AHSAY™ Ahsay Backup

Ahsay Online Backup Manager v7

StorageCraft ShadowProtect System Backup & Restore Guide

Ahsay Systems Corporation Limited

14 September 2018

A wholly owned subsidiary of
Ahsay Backup Software Development Company Limited
HKEx Stock Code: 8290

Copyright Notice

Trademarks

Ahsay, Ahsay Cloud Backup Suite, Ahsay Online Backup Suite, Ahsay Offsite Backup Server, Ahsay Online Backup Manager, Ahsay A-Click Backup, Ahsay Replication Server, Ahsay BackupBox Firmware, Ahsay Universal Backup System, Ahsay NAS Client Utility are trademarks of Ahsay Systems Corporation Limited.

Amazon S3 is registered trademark of Amazon Web Services, Inc. or its affiliates.

Apple and Mac OS X are registered trademarks of Apple Computer, Inc.

Dropbox is registered trademark of Dropbox Inc.

Google Cloud Storage and Google Drive are registered trademarks of Google Inc.

Lotus, Domino, Notes are registered trademark of IBM Corporation.

Microsoft, Windows, Microsoft Exchange Server, Microsoft SQL Server, Microsoft Hyper-V, Microsoft Azure, One Drive and One Drive for Business are registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Oracle, Oracle 10g, Oracle 11g and MySQL are registered trademarks of Oracle Corporation.

Rackspace and OpenStack are registered trademarks of Rackspace US, Inc.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo and JBoss are registered trademarks of Red Hat, Inc. www.redhat.com in the U.S. and other countries. Linux is a registered trademark of Linus Torvalds.

ShadowProtect is registered trademark of StorageCraft Technology Corporation.

VMware, ESX, ESXi, vCenter are registered trademarks of VMware, Inc.

All other product names are registered trademarks of their respective owners.

Disclaimer

Ahsay Systems Corporation Limited will not have or accept any liability, obligation or responsibility whatsoever for any loss, destruction or damage (including without limitation consequential loss, destruction or damage) however arising from or in respect of any use or misuse of reliance on this document. By reading and following the instructions in this document, you agree to accept unconditionally the terms of this Disclaimer and as they may be revised and/or amended from time to time by Ahsay Systems Corporation Limited without prior notice to you.

Revision History

Date	Descriptions	Type of modification
25 July 2018	First Draft	New
14 September 2018	Added requirement of Antivirus Exclusion for Ch.2.1.3; Updated Overview of backup process for Ch.3	New/ Modification

Table of Contents

1 Overview

1.1 Introduction

1.1.1 User Guide

This user guide aims at providing detailed information for backing up and restoring StorageCraft ShadowProtect system with AhsayOBM.

Please refer to the following link for further details about StorageCraft ShadowProtect: https://support.storagecraft.com/s/topic/0TO36000000Ln5VGAS/shadowprotect-windows?language=en_US

1.1.2 Bare-metal System Recovery

Bare-metal system recovery is a technique in the field of data recovery where the backup data is available and allowed one to restore a computer system from bare-metal computer that without any software or operating system installed.

For bare-metal system recovery, the hardware received the restore requirement to have an identical configuration to the hardware that was the source of the backup, although virtualization techniques and careful planning can enable a bare-metal restore to a hardware configuration different from the original.

Disk imaging applications enable bare-metal restores by storing images of the entire contents of hard disks to network storage or other external storage, such as AhsayCBS, and then writing those images to other physical disks. The disk image application itself can include an entire operating system, bootable from a live CD or network file server, which contains all the required application code to create and restore the disk images.

1.2 What is this software?

Ahsay brings you specialized client backup software, namely AhsayOBM, to provide a set of tools to protect your system. This includes backup and recovery of your system with snapshots / versioning, and retention policy to protect.

1.3 About This Document

1.3.1 Document Main Part

The document can be divided into 3 main parts.

Part 1: Preparation for ShadowProtect System Backup & Restore

Requirements
Requirements on AhsayOBM, ShadowProtect System and Windows Operating System

Limitation
Limitation for backup and restore of ShadowProtect System

Best Practice and Recommendation
Items recommended to pay attention to before performing backup and restore

Part 2: Perform Backup for ShadowProtect System Backup Set

Create Backup Set

Steps to create ShadowProtect System backup set

Run Backup Job

Run ShadowProtect System backup job

Part 3: Perform Restore for ShadowProtect System Backup Set

Perform Restore to Non-system Volume
Restore to non-system volume using AhsayOBM

Perform Restore to System Volume
Restore to system volume using ShadowProtect restore wizard based on bare-metal system recovery technique

1.3.2 What should I expect from this document?

After reading through this documentation, you can expect to have sufficient knowledge to set up your system to make StorageCraft ShadowProtect system on AhsayOBM, as well as to carry out an end-to-end backup and restore process.

1.3.3 Who should read this document?

This documentation is intended for backup administrators and IT professionals who are responsible for the StorageCraft ShadowProtect system backup and restore.

2 Preparation for Backup and Restore

2.1 Requirement

You are strongly recommended to configure or check all the settings below to confirm all the requirements are met before you proceed with the StorageCraft ShadowProtect system backup and restoration.

2.1.1 Hardware Requirement

Please refer to the following article for the list of hardware requirement for AhsayOBM:
Ahsay Hardware Requirement List (HRL) for version 7.3 or above

2.1.2 Software Requirement

Please refer to the following article for the list of compatible operating systems and application versions.
FAQ: Ahsay Software Compatibility List (SCL) for version 7.3 or above

2.1.3 Antivirus Exclusion Requirement

To optimize performance of AhsayOBM on Windows, and to avoid conflict with your antivirus software, refer to the following KB article the list of processes and directory paths that should be added to all antivirus software white-list / exclusion list:
http://wiki.ahsay.com/doku.php?id=public:5352_suggestion_on_antivirus_exclusions

NOTE

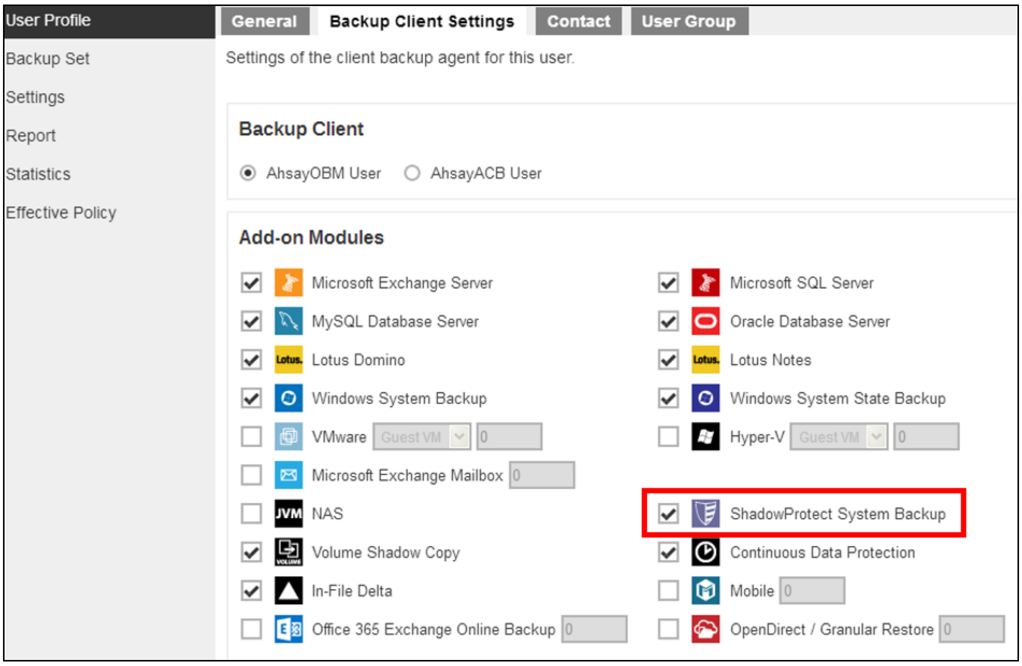
For AhsayOBM version 7.17 or above, the bJW.exe process is automatically added to Windows Defender exclusion list for Windows 10 and 2016, during installation / upgrade via installer or upgrade via AUA.

2.1.4 AhsayOBM Installation

The latest version of AhsayOBM must be installed on the backup machine on which StorageCraft ShadowProtect system has been installed.

2.1.5 ShadowProtect System Backup Add-On Module

Make sure the ShadowProtect System Backup feature has been enabled as an add-on module in your AhsayOBM user account. Please contact your backup service provider for more details.



Settings of the client backup agent for this user.

Backup Client

● AhsayOBM User ○ AhsayACB User

Add-on Modules

☑ Microsoft Exchange Server	☑ Microsoft SQL Server
☑ MySQL Database Server	☑ Oracle Database Server
☑ Lotus Domino	☑ Lotus Notes
☑ Windows System Backup	☑ Windows System State Backup
□ VMware Guest VM 0	□ Hyper-V Guest VM 0
□ Microsoft Exchange Mailbox 0	
□ NAS	☑ ShadowProtect System Backup
☑ Volume Shadow Copy	☑ Continuous Data Protection
☑ In-File Delta	□ Mobile 0
□ Office 365 Exchange Online Backup 0	□ OpenDirect / Granular Restore 0

2.1.6 Backup Quota Requirement

Make sure that your AhsayOBM user account has sufficient storage quota assigned to accommodate the storage of StorageCraft ShadowProtect system backup set and retention policy. Please contact your backup service provider for more details.

2.1.7 Java Heap Size

The default Java heap size setting on AhsayOBM is 2048MB. For ShadowProtect System backup, it is highly recommended to increase the Java heap size setting to be at least 4096MB to improve backup and restore performance. The actual heap size is dependent on amount of free memory available on your computer.

2.1.8 Temporary Directory Folder

To ensure optimal backup/restoration performance, it is recommended that the temporary directory folder is located on a local drive with sufficient free disk space.

As the ShadowProtect image file will be spooled to a temporary directory before being uploaded to the backup destination, it is recommended that the temporary directory has disk space of at least 150% of the total in-use size of all volumes selected for backup because the default Delta ratio is 50%. The actual free disk space required depends on various factors including the size of the volume(s), number of backup destinations, backup frequency, in-file delta settings etc.

2.1.9 Supported Operating System

Supported operating system: Windows 2003, 2008, 2008 R2, 2012, 2012 R2, and Windows XP, Vista, 7, 8, 8.1, 10.

NOTE

Please kindly note that AhsayOBM will provide best effort support for Windows 2003 and Windows

XP.

2.1.10 Supported StorageCraft ShadowProtect Version

ShadowProtect 5.2.7 Desktop/ Server is supported.

2.1.11 Supported File System

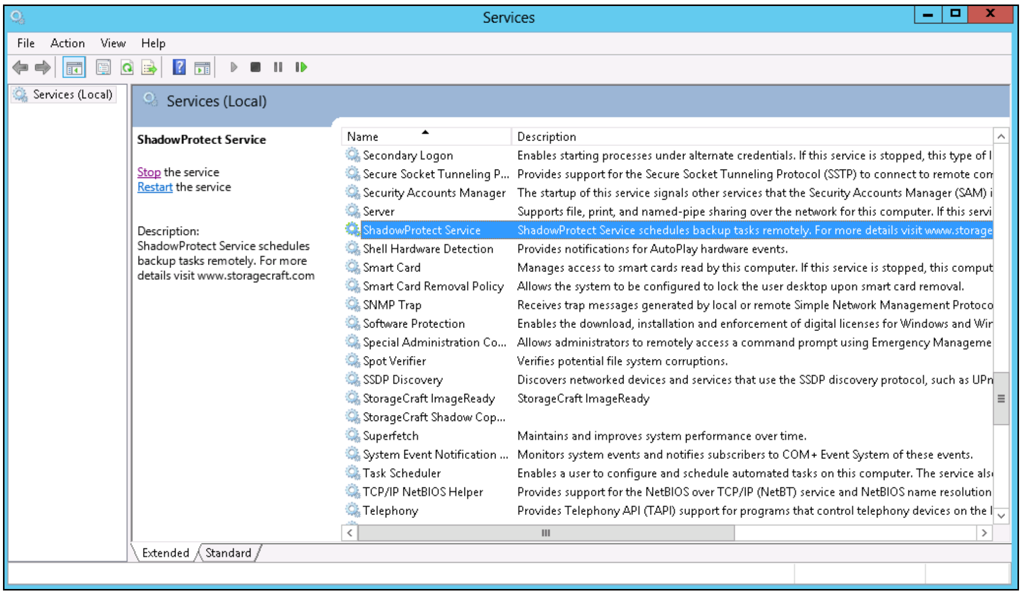
Supported file system: FAT16, FAT16X, FAT32, FAT32X, NTFS.

2.1.12 Port Configuration

TCP port 139 and 445 must be open for ShadowProtect to access network shares.

2.1.13 StorageCraft ShadowProtect related Windows Services

Make sure the “ShadowProtect Service” is “Running”.



ShadowProtect Service

Stop the service
Restart the service

Description:
ShadowProtect Service schedules backup tasks remotely. For more details visit www.storagecraft.com

Name	Description
Secondary Logon	Enables starting processes under alternate credentials. If this service is stopped, this type of l
Secure Socket Tunneling P...	Provides support for the Secure Socket Tunneling Protocol (SSTP) to connect to remote com
Security Accounts Manager	The startup of this service signals other services that the Security Accounts Manager (SAM) i
Server	Supports file, print, and named-pipe sharing over the network for this computer. If this servi
ShadowProtect Service	ShadowProtect Service schedules backup tasks remotely. For more details visit www.storage
Shell Hardware Detection	Provides notifications for AutoPlay hardware events.
Smart Card	Manages access to smart cards read by this computer. If this service is stopped, this comput
Smart Card Removal Policy	Allows the system to be configured to lock the user desktop upon smart card removal.
SNMP Trap	Receives trap messages generated by local or remote Simple Network Management Protoco
Software Protection	Enables the download, installation and enforcement of digital licenses for Windows and Wir
Special Administration Co...	Allows administrators to remotely access a command prompt using Emergency Manageme
Spot Verifier	Verifies potential file system corruptions.
SSDP Discovery	Discovers networked devices and services that use the SSDP discovery protocol, such as UPn
StorageCraft ImageReady	StorageCraft ImageReady
StorageCraft Shadow Cop...	
Superfetch	Maintains and improves system performance over time.
System Event Notification ...	Monitors system events and notifies subscribers to COM+ Event System of these events.
Task Scheduler	Enables a user to configure and schedule automated tasks on this computer. The service als
TCP/IP NetBIOS Helper	Provides support for the NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution
Telephony	Provides Telephony API (TAPI) support for programs that control telephony devices on the l

2.2 Limitation

1. ShadowProtect does not support Windows Cluster Shared Volumes (CSV).

2. ShadowProtect may not support:

   - exFAT or ReFS file systems
   - Windows Storage Spaces storage pools
   - Using VirtualBoot with UEFI-based system volumes

   Please consult with StorageCraft’s support to confirm which file systems are supported by which version of ShadowProtect

2.3 Best Practice and Recommendation

1. Turn off disk defrag software when using incremental backup. When ShadowProtect takes an incremental backup, it writes a file identifying those sectors that changed

since the last backup. Disk defrag software change many sectors on the disk, which greatly increases the time it takes to run the next incremental backup.

2. Test the StorageCraft Recovery Environment to make sure that you have access to both local drives and network devices that you might need.

3. Pay extra attention to the disk space usage where ShadowProtect stores backup images. If the location runs out of space, backup jobs will fail.

4. Use password encryption to protect backup image files. The default setting of algorithm for encryption key is RC4 128-bit (Fastest, but least secure), it is recommended to apply AES 256-bit (The most secure, but slowest).

> **NOTE**
>
> Please kindly note that the encryption key generated by checking the "Encrypt the image file in temporary directory" option CANNOT be recovered by Ahsay Encryption Key Recovery feature. So please keep the encryption key properly with several copies in case there is no way to recover the image.

