Exos® Protect 4006 Series VSS Hardware Provider Installation Guide

Abstract

This guide provides installation and usage instructions for the VSS Hardware Provider that works with Microsoft Windows Server and Seagate storage systems.

Part Number: 83-00007894-10-01
Revision: C
Published: March 2026

© 2026 Seagate Technology LLC or its affiliates. All rights reserved. Seagate, Seagate Technology, and the Spiral logo are registered trademarks of Seagate Technology LLC in the United States and/or other countries. Exos is either a trademark or registered trademark of Seagate Technology LLC or one of its affiliated companies in the United States and/or other countries. All other trademarks or registered trademarks are the property of their respective owners. When referring to drive capacity, one gigabyte (GB) equals one billion bytes, one terabyte (TB) equals one trillion bytes, and one petabyte (PB) equals one thousand terabytes. Your computer's operating system may use a different standard of measurement and report a lower capacity. In addition, some of the listed capacity is used for formatting and other functions, and thus will not be available for data storage. Actual data rates may vary depending on operating environment and other factors, such as chosen interface and drive capacity. The export or re-export of Seagate hardware or software is regulated by the U.S. Department of Commerce, Bureau of Industry and Security (for more information, visit www.bis.doc.gov), and may be controlled for export, import and use in other countries. All coded instruction and program statements contained herein remain copyrighted works and confidential proprietary and trade secret information of Seagate Technology LLC or its affiliates. Any use, derivation, disassembly, reverse engineering, dissemination, reproduction, or any attempt to modify, prepare derivative works, reproduce, distribute, disclose copyrighted material of Seagate Technology LLC, for any reason, in any manner, medium, or form, in whole or in part, if not expressly authorized, is strictly prohibited. Seagate reserves the right to change, without notice, product offerings or specifications.

For the latest regulatory and compliance information see www.seagate.com/support. Scroll down to the Compliance section.

Contents

1 The VSS Hardware Provider and the CAPI Proxy 4
Installation requirements 4
About VSS 4
Supported VSS features 5

2 Installing and using the VSS Hardware Provider 6
Creating shadow copies 6
LUN 0 mapping 7
64-bit VSS clients 7
Ensuring read-write access of VSS shadow copies 7
Restoring read-write access 7
Troubleshooting 8
Uninstalling the VSS Hardware Provider 9

1 The VSS Hardware Provider and the CAPI Proxy

This document describes the VSS Hardware Provider that is supported in Microsoft Windows Server environments with the following FC, iSCSI, and SAS storage systems:

- Seagate 5005/4005/3005 Series products
- Exos Protect 4006 Series products

The VSS Hardware Provider installation file includes the VSS Hardware Provider and a CAPI Proxy. The previous versions of VSS Hardware Provider required a separate installation of the CAPI Proxy. However, in the latest version, both are provided in a single installation file.

IMPORTANT In environments with Seagate 5005/4005/3005 Series systems using FC and iSCSI host interface ports in combination, do not connect both iSCSI and FC ports from the same controller to the same host.

IMPORTANT The VSS Hardware Provider can be used with virtual disk groups but not linear disk groups. Linear disk groups do not support snapshots.

Installation requirements

Each of the software components described in this document can be downloaded from the support website www.seagate.com/support/products.

All VSS/CAPI packages are typically included in a single archive file, such as `seagate-vss-4.1.0.x.zip`.

The VSS Hardware Provider requires Microsoft Windows Server 2019 or 2022.

About VSS

Microsoft Windows Server operating systems provide enhanced services for managing storage area networks, including Volume Shadow Copy Service (VSS). VSS, with its standard set of extensible APIs, provides the backup infrastructure for Windows Server, as well as a mechanism for creating consistent point-in-time copies of data known as shadow copies. VSS provides interfaces to ensure that volume shadow copies are in a consistent state.

The VSS Hardware Provider installs on a server running Windows Server and enables VSS to create hardware-resident shadow copies on any storage system attached to the server. With the VSS Hardware Provider, you can create a shadow copy of the source data volume on one server and then import the shadow copy onto another server, or back to the same server. Before creating the shadow copy, determine whether it will be imported back to the same host, because a snapshot created with the transportable option should not be imported back to the original host.

The VSS Hardware Provider does not include user interfaces or standalone functionality. Instead it enables other applications to manage Seagate storage products. `vshadow.exe` and `diskshadow.exe` are useful command-line tools for creating, deleting, querying, and managing shadow copies in a Microsoft Windows environment. Diskshadow is included in Windows Server, while VShadow is available from Microsoft as part of the Windows SDK.

Supported VSS features

The VSS Hardware Provider supports the following features provided by the Windows VSS subsystem:

- Creating shadow copies/snapshots. For more information, see "Creating shadow copies" on page 6.

  NOTE Before you can create shadow copies, a license key must be installed in the storage system to enable snapshot functionality for virtual volumes. Then you must enable shadow copies for a volume by using your configuration management tool. For more information, see "Creating shadow copies" on page 6.

