CASPER SECURE™

TECH EDITION 6.0

USER GUIDE

Future Systems SOLUTIONS

Copyright and Trademark Information

Table of Contents

Introduction

Casper Secure™ Tech Edition is a disk cloning and imaging solution engineered specifically for computer technicians, system integrators, and IT departments needing to upgrade, replace, back up, restore and re-image drives and hardware RAID arrays that have been encrypted with Windows® BitLocker® Drive Encryption or Symantec (PGP®) Encryption technology[1].

Casper Secure Tech Edition offers these unique benefits:

- **Only Drive Imaging and Backup Solution Designed Specifically for Whole Disk Encrypted Systems** — completely eliminates the security and compliance risks associated with other drive imaging and backup and recovery products by ensuring all data always remains in its original encrypted state. *Data is never left exposed when backed up or restored, preserving 100% compliance with data security directives.*

- **Complete Drive Cloning and Imaging for Whole Disk Encrypted Systems** — creates a completely encrypted copy of an encrypted drive in one step, eliminating hours of unproductive downtime. Unlike other drive cloning and drive imaging solutions that can produce only an unencrypted copy of a whole disk encrypted drive, Casper Secure Tech Edition creates a copy that retains all of the encrypted data in its original encrypted state.

- **Fast Encrypted Drive Upgrades and Replacements** — quickly duplicates a whole disk encrypted drive to another drive without requiring a laborious and time consuming backup, restore, and re-encryption process. Since all data is maintained in its original encrypted state, Casper Secure Tech Edition makes it extraordinarily easy to quickly upgrade a whole disk encrypted system to a larger hard disk or faster solid state drive.

- **Complete Encrypted Disk Image Backups** — provides complete support for creating, maintaining, and restoring disk image file backups for whole disk encrypted drives in their original encrypted state that can be stored safely just about anywhere, including network attached storage devices and on drives containing other data. In addition, exclusive SmartClone™ technology safely eliminates the redundant transfer of data during the imaging process, saving valuable time by dramatically reducing the time required to update a backup, restore, or re-image a Windows system using whole disk encryption technology.

- **Rapid Recovery, Re-imaging, and Deployment** — eliminates the arduous data restoration and lengthy re-encryption process required by other disk imaging and backup solutions. A backup created by Casper Secure Tech Edition can be used as an immediate and permanent replacement for a failed hard disk or restored to a new disk in its original encrypted state in a single step.

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

[1] Casper Secure Tech Edition currently supports only software-based drive encryption.

System Requirements

While Casper Secure Tech Edition is designed to run on virtually all Windows 2000 and later systems, installation and creation of the Casper Secure Tech Edition Startup Disk must be performed on a system running Windows XP (SP3) or later.

Installation Requirements

- Windows 11, Windows 10, Windows 8.x, Windows 7, Windows Vista, Windows XP (SP3), Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, Windows Server 2003 R2, or Windows Server 2003
- 10 GB available disk space
- 4 GB RAM (8 GB or more recommended)
- Windows 11 Assessment and Deployment Kit, Windows 10 Assessment and Deployment Kit, Windows 8 Assessment and Deployment Kit (ADK), or Windows 7 Automated Installation Kit (AIK)

Run-time Requirements

- Windows 11, Windows 10, Windows 8.x, Windows 7, Windows Vista, Windows XP, Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, Windows Server 2003 R2, Windows Server 2003, Windows 2000 Workstation, Windows ME, Windows 98, or Windows 95[2]
- Windows BitLocker Drive Encryption[3], Symantec Endpoint Encryption (SEE), Symantec Encryption Desktop (SED) version 10.x, or PGP Desktop version 9.6x or later[4]
- 500 MB available disk space
- 2 GB RAM (4 GB or more recommended)
- Periodic Internet connection for license activation and verification purposes

[2] Casper Secure Tech Edition is not designed for use with Windows NT, Windows 2000 Server, and Windows 2000 Advanced Server. Background copying not supported on Windows 2000. Windows ME, 98, and 95 systems may be imaged only when booting and running from Casper Secure Tech Edition Startup Disk. Virtual disk image file backups are supported only when running on Windows 7 and later or when booting and running from the Casper Secure Tech Edition Startup Disk. The VHDX image file format is supported only when running on Windows 8 and later or when booting and running from a Casper Secure Tech Edition Startup Disk created with the Windows 8 or later ADK.

[3] 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.

[4] 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.

Getting Help

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

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

Casper Secure Tech Edition Setup

The Casper Secure Tech Edition Setup program will install the Startup Disk Creator wizard, which is used to create and configure a startup disk from which Casper Secure Tech Edition can be run.

Installing Casper Secure Tech Edition

1. Start the Casper Secure Tech 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 Tech Edition Setup program.

Installing the Windows Preinstallation Environment

The Microsoft Windows Preinstallation Environment (WinPE) must be installed prior to creating a Casper Secure Tech Edition Startup Disk. The Startup Disk Creator is compatible with WinPE 3.x[5], WinPE 4.0, WinPE 5.x, WinPE 10, and WinPE 11. If a compatible version of WinPE is not available, the Startup Disk Creator will automatically download and install a copy for you.

[5] Casper Secure Tech Edition does not support the VHDX image file format when running within WinPE 3.x (Windows 7 AIK).

Creating, Updating, and Using a Startup Disk

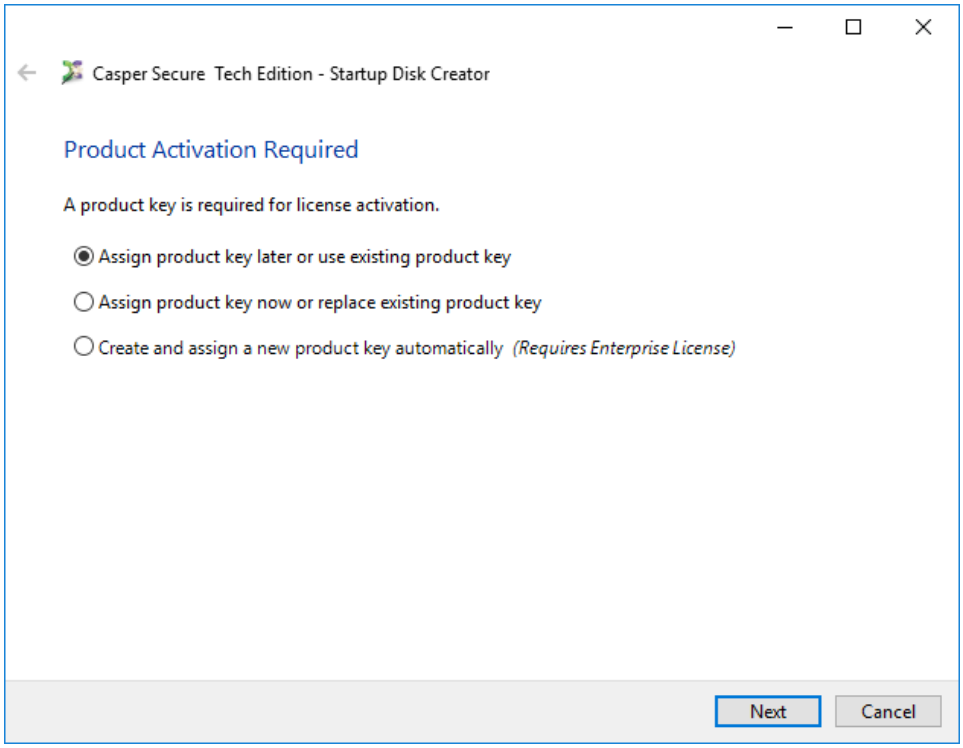
A Startup Disk allows you to use Casper Secure Tech Edition on a computer without having to separately install Casper Secure Tech Edition on the computer. It also can be used to boot a computer and run Casper Secure Tech Edition within a self-contained Windows environment (WinPE).

Creating or Updating a Casper Secure Tech Edition Startup Disk

1. Open **Startup Disk Creator**. (Start -> All Apps -> Startup Disk Creator for Casper Secure Tech Edition)

2. A Casper Secure Tech Edition Product Key is required to activate the software. There are three options:

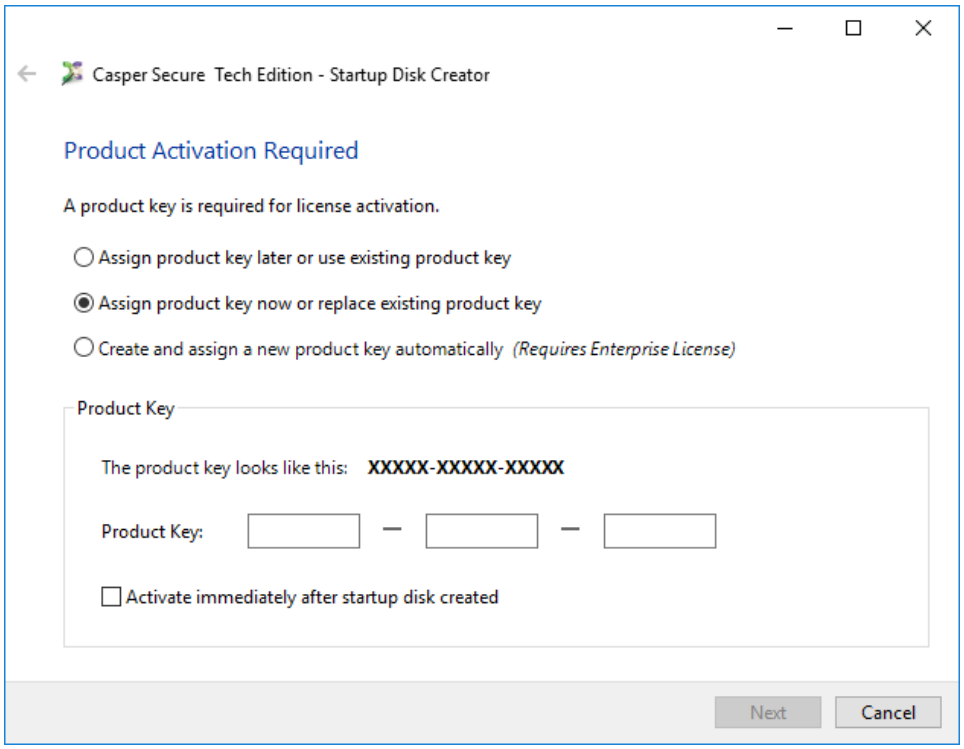
   Assign product key later or use existing product key:



   If you are creating a new Startup Disk and you choose to assign a product key later, you will be prompted to provide the product key when the Startup Disk is first used. This is useful when you are creating a Startup Disk for another user or when you need to create a Startup Disk that will be separately replicated and distributed to a group of users. When updating an existing Startup Disk, choose this option to retain the product key previously assigned to the Startup Disk.