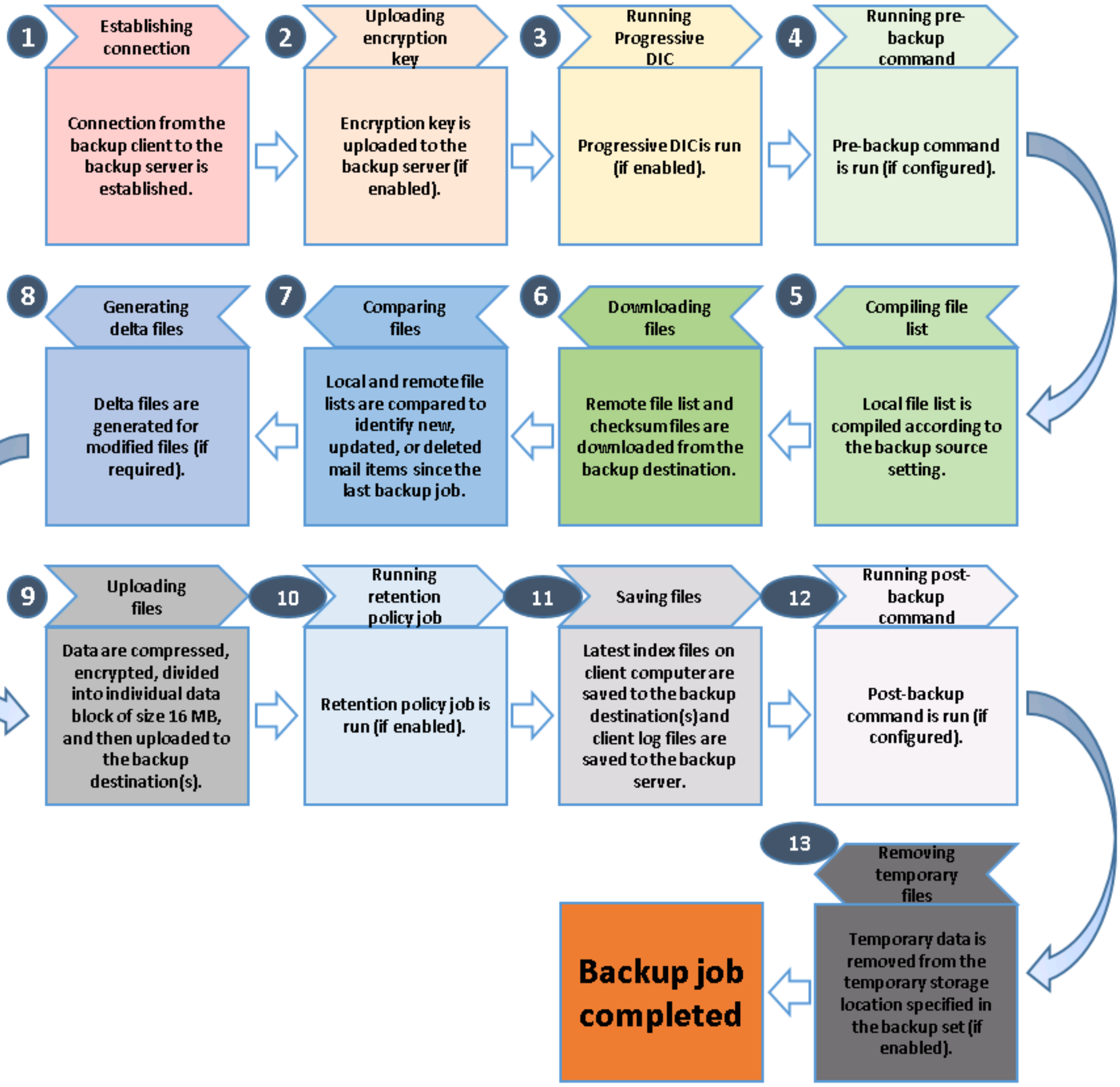
5. To provide maximum data protection and flexible restore options, it is recommended to configure:

   - At least one offsite or cloud destination
   - At least one local destination for fast recovery

6. Perform test restores periodically to ensure your backup is set up and performed properly. Performing recovery test can also help identify potential issues or gaps in your recovery plan. It is important that you do not try to make the test easier, as the objective of a successful test is not to demonstrate that everything is flawless. There might be flaws identified in the plan throughout the test and it is important to identify those flaws.

3 Overview of ShadowProtect System Backup Process

The following steps are performed during a ShadowProtect System backup job:



1 Establishing connection

Connection from the backup client to the backup server is established.

2 Uploading encryption key

Encryption key is uploaded to the backup server (if enabled).

3 Running Progressive DIC

Progressive DIC is run (if enabled).

4 Running pre-backup command

Pre-backup command is run (if configured).

5 Compiling file list

Local file list is compiled according to the backup source setting.

6 Downloading files

Remote file list and checksum files are downloaded from the backup destination.

7 Comparing files

Local and remote file lists are compared to identify new, updated, or deleted mail items since the last backup job.

8 Generating delta files

Delta files are generated for modified files (if required).

9 Uploading files

Data are compressed, encrypted, divided into individual data block of size 16 MB, and then uploaded to the backup destination(s).

10 Running retention policy job

Retention policy job is run (if enabled).

11 Saving files

Latest index files on client computer are saved to the backup destination(s) and client log files are saved to the backup server.

12 Running post-backup command

Post-backup command is run (if configured).

13 Removing temporary files

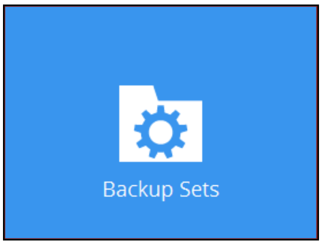
Temporary data is removed from the temporary storage location specified in the backup set (if enabled).

Backup job completed

4 Perform Backup for ShadowProtect System Backup Set

4.1 Create ShadowProtect System Backup Set

1. Click the **Backup Sets** icon on the main interface of AhsayOBM.

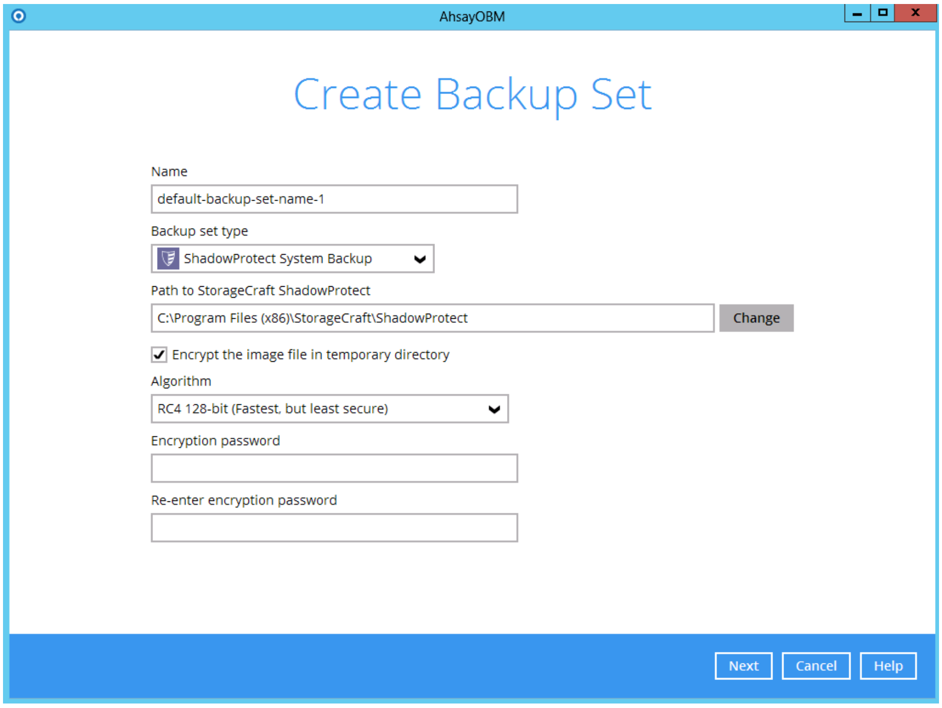


2. Create a new backup set by clicking the "**+**" icon next to **Add new backup set**.

3. Select the Backup set type as **ShadowProtect System Backup**. The system will automatically detect and select the Path to StorageCraft ShadowProtect, such as "C:\Program Files (x86)\StorageCraft\ShadowProtect". You can click on **Change** to modify the path if it is incorrect.

- Name your new backup set.

- Checked the "Encrypt the image file in temporary directory" if required.



Name: default-backup-set-name-1

Backup set type: ShadowProtect System Backup

Path to StorageCraft ShadowProtect: C:\Program Files (x86)\StorageCraft\ShadowProtect

☑ Encrypt the image file in temporary directory

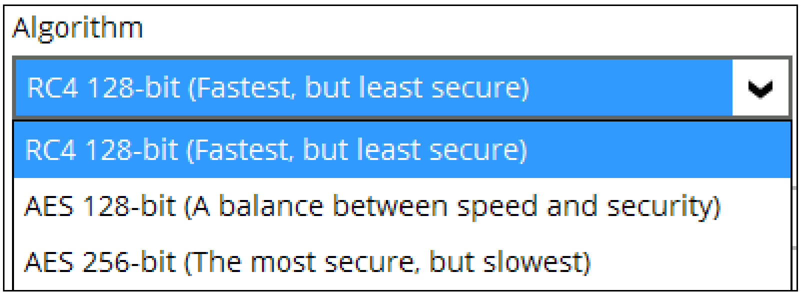
Algorithm: RC4 128-bit (Fastest, but least secure)

Encryption password

Re-enter encryption password

- Select the Algorithm from "RC4 128-bit (Fastest, but least secure)", "AES 128-bit (A balance between speed and security)", "AES 256-bit (The most secure, but slowest)". It is suggested to select **AES 256-bit (The most**

secure, but slowest) as the algorithm.



Algorithm

RC4 128-bit (Fastest, but least secure)

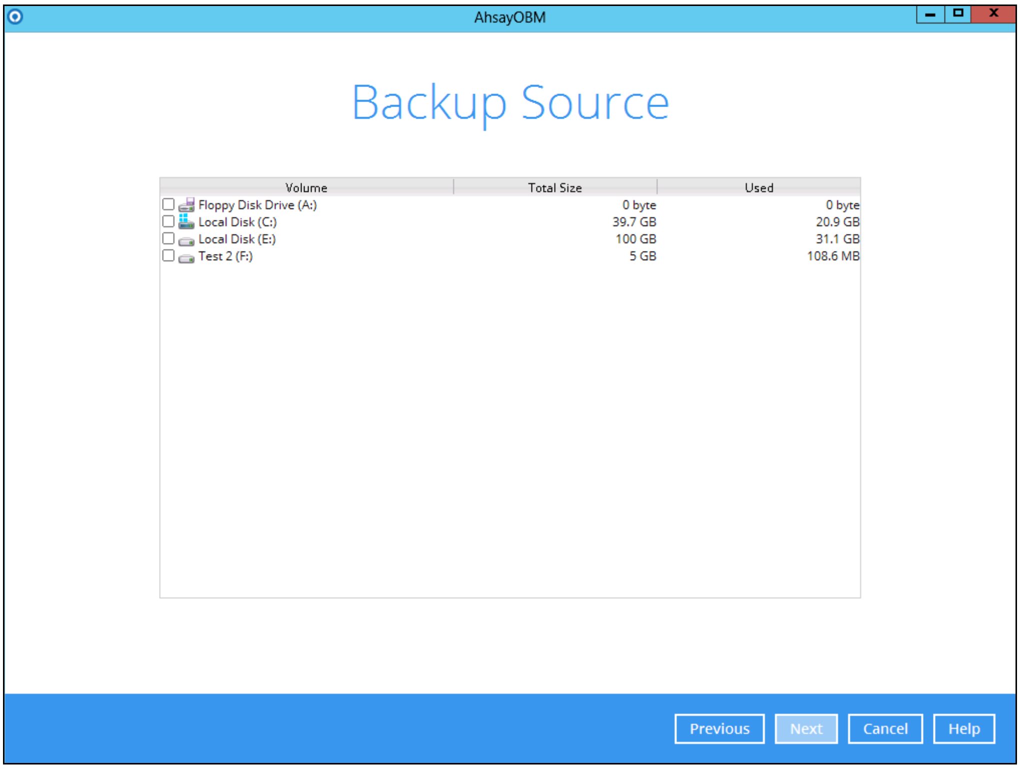
- RC4 128-bit (Fastest, but least secure)
- AES 128-bit (A balance between speed and security)
- AES 256-bit (The most secure, but slowest)

- Enter the Encryption password
- Re-enter encryption password

NOTE

Please kindly note that the encryption key generated by checking the "Encrypt the image file in temporary directory" option CANNOT be recovered by Ahsay Encryption Key Recovery feature. So please keep the encryption key properly with several copies in case there is no way to recover the image.

4. In the **Backup Source** menu, select the drive(s) to backup. Click **Next** to proceed when you are done.

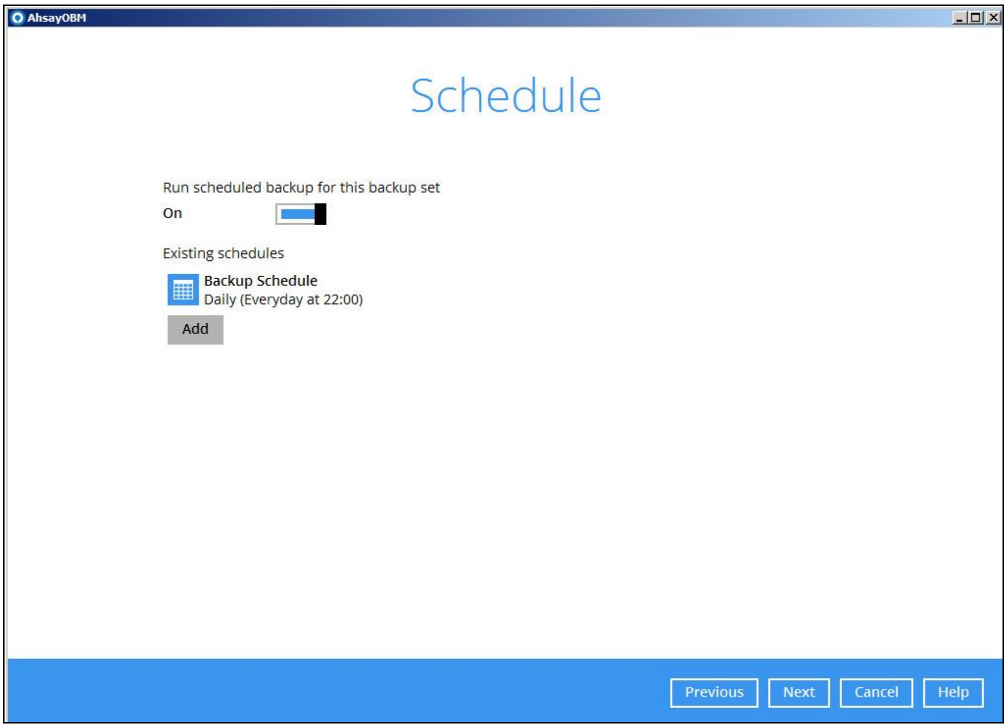


Backup Source

Volume	Total Size	Used
□ Floppy Disk Drive (A:)	0 byte	0 byte
□ Local Disk (C:)	39.7 GB	20.9 GB
□ Local Disk (E:)	100 GB	31.1 GB
□ Test 2 (F:)	5 GB	108.6 MB

5. In the Schedule menu, you can configure a backup schedule for backup job to run automatically at your specified time interval. Click **Add** to add a new schedule, then

click **Next** to proceed when you are done.



