Manage authentication keys (end-users)

REST API reference

NetApp
September 12, 2025

This PDF was generated from https://docs.netapp.com/us-en/ontap-restapi-9141/security_authentication_publickeys_owner.uuid_account.name_index_endpoint_overview.html on September 12, 2025. Always check docs.netapp.com for the latest.

Table of Contents

Manage authentication keys (end-users) . . . 1
- Security authentication publickeys owner.uuid account.name index endpoint overview . . . 1
  - Overview . . . 1
  - Examples . . . 1
- Delete a public key for a user account . . . 3
  - Related ONTAP commands . . . 3
  - Learn more . . . 3
  - Parameters . . . 3
  - Response . . . 4
  - Error . . . 4
  - Definitions . . . 4
- Retrieve public keys configured for a user account . . . 5
  - Related ONTAP commands . . . 5
  - Learn more . . . 5
  - Parameters . . . 5
  - Response . . . 7
  - Error . . . 8
  - Definitions . . . 9
- Update a public key for a user account . . . 11
  - Related ONTAP commands . . . 11
  - Learn more . . . 11
  - Parameters . . . 11
  - Request Body . . . 11
  - Response . . . 13
  - Error . . . 13
  - Definitions . . . 13

Manage authentication keys (end-users)

Security authentication publickeys owner.uuid account.name index endpoint overview

Overview

This API configures the public keys for end-user (non-cluster admin) accounts. Specify the owner UUID, the user account name, and the index in the URI path. The owner UUID corresponds to the UUID of the SVM containing the user account associated with the public key and can be obtained from the response body of the GET request performed on the API "/api/svm/svms".

The index value corresponds to the public key that needs to be modified or deleted (it is possible to create more than one public key for the same user account).

Examples

Retrieving the specific configured public key for user accounts

```
# The API:
GET
"/api/security/authentication/publickeys/{owner.uuid}/{account.name}/{inde
x}"

# The call:
curl -k https://<mgmt-ip>/api/security/authentication/publickeys/513a78c7-
8c13-11e9-8f78-005056bbf6ac/pubuser4/0
```