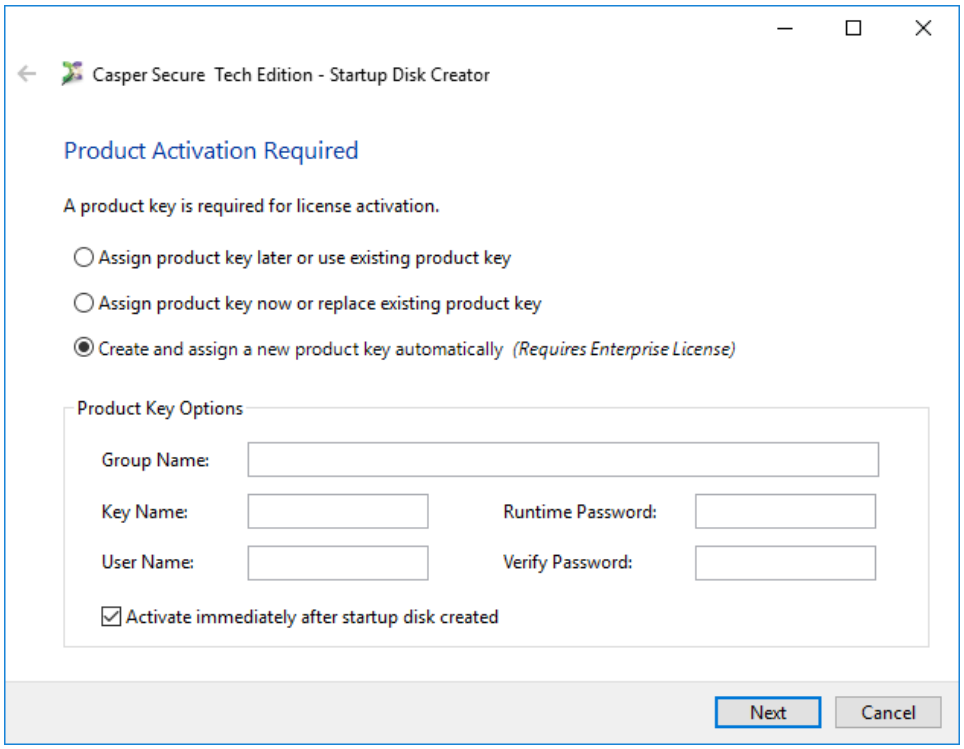
   Internet access is required to complete product activation. If you choose an option to assign or activate a product key later, Internet access will be required to complete the activation process on the computer on which the Startup Disk is first used.

Assign product key now or replace existing product key:



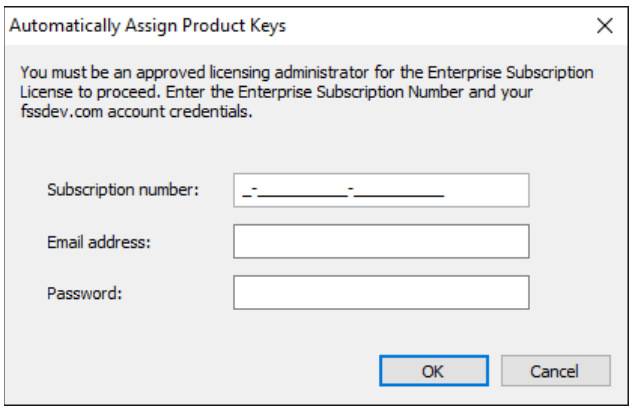
If you choose to assign a product key now, enter your product key and then choose when to complete the software activation process. You may activate the software immediately after the Startup Disk has been created or wait until you first use the Startup Disk. When updating an existing Startup Disk, the product key entered will replace any previously assigned product key.

Create and assign a new product key automatically:



If you are the license administrator for an enterprise subscription license, you may choose to have a new product key created and assigned automatically. This is the quickest and most efficient option when you need to create and distribute a large number of Startup Disks throughout an organization.

When you first select *Create and assign a new product key automatically*, you will be prompted to enter the enterprise subscription number and your fssdev.com account credentials.

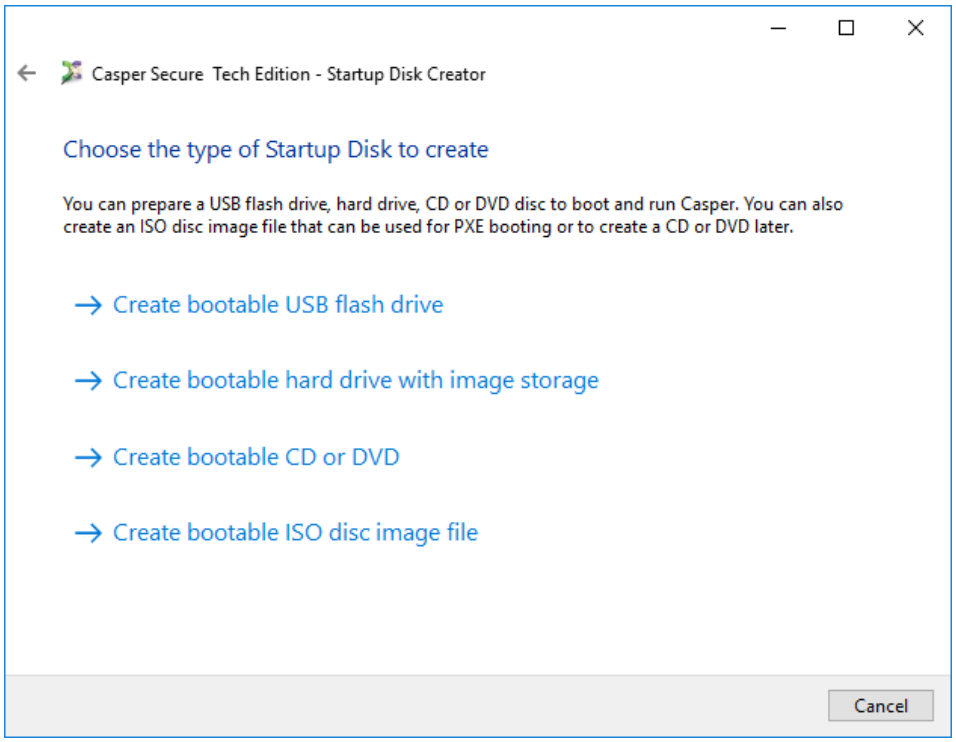


Once the subscription number and account credentials have been provided, and thereafter, you may optionally assign new keys to an organizational group or give each new key an unique identity to assist with tracking and usage.

To restrict usage a runtime authorization password may also be provided. The Startup Disk will prompt for the runtime password before permitting use of the software.

All of the *Product Key Options* are optional and may be left blank.

3. Choose the type of Startup Disk to create.



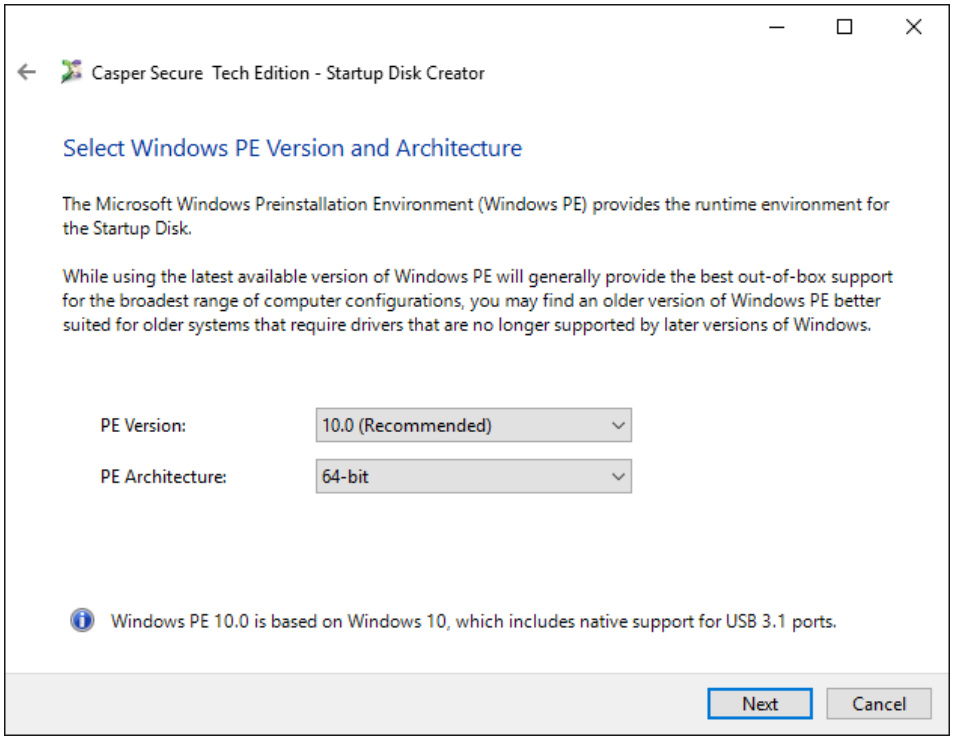
There are four options:

- **Create bootable USB flash drive.** This option will prepare a USB flash drive to boot and run Casper Secure Tech Edition.
- **Create bootable hard drive with image storage.** This option will prepare an external hard drive to boot and run Casper Secure Tech Edition and also store image backups.
- **Create bootable CD or DVD.** This option will prepare a CD or DVD disc to boot and run Casper Secure Tech Edition.
- **Create bootable ISO disc image file.** This option will create an ISO disc image file, which can be used to create a CD or DVD disc later or used to emulate a bootable Casper Secure Tech Edition CD within a virtual environment.

This step will be omitted if your license requires the use of a USB flash drive for the Startup Disk.

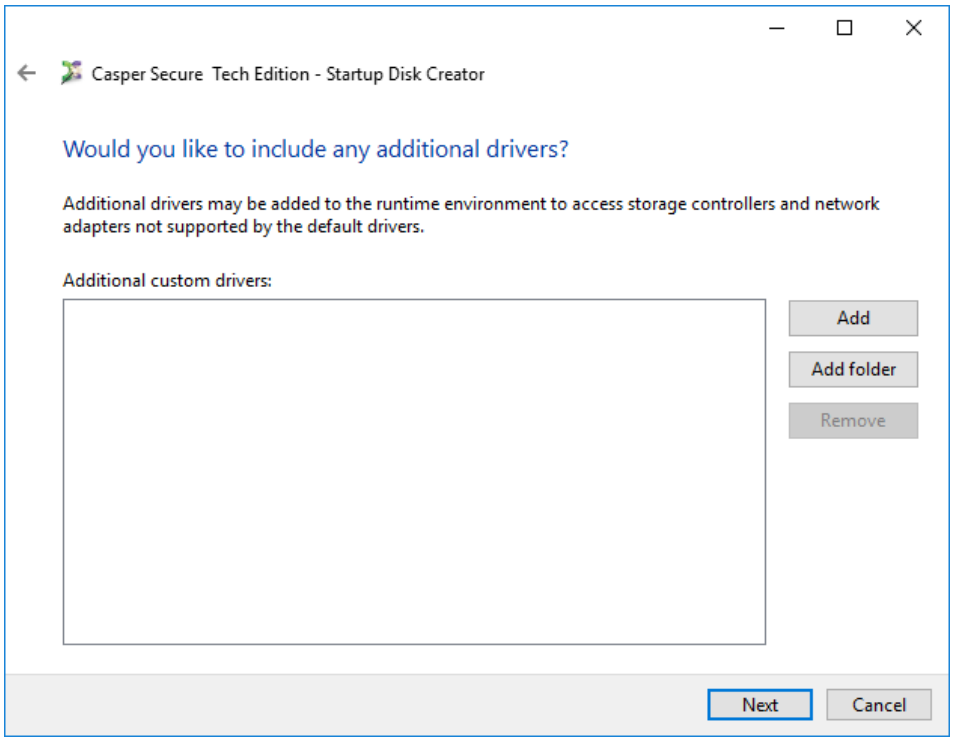
Internet access is required to use a bootable CD, DVD, or ISO disc image file. Other restrictions may also apply depending on the type of license acquired. For example, your license may not permit the creation of a CD, DVD, or ISO image file or it may permit only the creation of a temporary CD, DVD, or ISO disc image file that will cease to operate after 48 hours. For complete details, please consult the license agreement accompanying this software or contact your licensing administrator.