Schedule

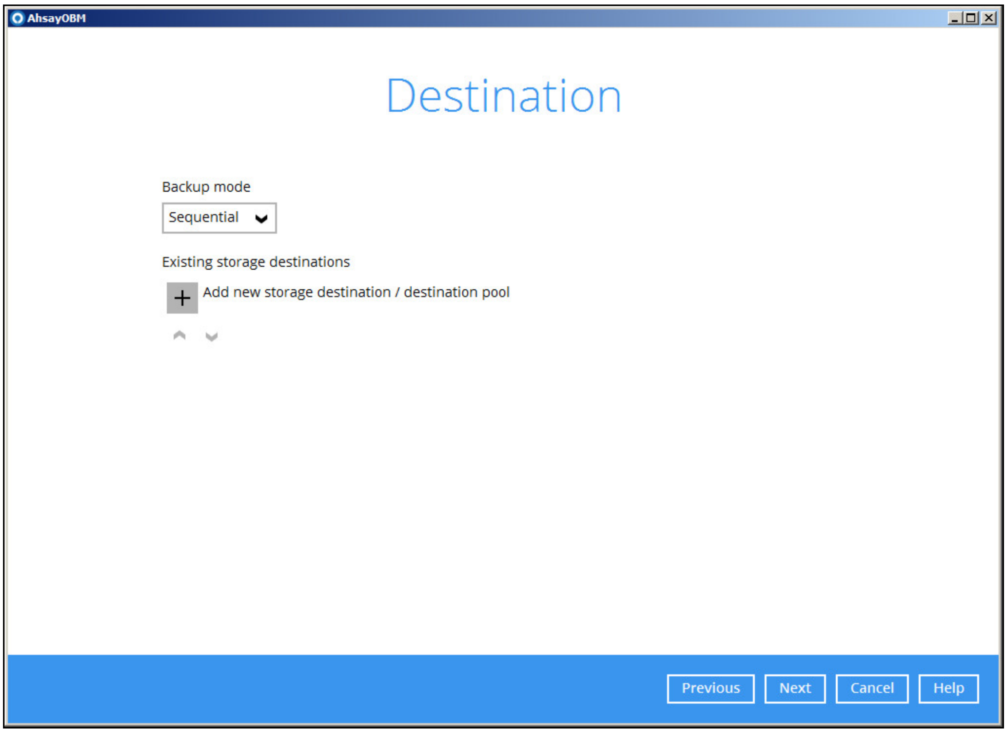
Run scheduled backup for this backup set

On

Existing schedules

Backup Schedule
Daily (Everyday at 22:00)

6. In the Destination menu, select backup mode from Sequential and Concurrent, and select a backup destination where the backup drive will be stored. Click the "**+**" icon next to **Add new storage destination / destination pool**.

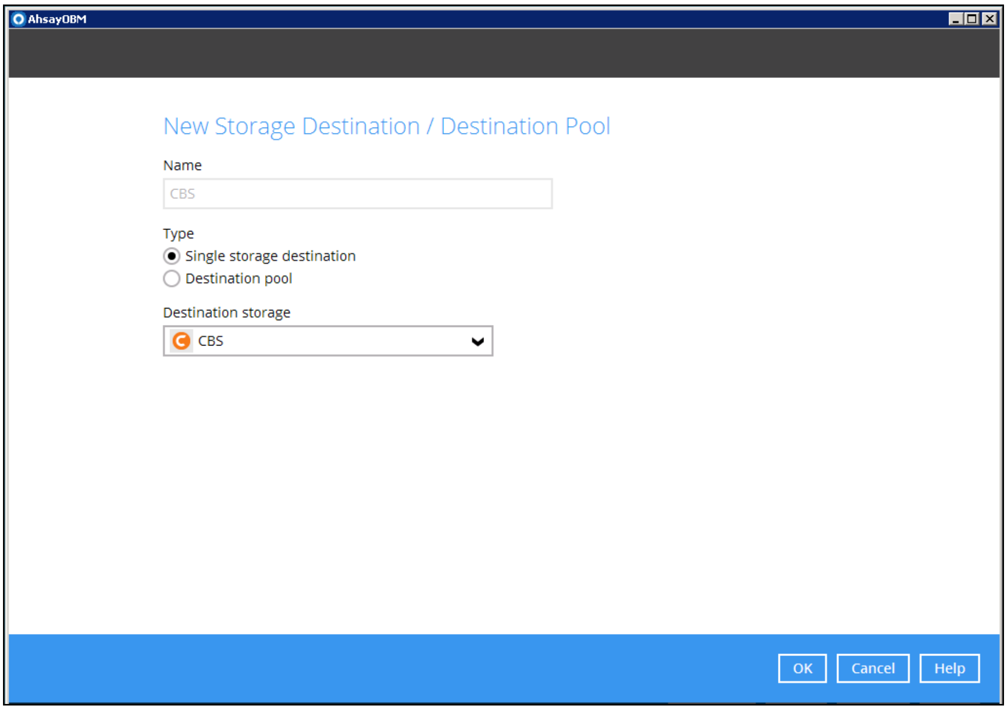


Destination

Backup mode: Sequential

Existing storage destinations

7. Select the destination type and destination storage, then click **OK** to proceed.



New Storage Destination / Destination Pool

Name

CBS

Type

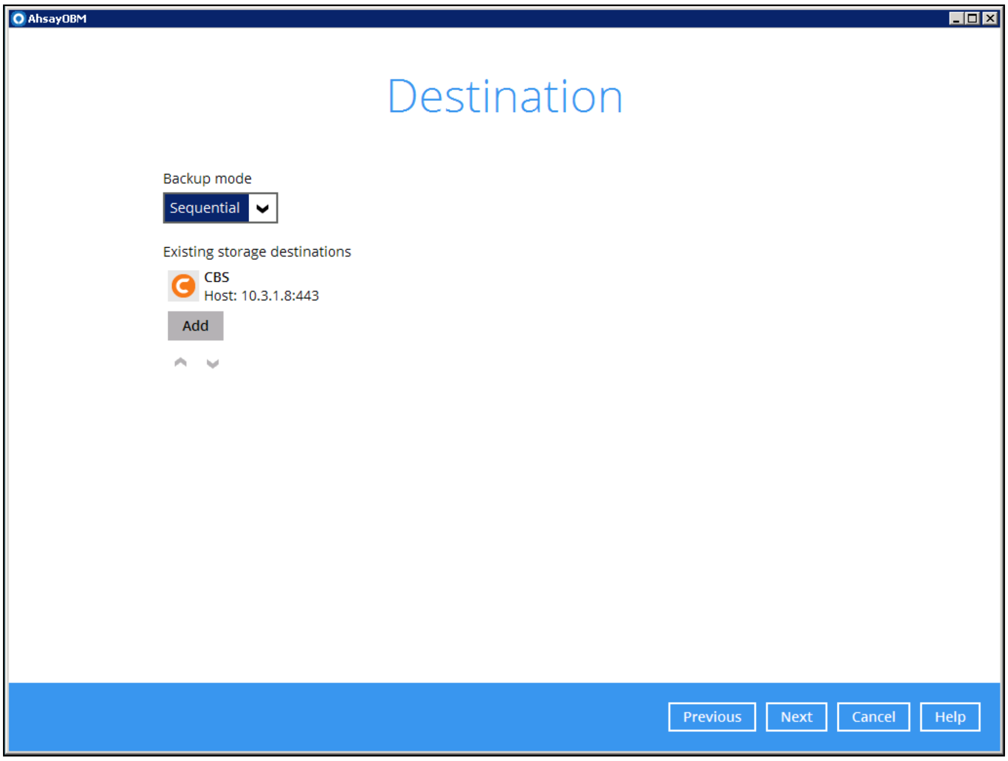
● Single storage destination

○ Destination pool

Destination storage

CBS

8. Click **Next** on the Destination menu page to proceed.



Destination

Backup mode

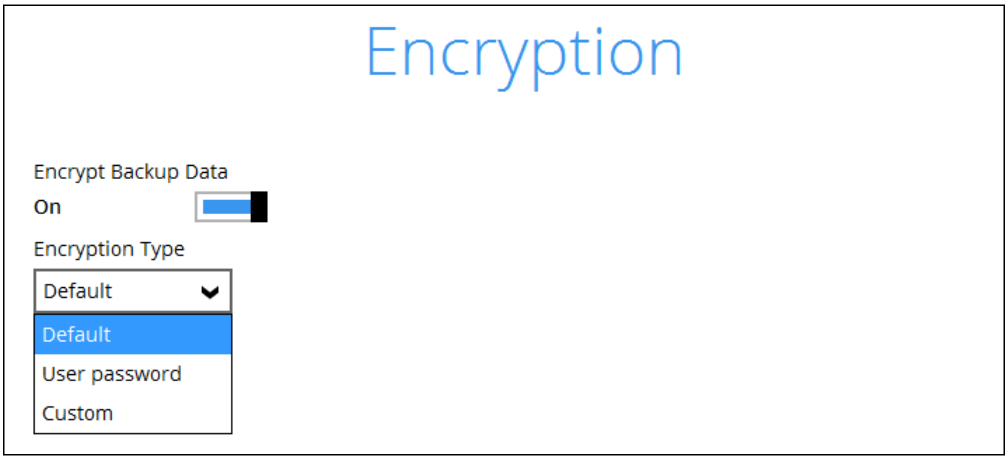
Sequential

Existing storage destinations

CBS
Host: 10.3.1.8:443

9. The Encryption window will only be shown if the “Encrypt the image file in temporary directory” is unchecked in Step 3, “create backup set”. The default **Encrypt Backup Data** option is enabled with an encryption key preset by the system which provides

the most secure protection.



Encryption

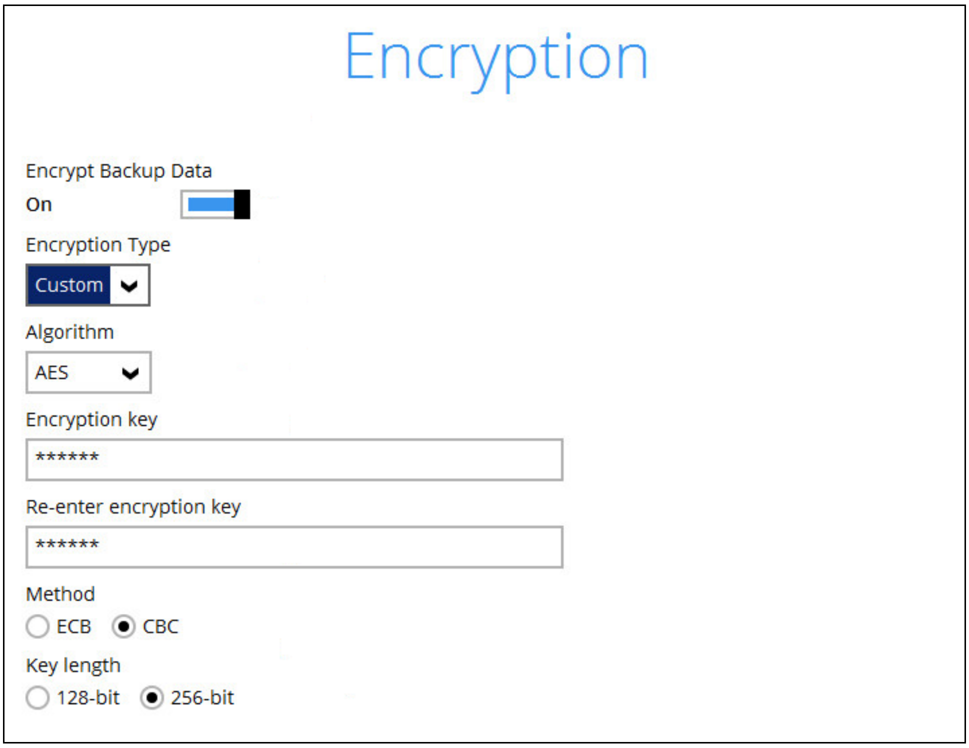
Encrypt Backup Data

On

Encryption Type

10. You can choose from one of the following three Encryption Type options:

- **Default** – an encryption key with 44 alpha numeric characters will be randomly generated by the system
- **User password** – the encryption key will be the same as the login password of your AhsayOBM at the time when this backup set is created. Please be reminded that if you change the AhsayOBM login password later, the encryption keys of the backup sets previously created with this encryption type will remain unchanged.
- **Custom** – you can customize your encryption key, where you can set your own algorithm, encryption key, method and key length.



Encryption

Encrypt Backup Data

On

Encryption Type: Custom

Algorithm: AES

Encryption key: ******

Re-enter encryption key: ******

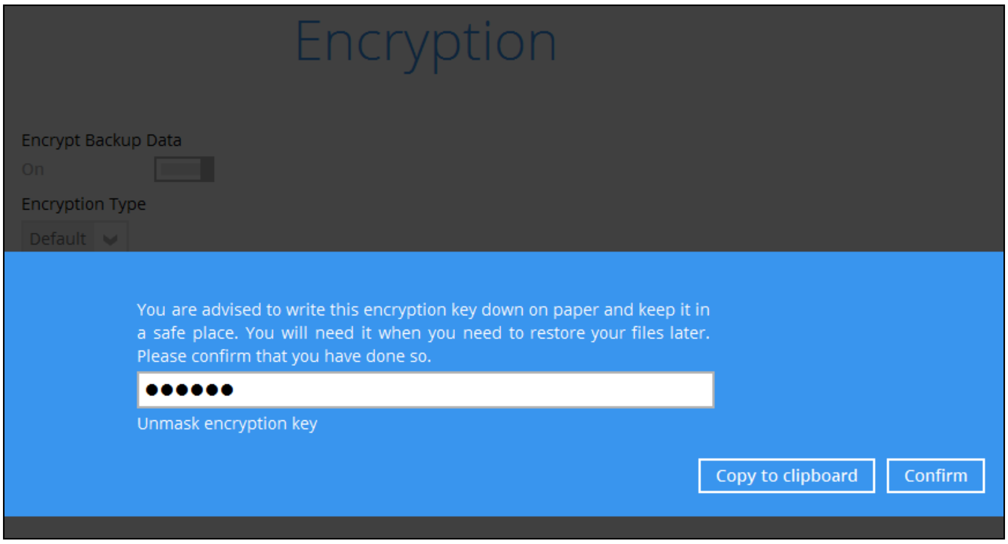
Method: ○ ECB ● CBC

Key length: ○ 128-bit ● 256-bit

Note: For best practice on managing your encryption key, refer to the following article: Best Practices for Managing Encryption Key on AhsayOBM or AhsayCBS Version 7

Click **Next** when you are done.

11. If you have enabled the Encryption Key feature in the previous step, the following pop-up window shows, no matter which encryption type you have selected.



Encryption

Encrypt Backup Data

On

Encryption Type

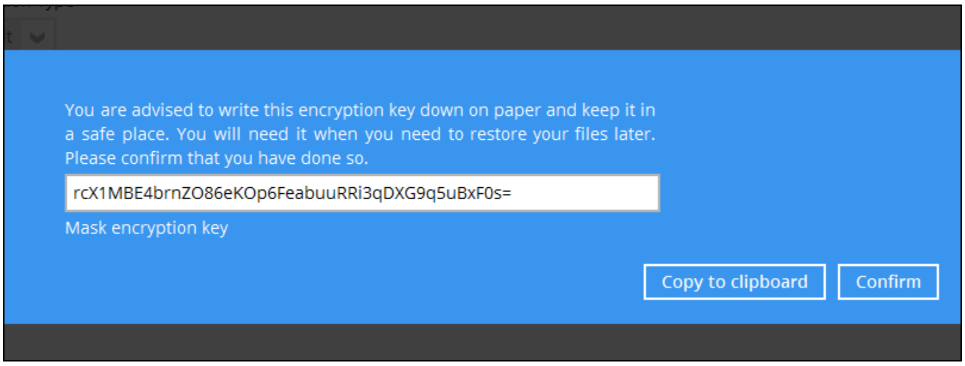
Default

You are advised to write this encryption key down on paper and keep it in a safe place. You will need it when you need to restore your files later. Please confirm that you have done so.

●●●●●●

The pop-up window has the following three options to choose from:

- **Unmask encryption key** – The encryption key is masked by default. Click this option to show the encryption key.



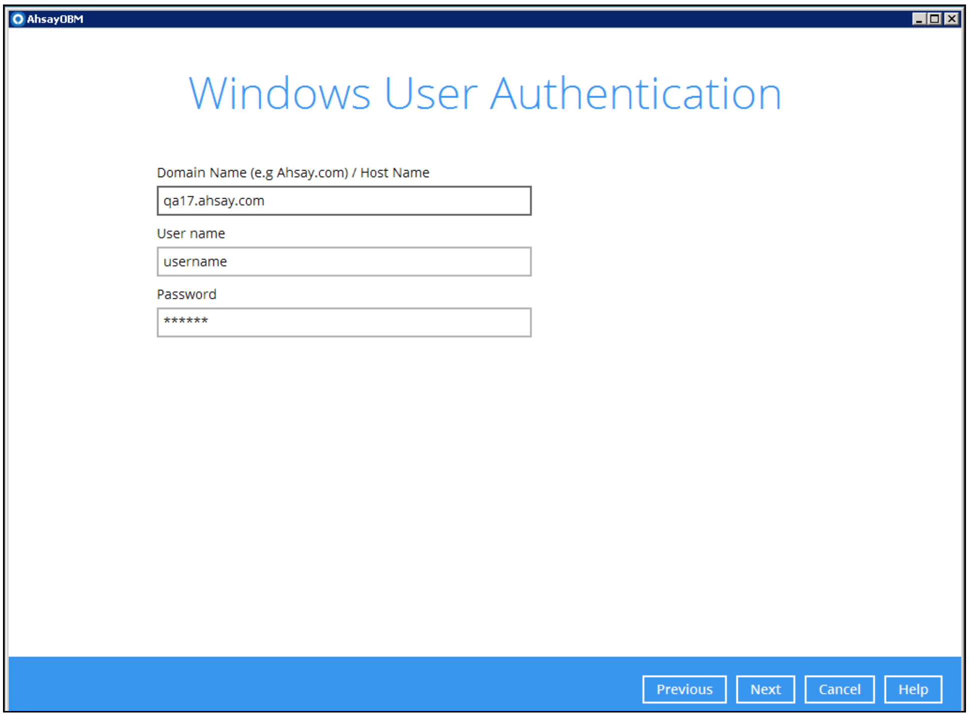
You are advised to write this encryption key down on paper and keep it in a safe place. You will need it when you need to restore your files later. Please confirm that you have done so.

rcX1MBE4brnZO86eKOp6FeabuuRRi3qDXG9q5uBxF0s=

- **Copy to clipboard** – Click to copy the encryption key, then you can paste it in another location of your choice.