- Exporting shadow copies/snapshots: prepare for use in another Windows Server system.
- Importing snapshots: prepare for local use after export from another Windows Server system.
- Determining when snapshots can be deleted and deleting them.
- Reverting snapshots using the `diskshadow resync` command or `vshadow -resync` option.

2 Installing and using the VSS Hardware Provider

This section describes how to install the VSS Hardware Provider.

NOTE In a cluster environment the VSS Hardware Provider cannot be installed unless a Microsoft Distributed Transaction Coordinator (MS DTC) cluster resource is configured. If the host part of a cluster and MS DTC is not running, installation will fail. Use http://support.microsoft.com/kb/301600 for instructions on configuring MS DTC.

1. Double-click the downloaded hardware provider file to launch the installation.
2. Select **Install**.
3. Follow the onscreen prompts to install the software.

   The provider is installed in the following directory:

   `C:\Program Files\Seagate\Exos X VSS Provider`

   If a previous version 3.x or 4.x of the VSS Hardware Provider is already installed, a message tells you that the software is installed and asks for confirmation before replacing it with the current version.
4. To verify the installation, run the `list providers` command, and make sure that the VSS Hardware Provider is displayed in the list of providers.

```
C:\> vssadmin list providers
vssadmin x.x - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-20xx Microsoft Corp.

Provider name: 'Microsoft File Share Shadow Copy provider'
   Provider type: Fileshare
   Provider Id: {89300202-3cec-4981-9171-19f59559e0f2}
   Version: 1.0.0.1

Provider name: 'Seagate Exos Protect VSS Hardware Provider'
   Provider type: Hardware
   Provider Id: {9d09666c-5cf8-45ca-9294-127c95562094}
   Version: 4.2.x.x

Provider name: 'Microsoft Software Shadow Copy provider 1.0'
   Provider type: System
   Provider Id: {b5946137-7b9f-4925-af80-51abd60b20d5}
   Version: 1.0.0.7
```

Creating shadow copies

To create a shadow copy of a volume in a virtual pool, create the shadow copy using a VSS requester such as Diskshadow (included in Windows Server or VShadow (available as a download from microsoft.com as part of the Windows SDK).

NOTE After the VSS Hardware Provider is installed, your backup software may take advantage of it to create temporary hardware snapshots on the system when your backups are run.

NOTE The VSS Hardware Provider takes shadow copies quickly (less than 5 seconds), but the Microsoft VSS subsystem can take longer time to recognize and import the new shadow copies. It may take up to 90 seconds to create and import a shadow copy. It takes longer if multiple RAID partitions are included in the same shadow copy set.

LUN 0 mapping

For best performance, avoid mapping any storage system volumes to the host using LUN 0, which is used by the VSS Hardware Provider to monitor and manage the system. The VSS Hardware Provider automatically assigns LUN numbers starting at LUN 1, but if you have manually mapped LUNs to the host using LUN 0, the VSS Hardware Provider has to compete with disk I/O traffic, and this may cause commands to run more slowly or time out.

64-bit VSS clients

When creating snapshots on a 64-bit OS, you must use a 64-bit VSS client application. Microsoft's VSS framework does not support 32-bit requestors on 64-bit operating systems.

Ensuring read-write access of VSS shadow copies

When VSS creates a shadow copy, it maps the LUN with the shadow copy data back to the host. Because this is generally used for backup, the storage system LUN is mapped read-write and the Windows volumes that reside on LUN are read-only. You can restore read-write access of the volumes on the server, as shown below.

NOTE Multiple terms for the same or similar storage elements can include disks, volumes, snapshots and LUNs, depending on whether the storage element is being referenced by an operating system, a storage device, or an application.

The read-only or read-write attribute may also be influenced by the SAN policy of Windows Server systems. The SAN policy in place on the server affects the access level for newly discovered disks, but volumes on the disks for VSS shadow copy snapshots are always initially discovered as read-only, regardless of the SAN policy or version of Windows operating system.

Restoring read-write access

On the server, clear the read-only status of the imported snapshots' disks and volumes using the commands below. Select the disk that corresponds to the LUN with the snapshot data. After selecting the disk and clearing the disk's read-only status, select the volume and clear the volume's read-only status.

Relative to the tables below, invoke the Microsoft DiskPart utility by typing `diskpart` at the command line. Once invoked, `DISKPART>` appears as a prompt for entering the commands listed in the tables below. Type `exit` to quit the Microsoft DiskPart utility.

Table 1 DiskPart utility: disk commands

Command/sequence		Description
1	`list disk`	Allows you to determine which disk number to use in the following command.

Table 1 DiskPart utility: disk commands (continued)

2	`select disk x`	Selects a disk where `x` refers to the disk number from the `list disk` command.
3	`detail disk`	Use the command to verify the disk is in an offline and/or read-only state.
4	`online disk`	Brings the selected disk online.
5	`attributes disk clear readonly`	Clears the `readonly` attribute, allowing this host to write to the disk.
6	`list volume`	Allows you to get a list of volumes residing on disk, if any. The volume number displayed will be used in the `select volume` command.

The commands in the following table are repeated for each volume on the LUN; typically, there will be only one volume—or none—for a newly-provisioned LUN.

