security ssl commands

Command reference

NetApp
February 02, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap-cli/security-ssl-modify.html on February 02, 2026. Always check docs.netapp.com for the latest.

Table of Contents

security ssl commands . . . 1
- security ssl modify . . . 1
  - Description . . . 1
  - Parameters . . . 1
  - Examples . . . 2
  - Related Links . . . 3
- security ssl show . . . 3
  - Description . . . 3
  - Parameters . . . 3
  - Examples . . . 5
  - Related Links . . . 5

security ssl commands

security ssl modify

Modify the SSL configuration for HTTP servers

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command modifies the configuration of encrypted HTTP (SSL) for Vservers in the cluster. Depending on the requirements of the individual node's or cluster's web services (displayed by the vserver services web show command), this encryption might or might not be used. If the Vserver does not have a certificate associated with it, SSL will not be available.

Parameters

`-vserver <Vserver Name>` - Vserver

Identifies a Vserver for hosting SSL-encrypted web services.

`[-ca <text>]` - Server Certificate Issuing CA

Identifies a Certificate Authority (CA) of a certificate to be associated with the instance of a given Vserver. If this parameter, along with serial, is omitted during modification, a self-signed SSL certificate can be optionally generated for that Vserver.

`[-serial <text>]` - Server Certificate Serial Number

Identifies a serial number of a certificate to be associated with the instance of a given Vserver. If this parameter, along with ca, is omitted during modification, a self-signed SSL certificate can be optionally generated for that Vserver.

`[-common-name <FQDN or Custom Common Name>]` - Server Certificate Common Name

Identifies the common name (CN) of a certificate to be associated with the instance of a given Vserver. This parameter becomes optional if serial and ca are specified. You can use the security certificate create and security certificate install commands to add new certificates to Vservers.

The use of self-signed SSL certificates exposes users to man-in-the-middle security attacks. Where possible, obtain a certificate that is signed by a reputable certificate authority (CA) and use the security certificate install command to configure it before enabling SSL on a Vserver.

`[-server-enabled {true|false}]` - SSL Server Authentication Enabled

Defines the working condition of SSL server authentication in an instance of the Vserver. Any Vserver with a valid certificate of type server is server-enabled.

`[-client-enabled {true|false}]` - SSL Client Authentication Enabled

Defines the working condition of SSL client authentication in an instance of the Vserver. Any Vserver with a valid certificate of type client-ca is client-enabled. It can only be enabled if server-enabled is true.

[-ocsp-enabled {true|false}] - Online Certificate Status Protocol Validation Enabled

This parameter enables OCSP validation of the client certificate chain. When this parameter is enabled, certificates in the certificate chain of the client will be validated against an OCSP responder after normal verification (including CRL checks) has occurred. The OCSP responder used for validation process is either extracted from the certificate itself, or it is derived by configuration.

[-ocsp-default-responder <text>] - URI of the Default Responder for OCSP Validation

This parameter sets the default OCSP responder to use. If this parameter is not enabled, the URI given will be used only if no responder URI is specified in the certificate that are being verified.

[-ocsp-override-responder {true|false}] - Force the Use of the Default Responder URI for OCSP Validation

This parameter forces the configured default OCSP responder to be used during OCSP certificate validation, even if the certificate that is being validated references an OCSP responder.

[-ocsp-responder-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>] - Timeout for OCSP Queries

Use this parameter to specify the timeout in seconds for OSCP responders. Specify zero for the minimum possible timeout. The default value is 10 seconds.

[-ocsp-max-response-age <integer_or_unlimited>] - Maximum Allowable Age for OCSP Responses (secs)

This parameter sets the maximum allowable age (freshness) in seconds for the OCSP responses. The default value for this parameter is unlimited, which does not enforce a maximum age and the OCSP responses are considered valid as long as their expiration date field is in the future.

[-ocsp-max-response-time-skew <[<integer>d][<integer>h][<integer>m][<integer>s]>] - Maximum Allowable Time Skew for OCSP Response Validation

This parameter sets the maximum allowable time difference for OCSP responses (when validating their "ThisUpdate" and "NextUpdate" fields).

[-ocsp-use-request-nonce {true|false}] - Use a NONCE within OCSP Queries

This parameter determines whether the queries to the OCSP responders should contain a NONCE or not. By default, a query NONCE is always used and checked against the OCSP response. When the responder does not use NONCEs, this parameter should be disabled.