- **Confirm** – Click to exit this pop-up window and proceed to the next step

12. Enter the Windows login credentials for user authentication. Click **Next** to proceed.



Windows User Authentication

Domain Name (e.g Ahsay.com) / Host Name
qa17.ahsay.com

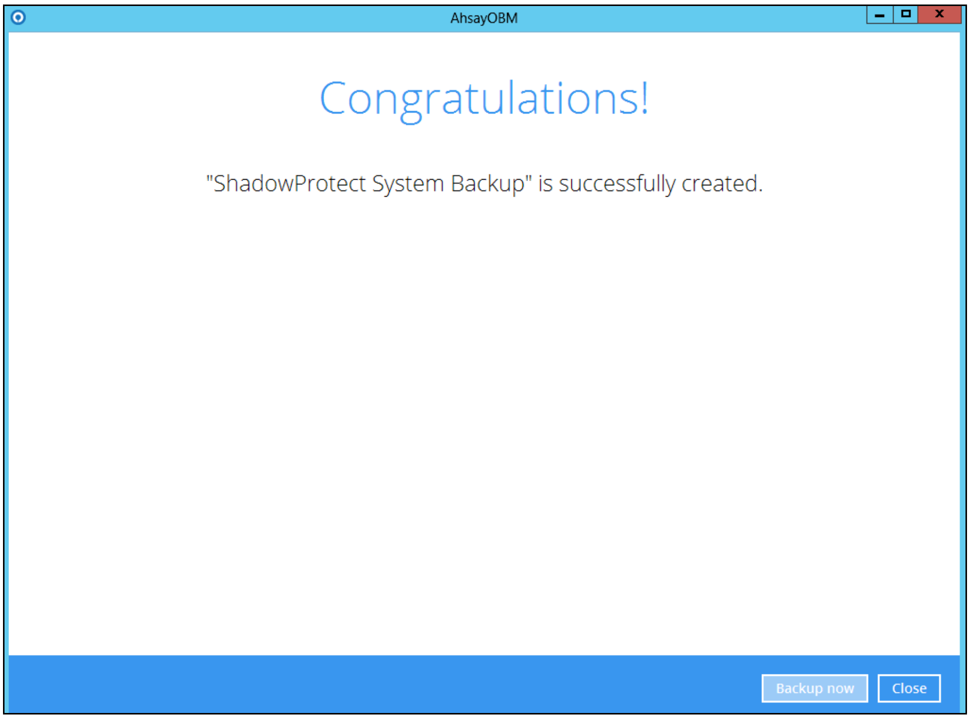
User name
username

Password
******

NOTE

The Windows User Authentication interface will show only if scheduled backup is enabled and set successfully.

13. The following screen shows when the new backup set is created successfully.



Congratulations!

"ShadowProtect System Backup" is successfully created.

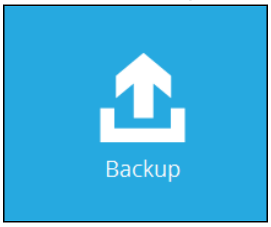
14. Click **Backup now** to start a backup immediately, or you can run a backup job later by following the instructions in Run Backup Job

4.2 Run Backup Job

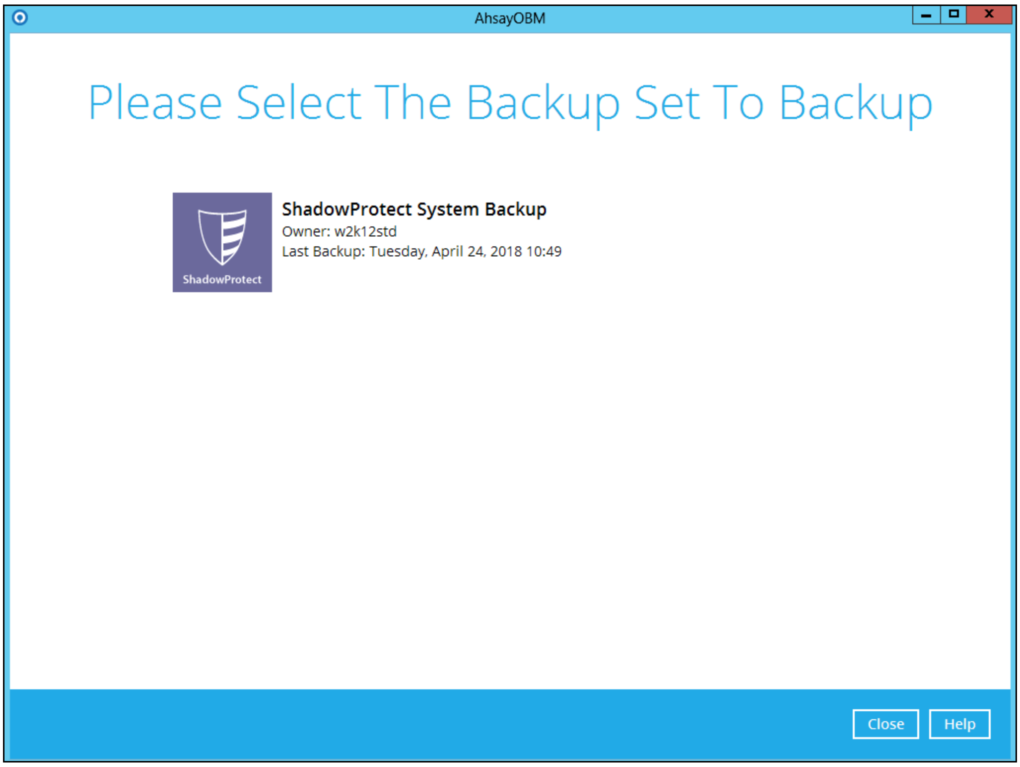
Below are the steps for backup process.

1. Log in to AhsayOBM.

2. Click the Backup icon on the main interface of AhsayOBM.



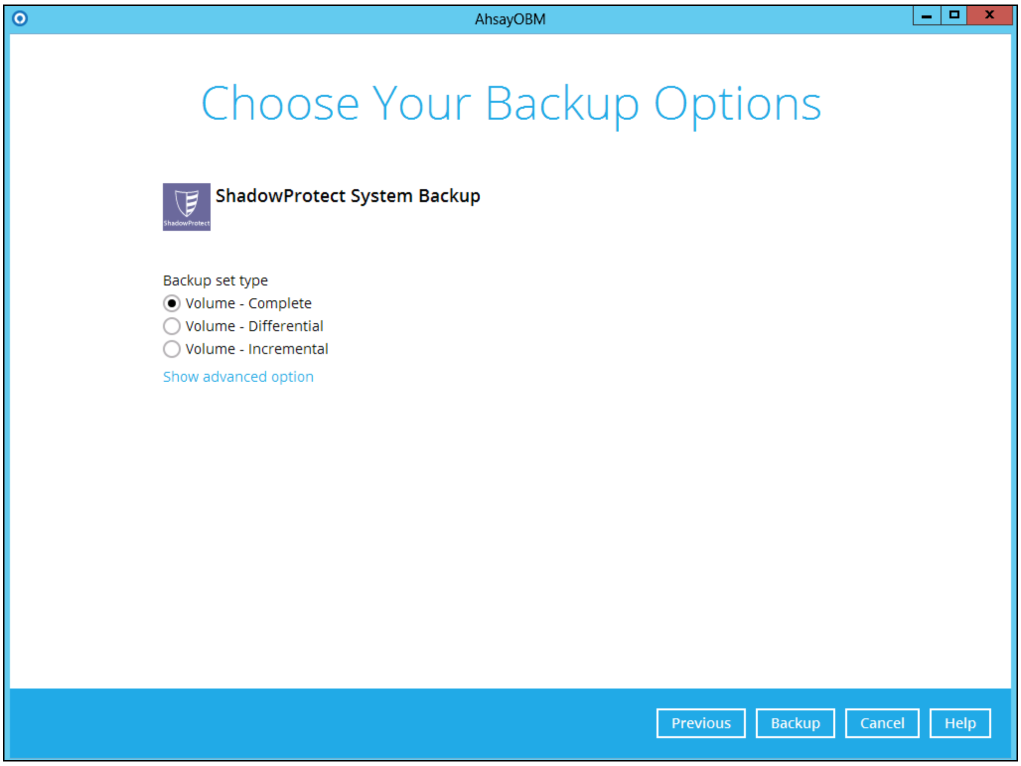
3. Select the backup set which you would like to start a ShadowProtect System backup for.



Please Select The Backup Set To Backup

ShadowProtect System Backup
Owner: w2k12std
Last Backup: Tuesday, April 24, 2018 10:49

4. Choose the backup set type from “Volume - Complete”, “Volume - Differential” and “Volume - Incremental”.



Choose Your Backup Options

ShadowProtect System Backup

Backup set type

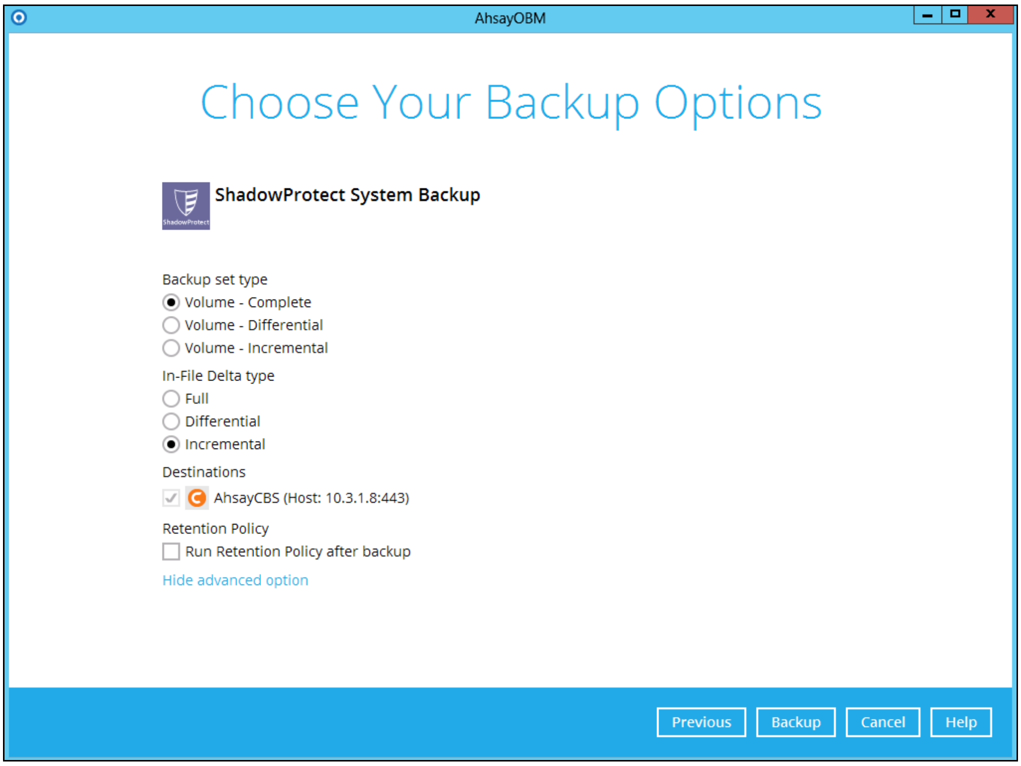
● Volume - Complete

○ Volume - Differential

○ Volume - Incremental

Show advanced option

If you would like to modify the In-File Delta type, Destinations and Retention Policy settings, click **Show advanced option**.



Choose Your Backup Options

ShadowProtect System Backup

Backup set type

● Volume - Complete

○ Volume - Differential

○ Volume - Incremental

In-File Delta type

○ Full

○ Differential

● Incremental

Destinations

☑ AhsayCBS (Host: 10.3.1.8:443)

Retention Policy

□ Run Retention Policy after backup

Hide advanced option

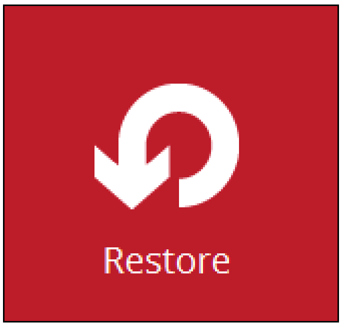
5. Click **Backup** to start the backup.

5 Perform Restore for ShadowProtect System Backup Set

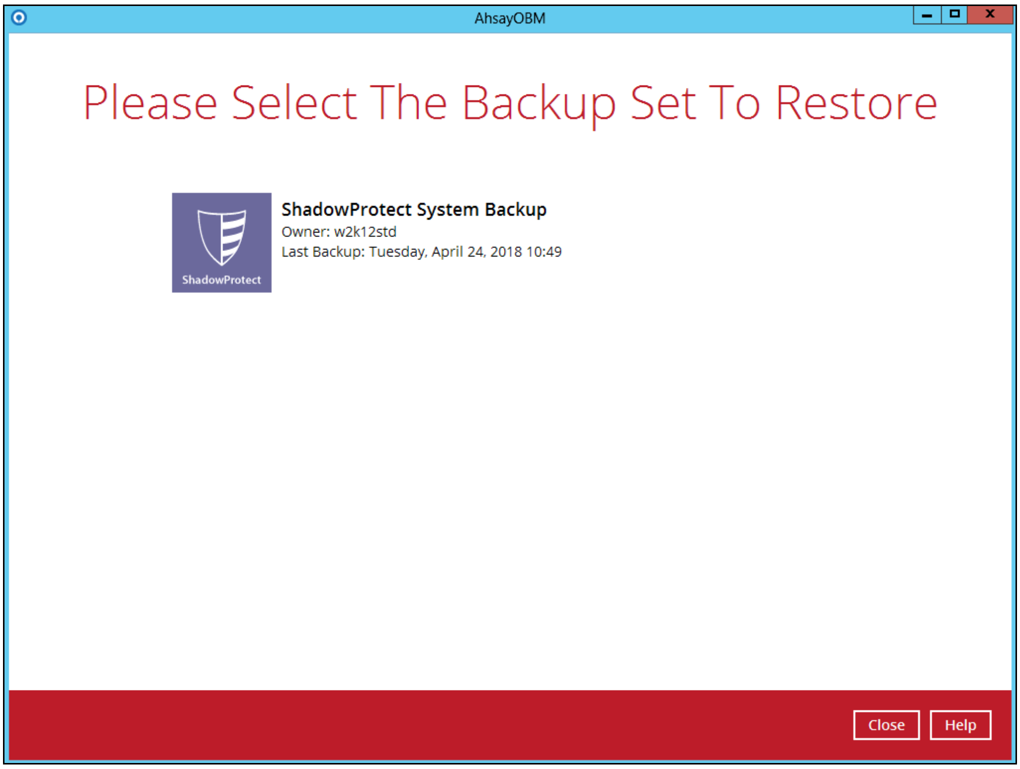
5.1 Restore to Non-system Volume

Below are the steps for restore process.

