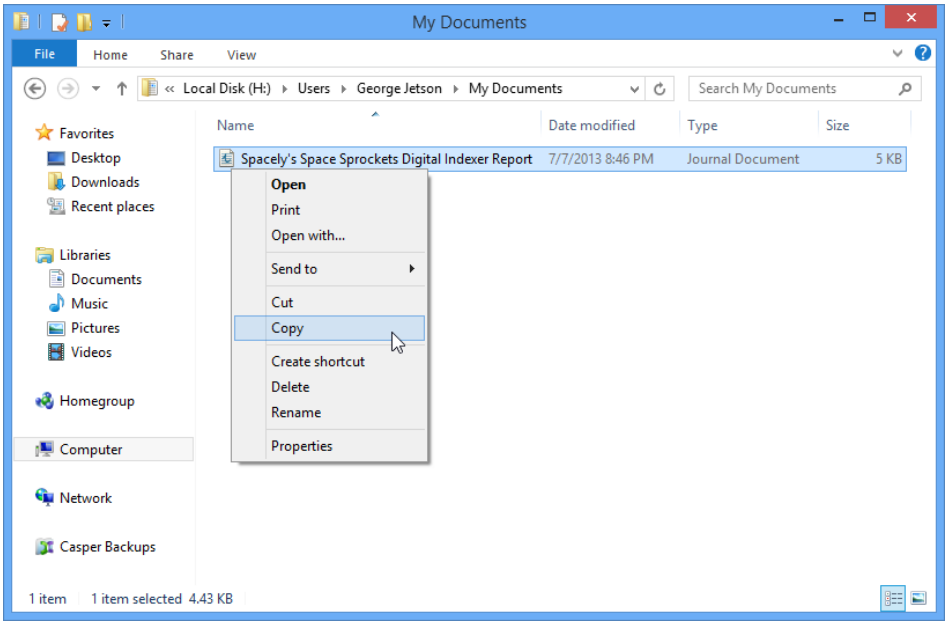


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

7. Double-click the [**My**] **Documents** folder to access the contents of the *Documents* folder. The contents of this folder will represent the original contents of the *Documents* folder appearing on the system drive when the backup was created.

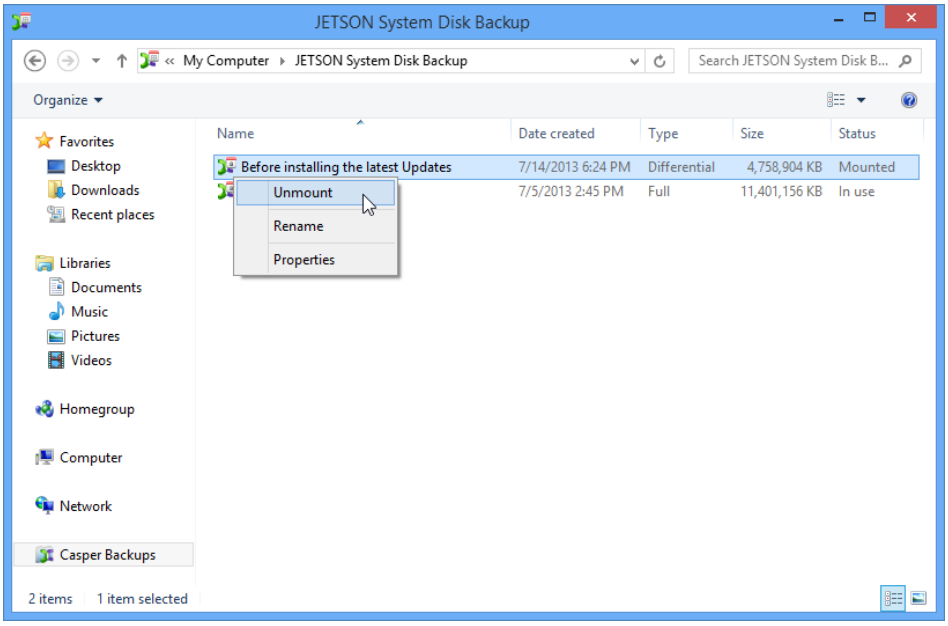


8. Once you have located the desired file or folder, you can access or copy it as you would any other file on the original drive.



© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved. January 2025

9. When you have finished accessing the contents of the restore-point, right-click on the restore-point and select **Unmount**.



© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

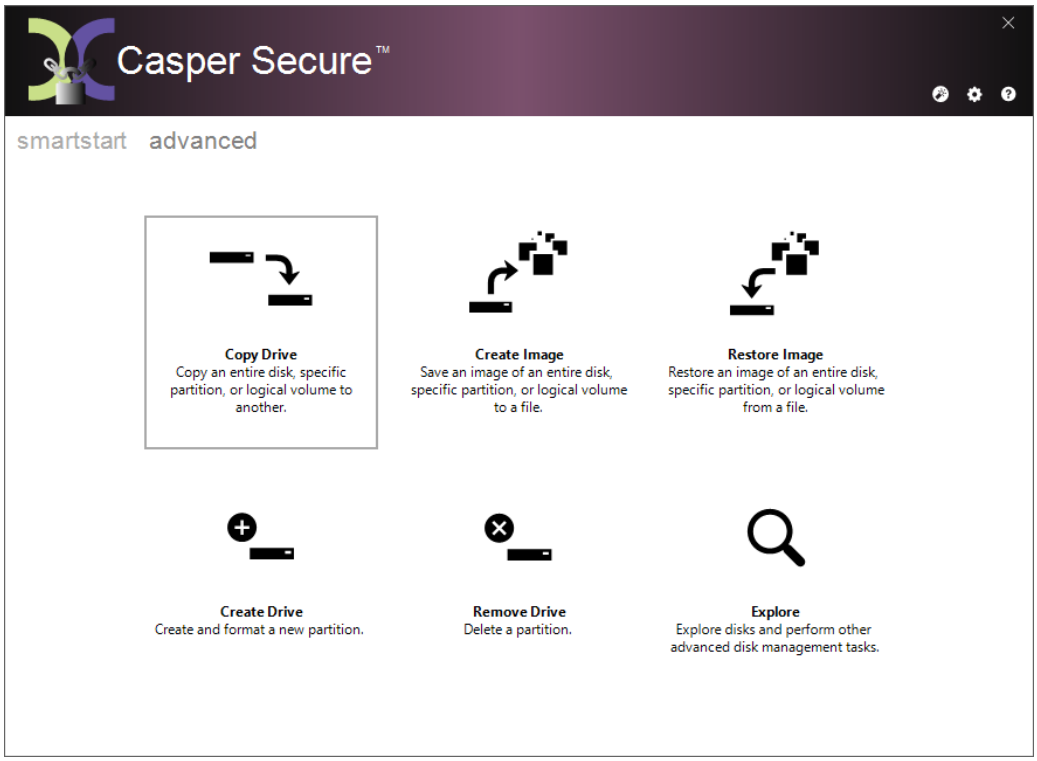
Upgrading a Hard Disk

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 device using an external USB, Firewire, or eSATA enclosure or bridge adapter.

Example 17: Upgrading a Hard Disk

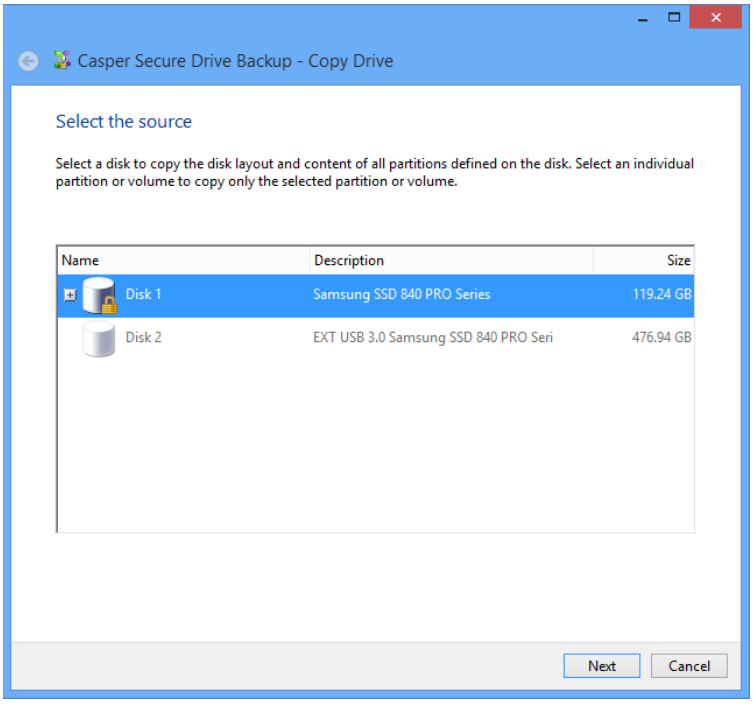
Assuming the new disk device is currently installed or attached to the system, the following procedure illustrates how Casper may be used to clone the original disk device to the new disk device and complete the upgrade.

