security webauthn commands

Command reference

NetApp
February 02, 2026

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

Table of Contents

security webauthn commands . . . 1
- security webauthn show . . . 1
  - Description . . . 1
  - Parameters . . . 1
  - Examples . . . 1
- security webauthn credentials delete . . . 2
  - Description . . . 2
  - Parameters . . . 2
  - Examples . . . 2
- security webauthn credentials show . . . 3
  - Description . . . 3
  - Parameters . . . 3
  - Examples . . . 4
- security webauthn supported-algorithms show . . . 5
  - Description . . . 5
  - Parameters . . . 5
  - Examples . . . 5

security webauthn commands

security webauthn show

Show Webauthn Global Settings

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

Description

The `security webauthn show` displays information on the global FIDO2/WebAuthn settings.

Parameters

{ [-fields <fieldname>,…]

Selects the fields that you specify.

| [-instance] }

Displays all the fields for the global WebAuthn settings.

[-vserver <vserver name>] - Vserver

Selects the WebAuthn settings that match this parameter value. If not specified, all cluster-level and Vserver-level settings are displayed.

[-timeout <integer>] - Timeout (ms)

Displays all the fields for the FIDO2/WebAuthn global settings.

[-attestation {none|indirect|direct|enterprise}] - Attestation Conveyance Type

Displays all the fields for the FIDO2/WebAuthn global settings.

[-require-rk {true|false}] - Require Resident Key

Displays all the fields for the FIDO2/WebAuthn global settings.

[-resident-key {required|preferred|discouraged}] - Resident Key

Displays all the fields for the FIDO2/WebAuthn global settings.

[-user-verification {required|preferred|discouraged}] - User Verification

Displays all the fields for the FIDO2/WebAuthn global settings.

[-scope {svm|cluster}] - Cluster or SVM

Displays all the fields for the FIDO2/WebAuthn global settings.

Examples

The example below displays information on FIDO2/WebAuthn global settings:

```
cluster1::> security webauthn show
Vserver: cluster1
               Timeout (ms): 600000
Attestation Conveyance Type: none
       Require Resident Key: false
               Resident Key: discouraged
          User Verification: discouraged
```

security webauthn credentials delete

Delete Webauthn Credentials Data

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

Description

The `security webauthn credentials delete` command deletes a previously registered FIDO2/WebAuthn credential. All users can delete their own registered FIDO2/WebAuthn credentials, regardless of their authorization role. Only users with *`admin`* privileges can delete FIDO2/WebAuthn credentials belonging to other users.

Parameters

`-vserver <vserver name>` - Vserver

This parameter optionally specifies the Vserver associated with the FIDO2/WebAuthn credential. If not specified, this defaults to the cluster Vserver.

`-username <text>` - Username

Name of the user whose credential is to be deleted.

`-index <integer>` - Index

The index of the FIDO2/WebAuthn credential to be deleted. This is used to identify the specific credential if the user has multiple FIDO2/WebAuthn credentials registered and only one of them is to be deleted.

`-rpId <text>` - Relying Party ID

The rpId of the FIDO2/WebAuthn credential to be deleted.

Examples

The following command, when executed by a user with admin privileges, deletes all registered FIDO2/WebAuthn credentials for the Administrative Vserver. When executed by users without admin privileges, the command only deletes that user's own registered credentials:

```
cluster1::> security webauthn credentials delete *
4 entries were deleted.
```

The following command, when executed by a user with admin privileges, deletes all registered FIDO2/WebAuthn credentials for the Administrative Vserver for the username *user1* :

```
cluster1::> security webauthn credentials delete -username user1 *
1 entry was deleted.
```

The following command, when executed by a user with admin privileges, deletes the registered FIDO2/WebAuthn credentials for the Administrative Vserver for the username *user1* at index *1* for the rpId *myontap.example.com* :

```
cluster1::> security webauthn credentials delete -username user1 -index 1
-rpId myontap.example.com
1 entry was deleted.
```

security webauthn credentials show

Show Webauthn Credentials Data

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

Description

The `security webauthn credentials show` displays information on the FIDO2/WebAuthn registered credentials.