4. Choose the Windows PE version and architecture to use for the Startup Disk. The default selection is recommended.



The PE version does need to be based on the same version of Windows running on the computer. For example, if the computer is running Windows 7, you may choose to use PE version 10.0, which is based on Windows 10.

5. Specify additional drivers to add to the runtime environment. Additional drivers may be required to provide access to storage devices and network resources not supported by the drivers included within the Windows AIK or Windows ADK.



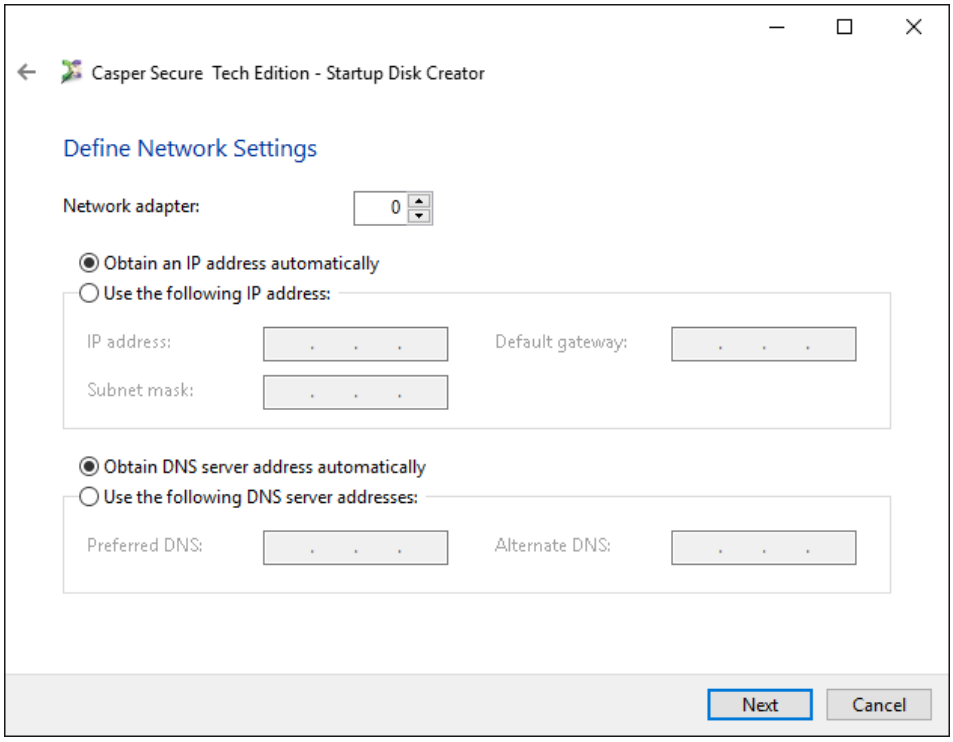
Click **Add** and select the Setup Information File (INF) to include a specific driver. To add more than one driver at time, click **Add folder** and select the folder containing the drivers. All drivers within the selected folder and within any subfolders will be added to the runtime environment. Incompatible drivers will be ignored.

When creating a Startup Disk with Windows PE version 3.0 (WinPE 3.0), a collection of popular third-party storage controller drivers and network drivers may be added by checking the **Include additional storage drivers** and **Include additional network drivers** options. Both of these options provide out-of-the-box support for a broad range of hardware when using WinPE 3.0.

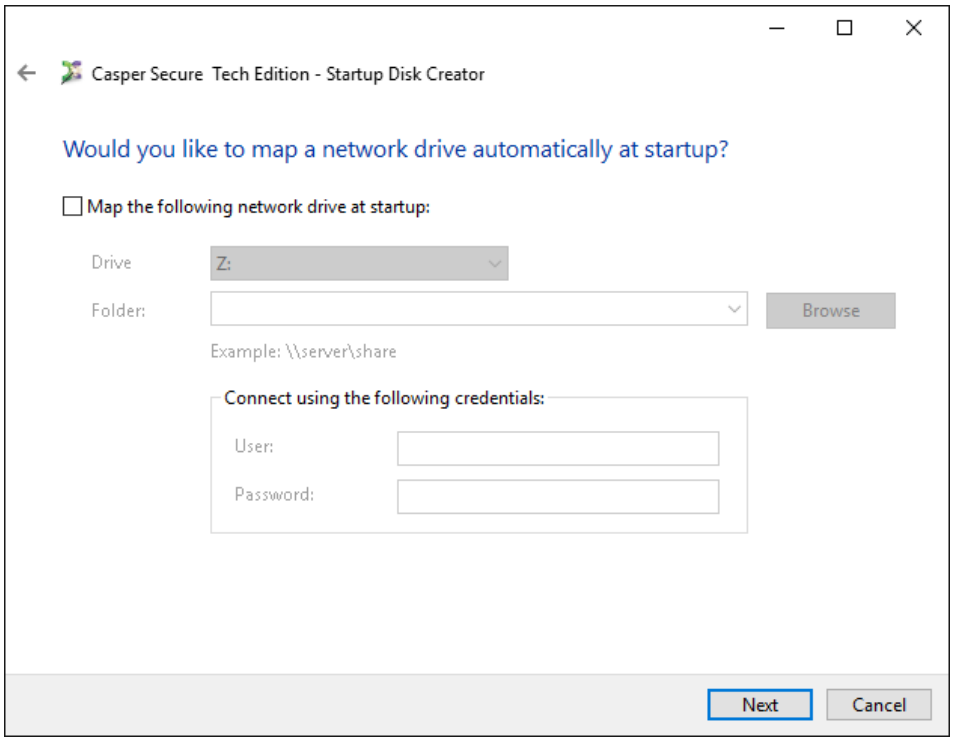
*The **Include additional storage drivers** and **Include additional network drivers** options are available only when using WinPE 3.0. These options will not appear when using a later version of WinPE to create the Startup Disk.*

*Adding a large number of custom drivers with **Add** or **Add folder** can significantly increase the amount of time required to create the Startup Disk.*

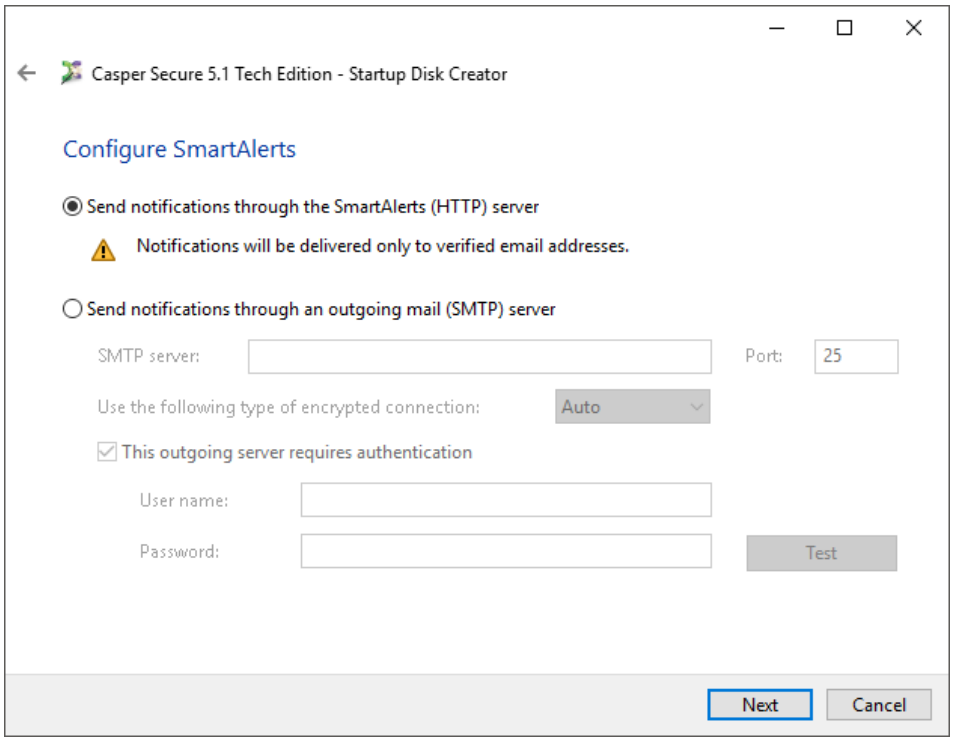
6. Define the network configuration for the runtime environment. You can configure a specific network configuration for each adapter discovered within the runtime environment.



7. Choose whether to have a network drive mapped automatically at startup. The **User** and **Password** fields are optional and may be left blank. You will be prompted to provide the missing credentials if necessary at startup.



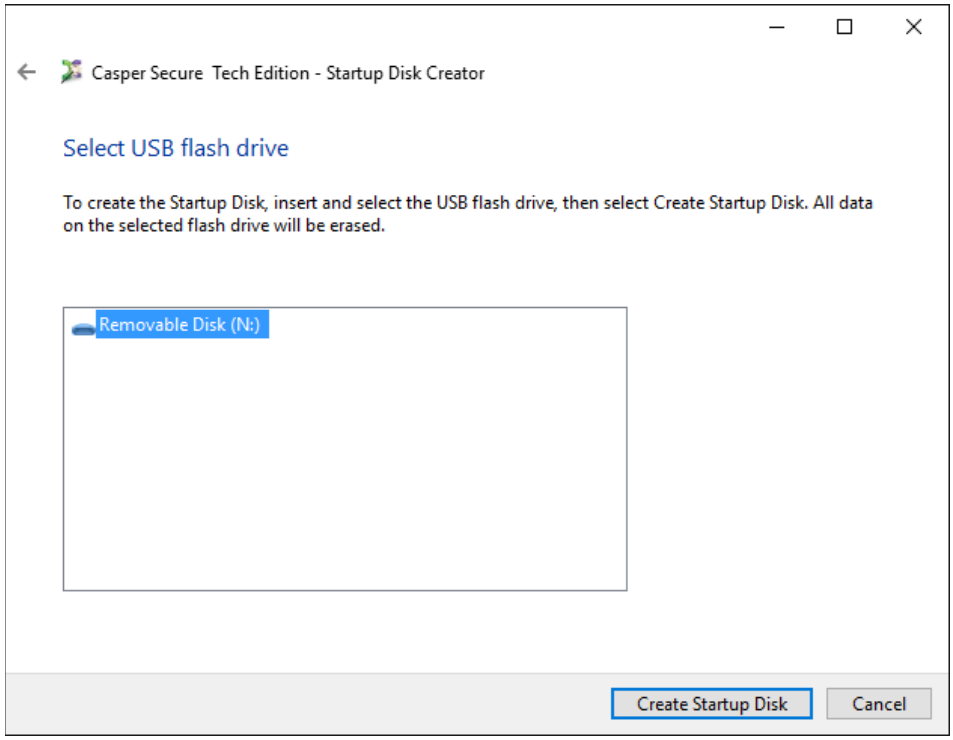
8. Configure how SmartAlert notifications are delivered.



