GRIDINSOFT
HELP CENTER

OFFICIAL SUPPORT GUIDE

S

Windows Shadow Copy: VSS, Recovery, and Disk Space

A Windows shadow copy is a point-in-time volume snapshot created through VSS. Learn how snapshots support backups and Previous Versions, why they consume disk space, and how to inspect or resize storage safely.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 How VSS creates a snapshot

02 Shadow Copy, System Restore, Previous Versions, and backup

03 Why shadow copies use disk space

04 How to inspect shadow-copy storage

05 How to reclaim space safely

06 Security and recovery guidance

07 Frequently asked questions

A **shadow copy** is a point-in-time snapshot of a Windows volume. The **Volume Shadow Copy Service (VSS)** coordinates applications, backup software, storage providers, and the operating system so a snapshot can be created while files remain in use. Backup

products, System Restore, and the Previous Versions feature may use VSS, but they are not all the same thing.

Microsoft describes a shadow copy as a view of a volume at one well-defined instant. It is useful because normal applications can continue writing to the live volume while backup or recovery software reads the snapshot.

01 How VSS creates a snapshot

1. A VSS requester, such as backup software, asks for a snapshot.
2. VSS tells participating writers to prepare application data and briefly freeze writes.
3. A storage provider creates the snapshot, usually using copy-on-write or another space-efficient method rather than duplicating every byte immediately.
4. Applications resume normal writes, while the snapshot preserves the older state needed for recovery or backup.

Without application-aware writers, a snapshot may be only **crash-consistent**: comparable to the disk state after an unexpected shutdown. Open files exist, but an application transaction may not be complete. A successful snapshot is therefore not proof that every database can be restored correctly.

02 Shadow Copy, System Restore, Previous Versions, and backup

Feature	Purpose	Key limitation
VSS shadow copy	Point-in-time volume view used by other tools	Availability and consistency depend on configuration and requester
System Restore	Rolls back selected system files, registry, drivers, and settings	It is not a complete personal-file backup

Feature	Purpose	Key limitation
Previous Versions	Exposes recoverable earlier file or folder versions	The tab may be empty if no usable snapshot or backup exists
Independent backup	Stores recoverable data on separate, protected media or service	Must be configured, monitored, and tested

A shadow copy on the same disk is not an independent backup. Disk failure, storage cleanup, administrative deletion, or ransomware can remove both the live data and its snapshots.

03 Why shadow copies use disk space

Windows reserves a shadow-storage area, sometimes called the diff area, to preserve changed blocks. Usage grows as the live volume changes and as more snapshots are retained. When the configured area fills, Windows can delete older copies first. Large updates, databases, frequently changing virtual disks, or an undersized allocation can make copies disappear sooner than expected.

04 How to inspect shadow-copy storage

Open Command Prompt or Windows Terminal as an administrator and use:

- `vssadmin list shadows` to list system-provider shadow copies.
- `vssadmin list shadowstorage` to show used, allocated, and maximum storage associations.
- `vssadmin list writers` to review registered writer states when backups fail.

These commands do not necessarily show every snapshot made by every hardware or software provider. Check the backup product’s console and documentation as well.

05 How to reclaim space safely

1. Confirm that shadow storage, rather than temporary files or another workload, is consuming the space.
2. Verify that recent independent backups are successful and restorable.
3. Identify which feature or backup product created and depends on the snapshots.
4. Use the product's retention controls where possible. On supported systems, an administrator can use `vssadmin resize shadowstorage` to set a suitable maximum.
5. Recheck backup jobs and create a test restore after any change.

Warning: Microsoft notes that resizing shadow storage may cause shadow copies to disappear. Avoid copying an unverified "delete all shadows" command from the internet. Deleting snapshots is irreversible and can remove a useful recovery option.

06 Security and recovery guidance

Monitor failed VSS writers, unexplained snapshot deletion, and commands that alter shadow storage. During a malware incident, isolate the system and preserve evidence before restoration. Clean or rebuild the affected system first; otherwise restored files may be encrypted or damaged again. Keep offline, immutable, or separately administered backups and test them regularly. For accidental deletion, minimize new writes and follow a broader data-loss recovery plan.

07 Frequently asked questions

Can I delete shadow copies?

An administrator can, but should first understand which restore points and backup jobs depend on them. Deletion cannot be undone.

Why are my Previous Versions missing?

No usable copy may exist, retention storage may have filled, System Protection or a schedule may be disabled, or the backup product may store versions elsewhere.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com