



# **Securely purge data on an encrypted volume**

**ONTAP 9**

NetApp

February 12, 2026

# Table of Contents

Securely purge data on an encrypted volume . . . . .	1
Learn about securely purging data from an encrypted ONTAP volume . . . . .	1
Considerations for using secure purge . . . . .	1
Scrub data from an encrypted ONTAP volume without a SnapMirror relationship . . . . .	2
Scrub data from an encrypted ONTAP volume with an SnapMirror asynchronous relationship . . . . .	3
Scrub data from an encrypted ONTAP volume with a SnapMirror synchronous relationship . . . . .	5

# Securely purge data on an encrypted volume

## Learn about securely purging data from an encrypted ONTAP volume

Beginning with ONTAP 9.4, you can use secure purge to non-disruptively scrub data on NVE-enabled volumes. Scrubbing data on an encrypted volume ensures that it cannot be recovered from the physical media, for example, in cases of “spillage,” where data traces may have been left behind when blocks were overwritten, or for securely deleting a vacating tenant’s data.

Secure purge works only for previously deleted files on NVE-enabled volumes. You cannot scrub an unencrypted volume. You must use KMIP servers to serve keys, not the onboard key manager.

### Considerations for using secure purge

- Volumes created in an aggregate enabled for NetApp Aggregate Encryption (NAE) do not support secure purge.
- Secure purge works only for previously deleted files on NVE-enabled volumes.
- You cannot scrub an unencrypted volume.
- You must use KMIP servers to serve keys, not the onboard key manager.

Secure purge functions differently depending upon your version of ONTAP.

## ONTAP 9.8 and later

- Secure purge is supported by MetroCluster and FlexGroup.
- If the volume being purged is the source of a SnapMirror relationship, you do not have to break the SnapMirror relationship to perform a secure purge.
- The re-encryption method is different for volumes using SnapMirror data protection versus volumes not using SnapMirror data protection (DP) or those using SnapMirror extended data protection..
  - By default, volumes using SnapMirror data protection (DP) mode re-encrypt data using the volume move re-encryption method.
  - By default, volumes not using SnapMirror data protection or volumes using SnapMirror extended data protection (XDP) mode use the in-place re-encryption method.
  - These defaults can be changed using the `secure purge re-encryption-method [volume-move|in-place-rekey]` command.
- By default, all snapshots in FlexVol volumes are automatically deleted during the secure purge operation. By default, Snapshots in FlexGroup volumes and volumes using SnapMirror data protection are not automatically deleted during the secure purge operation. These defaults can be changed using the `secure purge delete-all-snapshots [true|false]` command.

## ONTAP 9.7 and earlier:

- Secure purge does not support the following:
  - FlexClone
  - SnapVault
  - FabricPool
- If the volume being purged is the source of a SnapMirror relationship, you must break the SnapMirror relationship before you can purge the volume.

If there are busy snapshots in the volume, you must release the snapshots before you can purge the volume. For example, you may need to split a FlexClone volume from its parent.

- Successfully invoking the secure-purge feature triggers a volume move that re-encrypts the remaining, unpurged data with a new key.

The moved volume remains on the current aggregate. The old key is automatically destroyed, ensuring that purged data cannot be recovered from the storage media.

## Scrub data from an encrypted ONTAP volume without a SnapMirror relationship

Beginning with ONTAP 9.4, you can use secure-purge to non-disruptively “scrub” data on NVE-enabled volumes.

### About this task

Secure-purge may take from several minutes to many hours to complete, depending on the amount of data in the deleted files. You can use the `volume encryption secure-purge show` command to view the status of the operation. You can use the `volume encryption secure-purge abort` command to terminate the operation.



In order to do a secure purge on a SAN host, you must delete the entire LUN containing the files you want to purge, or you must be able to punch holes in the LUN for the blocks that belong to the files you want purge. If you cannot delete the LUN or your host operating system does not support punching holes in the LUN, you cannot perform a secure purge.

### Before you begin

- You must be a cluster administrator to perform this task.
- Advanced privileges are required for this task.

### Steps

1. Delete the files or the LUN you want to securely purge.
  - On a NAS client, delete the files you want to securely purge.
  - On a SAN host, delete the LUN you want to securely purge or punch holes in the LUN for the blocks that belong to the files you want to purge.
2. On the storage system, change to advanced privilege level:

```
set -privilege advanced
```

3. If the files you want to securely purge are in snapshots, delete the snapshots:

```
snapshot delete -vserver SVM_name -volume volume_name -snapshot
```

4. Securely purge the deleted files:

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name
```

The following command securely purges the deleted files on `vol1` on `SVMvs1`:

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume vol1
```

5. Verify the status of the secure-purge operation:

```
volume encryption secure-purge show
```

## Scrub data from an encrypted ONTAP volume with an SnapMirror asynchronous relationship

Beginning with ONTAP 9.8, you can use a secure purge to non-disruptively “scrub” data on NVE-enabled volumes with an SnapMirror asynchronous relationship.

### Before you begin

- You must be a cluster administrator to perform this task.
- Advanced privileges are required for this task.