When choosing to send notifications through the SmartAlerts (HTTP) server, you must confirm receipt of a verification email that is sent by the SmartAlerts server whenever an email address is used for the first time. No SmartAlert notifications will be delivered to the email address until the link within the verification email has been clicked.

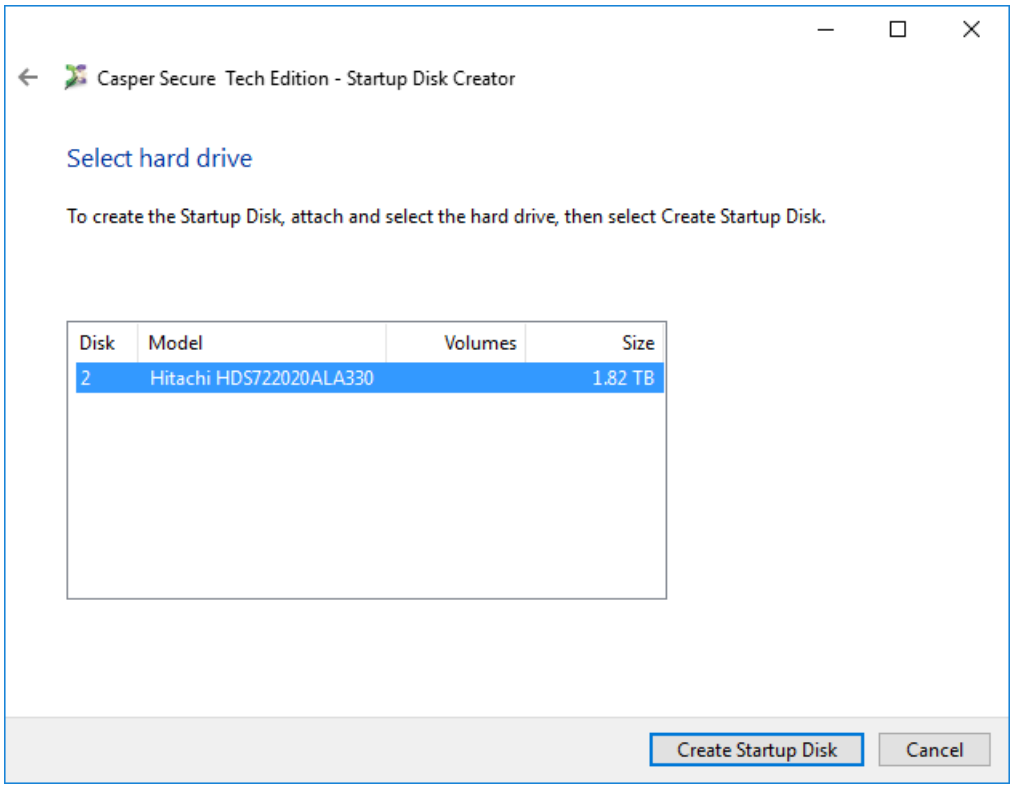
While email address verification is not required when choosing to send notifications through an SMTP server, the specified SMTP server may require authentication to send mail. This authentication can be requested by checking **This outgoing server requires authentication** and specifying the **User name** and **Password** credentials to use.

9. If creating a bootable USB flash drive, insert and select the USB flash drive, then click **Create Startup Disk**. All data on the flash drive will be erased.



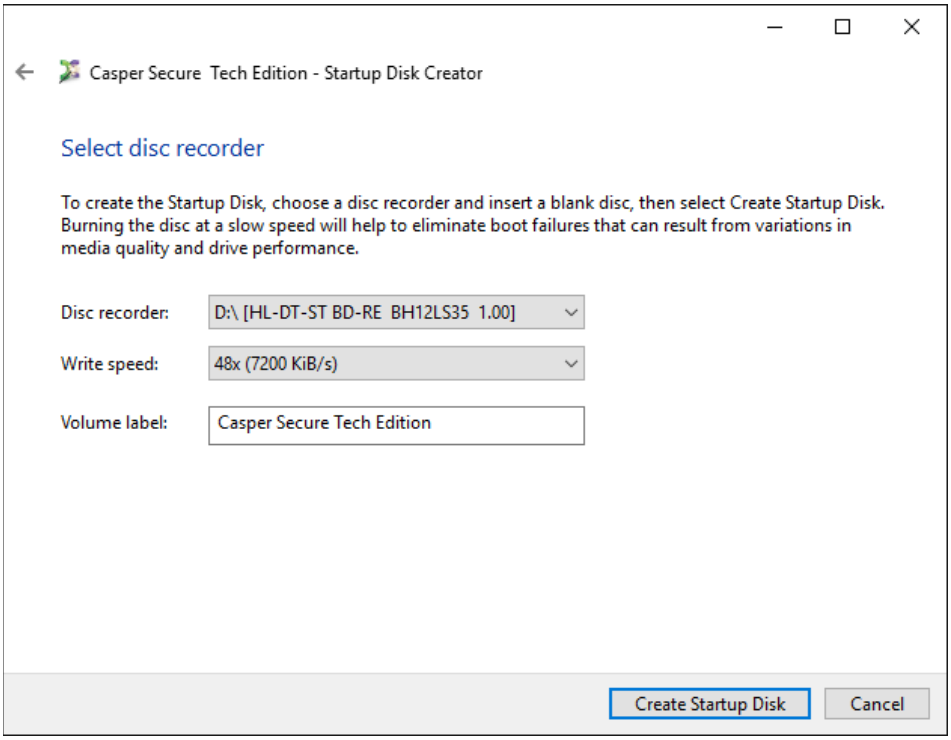
Except when selecting a USB flash drive that is presently configured as a Casper Startup Disk, all data on the flash drive will be erased. If the flash drive is currently configured as a Casper Startup Disk, only existing Casper settings will be preserved along with any files and folders located within the \Drivers and \Private folders.

If creating a bootable hard drive with image storage, select the hard drive to use and then click **Create Startup Disk**.

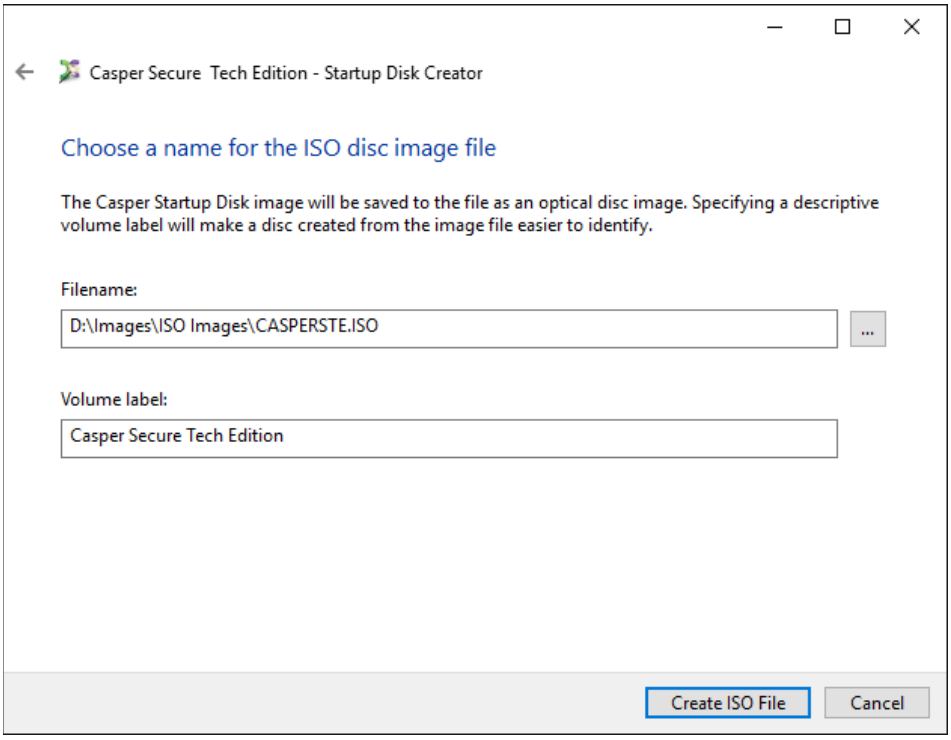


Only drives that are uninitialized, empty, or that have already been configured as a Casper Startup Disk will be listed.

If creating a bootable CD or DVD, select a disc recorder and insert a blank disc, then click **Create Startup Disk**.



If creating a bootable ISO disc image file, type a name for the file and click **Create ISO File**.



Using the Casper Secure Tech Edition Startup Disk

You can run Casper Secure Tech Edition either by executing the program from the Startup Disk within a supported Windows environment or by booting a computer from the Startup Disk. When the Startup Disk is used to boot a computer, Casper Secure Tech Edition will start automatically.

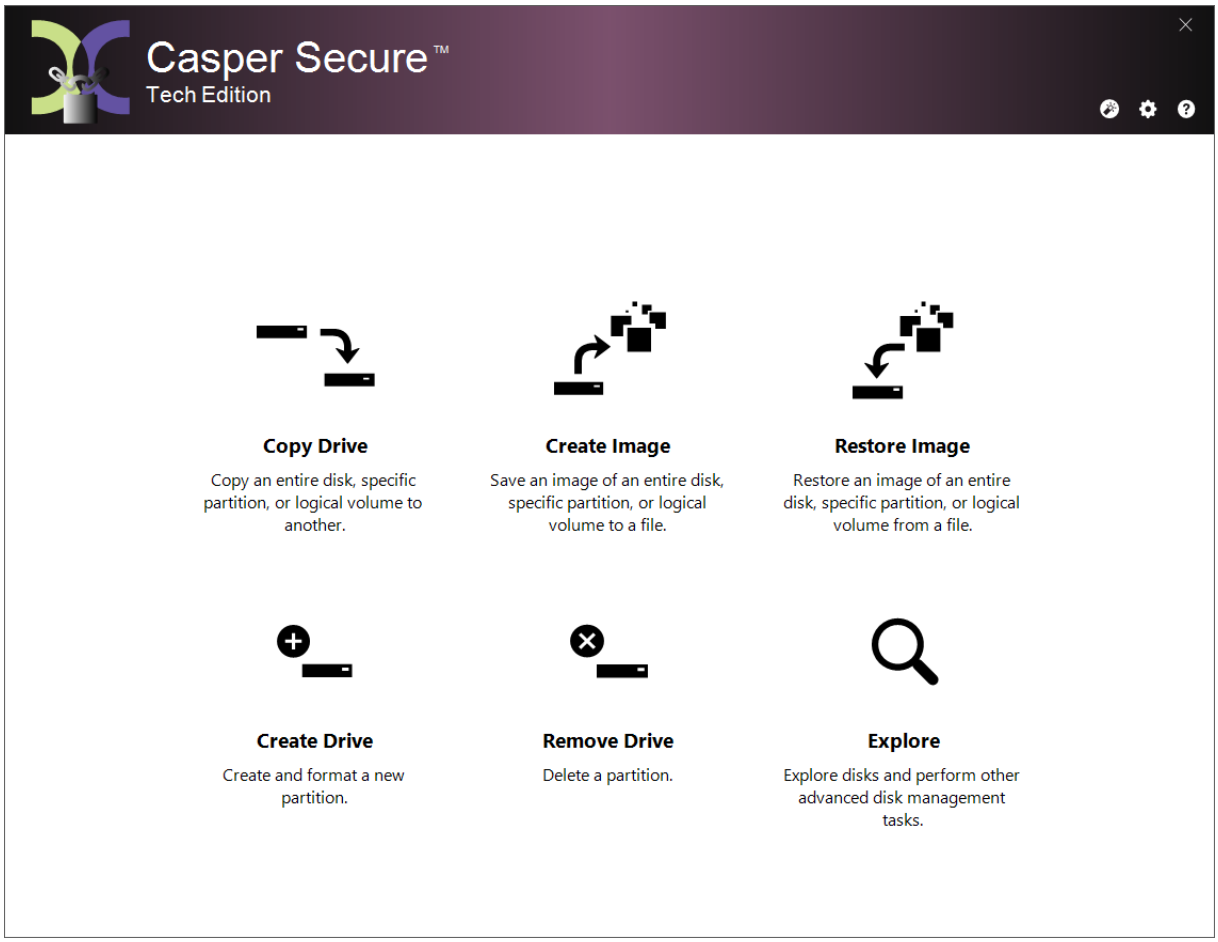
Running Casper Secure Tech Edition within Windows