1. Select **Copy Drive**.

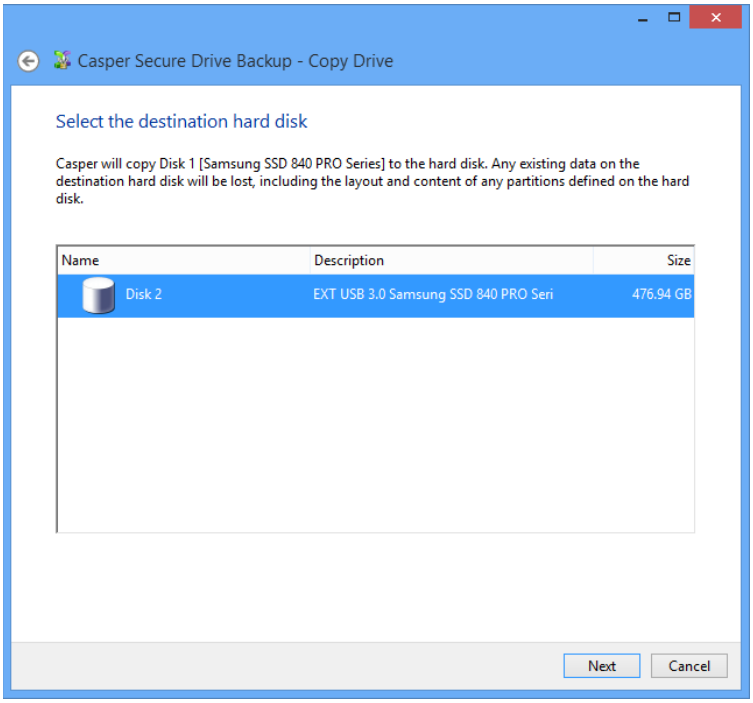


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

2. Select the disk device to be upgraded (e.g., the hard disk or RAID array on which Windows Server has been installed) as the source and click **Next**.

