



Manage SSH security configuration

REST API reference

NetApp
September 12, 2025

Table of Contents

- Manage SSH security configuration 1
 - Security SSH svms svm.uuid endpoint overview 1
 - Overview 1
 - Examples 1
- Retrieve the SSH server configuration for an SVM 2
 - Related ONTAP commands 3
 - Parameters 3
 - Response 3
 - Error 4
 - Definitions 5
- Update the SSH server configuration for an SVM 7
 - Optional parameters 7
 - Related ONTAP commands 7
 - Parameters 7
 - Request Body 7
 - Response 8
 - Error 8
 - Definitions 9

Manage SSH security configuration

Security SSH svms svm.uuid endpoint overview

Overview

This endpoint is used to retrieve or modify the SSH security configuration to an SVM.

The SSH security algorithms include key exchange algorithms, ciphers for payload encryption, MAC algorithms, and the maximum authentication retry attempts allowed before closing the connection. `svm.uuid` corresponds to the UUID of the SVM for which the SSH security setting is being retrieved or modified and it is obtained from the response body of a GET operation performed on the `api/security/ssh/svms` API.

Examples

Updating the SSH security parameters

Specify the algorithms in the body of the PATCH request.

```
# The API:
PATCH "/api/security/ssh/svms/{svm.uuid}"

# The call:
curl -X PATCH "https://<mgmt-ip>/api/security/ssh/svms/02c9e252-41be-11e9-81d5-00a0986138f7" -d '{ "ciphers": [ "aes256_ctr", "aes192_ctr" ],
"key_exchange_algorithms": [ "diffie_hellman_group_exchange_sha256",
"ecdh_sha2_nistp256" ], "mac_algorithms": [ "hmac_sha2_512_etm",
"umac_128_etm" ], "max_authentication_retry_count": 3 }'
```

Retrieving the SSH security configuration of an SVM

```

# The API:
GET "/api/security/ssh/svms/{svm.uuid}"

# The call:
curl -X GET "https://<mgmt-ip>/api/security/ssh/svms/02c9e252-41be-11e9-81d5-00a0986138f7"

# The response:
{
  "ciphers": [
    "aes256_ctr",
    "aes192_ctr"
  ],
  "key_exchange_algorithms": [
    "diffie_hellman_group_exchange_sha256",
    "ecdh_sha2_nistp256"
  ],
  "mac_algorithms": [
    "hmac_sha2_512_etm",
    "umac_128_etm"
  ],
  "max_authentication_retry_count": 3,
  "svm": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7",
    "_links": {
      "self": {
        "href": "/api/svm/svms/02c9e252-41be-11e9-81d5-00a0986138f7"
      }
    }
  },
  "_links": {
    "self": {
      "href": "/api/security/ssh/svms/02c9e252-41be-11e9-81d5-00a0986138f7"
    }
  }
}

```

Retrieve the SSH server configuration for an SVM

GET /security/ssh/svms/{svm.uuid}

Introduced In: 9.10

Retrieves the SSH server configuration for the specified SVM.

Related ONTAP commands

- `security ssh`

Parameters

| Name | Type | In | Required | Description |
|----------|---------------|-------|----------|-------------------------------|
| svm.uuid | string | path | True | SVM UUID |
| fields | array[string] | query | False | Specify the fields to return. |

Response

Status: 200, Ok

| Name | Type | Description |
|--------------------------------|------------------------|---|
| _links | _links | |
| ciphers | array[string] | Ciphers for encrypting the data. |
| key_exchange_algorithms | array[string] | Key exchange algorithms. |
| mac_algorithms | array[string] | MAC algorithms. |
| max_authentication_retry_count | integer | Maximum authentication retries allowed before closing the connection. |
| svm | svm | SVM name and UUID for which the SSH server is configured. |

Example response

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "ciphers": [
    "aes256_ctr",
    "aes192_ctr",
    "aes128_ctr"
  ],
  "key_exchange_algorithms": [
    "diffie_hellman_group_exchange_sha256",
    "ecdh_sha2_nistp256"
  ],
  "mac_algorithms": [
    "hmac_sha2_512",
    "hmac_sha2_512_etm"
  ],
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```

Error

Status: Default, Error

| Name | Type | Description |
|-------|--------------------------------|-------------|
| error | returned_error | |