1. In the AhsayOBM main interface, click the **Restore** icon.



2. Select the backup set that you would like to restore ShadowProtect System from.

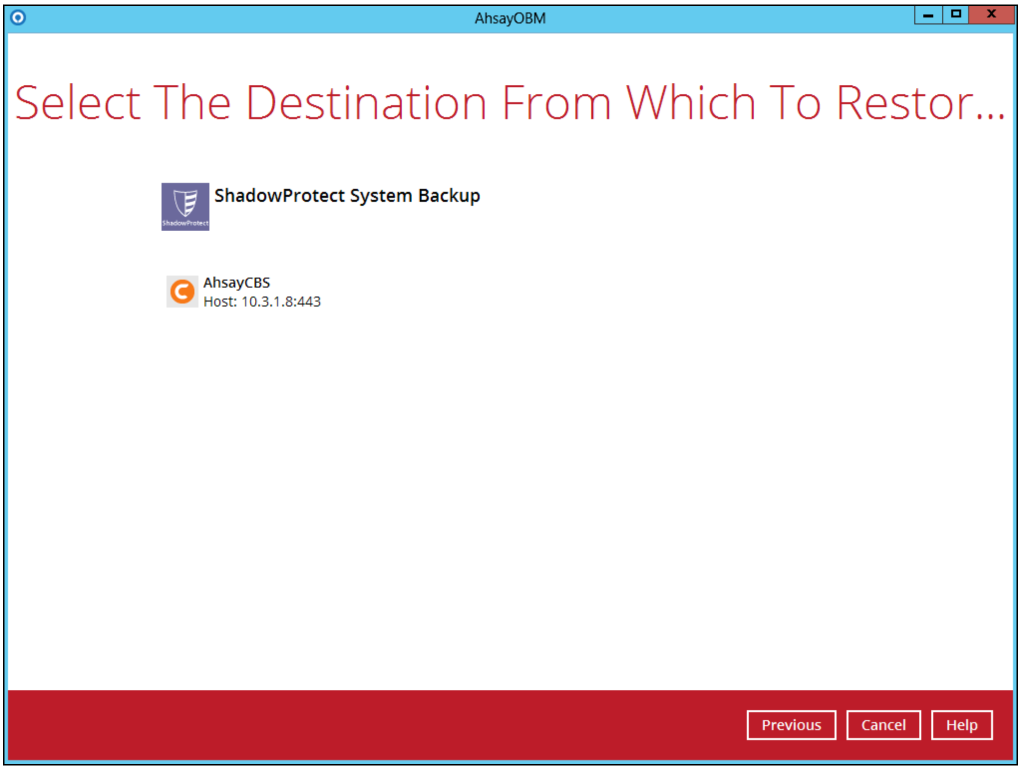


AhsayOBM

Please Select The Backup Set To Restore

ShadowProtect System Backup
Owner: w2k12std
Last Backup: Tuesday, April 24, 2018 10:49

3. Select the backup destination that contains the ShadowProtect System that you would like to restore.

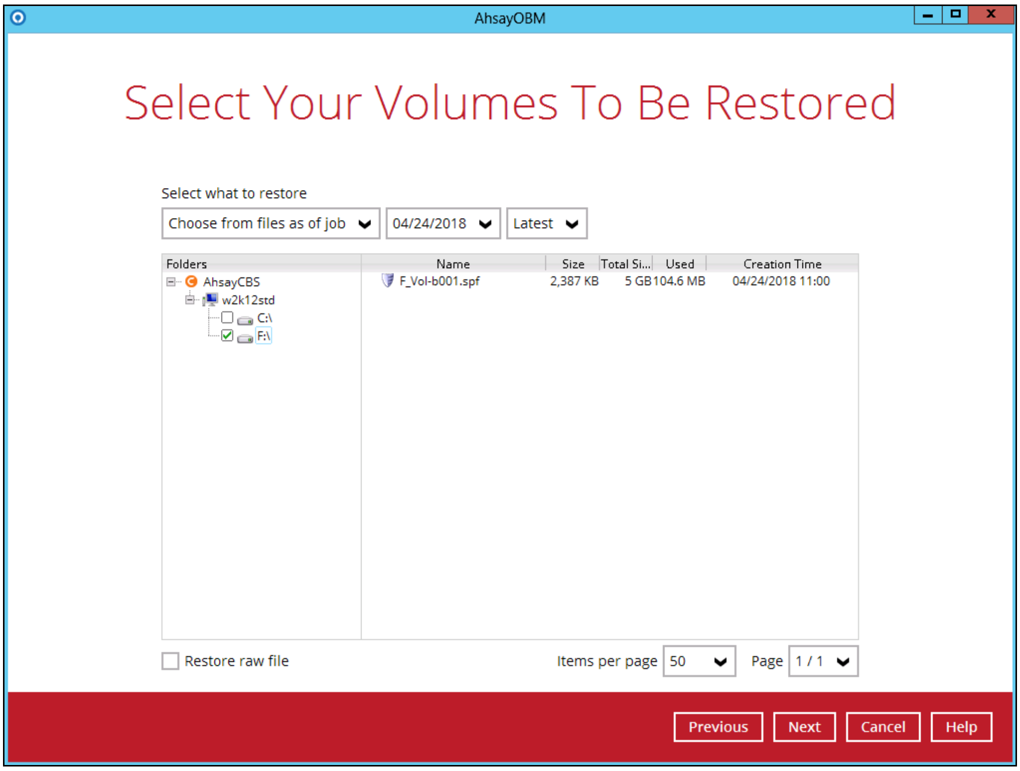


Select The Destination From Which To Restor...

ShadowProtect System Backup

AhsayCBS
Host: 10.3.1.8:443

4. Click to select which volume to restore. Click **Next** to proceed.



Select Your Volumes To Be Restored

Select what to restore

Choose from files as of job | 04/24/2018 | Latest

Folders
- AhsayCBS
  - w2k12std
    - □ C:\
    - ☑ F:\

Name	Size	Total Si...	Used	Creation Time
F_Vol-b001.spf	2,387 KB	5 GB	104.6 MB	04/24/2018 11:00

□ Restore raw file

Items per page 50 | Page 1 / 1

i. Normal Restore

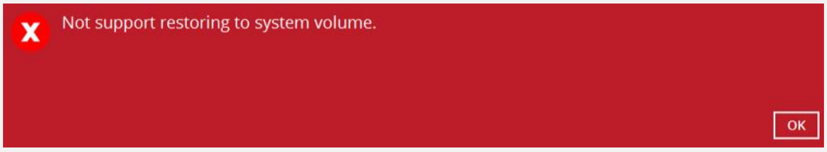
Select the restore volume and select to restore the ShadowProtect System to Original location or to Alternate location.

NOTE

Please kindly note that it is not supported to restore to system volume using AhsayOBM. If:

- select system volume as restore volume and select restore to original location;
- select non-system volume as resotre volume and select restore to alternate location that is system volume;

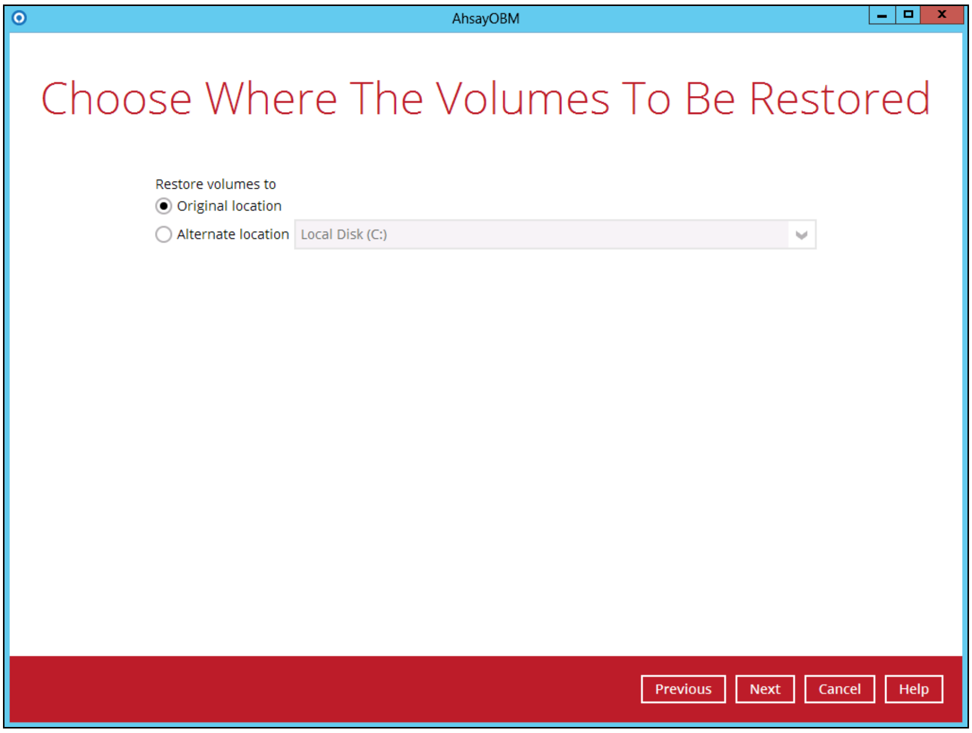
the following error will prompt.



Not support restoring to system volume.

Restore to Original Location

Select the **Original location** option, then press **Next** to proceed.



Choose Where The Volumes To Be Restored

Restore volumes to

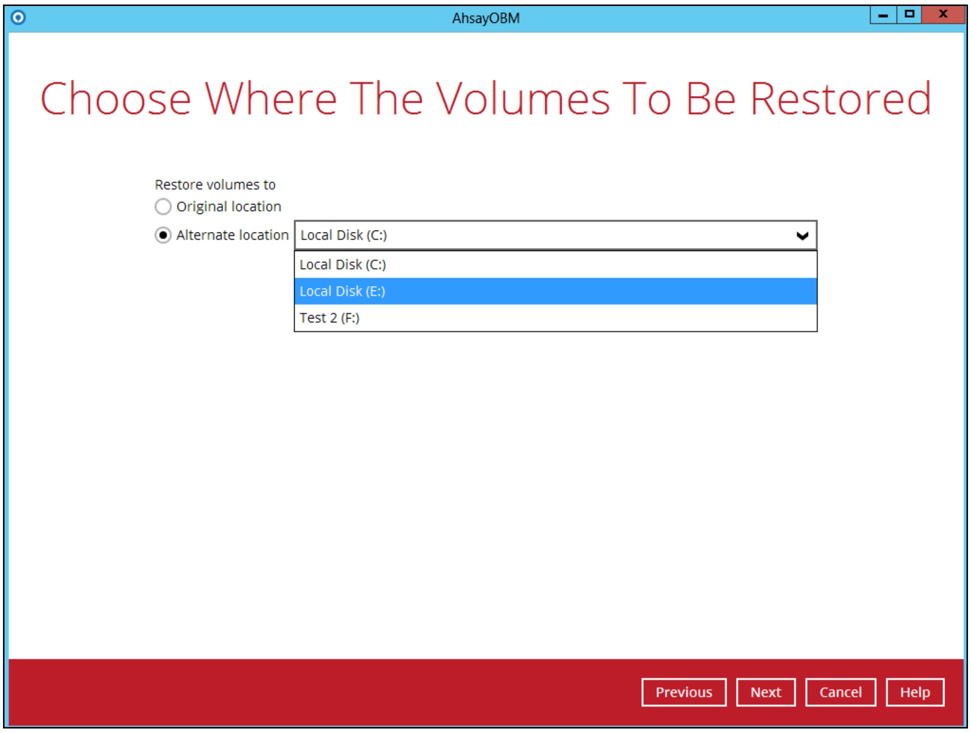
● Original location

○ Alternate location Local Disk (C:)

Restore to Alternate Location

You can choose to restore ShadowProtect System to alternate location. Select the **Alternate location** option and the desired volume destination, then press

Next to proceed.



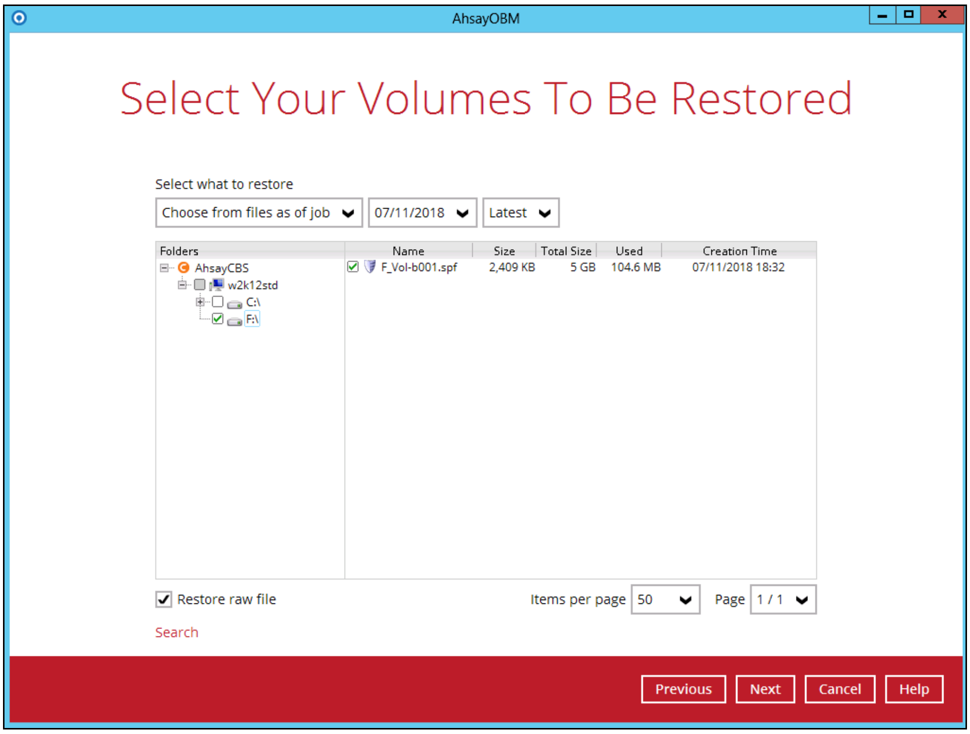
Choose Where The Volumes To Be Restored

Restore volumes to
○ Original location
● Alternate location Local Disk (C:)
Local Disk (C:)
Local Disk (E:)
Test 2 (F:)

ii. Restore Raw File

Restore raw file option will restore the spf file to the current computer and need to apply ShadowProtect restore wizard to restore the volume. For detailed steps please refer to Restore to System Volume option.

Check "**Restore raw file**" option and select the spf file to be restored. Click **Next** to continue.



Select Your Volumes To Be Restored

Select what to restore
Choose from files as of job | 07/11/2018 | Latest

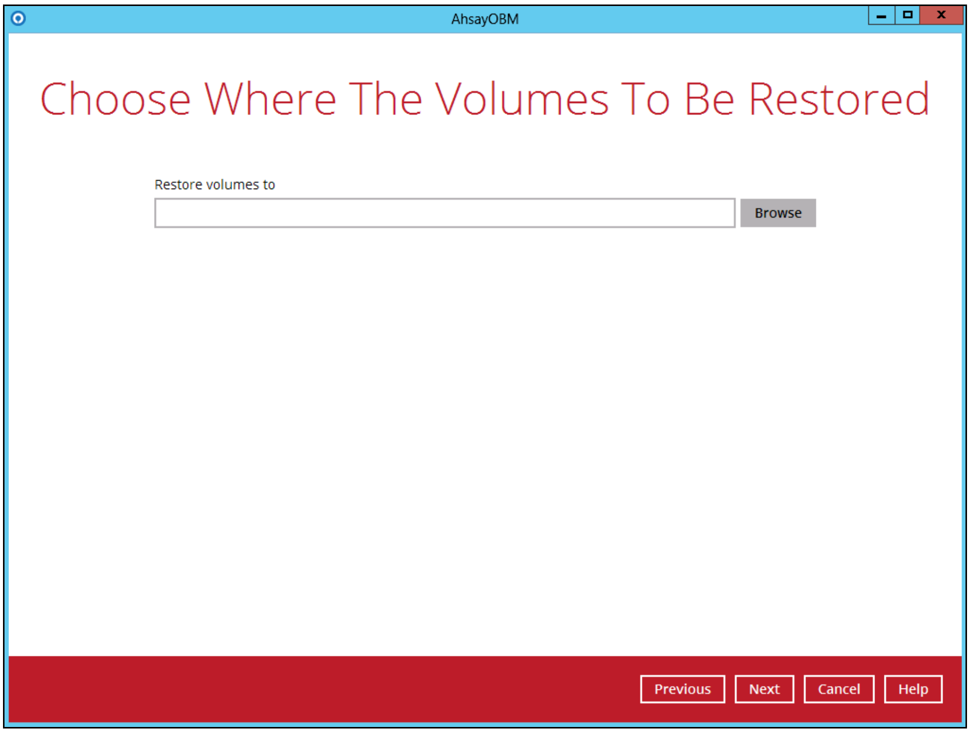
Folders: AhsayCBS > w2k12std > C:\ , ☑ F:\

	Name	Size	Total Size	Used	Creation Time
☑	F_Vol-b001.spf	2,409 KB	5 GB	104.6 MB	07/11/2018 18:32

☑ Restore raw file

Items per page 50 Page 1 / 1

Click **Browse** to choose where the volume to be restored. Click **Next** to continue.