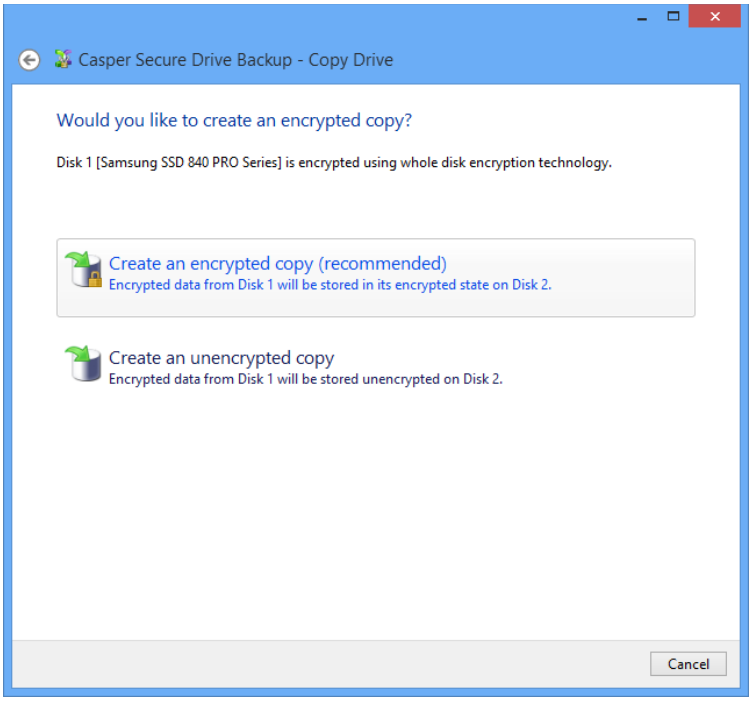


3. Select the new disk device as the destination and click **Next**.

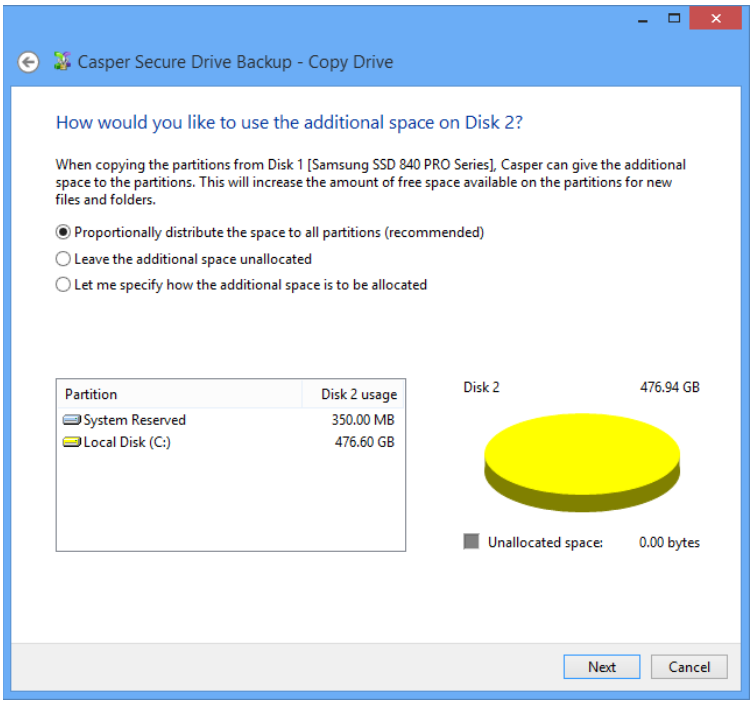


© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

4. If the source device is encrypted using a supported drive encryption technology, Casper will offer the option of creating an unencrypted copy unless prohibited by administrative policy settings. Click **Create an encrypted copy**.

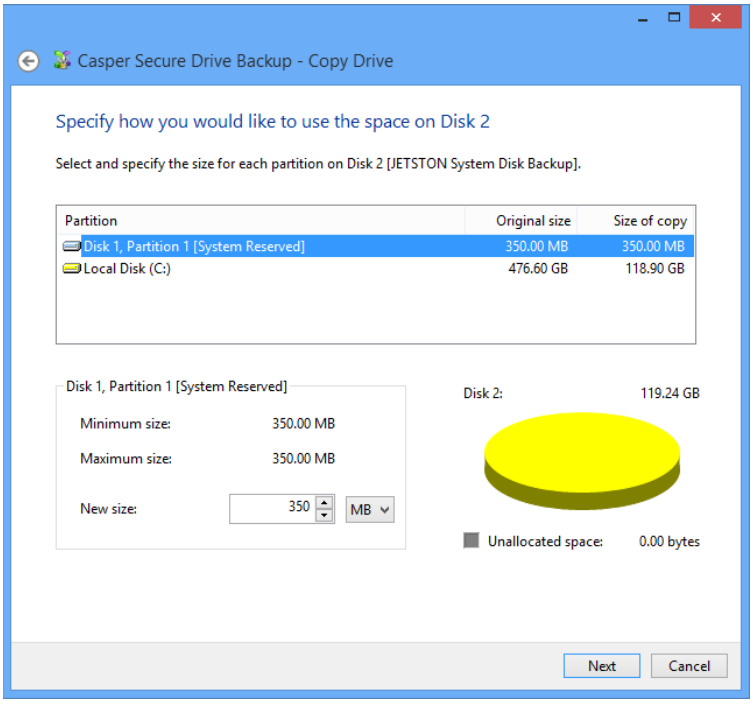


5. When prompted to specify how the additional space on the new hard disk is to be used, retain the default selection and click **Next**. When the new hard disk is larger than the original disk, the default option will be *Give all of the space to the partition* or *Proportionally distribute the space to all partitions* when there is more than one partition defined.