Example error

```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

| Name | Type | Description |
|------|--------|-------------|
| href | string | |

_links

| Name | Type | Description |
|------|----------------------|-------------|
| self | href | |

svm

SVM name and UUID for which the SSH server is configured.

| Name | Type | Description |
|--------|------------------------|---|
| _links | _links | |
| name | string | The name of the SVM. This field cannot be specified in a PATCH method. |
| uuid | string | The unique identifier of the SVM. This field cannot be specified in a PATCH method. |

error_arguments

| Name | Type | Description |
|---------|--------|------------------|
| code | string | Argument code |
| message | string | Message argument |

returned_error

| Name | Type | Description |
|-----------|--|---|
| arguments | array[error_arguments] | Message arguments |
| code | string | Error code |
| message | string | Error message |
| target | string | The target parameter that caused the error. |

Update the SSH server configuration for an SVM

PATCH /security/ssh/svms/{svm.uuid}

Introduced In: 9.10

Updates the SSH server configuration for the specified SVM.

Optional parameters

- `ciphers` - Encryption algorithms for the payload
- `key_exchange_algorithms` - SSH key exchange algorithms
- `mac_algorithms` - MAC algorithms
- `max_authentication_retry_count` - Maximum authentication retries allowed before closing the connection

Related ONTAP commands

- `security ssh`

Parameters

| Name | Type | In | Required | Description |
|----------|--------|------|----------|-------------|
| svm.uuid | string | path | True | SVM UUID |

Request Body

| Name | Type | Description |
|---|---------------------|---|
| <code>ciphers</code> | array[string] | Ciphers for encrypting the data. |
| <code>key_exchange_algorithms</code> | array[string] | Key exchange algorithms. |
| <code>mac_algorithms</code> | array[string] | MAC algorithms. |
| <code>max_authentication_retry_count</code> | integer | Maximum authentication retries allowed before closing the connection. |
| <code>svm</code> | svm | SVM name and UUID for which the SSH server is configured. |

Example request

```
{
  "ciphers": [
    "aes256_ctr",
    "aes192_ctr",
    "aes128_ctr"
  ],
  "key_exchange_algorithms": [
    "diffie_hellman_group_exchange_sha256",
    "ecdh_sha2_nistp256"
  ],
  "mac_algorithms": [
    "hmac_sha2_512",
    "hmac_sha2_512_etm"
  ],
  "svm": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
```

Response

Status: 200, Ok

Error

Status: Default

ONTAP Error Response Codes

| Error Code | Description |
|------------|--|
| 10682372 | There must be at least one key exchange algorithm associated with the SSH configuration. |
| 10682373 | There must be at least one cipher associated with the SSH configuration. |
| 10682375 | Failed to modify SSH key exchange algorithms. |
| 10682378 | Failed to modify SSH ciphers. |

| Error Code | Description |
|------------|--|
| 10682399 | Key exchange algorithm not supported in FIPS-enabled mode. |
| 10682400 | Failed to modify SSH MAC algorithms. |
| 10682401 | MAC algorithm not supported in FIPS-enabled mode. |
| 10682403 | There must be at least one MAC algorithm with the SSH configuration. |
| 10682413 | Failed to modify maximum authentication retry attempts. |
| 10682418 | Cipher not supported in FIPS-enabled mode. |

Also see the table of common errors in the [Response body](#) overview section of this documentation.

Definitions

See Definitions

href

| Name | Type | Description |
|------|--------|-------------|
| href | string | |

_links

svm

SVM name and UUID for which the SSH server is configured.

| Name | Type | Description |
|------|--------|---|
| name | string | The name of the SVM. This field cannot be specified in a PATCH method. |
| uuid | string | The unique identifier of the SVM. This field cannot be specified in a PATCH method. |

svm_ssh_server

| Name | Type | Description |
|--------------------------------|---------------------|---|
| ciphers | array[string] | Ciphers for encrypting the data. |
| key_exchange_algorithms | array[string] | Key exchange algorithms. |
| mac_algorithms | array[string] | MAC algorithms. |
| max_authentication_retry_count | integer | Maximum authentication retries allowed before closing the connection. |
| svm | svm | SVM name and UUID for which the SSH server is configured. |

error_arguments

| Name | Type | Description |
|---------|--------|------------------|
| code | string | Argument code |
| message | string | Message argument |

returned_error

| Name | Type | Description |
|-----------|--|---|
| arguments | array[error_arguments] | Message arguments |
| code | string | Error code |
| message | string | Error message |
| target | string | The target parameter that caused the error. |

Copyright information

Copyright © 2025 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.