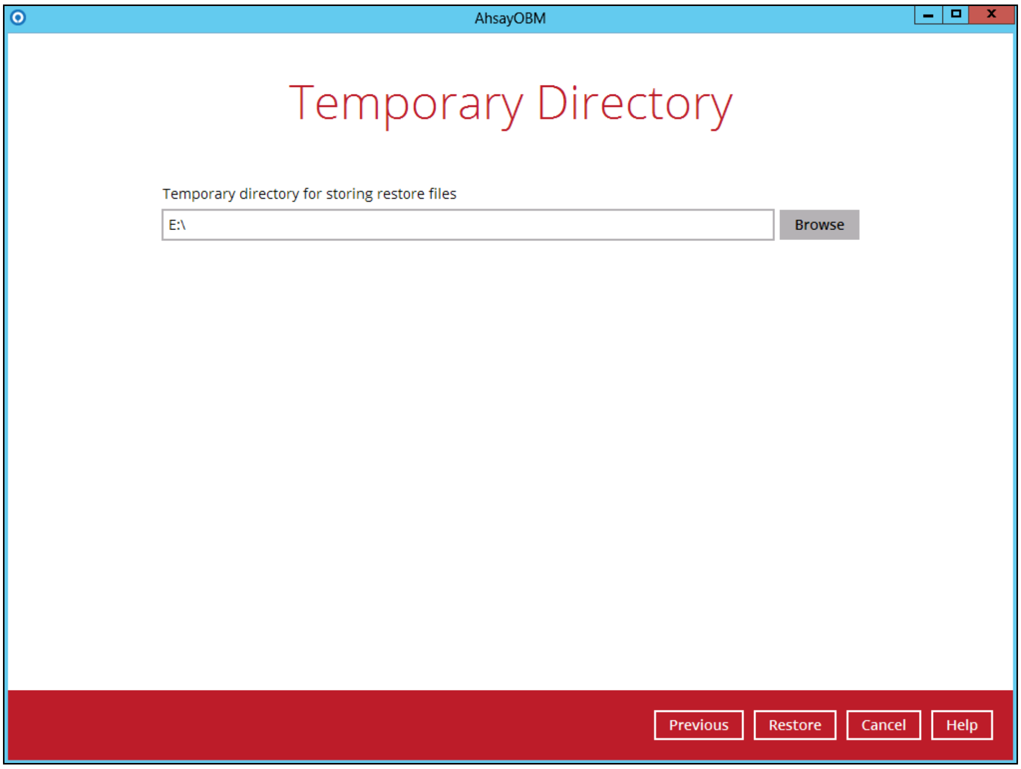


AhsayOBM

Choose Where The Volumes To Be Restored

Restore volumes to

5. Select the temporary directory for storing temporary files, click **Restore** to start the restoration.



AhsayOBM

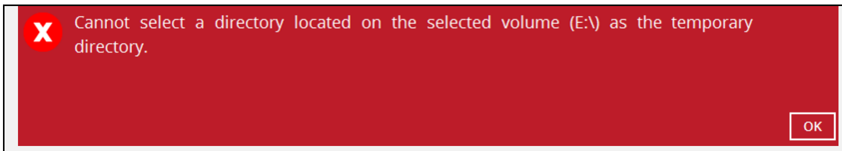
Temporary Directory

Temporary directory for storing restore files

E:\

NOTE

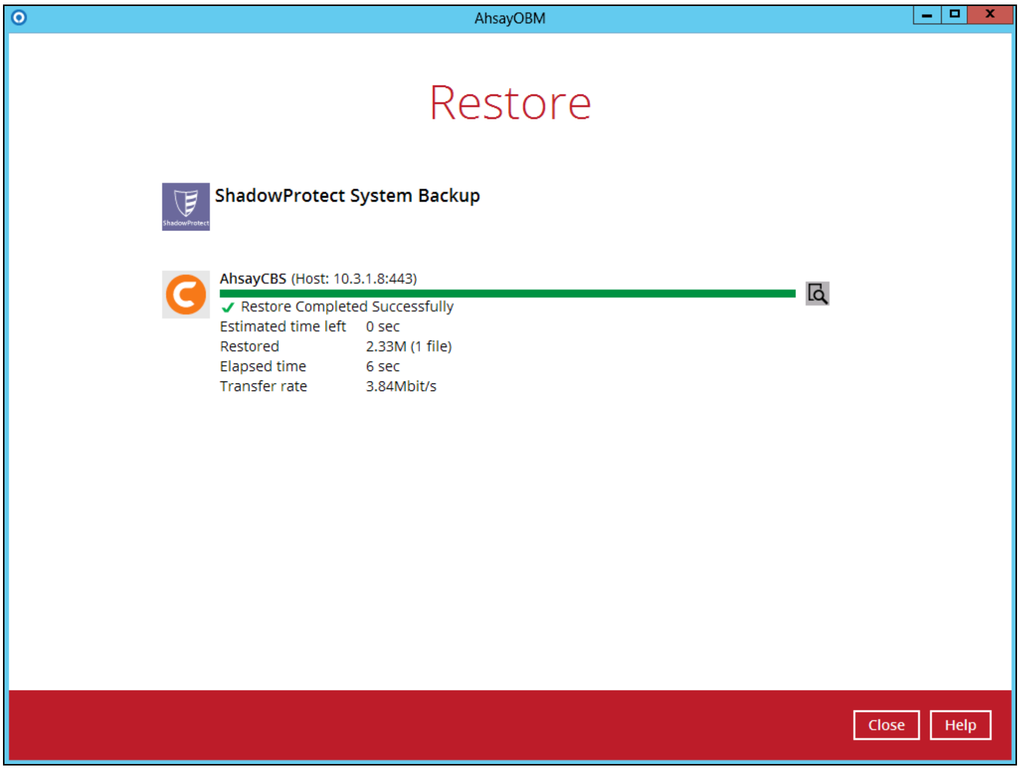
Please kindly note that for normal restore, it is not supported to select directory within restore destination as temporary directory. For example: if E drive is chosen as the restore destination, you cannot choose the directory within E drive as temporary directory, otherwise the following error will be prompted.



Cannot select a directory located on the selected volume (E:\) as the temporary directory.

The restriction is not applied to “Restore raw file” option.

6. The following screen with the text **Restore Completed Successfully** shows when the restoration is completed.



Restore

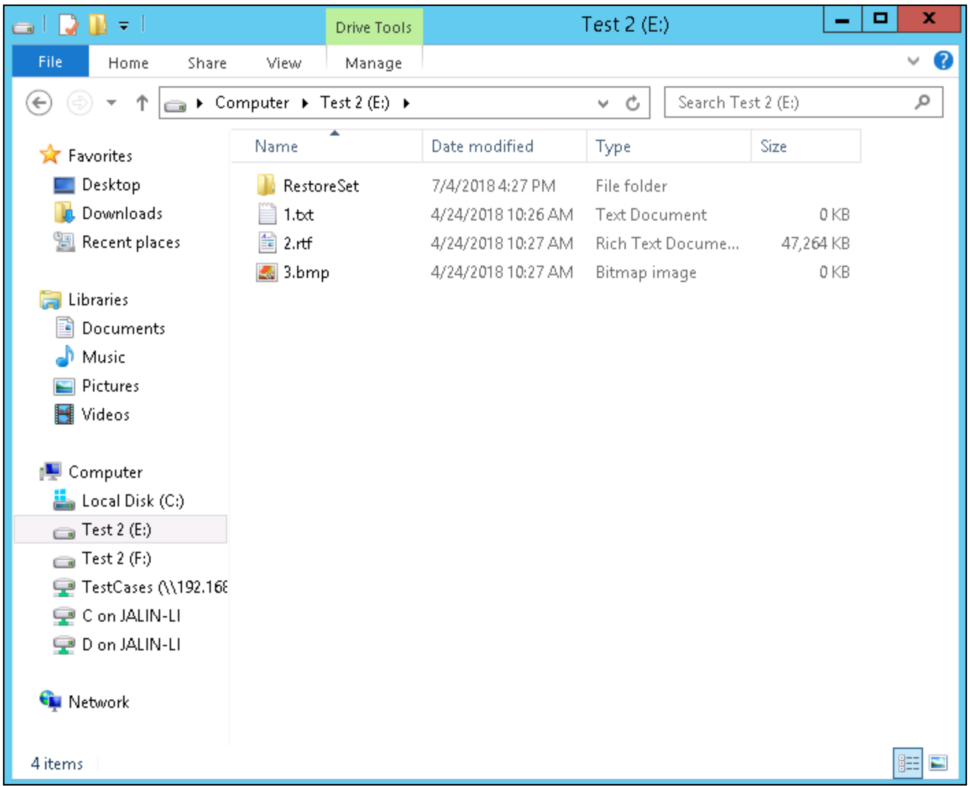
ShadowProtect System Backup

AhsayCBS (Host: 10.3.1.8:443)

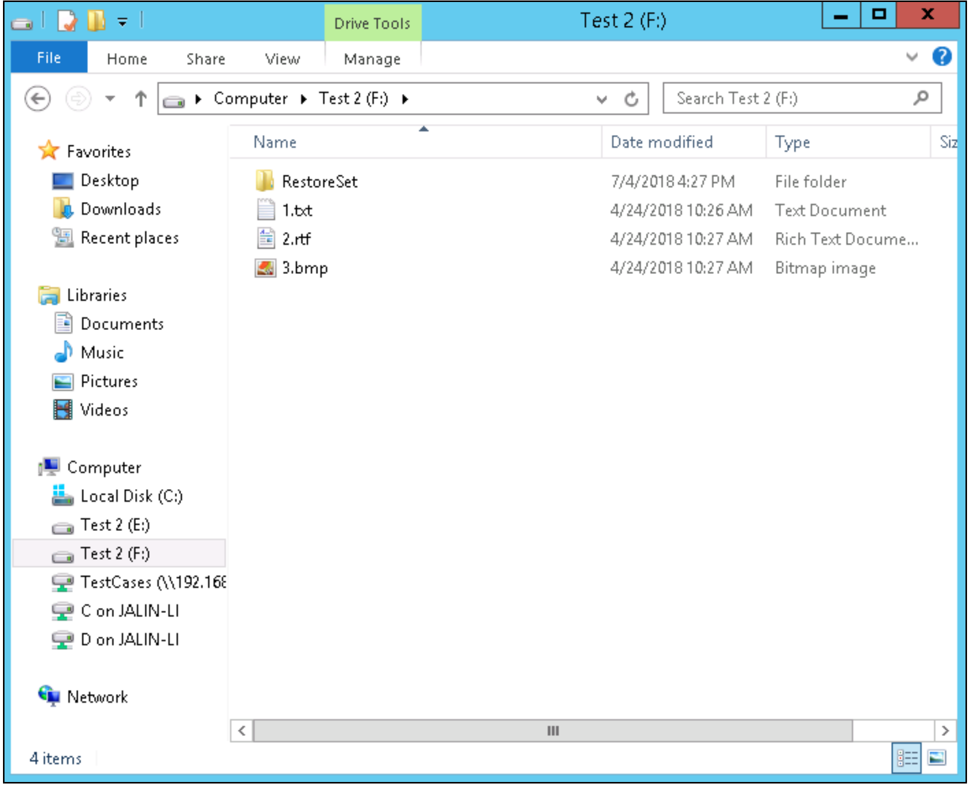
✓ Restore Completed Successfully

Estimated time left	0 sec
Restored	2.33M (1 file)
Elapsed time	6 sec
Transfer rate	3.84Mbit/s

7. Open **Computer** to check the volume situation. If restore the F:\ drive to E:\ drive, after successful restoration you will find that the contents in E:\ drive will be exactly the same with the contents in F:\ drive.



Name	Date modified	Type	Size
RestoreSet	7/4/2018 4:27 PM	File folder	
1.txt	4/24/2018 10:26 AM	Text Document	0 KB
2.rtf	4/24/2018 10:27 AM	Rich Text Docume...	47,264 KB
3.bmp	4/24/2018 10:27 AM	Bitmap image	0 KB



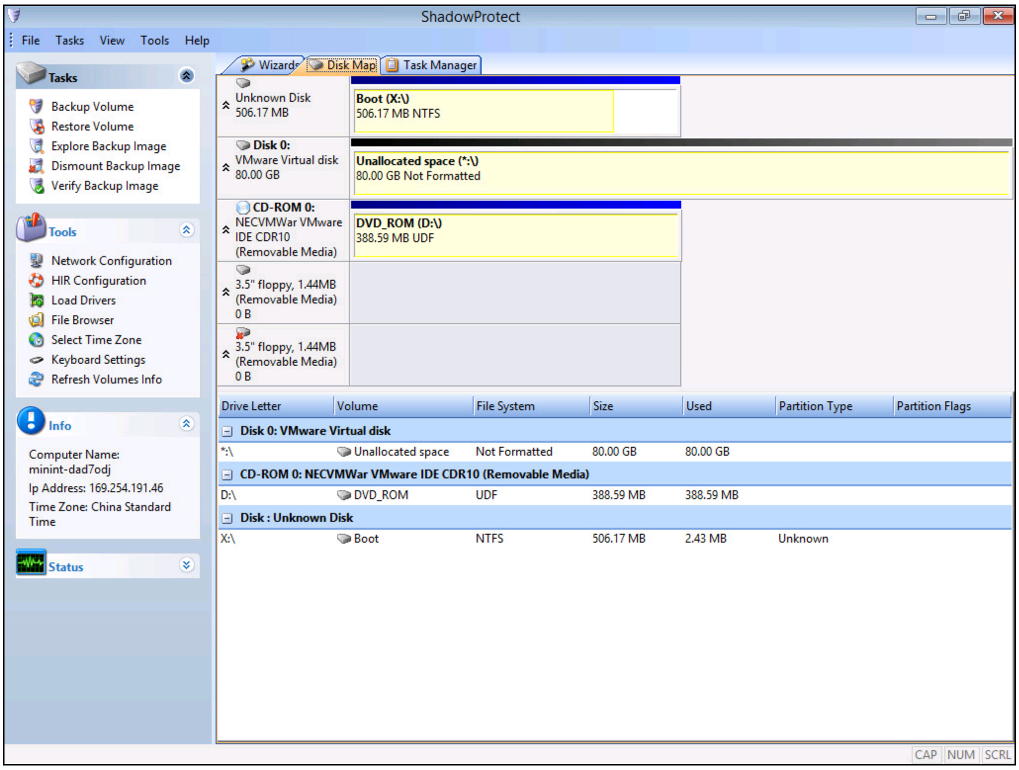
Name	Date modified	Type	Siz
RestoreSet	7/4/2018 4:27 PM	File folder	
1.txt	4/24/2018 10:26 AM	Text Document	
2.rtf	4/24/2018 10:27 AM	Rich Text Docume...	
3.bmp	4/24/2018 10:27 AM	Bitmap image	

5.2 Restore to System Volume

Below are the steps for restore process.