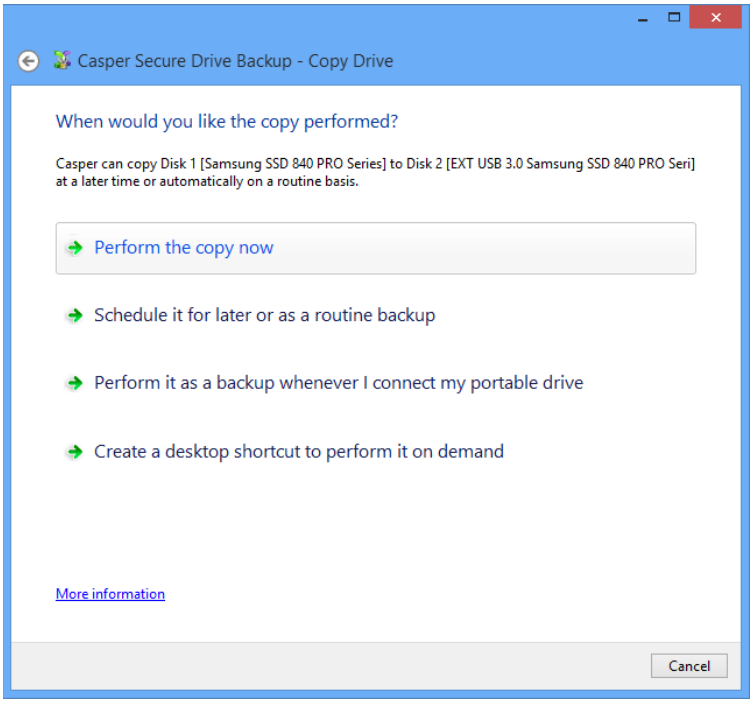
© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

If the new disk device is the same size or smaller than the original disk device, Casper will ask you to manually configure how the space is to be used.



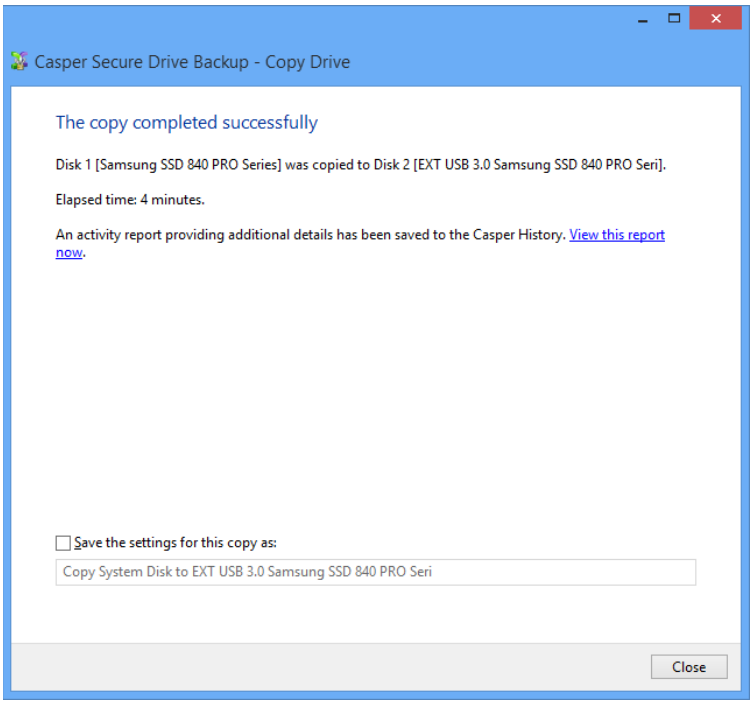
Simply clicking **Next** to accept the default selection or value is usually best. For additional help with making a selection, press **F1**.

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



© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.

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



8. Shutdown and power-off the server.
9. Reconfigure the server to replace the original disk device with the new disk device.

© Copyright 2005-2025 Future Systems Solutions, Inc. All Rights Reserved.