1. Insert the Casper Secure Tech Startup Disk and browse to the **CASPERSTE** folder.
2. Double-click on **CASPERSTE.EXE** to open Casper Secure Tech Edition.

Booting and Running Casper Secure Tech Edition from the Startup Disk

The Casper Secure Tech Startup Disk may be used to boot a computer and run Casper Secure Tech Edition. When booting a computer from the Startup Disk, Casper Secure Tech Edition will start automatically.

Booting a computer from the Startup Disk may take several minutes. Once it has completed the boot process, the Casper Secure Tech Edition console will display.



Loading specific drivers after booting from the Startup Disk

The Startup Disk boots and runs Casper Secure Tech Edition within a self-contained Windows Preinstallation (WinPE) environment. If you need to load a driver that was not included when the Startup Disk was created, you can load the driver after booting the computer from the Startup Disk.

Follow this procedure:

1. Click **Explore** to open Casper Explorer
2. From the **Tools** menu, click **Load driver**
3. Browse to the Setup Information File (.INF) of the driver package that contains the hardware driver to load and click **Open**.

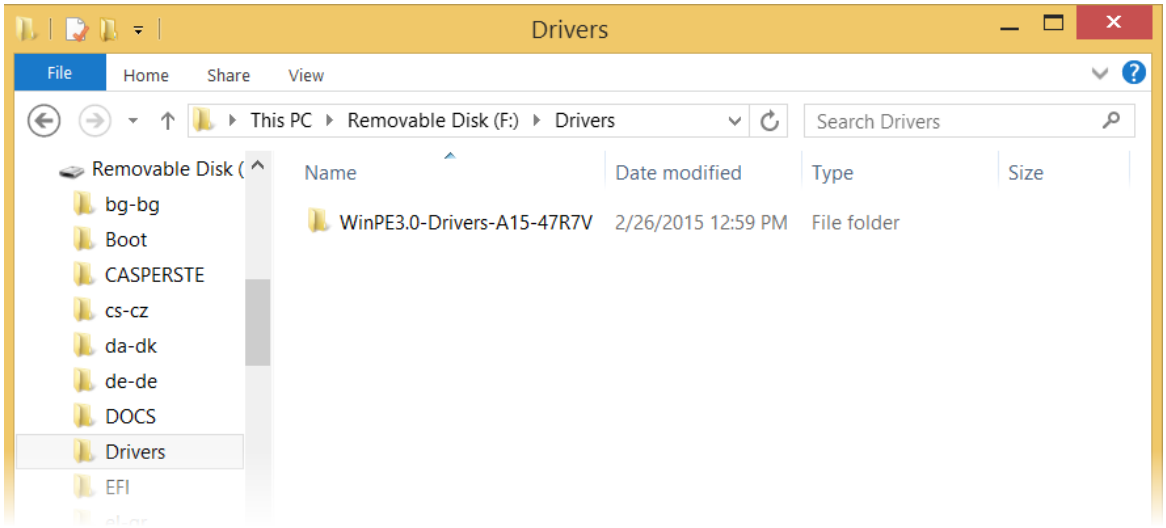
> The driver must have the same architecture as the Casper Secure TE Startup Disk. For example, if the Startup Disk was created using a 32-bit version of Windows PE, the driver must be 32-bit. If the Startup Disk was created using a 64-bit version of Windows PE, the driver must be 64-bit.

Automatically loading additional drivers when booting from the Startup Disk

When using a USB flash drive for the Startup Disk, additional drivers may be added by copying the driver files to the **Drivers** folder located in the root directory of the Startup Disk (e.g., “E:\Drivers”). Each time the Startup Disk is used to boot a computer the **Drivers** folder is recursively searched and all compatible drivers are loaded.

The **Drivers** folder makes it possible to reconfigure the drivers for a Startup Disk after the disk has been created.

The following screenshot shows the contents of a **Drivers** folder, which has been customized with a Dell Driver Pack (CAB).



Upgrading a Hard Disk

Casper Secure Tech Edition makes short work of upgrading and replacing a hard disk, including one encrypted with BitLocker drive encryption or PGP whole disk encryption. Automatic partition resizing and alignment optimization ensure effortless migration to both larger and smaller drives alike, including solid state (SSD) and Advanced Format (AFD) drives.

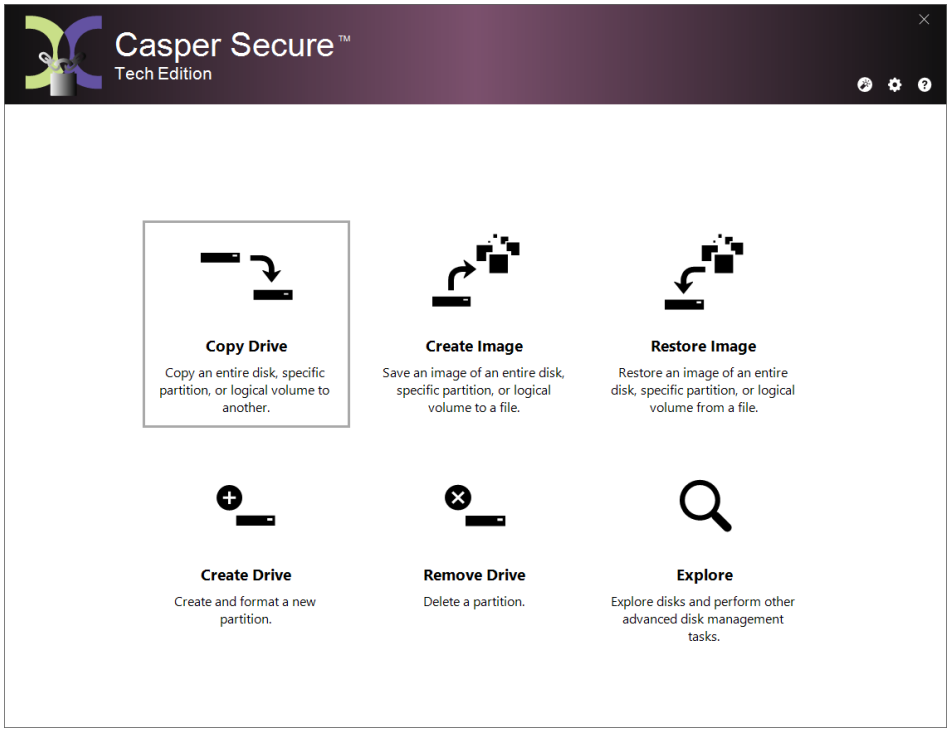
When cloning a BitLocker encrypted or PGP whole disk encrypted hard disk, Casper Secure Tech Edition will retain all of the encrypted data in its original encrypted state. This results in a hard disk that can be used as an immediate and complete replacement for the original hard disk without requiring an unencrypted copy or separate time-consuming re-encryption step.

The procedure for upgrading a hard disk is basically the same whether you are upgrading a hard disk in a desktop or a notebook. For a desktop system, the new hard disk is temporarily installed as a secondary hard disk in the computer or attached as an external hard disk using an external USB, Firewire, or eSATA hard disk enclosure or bridge adapter. For a notebook computer, a secondary media bay or external USB, Firewire, eSATA, or PCMCIA hard disk enclosure or bridge adapter is required to connect the new hard disk to the notebook.

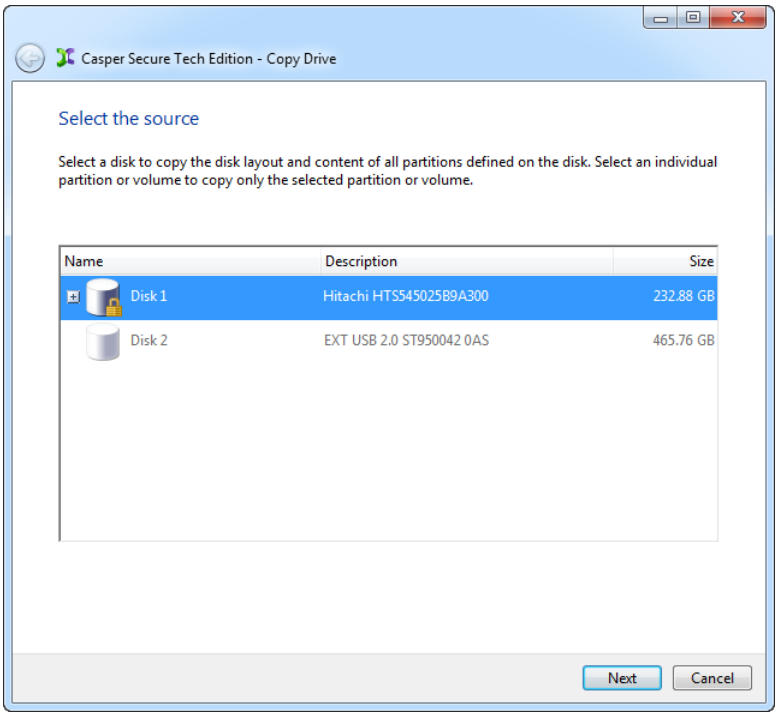
Example 1: Upgrading a Hard Disk

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

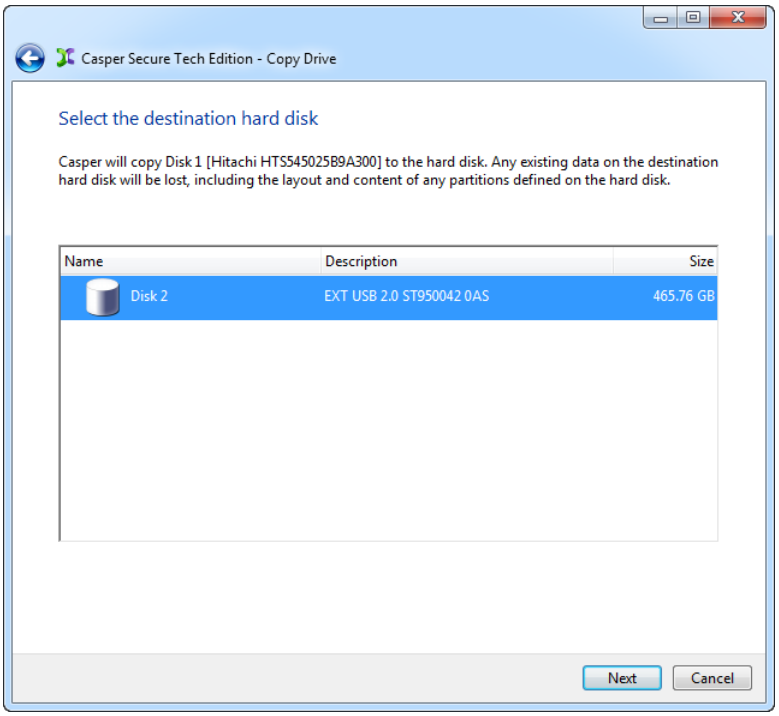
1. Start Casper Secure Tech Edition
2. Select **Copy Drive**