1. Open ShadowProtect wizard.

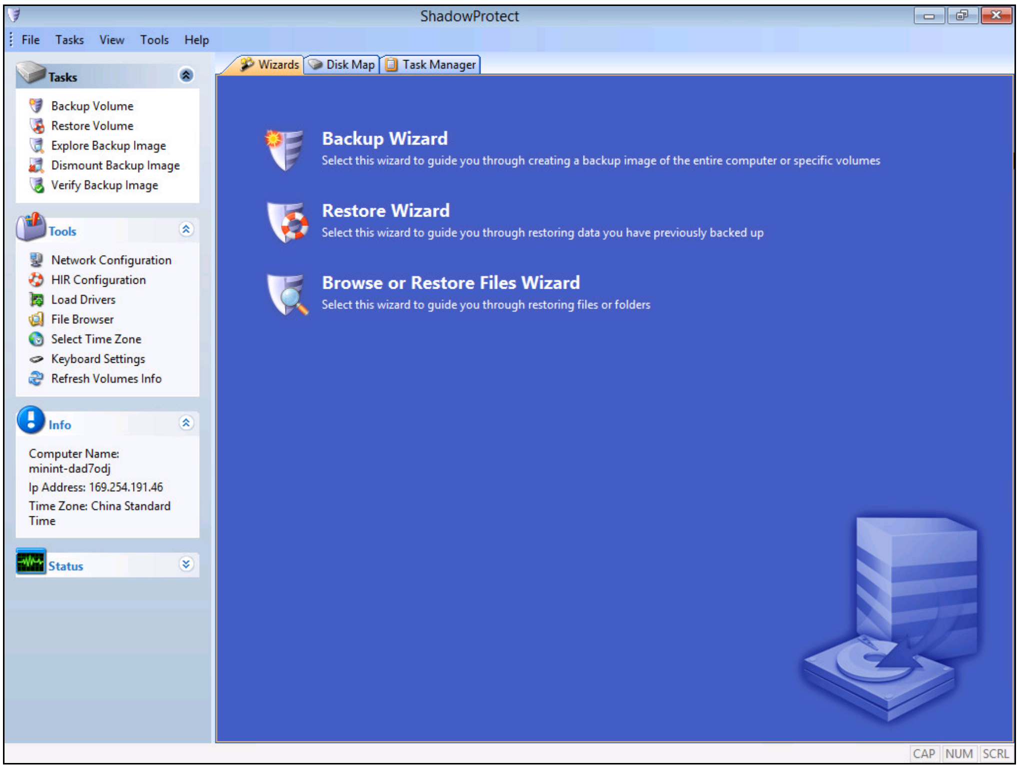
2. Click **Disk Map** to check current disk situation.



Computer Name: minint-dad7odj
Ip Address: 169.254.191.46
Time Zone: China Standard Time

Drive Letter	Volume	File System	Size	Used	Partition Type	Partition Flags
Disk 0: VMware Virtual disk						
*:\	Unallocated space	Not Formatted	80.00 GB	80.00 GB		
CD-ROM 0: NECVMWar VMware IDE CDR10 (Removable Media)						
D:\	DVD_ROM	UDF	388.59 MB	388.59 MB		
Disk : Unknown Disk						
X:\	Boot	NTFS	506.17 MB	2.43 MB	Unknown	

3. Click **Wizards** and **Restore Wizard** to continue.



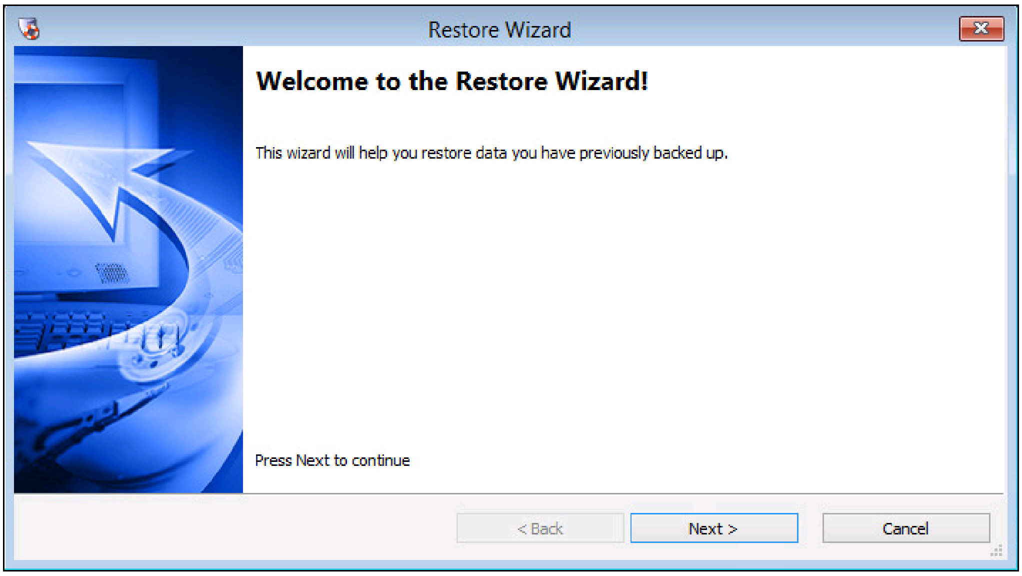
Computer Name: minint-dad7odj
Ip Address: 169.254.191.46
Time Zone: China Standard Time

Backup Wizard
Select this wizard to guide you through creating a backup image of the entire computer or specific volumes

Restore Wizard
Select this wizard to guide you through restoring data you have previously backed up

Browse or Restore Files Wizard
Select this wizard to guide you through restoring files or folders

4. Click **Next** to continue.



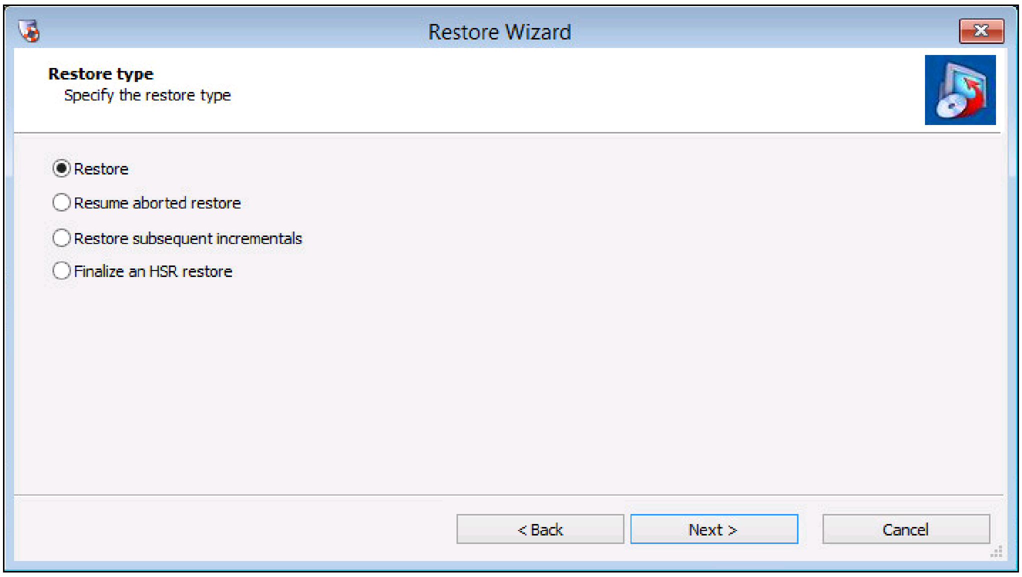
Restore Wizard

Welcome to the Restore Wizard!

This wizard will help you restore data you have previously backed up.

Press Next to continue

5. Specify the restore type from “Restore”, “Resume aborted restore”, “Restore subsequent incremental” and “Finalize an HSR restore”. Click **Next** to continue.



Restore Wizard

Restore type

Specify the restore type

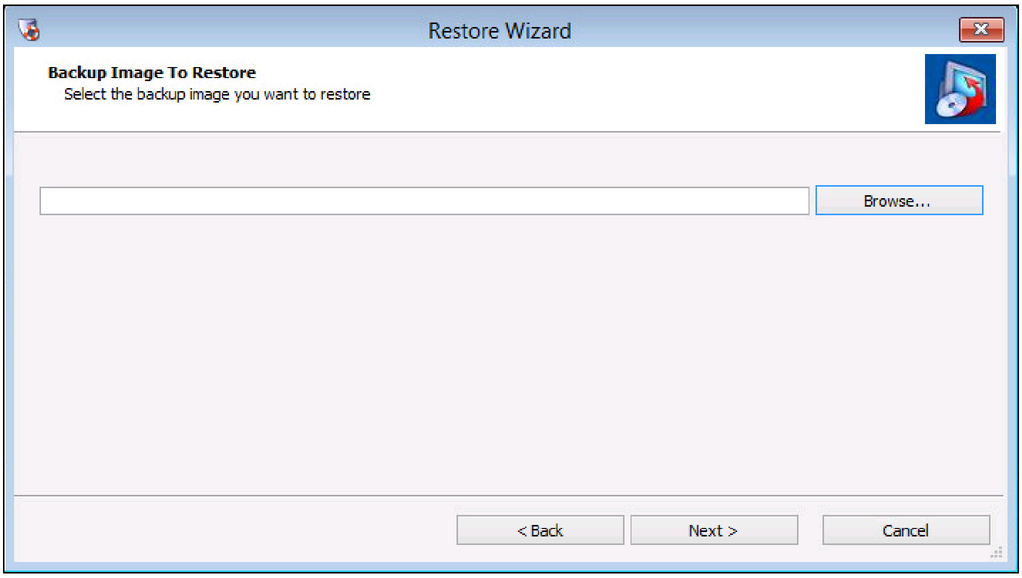
● Restore

○ Resume aborted restore

○ Restore subsequent incrementals

○ Finalize an HSR restore

6. Click **Browse** to select the network location or local path which contains the backup image and select the backup image you want to restore. Click **Next** to continue.

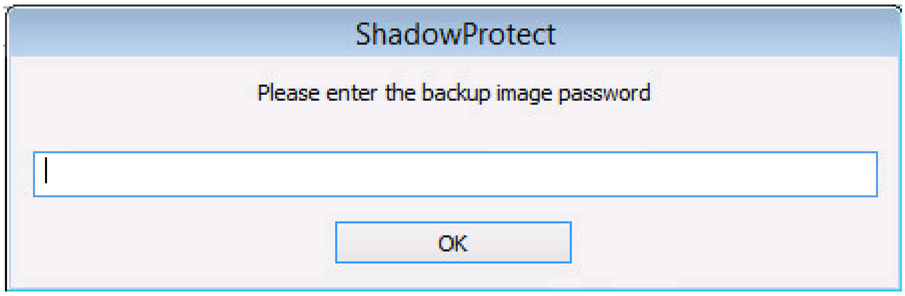


Restore Wizard

Backup Image To Restore

Select the backup image you want to restore

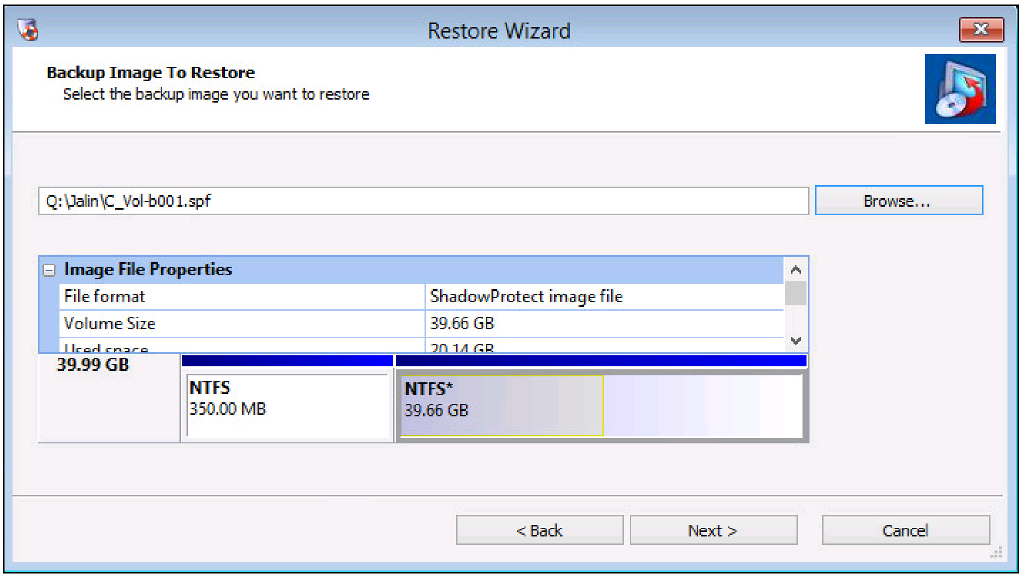
7. Enter the backup image encryption password. The page will be shown only if the encryption feature was enabled during creating backup set. Click **OK** to continue.



ShadowProtect

Please enter the backup image password

8. Verify current selection or select another point in time. Click **Next** to continue.



Restore Wizard

Backup Image To Restore

Select the backup image you want to restore

Q:\Jalin\C_Vol-b001.spf

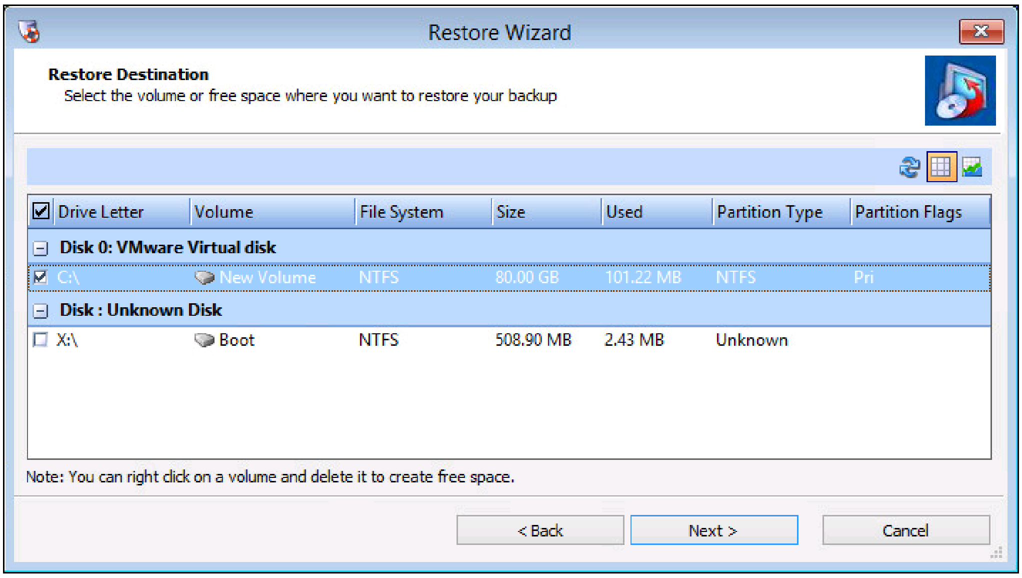
Image File Properties	
File format	ShadowProtect image file
Volume Size	39.66 GB
Used space	20.14 GB

39.99 GB

NTFS 350.00 MB

NTFS* 39.66 GB

9. Select the system volume as restore destination. Click **Next** to continue.



Restore Wizard

Restore Destination

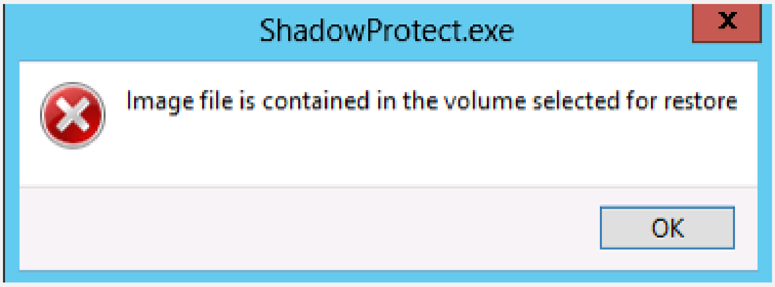
Select the volume or free space where you want to restore your backup

☑ Drive Letter	Volume	File System	Size	Used	Partition Type	Partition Flags
⊟ **Disk 0: VMware Virtual disk**						
☑ C:\	New Volume	NTFS	80.00 GB	101.22 MB	NTFS	Pri
⊟ **Disk : Unknown Disk**						
☐ X:\	Boot	NTFS	508.90 MB	2.43 MB	Unknown	

Note: You can right click on a volume and delete it to create free space.

