



# EnableEncryptionAtRest

Element Software

Michael Wallis, Dave Bagwell  
April 19, 2021

# Table of Contents

- EnableEncryptionAtRest ..... 1
  - Parameters ..... 1
  - Return values ..... 1
  - Request example ..... 1
  - Response examples ..... 2
  - New since version ..... 3

# EnableEncryptionAtRest

You can use the `EnableEncryptionAtRest` method to enable the Advanced Encryption Standard (AES) 256-bit encryption at rest on the cluster so that the cluster can manage the encryption key used for the drives on each node. This feature is not enabled by default.



This method does not enable software encryption at rest. This can only be done using the [create cluster method](#) with `enableSoftwareEncryptionAtRest` set to true.

When you enable Encryption at Rest, the cluster automatically manages encryption keys internally for the drives on each node in the cluster.

If a `keyProviderID` is specified, the password is generated and retrieved according to the type of key provider. This is usually done using a Key Management Interoperability Protocol (KMIP) key server in the case of a KMIP key provider. After this operation, the specified provider is considered active and cannot be deleted until Encryption at Rest is disabled using the `DisableEncryptionAtRest` method.



If you have a node type with a model number ending in "-NE", the `EnableEncryptionAtRest` method call will fail with a response of "Encryption not allowed. Cluster detected non-encryptable node".



You should only enable or disable encryption when the cluster is running and in a healthy state. You can enable or disable encryption at your discretion and as often as you need.



This process is asynchronous and returns a response before encryption is enabled. You can use the `GetClusterInfo` method to poll the system to see when the process has completed.

## Parameters

This method has the following input parameters:

| Name                       | Description                           | Type    | Default value | Required |
|----------------------------|---------------------------------------|---------|---------------|----------|
| <code>keyProviderID</code> | The ID of a KMIP key provider to use. | integer | None          | No       |

## Return values

This method has no return values.

## Request example

Requests for this method are similar to the following example:

```
{
  "method": "EnableEncryptionAtRest",
  "params": {},
  "id": 1
}
```

## Response examples

This method returns a response similar to the following example from the `EnableEncryptionAtRest` method. There is no result to report.

```
{
  "id": 1,
  "result": {}
}
```

While Encryption At Rest is being enabled on a cluster, `GetClusterInfo` returns a result describing the state of Encryption at Rest (`"encryptionAtRestState"`) as `"enabling"`. After Encryption at Rest is fully enabled, the returned state changes to `"enabled"`.

```
{
  "id": 1,
  "result": {
    "clusterInfo": {
      "attributes": { },
      "encryptionAtRestState": "enabling",
      "ensemble": [
        "10.10.5.94",
        "10.10.5.107",
        "10.10.5.108"
      ],
      "mvip": "192.168.138.209",
      "mvipNodeID": 1,
      "name": "Marshall",
      "repCount": 2,
      "svip": "10.10.7.209",
      "svipNodeID": 1,
      "uniqueID": "91dt"
    }
  }
}
```

## New since version

9.6

## Find more information

- [SecureEraseDrives](#)
- [GetClusterInfo](#)
- [NetApp SolidFire Resources Page](#)
- [Documentation for earlier versions of NetApp SolidFire and Element products](#)

## Copyright Information

Copyright © 2021 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## 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.