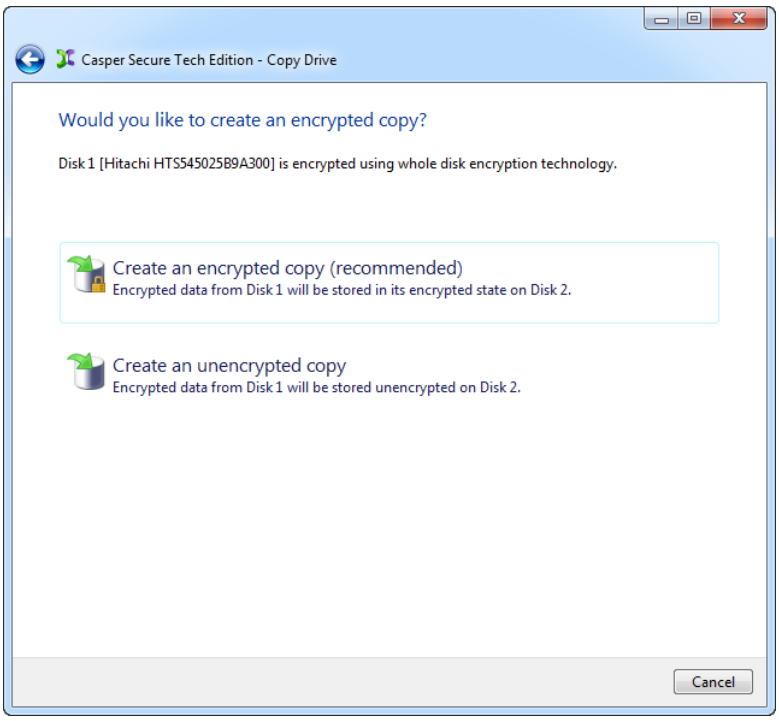
3. Select the hard disk to be upgraded as the source and click **Next**.



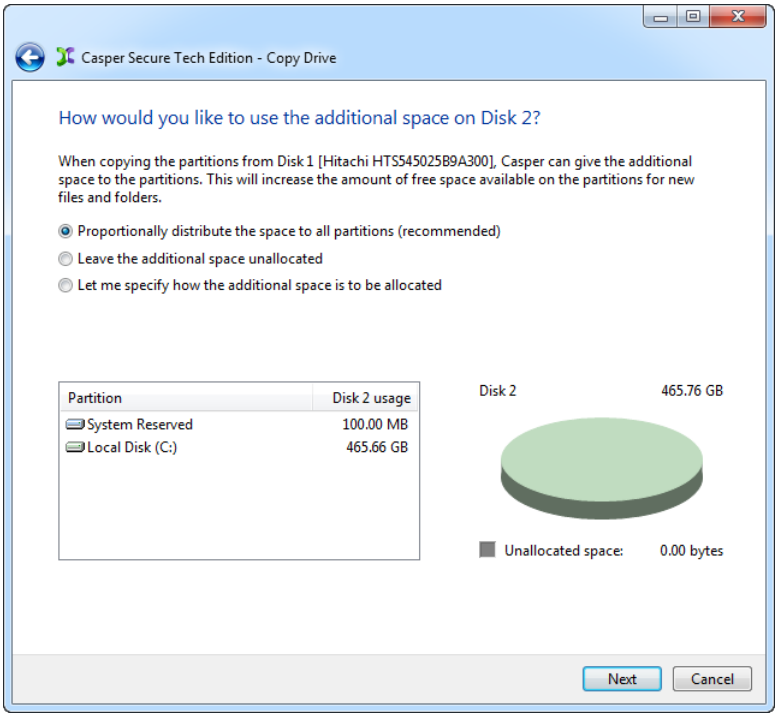
4. Select the new hard disk as the destination and click **Next**.



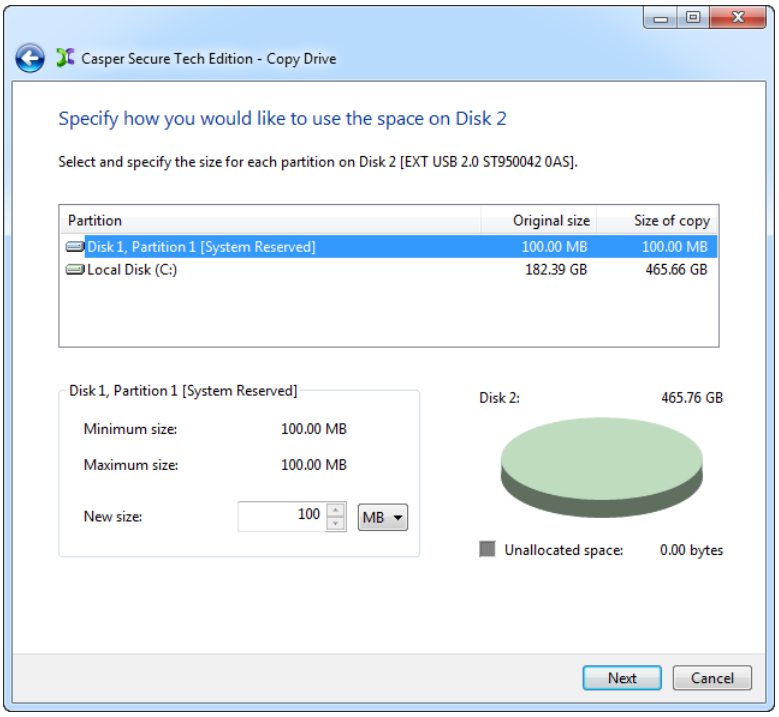
5. If the source hard disk is encrypted using BitLocker drive encryption or PGP whole disk encryption, Casper will offer the option of creating an unencrypted copy unless prohibited by BitLocker or PGP administrative policy settings. Click **Create an encrypted copy**.



6. When prompted to specify how the space on the new hard disk is to be used, click **Next** to accept the default. If upgrading to a larger capacity hard 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 on the source disk.

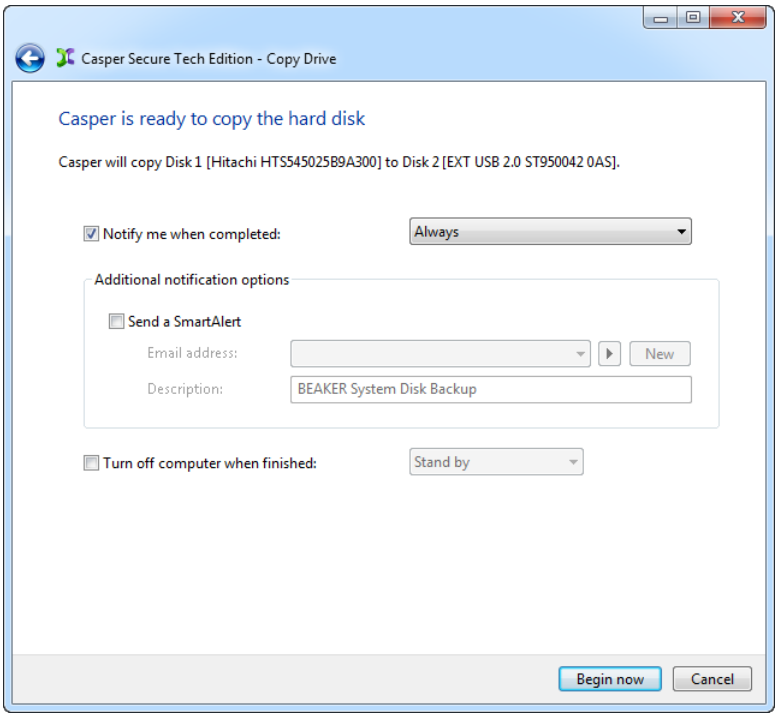


If the capacity of the new hard disk is equal to or less than the capacity of the source hard disk, Casper will offer the option to reconfigure the available space.

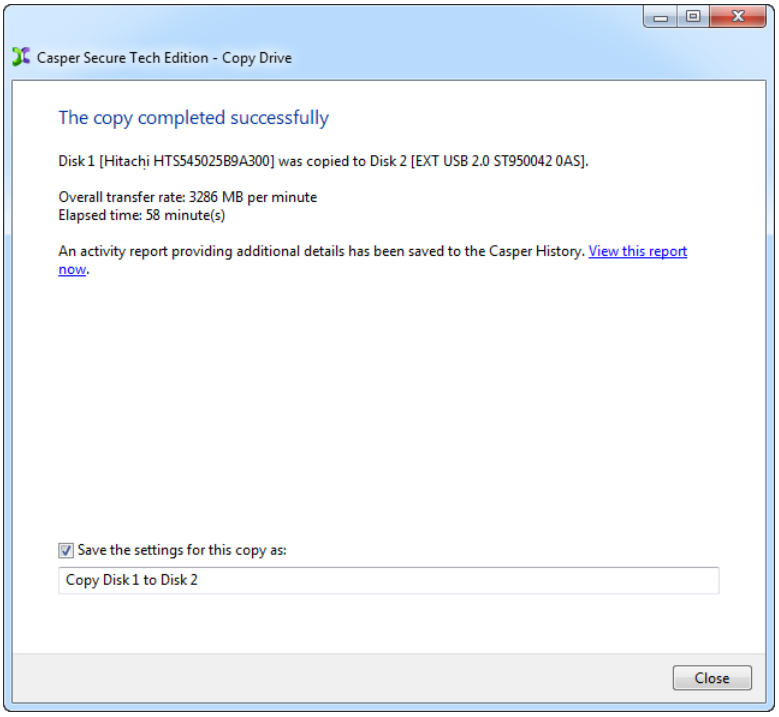


For additional help with making a selection, press **F1.**

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



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



9. Shutdown and power-off the computer.

10. Reconfigure the computer to replace the original hard disk with the new hard disk.

    If the new hard disk is installed in a secondary media bay of a notebook, or installed in an external USB, Firewire, eSATA, or PCMCIA enclosure, simply remove the hard disk from its enclosure and exchange it with the original hard disk.