NOTE

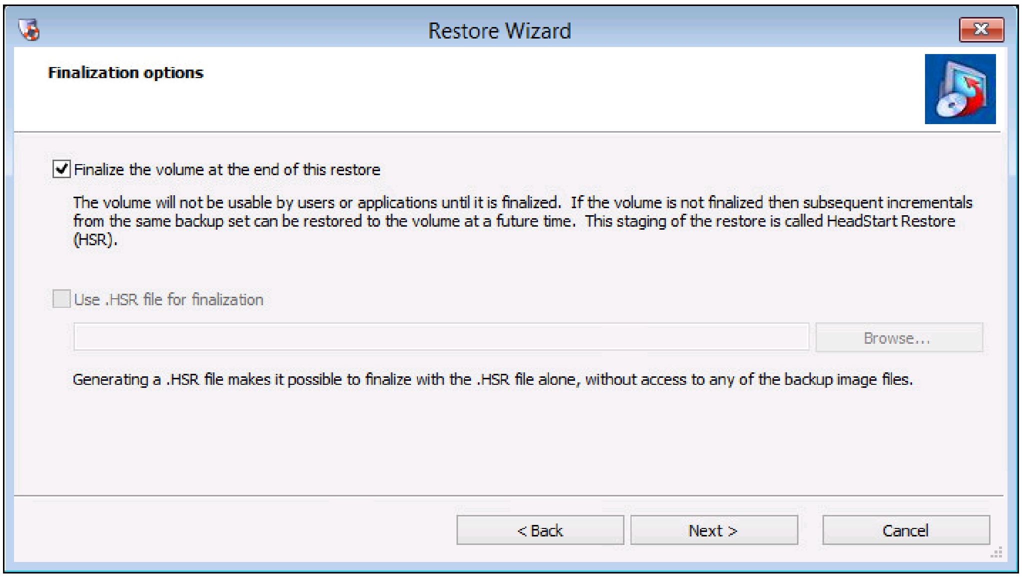
Please kindly note that the backup image files selected for restore cannot be contained in the system volume as the backup image files selected for restore cannot be contained in the volume selected for restore, otherwise there will be error prompted.



ShadowProtect.exe

Image file is contained in the volume selected for restore

10. Specify the finalization options.



Restore Wizard

Finalization options

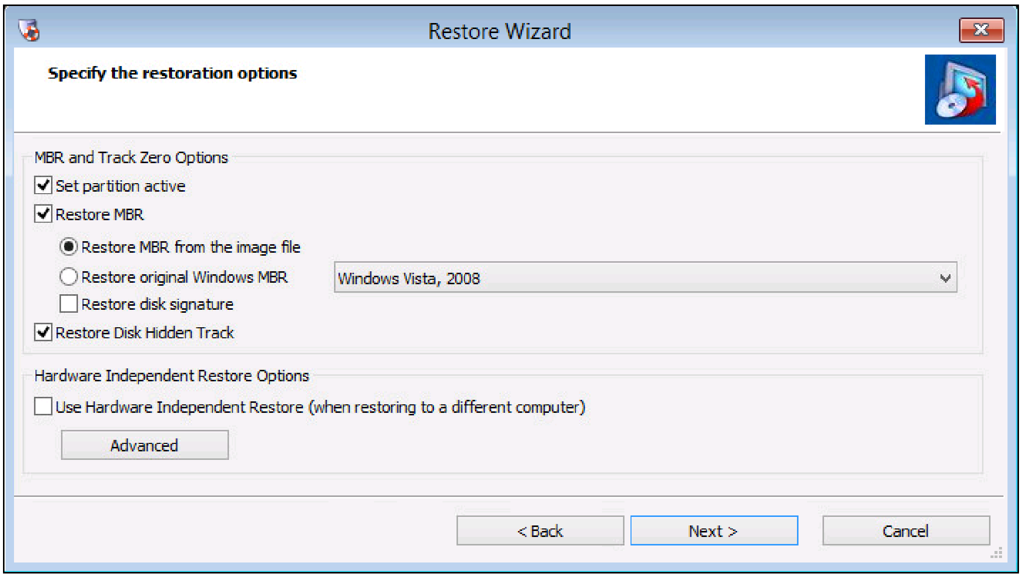
☑ Finalize the volume at the end of this restore

The volume will not be usable by users or applications until it is finalized. If the volume is not finalized then subsequent incrementals from the same backup set can be restored to the volume at a future time. This staging of the restore is called HeadStart Restore (HSR).

☐ Use .HSR file for finalization

Generating a .HSR file makes it possible to finalize with the .HSR file alone, without access to any of the backup image files.

11. Specify the restoration options.



Restore Wizard

Specify the restoration options

MBR and Track Zero Options

☑ Set partition active

☑ Restore MBR

● Restore MBR from the image file

○ Restore original Windows MBR — Windows Vista, 2008

□ Restore disk signature

☑ Restore Disk Hidden Track

Hardware Independent Restore Options

□ Use Hardware Independent Restore (when restoring to a different computer)

i. Set Partition Active - This will make the restored drive the active partition (the drive that the machine boots from).

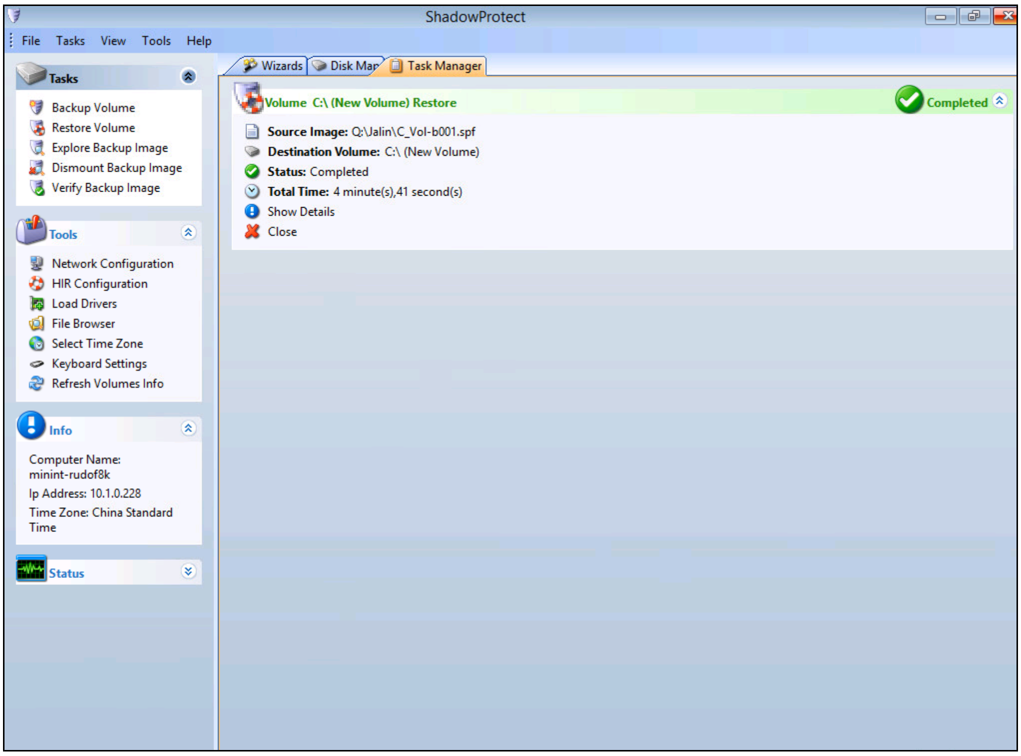
ii. Restore MBR - Restore the master boot record.
The master boot record is contained in the first sector of the first physical hard drive; it consists of a master boot program and a partition table that describes the disk partitions.
The master boot program looks at the partition table to see which primary partition is active. It then starts the boot program from the boot sector of the active partition.
You can restore the MBR from the image file that was saved with the backup image or you can restore an original Windows MBR.

iii. Restore disk signature - Restores the original physical disk signature of the hard drive.
Disk signatures are included in Windows Server 2003, and are necessary before the hard drive can be used.

iv. Restore Disk Hidden Track - Restore the first 63 sectors of a drive, some boot loaded applications required this for the system to boot.

Click **Next** to start the restore process.

12. The following screen with the status: **Completed** shows when the restoration is completed.

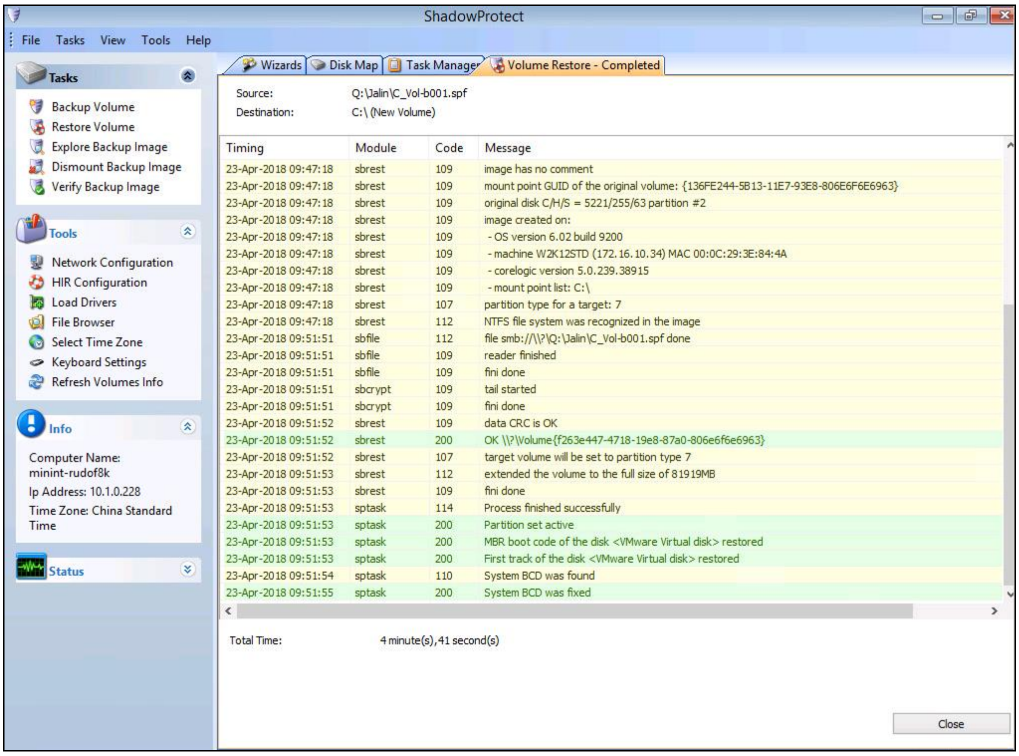


Computer Name: minint-rudof8k
Ip Address: 10.1.0.228
Time Zone: China Standard Time

Volume C:\ (New Volume) Restore — Completed

Source Image: Q:\Jalin\C_Vol-b001.spf
Destination Volume: C:\ (New Volume)
Status: Completed
Total Time: 4 minute(s),41 second(s)
Show Details
Close

13. Click **Show details** to check the restore details.



Computer Name: minint-rudof8k
Ip Address: 10.1.0.228
Time Zone: China Standard Time

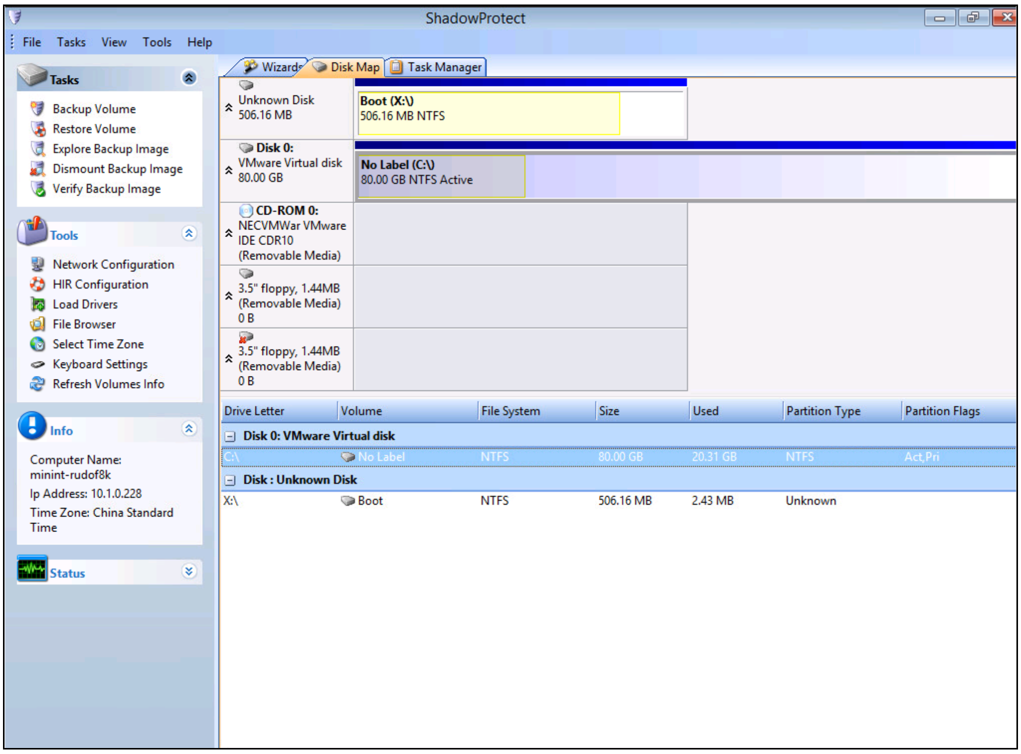
Source: Q:\Jalin\C_Vol-b001.spf
Destination: C:\ (New Volume)

Timing	Module	Code	Message
23-Apr-2018 09:47:18	sbrest	109	image has no comment
23-Apr-2018 09:47:18	sbrest	109	mount point GUID of the original volume: {136FE244-5B13-11E7-93E8-806E6F6E6963}
23-Apr-2018 09:47:18	sbrest	109	original disk C/H/S = 5221/255/63 partition #2
23-Apr-2018 09:47:18	sbrest	109	image created on:
23-Apr-2018 09:47:18	sbrest	109	- OS version 6.02 build 9200
23-Apr-2018 09:47:18	sbrest	109	- machine W2K12STD (172.16.10.34) MAC 00:0C:29:3E:84:4A
23-Apr-2018 09:47:18	sbrest	109	- corelogic version 5.0.239.38915
23-Apr-2018 09:47:18	sbrest	109	- mount point list: C:\
23-Apr-2018 09:47:18	sbrest	107	partition type for a target: 7
23-Apr-2018 09:47:18	sbrest	112	NTFS file system was recognized in the image
23-Apr-2018 09:51:51	sbfile	112	file smb://\\?\Q:\Jalin\C_Vol-b001.spf done
23-Apr-2018 09:51:51	sbfile	109	reader finished
23-Apr-2018 09:51:51	sbfile	109	fini done
23-Apr-2018 09:51:51	sbcrypt	109	tail started
23-Apr-2018 09:51:51	sbcrypt	109	fini done
23-Apr-2018 09:51:52	sbrest	109	data CRC is OK
23-Apr-2018 09:51:52	sbrest	200	OK \\?\Volume{f263e447-4718-19e8-87a0-806e6f6e6963}
23-Apr-2018 09:51:52	sbrest	107	target volume will be set to partition type 7
23-Apr-2018 09:51:53	sbrest	112	extended the volume to the full size of 81919MB
23-Apr-2018 09:51:53	sbrest	109	fini done
23-Apr-2018 09:51:53	sptask	114	Process finished successfully
23-Apr-2018 09:51:53	sptask	200	Partition set active
23-Apr-2018 09:51:53	sptask	200	MBR boot code of the disk <VMware Virtual disk> restored
23-Apr-2018 09:51:53	sptask	200	First track of the disk <VMware Virtual disk> restored
23-Apr-2018 09:51:54	sptask	110	System BCD was found
23-Apr-2018 09:51:55	sptask	200	System BCD was fixed

Total Time: 4 minute(s),41 second(s)

Or click **Close** to finish the restore process.

14. Go back to **Disk Map** to check current disk situation. You will find C drive has been restored.



Computer Name:
minint-rudof8k
Ip Address: 10.1.0.228
Time Zone: China Standard Time

Drive Letter	Volume	File System	Size	Used	Partition Type	Partition Flags
Disk 0: VMware Virtual disk						
C:\	No Label	NTFS	80.00 GB	20.31 GB	NTFS	Act,Pri
Disk : Unknown Disk						
X:\	Boot	NTFS	506.16 MB	2.43 MB	Unknown	

15. Reboot the computer and open Computer to check the system volume. Ensure the data has been restored successfully.

6 Contact Ahsay

6.1 Technical Assistance

To contact Ahsay support representatives for technical assistance, visit the following website:

https://www.ahsay.com/jsp/en/contact/kbQuestion.jsp

Also use the Ahsay Knowledge Base for resource such as Hardware Compatibility List, Software Compatibility List, and other product information:

https://wiki.ahsay.com

6.2 Documentation

Documentations for all Ahsay products are available at:

https://www.ahsay.com/jsp/en/home/index.jsp?pageContentKey=ahsay_downloads_documentation_guides

You can send us suggestions for improvements or report on issues in the documentation, by contacting us at:

https://www.ahsay.com/jsp/en/contact/kbQuestion.jsp

Please specify the specific document title as well as the change required/suggestion when contacting us.