### About this task

Secure-purge may take from several minutes to many hours to complete, depending on the amount of data in the deleted files. You can use the `volume encryption secure-purge show` command to view the status of the operation. You can use the `volume encryption secure-purge abort` command to terminate the operation.

 In order to do a secure purge on a SAN host, you must delete the entire LUN containing the files you want to purge, or you must be able to punch holes in the LUN for the blocks that belong to the files you want purge. If you cannot delete the LUN or your host operating system does not support punching holes in the LUN, you cannot perform a secure purge.

## Steps

1. On the storage system, switch to the advanced privilege level:

```
set -privilege advanced
```

2. Delete the files or the LUN you want to securely purge.

- On a NAS client, delete the files you want to securely purge.
- On a SAN host, delete the LUN you want to securely purge or punch holes in the LUN for the blocks that belong to the files you want purge.

3. Prepare the destination volume in the Asynchronous relationship to be securely purged:

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name  
-prepare true
```

Repeat this step on each volume in your SnapMirror asynchronous relationship.

4. If the files you want to securely purge are in snapshots, delete the snapshots:

```
snapshot delete -vserver SVM_name -volume volume_name -snapshot
```

5. If the files you want to securely purge are in the base snapshots, do the following:

- a. Create a snapshot on the destination volume in the SnapMirror asynchronous relationship:

```
volume snapshot create -snapshot snapshot_name -vserver SVM_name -volume  
volume_name
```

- b. Update SnapMirror to move the base snapshot forward:

```
snapmirror update -source-snapshot snapshot_name -destination-path  
destination_path
```

Repeat this step for each volume in the SnapMirror asynchronous relationship.

- c. Repeat steps (a) and (b) equal to the number of base snapshots plus one.

For example, if you have two base snapshots, you should repeat steps (a) and (b) three times.

- d. Verify that the base snapshot is present:

```
snapshot show -vserver SVM_name -volume volume_name
```

- e. Delete the base snapshot:

```
snapshot delete -vserver SVM_name -volume volume_name -snapshot snapshot
```

6. Securely purge the deleted files:

```
volume encryption secure-purge start -vserver svm_name -volume volume_name
```

Repeat this step on each volume in the SnapMirror asynchronous relationship.

The following command securely purges the deleted files on "vol1" on SVM "vs1":

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume vol1
```

7. Verify the status of the secure purge operation:

```
volume encryption secure-purge show
```

#### Related information

- [snapmirror update](#)

## Scrub data from an encrypted ONTAP volume with a SnapMirror synchronous relationship

Beginning with ONTAP 9.8, you can use a secure purge to non-disruptively "scrub" data on NVE-enabled volumes with a SnapMirror synchronous relationship.

#### About this task

A secure purge might take from several minutes to many hours to complete, depending on the amount of data in the deleted files. You can use the `volume encryption secure-purge show` command to view the status of the operation. You can use the `volume encryption secure-purge abort` command to terminate the operation.

 In order to do a secure purge on a SAN host, you must delete the entire LUN containing the files you want to purge, or you must be able to punch holes in the LUN for the blocks that belong to the files you want purge. If you cannot delete the LUN or your host operating system does not support punching holes in the LUN, you cannot perform a secure purge.

#### Before you begin

- You must be a cluster administrator to perform this task.
- Advanced privileges are required for this task.

#### Steps

1. On the storage system, change to advanced privilege level:

```
set -privilege advanced
```

2. Delete the files or the LUN you want to securely purge.

- On a NAS client, delete the files you want to securely purge.
- On a SAN host, delete the LUN you want to securely purge or punch holes in the LUN for the blocks that belong to the files you want purge.

3. Prepare the destination volume in the Asynchronous relationship to be securely purged:

```
volume encryption secure-purge start -vserver <SVM_name> -volume <volume_name>  
-prepare true
```

Repeat this step for the other volume in your SnapMirror synchronous relationship.

4. If the files you want to securely purge are in snapshots, delete the snapshots:

```
snapshot delete -vserver <SVM_name> -volume <volume_name> -snapshot <snapshot>
```

5. If the secure purge file is in the base or common snapshots, update the SnapMirror to move the common snapshot forward:

```
snapmirror update -source-snapshot <snapshot_name> -destination-path  
<destination_path>
```

There are two common snapshots, so this command must be issued twice.

6. If the secure purge file is in the application-consistent snapshot, delete the snapshot on both volumes in the SnapMirror synchronous relationship:

```
snapshot delete -vserver <SVM_name> -volume <volume_name> -snapshot <snapshot>
```

Perform this step on both volumes.

7. Securely purge the deleted files:

```
volume encryption secure-purge start -vserver <SVM_name> -volume <volume_name>
```

Repeat this step on each volume in the SnapMirror synchronous relationship.

The following command securely purges the deleted files on “vol1” on SVM “vs1”.

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume  
vol1
```

8. Verify the status of the secure purge operation:

```
volume encryption secure-purge show
```

#### Related information

- [snapmirror update](#)

## Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

**LIMITED RIGHTS LEGEND:** Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.