Parameters

{ [-fields <fieldname>,…]

Selects the fields that you specify.

| [-instance] }

Displays all the fields for the FIDO2/WebAuthn registered credentials.

[-vserver <vserver name>] - Vserver

Selects the FIDO2/WebAuthn registered credentials that match this parameter value. Only cluster-level credentials are supported at this time.

[-username <text>] - Username

Selects the FIDO2/WebAuthn registered credentials that match this parameter value.

[-index <integer>] - Index

Selects the FIDO2/WebAuthn registered credentials that match this parameter value.

[-rpId <text>] - Relying Party ID

Selects the FIDO2/WebAuthn registered credentials that match this parameter value.

[-credential-id-sha <text>] - SHA-256 Hashed Credential ID

Selects the FIDO2/WebAuthn registered credentials that match this parameter value.

[-publickey-algorithm <text>] - Public Key Algorithm

Selects the FIDO2/WebAuthn registered credentials that match this parameter value.

[-publickey <text>] - Public Key

Selects the FIDO2/WebAuthn registered credentials that match this parameter value.

[-display-name <text>] - Display Name

Selects the FIDO2/WebAuthn registered credentials that match this parameter value.

[-credential-type <public-key>] - Credential Type

Selects the FIDO2/WebAuthn registered credentials that match this parameter value.

[-rpName <text>] - Relying Party Name

Selects the FIDO2/WebAuthn registered credentials that match this parameter value.

[-creation-time <MM/DD/YYYY HH:MM:SS>] - Creation Time

Selects the FIDO2/WebAuthn registered credentials that match this parameter value.

[-last-used <MM/DD/YYYY HH:MM:SS>] - Last Used

Selects the FIDO2/WebAuthn registered credentials that match this parameter value.

[-scope {svm|cluster}] - Cluster or SVM

Selects the FIDO2/WebAuthn registered credentials that match this parameter value.

Examples

The example below displays information on the FIDO2/WebAuthn registered credentials:

```
cluster1::> security webauthn credentials show
Vserver: cluster1
                             Username: admin
                                Index: 0
                    Relying Party ID: myontap.example.com
          SHA-256 Hashed Credential ID: aaaaaaaaaaaaaaaaaaaaaaaaaa
                  Public Key Algorithm: ES256
                            Public Key: abcd=
                          Display Name: admin
                       Credential Type: public-key
                    Relying Party Name: myontap.example.com
                         Creation Time: 6/10/2024 15:01:00
                             Last Used: 6/10/2024 15:01:00
```

security webauthn supported-algorithms show

Show WebAuthn Supported Algorithms

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

Description

The `security webauthn supported-algorithms show` displays information on the FIDO2/WebAuthn supported algorithms.

Parameters

{ [-fields <fieldname>,…]

Selects the fields that you specify.

| [-instance] }

Displays all the fields for the FIDO2/WebAuthn supported algorithms.

[-vserver <vserver name>] - Vserver

Selects the FIDO2/WebAuthn settings that match this parameter value. If not specified, all cluster-level and Vserver-level settings are displayed.

[-alg-name <text>] - Algorithm Name

Displays all the fields for the FIDO2/WebAuthn supported algorithms.

[-alg-id <integer>] - Algorithm ID

Displays all the fields for the FIDO2/WebAuthn supported algorithms.

[-alg-type <public-key>] - Algorithm Type

Displays all the fields for the FIDO2/WebAuthn supported algorithms.

[-scope {svm|cluster}] - Cluster or SVM

Displays all the fields for the FIDO2/WebAuthn supported algorithms.

Examples

The example below displays information on the FIDO2/WebAuthn supported algorithms:

```
cluster1::> security webauthn supported-algorithms show

Vserver: cluster1

ID         Name        Type
------     -------     -----
    -7     ES-256      public-key
   -35     ES-384      public-key
  -257     RS-256      public-key
3 entries were displayed.
```

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.