    For a new hard disk that has been temporarily mounted as a secondary internal hard disk, change the cable connection as required to make the new hard disk the master on the primary SATA controller.

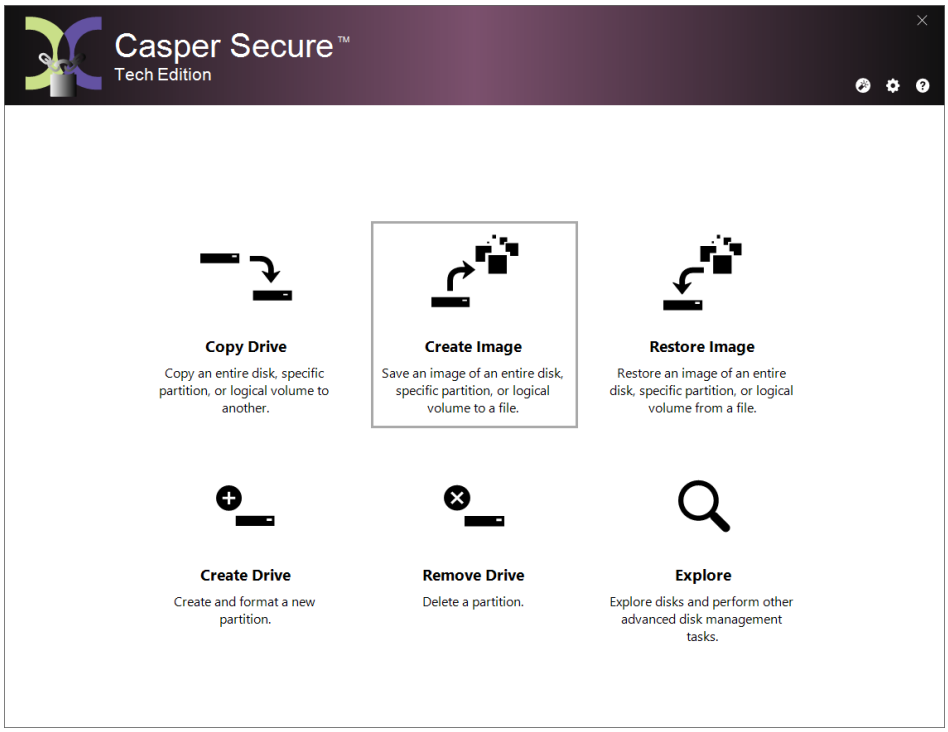
Creating and Restoring Disk Image Backups

A disk image backup stores a complete image of a disk in a file, which can be stored virtually anywhere, including on a drive containing other files or remotely on a network attached storage device.

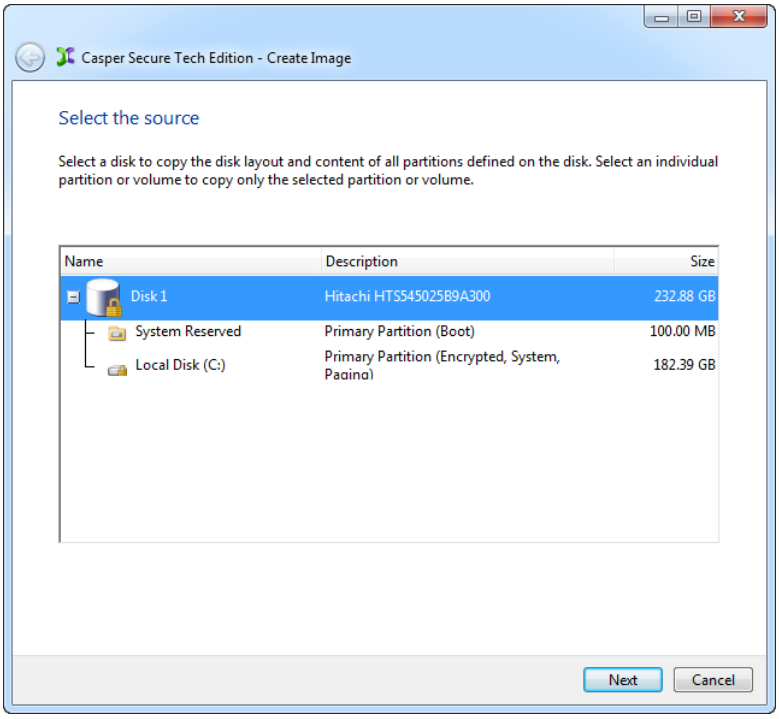
When creating a disk image backup for a drive encrypted with BitLocker Drive Encryption or PGP Whole Disk Encryption technology, Casper Secure Tech Edition retains all of the data in its original encrypted state.

Example 2: Creating a Disk Image Backup

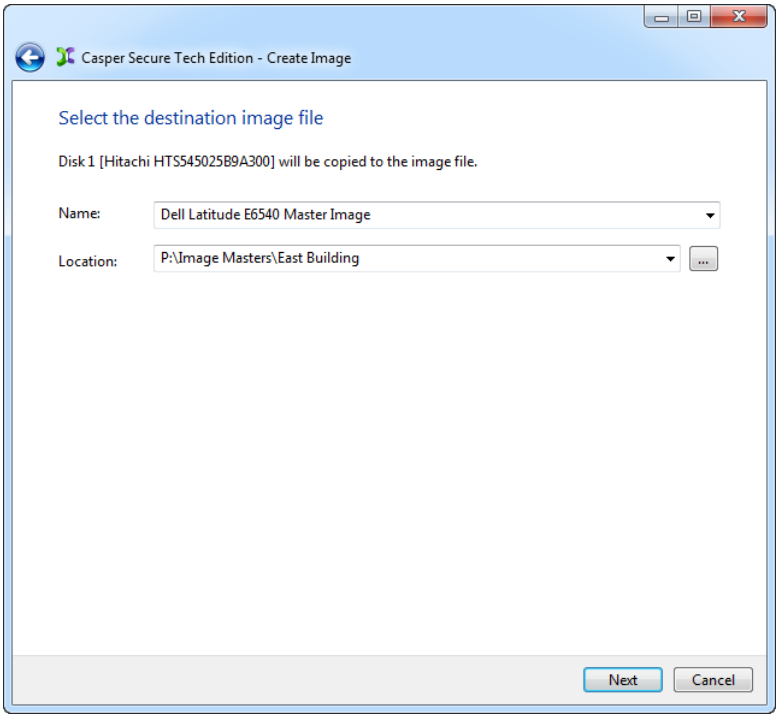
1. Start Casper Secure Tech Edition
2. Select **Create Image**



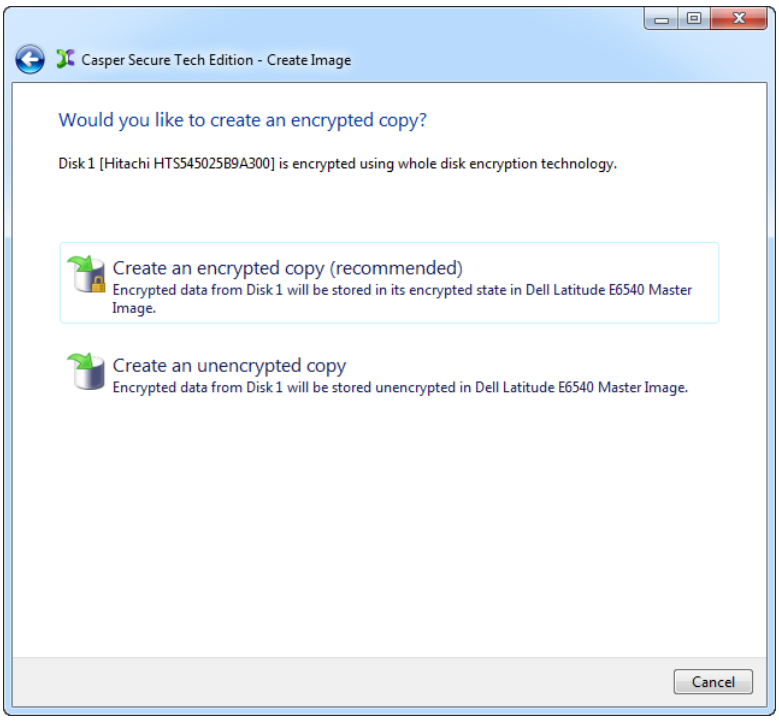
3. Select the hard disk to copy and click **Next**.



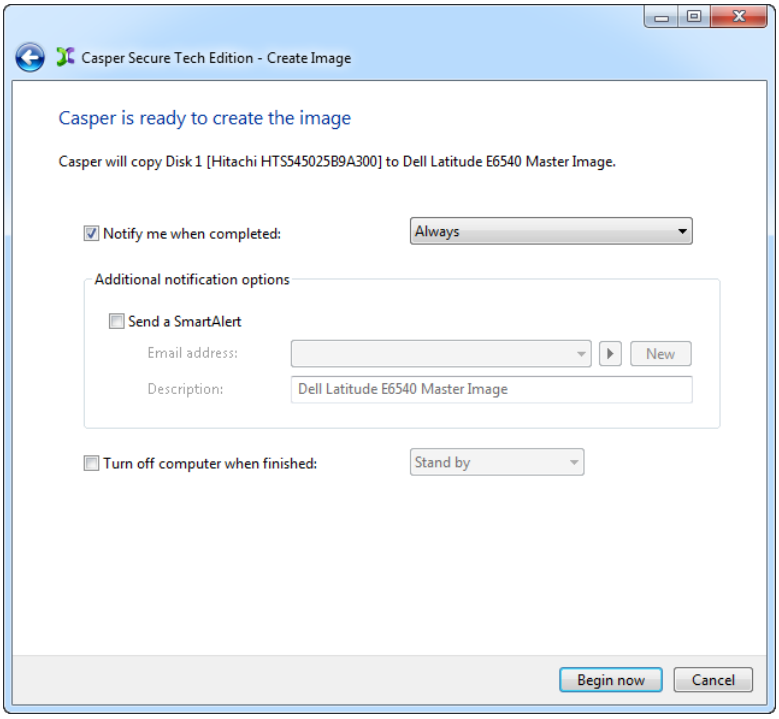
4. Select the destination image file and click **Next**. The image file can be stored virtually anywhere, including on a network attached storage device.



