



# **Enable FIPS 140-2 for HTTPS on your cluster**

Element Software

NetApp  
April 17, 2024

This PDF was generated from [https://docs.netapp.com/us-en/element-software/storage/reference\\_system\\_manage\\_fips\\_ssl\\_cipher\\_changes.html](https://docs.netapp.com/us-en/element-software/storage/reference_system_manage_fips_ssl_cipher_changes.html) on April 17, 2024. Always check docs.netapp.com for the latest.

# Table of Contents

- Enable FIPS 140-2 for HTTPS on your cluster ..... 1
  - Find more information ..... 1
  - SSL ciphers ..... 1

# Enable FIPS 140-2 for HTTPS on your cluster

You can use the EnableFeature API method to enable the FIPS 140-2 operating mode for HTTPS communications.

With NetApp Element software, you can choose to enable Federal Information Processing Standards (FIPS) 140-2 operating mode on your cluster. Enabling this mode activates the NetApp Cryptographic Security Module (NCSM) and leverages FIPS 140-2 Level 1 certified encryption for all communication via HTTPS to the NetApp Element UI and API.



After you enable FIPS 140-2 mode, it cannot be disabled. When FIPS 140-2 mode is enabled, each node in the cluster reboots and runs through a self-test ensuring that the NCSM is correctly enabled and operating in the FIPS 140-2 certified mode. This causes an interruption to both management and storage connections on the cluster. You should plan carefully and only enable this mode if your environment needs the encryption mechanism it offers.

For more information, see the Element API information.

The following is an example of the API request to enable FIPS:

```
{
  "method": "EnableFeature",
  "params": {
    "feature" : "fips"
  },
  "id": 1
}
```

After this operating mode is enabled, all HTTPS communication uses the FIPS 140-2 approved ciphers.

## Find more information

- [SSL ciphers](#)
- [Manage storage with the Element API](#)
- [SolidFire and Element Software Documentation](#)
- [NetApp Element Plug-in for vCenter Server](#)

## SSL ciphers

SSL ciphers are encryption algorithms used by hosts to establish a secure communication. There are standard ciphers that Element software supports and non-standard ones when FIPS 140-2 mode is enabled.

The following lists provide the standard Secure Socket Layer (SSL) ciphers supported by Element software and the SSL ciphers supported when FIPS 140-2 mode is enabled:

- **FIPS 140-2 disabled**

TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (dh 2048) - A  
TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (dh 2048) - A  
TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256 (dh 2048) - A  
TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (dh 2048) - A  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (secp256r1) - A  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (secp256r1) - A  
TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 (secp256r1) - A  
TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (secp256r1) - A  
TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (rsa 2048) - C  
TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (rsa 2048) - A  
TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (rsa 2048) - A  
TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (rsa 2048) - A  
TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (rsa 2048) - A  
TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 (rsa 2048) - A  
TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (rsa 2048) - A  
TLS\_RSA\_WITH\_CAMELLIA\_128\_CBC\_SHA (rsa 2048) - A  
TLS\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA (rsa 2048) - A  
TLS\_RSA\_WITH\_IDEA\_CBC\_SHA (rsa 2048) - A  
TLS\_RSA\_WITH\_RC4\_128\_MD5 (rsa 2048) - C  
TLS\_RSA\_WITH\_RC4\_128\_SHA (rsa 2048) - C  
TLS\_RSA\_WITH\_SEED\_CBC\_SHA (rsa 2048) - A

- **FIPS 140-2 enabled**

TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (dh 2048) - A  
TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (dh 2048) - A  
TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256 (dh 2048) - A  
TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (dh 2048) - A  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (sect571r1) - A

TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (secp256r1) - A  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (secp256r1) - A  
TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (sect571r1) - A  
TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 (sect571r1) - A  
TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 (secp256r1) - A  
TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (secp256r1) - A  
TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (sect571r1) - A  
TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (rsa 2048) - C  
TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (rsa 2048) - A  
TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (rsa 2048) - A  
TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (rsa 2048) - A  
TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (rsa 2048) - A  
TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 (rsa 2048) - A  
TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (rsa 2048) - A

## Find more information

[Enable FIPS 140-2 for HTTPS on your cluster](#)

## Copyright information

Copyright © 2024 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.