Table 2 DiskPart utility: volume on LUN commands

Command/sequence		Description
1	`select volume y`	Selects a volume, where `y` refers to the volume shown in the `list volume` command.
2	`detail volume`	Use the command to verify the volume is read-only.
3	`attributes volume clear readonly`	Clears the `readonly` attribute for the volume.

Troubleshooting

This section contains troubleshooting information for the VSS Hardware Provider.

Table 3 Troubleshooting the VSS Hardware Provider

Problem	Recommended actions
The VSS Hardware Provider cannot create a snapshot. The following error is reported: `VSS_E_PROVIDER_VETO`	• The maximum number of snapshots allowed by the snapshot license has already been created.

	• The storage system has failed to execute the commands from the VSS Hardware Provider, or the communication between the VSS Hardware Provider and the system is broken, due to any of the following conditions:
	  • The serial number cannot be obtained for the controller owning the master volume partition.
	  • The snapshot cannot be found in the VSS Hardware Provider's snapshot list.
	  • The partition is not a snapshot.
	  • The LUN assignment to the newly created snapshot failed.
	  • The snapshot that will be deleted is not a Seagate snapshot.
	  • A firmware upgrade operation may temporarily prevent VSS from managing the system.

The shadow copy does not exist on the controller.	• The backup utility automatically deletes the shadow copy when the backup is complete
	• You might have used the Windows Explorer shadow copy shell extension context menu to create a shadow copy, which is to be used for creating a Windows software shadow copy, not hardware shadow copies.
	• Make sure you have created the shadow copy using the persistent (`-p`) attribute.
	• If you use the `Vssadmin` tool from Microsoft to create shadow copies, it is not designed to work with the VSS Hardware Provider. Vssadmin create shadow only works with the Microsoft software shadow copy provider built into Windows.

Table 3 Troubleshooting the VSS Hardware Provider (continued)

Problem	Recommended actions
An error in the Windows application event log states: `ssproxy requires that the HBA can handle 256-Kbyte transfers. You might need to set the MaximumSGList to a value of 65 or higher if using a SCSIPort driver.`	See the alternative descriptions for assigning the `large_io setting`. See "Changing iSCSI driver configuration parameters for VSS support".
	The CAPI Proxy requires the maximum data for the CAPI command to be 256 Kbyte. This does not apply to Storport HBA drivers. • For SCSIport HBA drivers, create a `MaximumSGList` registry entry if it does not already exist and set it to a value of 65 or higher, if it has not already been set. For more information, see: msdn.microsoft.com/en-us/library/windows/hardware/ff563970(v=vs.85).aspx **NOTE** The SCSIport host-bus adapter driver was removed in Windows Server 2012. Instead, use either a Storport driver or a different host-bus adapter.
	• To set the registry for QLogic cards using the SCSIport driver, double-click `qla2300.reg` in the following directory: `C:\Program Files\Seagate\Seagate VSS Provider\qla2300.reg`
It is taking a long time to create the shadow copy.	The VSS Hardware Provider takes shadow copies quickly (less than 5 seconds), but the Microsoft VSS subsystem can take a long time to recognize and import the new shadow copies. It may take up to 90 seconds to create and import a shadow copy. It takes longer if more RAID partitions are included in the same shadow copy set.
Not Implemented or 0x80004001 error when `revert` command used in `VShadow` or `Diskshadow`.	The `revert` option is meant for host-based snapshots and is not supported for storage system-based snapshots. Use the `resync` command instead.
`VSS_E_MISSING_DISK` error when using the `RESYNC` command	This error can occur if the target volume is in use when the `RESYNC` command is issued. The target volume may be left in an offline state; use Disk Management or `DISKPART` to bring the target volume back online. To minimize the likelihood of this error occurring, stop the VSS subsystem with the command `NET STOP VSS` prior to performing the `RESYNC` operation; the VSS subsystem will automatically restart when you launch a VSS client. If necessary, use `MOUNTVOL` to unmount the volume prior to issuing the `RESYNC` command to ensure that other applications are not accessing the volume.
`VSS_E_PROVIDER_VETO` error when using the `RESYNC` command	This error can occur if a previous operation in the system is still in progress and the `resync` operation cannot proceed. The target volume may be left in an offline state; use Disk Management or `DISKPART` to bring the target volume back online. Review the event log in the system and wait for any operation in progress to complete before retrying the operation.
A "0mb" volume may appear in the Disk Management applet after creating a hardware snapshot of a GPT-formatted volume.	The Disk Management Control Panel applet may display an unnamed volume with a capacity of 0mb after a snapshot is created on a GPT disk. These are associated with special metadata partitions that Windows creates as part of the snapshot process and may safely be ignored. If they are bothersome, they can be deleted using the `DISKPART` command, by looking for a 256KB partition with an "Unknown" partition type. Volumes formatted with a traditional MBR partition table are not affected.

Uninstalling the VSS Hardware Provider

To uninstall the VSS Hardware Provider, perform the following steps.

1. Select **Start > Control Panel > Programs and Features**.
2. Select **Exos X VSS Provider** and select **Uninstall**.
3. Respond appropriately to the prompts.