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



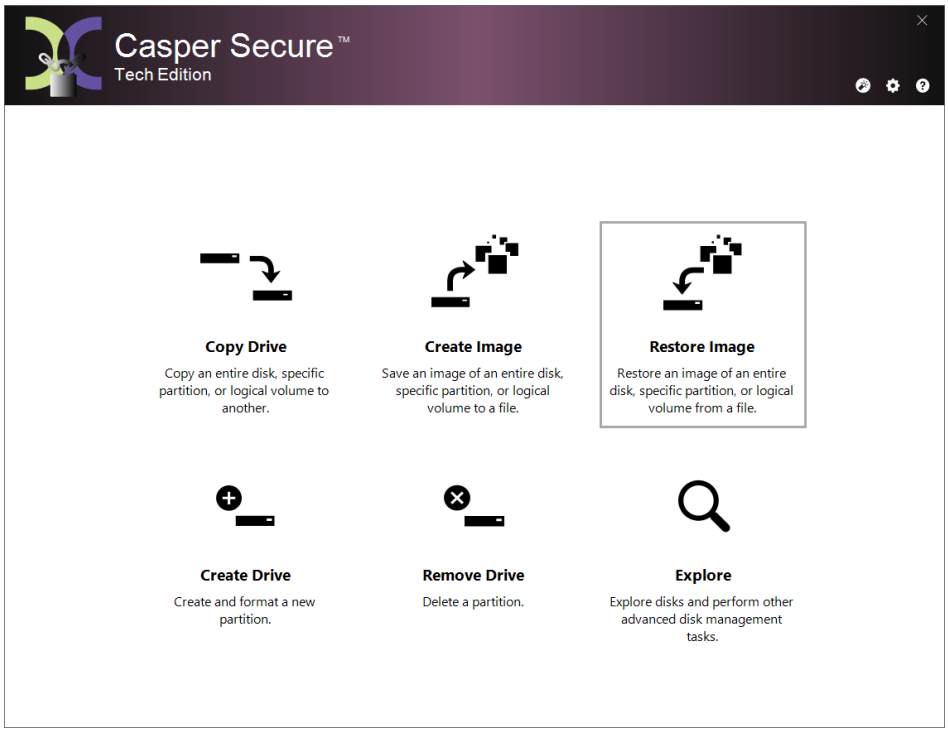
6. Click **Begin now** to create the image file.



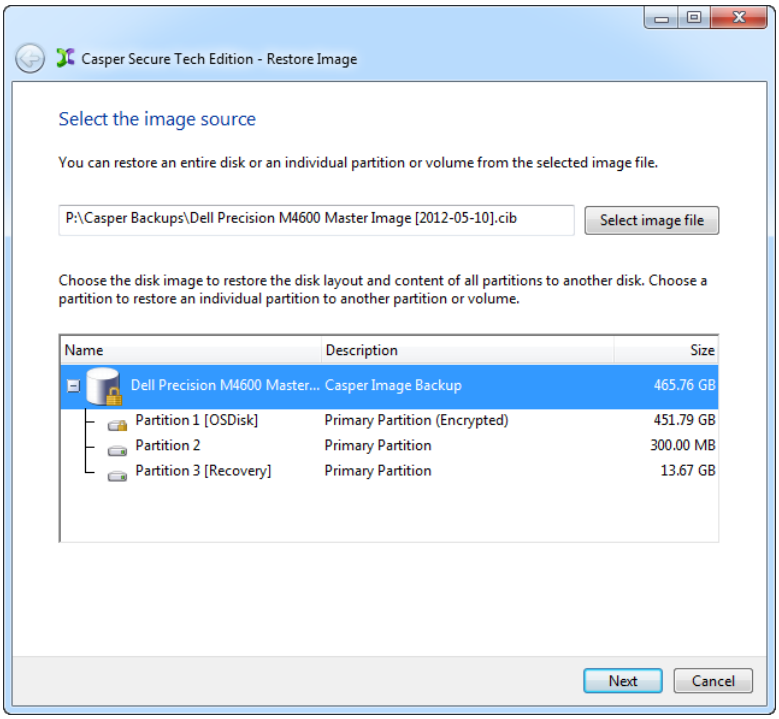
Example 3: Restoring a Disk Image Backup

1. Start Casper Secure Tech Edition

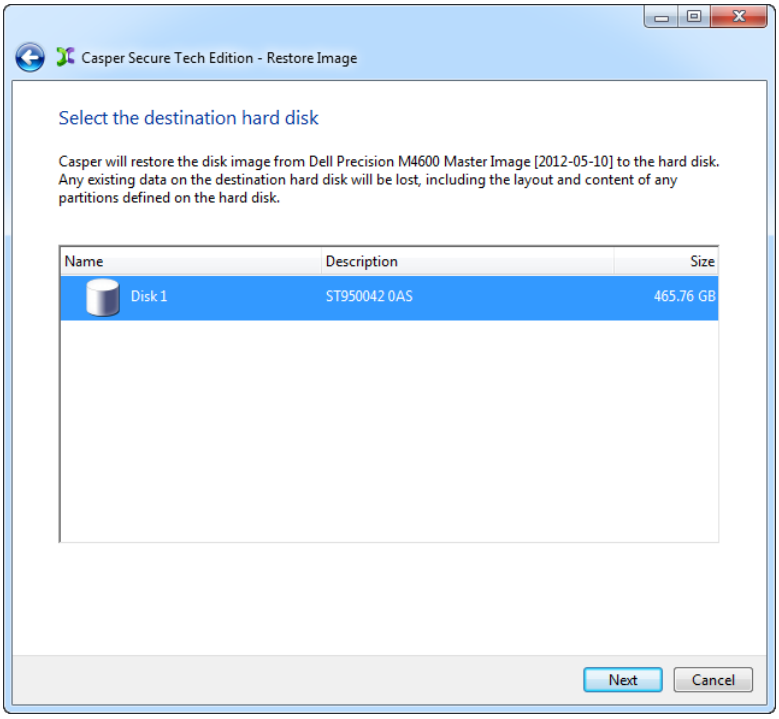
2. Select **Restore Image**



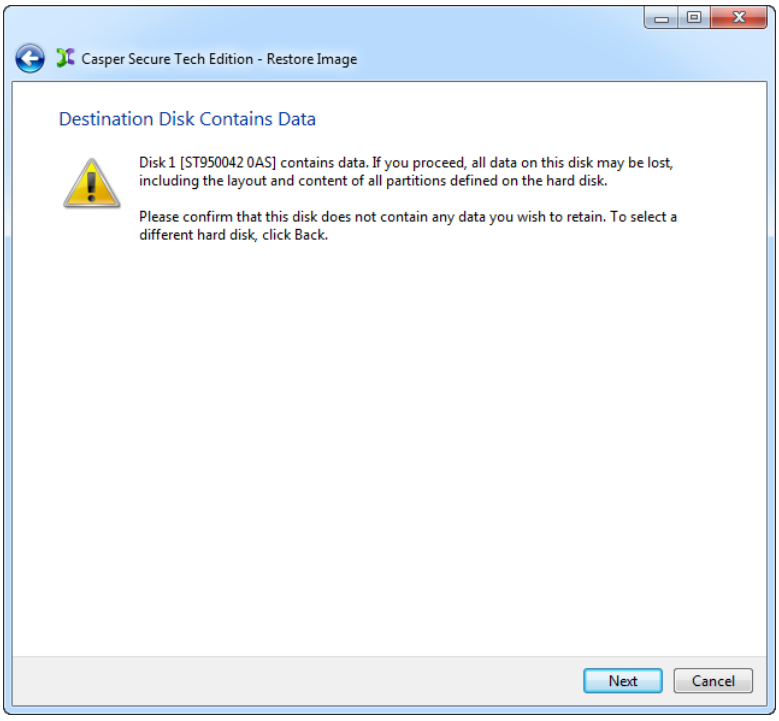
3. Select the image source and click **Next**.



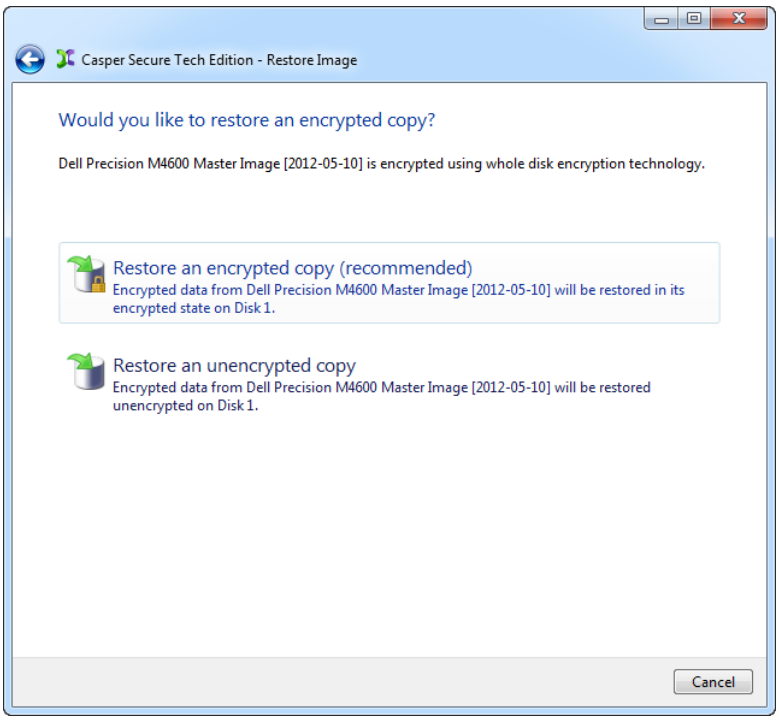
4. Select the destination and click **Next**.



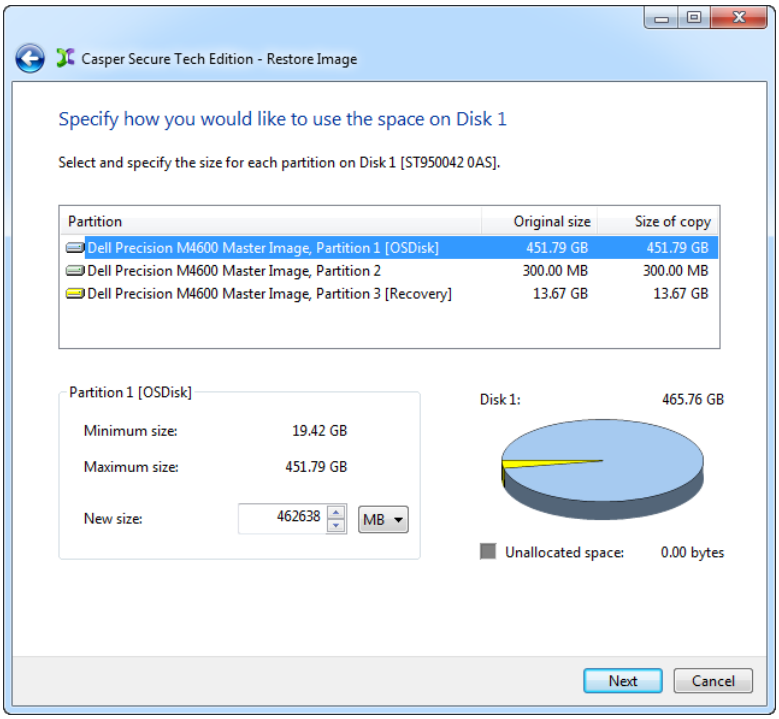
5. If the selected destination hard disk defines a partition or contains data, Casper will warn you that the contents will be overwritten. Confirm you have selected the correct hard disk to receive the backup, and click **Next**.



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



7. When prompted to specify how the space on the destination hard disk is to be used, click **Next** to accept the default. If the size of the original image equals or exceeds the capacity of the destination hard disk, Casper will offer the option to reconfigure the available space.



If the original image size is smaller than the destination hard disk, Casper will offer the option of giving all of the additional space to the restored image, or proportionally distributing the additional space when there is more than one partition defined in the image.

8. Click **Begin now** to restore the image.