A NONCE is a unique identifier included in each OCSP request or OCSP response to prevent a replay attack.

Examples

The following example enables SSL server authentication for a Vserver named vs0 with a certificate that has ca as www.example.com and serial as 4F4EB629.

```
cluster1::> security ssl modify -vserver vs0 -ca www.example.com -serial
4F4EB629 -server-enabled true
```

The following example disables SSL server authentication for a Vserver name vs0.

```
cluster1::> security ssl modify -vserver vs0 -server-enabled false
```

The following example enables SSL client authentication for a Vserver named vs0.

```
cluster1::> security ssl modify -vserver vs0 -client-enabled true
```

The following example disables SSL client authentication for a Vserver named vs0.

```
cluster1::> security ssl modify -vserver vs0 -client-enabled false
```

Related Links

- vserver services web show
- security certificate create
- security certificate install

security ssl show

Display the SSL configuration for HTTP servers

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

This command displays the configuration of encrypted HTTP (SSL) for Vservers in the cluster. Depending on the requirements of the individual node's or cluster's web services (displayed by the vserver services web show command), this encryption might or might not be used. If the Vserver does not have a certificate associated with it, SSL will not be available.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-ocsp]

If you specify the `-ocsp` parameter, the command displays the Online Certificate Status Protocol configuration.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <Vserver Name>] - Vserver

Identifies a Vserver for hosting SSL-encrypted web services.

[-ca <text>] - Server Certificate Issuing CA

Filters the display of SSL configuration by specifying the Certificate Authority (CA) that issued the server certificate.

[-serial <text>] - Server Certificate Serial Number

Filters the display of SSL configuration by specifying the serial number of a server certificate.

[-common-name <FQDN or Custom Common Name>] - Server Certificate Common Name

Filters the display of SSL configuration by specifying the common name for the server certificate.

[-server-enabled {true|false}] - SSL Server Authentication Enabled

Filters the display of SSL configuration according to whether the SSL server authentication is enabled or disabled. Vservers have self-signed certificates automatically generated during their creation. These Vserver self-signed certificates are server-enabled by default.

[-client-enabled {true|false}] - SSL Client Authentication Enabled

Filters the display of SSL configuration according to whether the SSL client authentication is enabled or disabled. You can enable client authentication only when server authentication is enabled.

[-ocsp-enabled {true|false}] - Online Certificate Status Protocol Validation Enabled

Filters the display of SSL configuration when the Online Certificate Status Protocol validation is enabled.

[-ocsp-default-responder <text>] - URI of the Default Responder for OCSP Validation

Filters the display of SSL configuration according to the URI of the default responder for OCSP validation.

[-ocsp-override-responder {true|false}] - Force the Use of the Default Responder URI for OCSP Validation

Filters the display of SSL configuration, which forces the use of the default responder URI for OCSP validation.

[-ocsp-responder-timeout <[<integer>d][<integer>h][<integer>m][<integer>s]>] - Timeout for OCSP Queries

Filters the display of SSL configuration according to the timeout for queries to OCSP responders.

[-ocsp-max-response-age <integer_or_unlimited>] - Maximum Allowable Age for OCSP Responses (secs)

Filters the display of SSL configuration according to the maximum allowable age (freshness) in seconds for the OCSP responses.

[-ocsp-max-response-time-skew <[<integer>d][<integer>h][<integer>m][<integer>s]>] - Maximum Allowable Time Skew for OCSP Response Validation

Filters the display of SSL configuration according to the maximum allowable time difference for OCSP responses (when validating their "ThisUpdate" and "NextUpdate" fields).

[-ocsp-use-request-nonce {true|false}] - Use a NONCE within OCSP Queries

Filters the display of SSL configuration by specifying whether the queries to the OCSP responders should contain a NONCE or not.

A NONCE is a unique identifier included in each OCSP request or OCSP response to prevent a replay attack.

Examples

The following example displays the configured certificates for Vservers.

```
cluster1::security ssl> show
          Serial                                          Server  Client
Vserver   Number Common Name                               Enabled Enabled
--------- ------ ---------------------------------------- ------- -------
cluster1  516C3CB3
                 cluster1.company.com                     true    true
vs0       516816D4
                 vs0.company.com                          true    false
2 entries were displayed.
```

Related Links

- vserver services web show

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.