Updating the public key, certificate, and comment for user accounts

```
# The API:
PATCH
"/api/security/authentication/publickeys/{owner.uuid}/{account.name}/{inde
x}"

# The call:
curl -k https://<mgmt-ip>/api/security/authentication/publickeys/d49de271-
8c11-11e9-8f78-005056bbf6ac/pubuser1/0 --request PATCH --data '{
"comment": "Cserver-modification", "certificate": "-----BEGIN
CERTIFICATE-----
\nMIIFrTCCA5WgAwIBAgICEAMwDQYJKoZIhvcNAQELBQAwYDELMAkGA1UEBhMCVVMx\nCzAJBg
NVBAgMAk5DMQwwCgYDVQQHDANSVFAxDzANBgNVBAoMBk5FVEFQUDENMAsG\nA1UECwwETlRBUD
EWMBQGA1UEAwwNTlRBUC1JTlRFUkNBMjAeFw0yMzAxMTkwOTE4\nMzBaFw0yNDAxMjkwOTE4Mz
BaMFcxCzAJBgNVBAYTAklOMQswCQYDVQQIDAJLQTEM\nMAoGA1UEBwwDQkxSMQ0wCwYDVQQKDA
ROVEFQMQ0wCwYDVQQLDAROVEFQMQ8wDQYD\nVQQDDAZNWU5UQVAwggEiMA0GCSqGSIb3DQEBAQ
UAA4IBDwAwggEKAoIBAQDfkWQD\n4kQcInzLQh95eNMXOP6AK9DIzM1e5V7350xTiWmrmiqREh
96Asms4RxOHTI4Q1ox\nghn3NugjWy/y9aCao+Uz6nIG8gAP+NIYb3TU/WeGJFKF6fRJgaZxIz
Bjla3x1QQ5\nrCWZMPuEiKZeBtnyHnoz6g3d5Cz4Ahu2mmHUDbAah25nNuYA9vbroP4GPtE4KQ
YQ\n2lKtXnw8UKvyTYBOU3KzM2PP+lhtNmh3l/rgFhx99x1P6x8I8c6xRRQIjfIhHH9n\n8mLk
Elc3SMSeRNLIQn8JSd9gly6FyHDF2jsPWdRjTlPyvGeN+LNUsBrBgmeyuFvA\nTq0/7lavqoNi
wA4dAgMBAAGjggF4MIIBdDAJBgNVHRMEAjAAMBEGCWCGSAGG+EIB\nAQQEAwIGQDAzBglghkgB
hvhCAQ0EJhYkT3BlblNTTCBHZW5lcmF0ZWQgU2VydmVy\nIENlcnRpZmljYXRlMB0GA1UdDgQW
BBQkJGop1KmP0D5jkblSGk3nSGHf5jCBiwYD\nVR0jBIGDMIGAgBQqjApAoQETk23RqM0Fo7u6
0SsmL6FkpGIwYDELMAkGA1UEBhMC\nVVMxCzAJBgNVBAgMAk5DMQwwCgYDVQQHDANSVFAxDzAN
BgNVBAoMBk5FVEFQUDEN\nMAsGA1UECwwETlRBUDEWMBQGA1UEAwwNTlRBUC1JTlRFUkNBMYIC
EAAwDgYDVR0P\nAQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBME0GCCsGAQUFBwEBBEEw
PzA9\nBggrBgEFBQcwAYYxaHR0cDovL3Njc3ByMjY5Mjc4OTAyMS5nZGwuZW5nbGFiLm5l\ndG
FwcC5jb206MjU2MDANBgkqhkiG9w0BAQsFAAOCAgEASSs8BR96qNipv4X8ZS49\nhW5MpkuQmH
g2E7ICXYPP+r0qHeAa0fVpstLoju7ICo1HyfszwlncO8X2V37cQsCB\nMsMq1THVhKExPuAwUj
Tk6aP6kiun8Werr7rOqFKheZDkCxIMQ0E2mK+O5z6wZaqc\nOa1o4jmAEDUvLBYLYxa0qXa1Eu
nLpOOJTg0fkCW8SOwGDT7CWhpk1AiqivnGnsaz\nhN54gPbinI6La9elEfbNJSOLQUGzvp9nhk
FGNssx5tl0Ij+qzxV6DrzbY8qAeCH2\nrZnasMILUGISQC1LvxxeGcZ7da4AX3V8/ixHeKoUsk
5kA+ucHEB+GP15L0KGU5xa\nY/Uy7Uoh1GRPmvILelxzf2jK+z4x8hudJ9TUrskrLHkrsAm68e
W5IikIJmQsCBiM\nioGib6tWl250etSiC9byQ48W99yOlyShe8EQStogOeshXJfMyY7VZa0YA/
4KMtvi\nO+fxF6LdeFMeu0qxvYLYnIbNPmc2ohGrZwffnL/Kc9s9RF5dk9bjchCKuL3+bdBm\n
IdcvjGi1gGHzgvsg7W54/ctwFH/qW5N68SE7JCv0DtydjUhtlU34I1RfrJD72L3X\nLAb0KlLG
92Oun5psy49vprr143X7eOlGB4TNjUsXW9lNP/R8J3o1ZNnoZq7E32XI\ntsi/5Ttkq7aT975a
lerJoAU=\n-----END CERTIFICATE-----" , "public_key": "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDfkWQD4kQcInzLQh95eNMXOP6AK9DIzM1e5V7350xTiW
mrmiqREh96Asms4RxOHTI4Q1oxghn3NugjWy/y9aCao+Uz6nIG8gAP+NIYb3TU/WeGJFKF6fRJ
gaZxIzBjla3x1QQ5rCWZMPuEiKZeBtnyHnoz6g3d5Cz4Ahu2mmHUDbAah25nNuYA9vbroP4GPt
E4KQYQ2lKtXnw8UKvyTYBOU3KzM2PP+lhtNmh3l/rgFhx99x1P6x8I8c6xRRQIjfIhHH9n8mLk
Elc3SMSeRNLIQn8JSd9gly6FyHDF2jsPWdRjTlPyvGeN+LNUsBrBgmeyuFvATq0/7lavqoNiwA
4d" }'
```

Deleting the public key for user accounts

```
# The API:
DELETE
"/api/security/authentication/publickeys/{owner.uuid}/{account.name}/{inde
x}"

# The call:
curl -k https://<mgmt-ip>/api/security/authentication/publickeys/d49de271-
8c11-11e9-8f78-005056bbf6ac/pubuser1/0 --request DELETE
```

Delete a public key for a user account

DELETE `/security/authentication/publickeys/{owner.uuid}/{account.name}/{index}`

Introduced In: 9.7

Deletes the public key for a user account.

Related ONTAP commands

- `security login publickey delete`

Learn more

- DOC /security/authentication/publickeys/{owner.uuid}/{account.name}/{index}
- DOC /security/accounts

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	Account owner UUID
account.name	string	path	True	User account name
index	integer	path	True	Index number for the public key (where there are multiple keys for the same account). • Max value: 99 • Min value: 0

Response

```
Status: 200, Ok
```

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

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.

Retrieve public keys configured for a user account

GET `/security/authentication/publickeys/{owner.uuid}/{account.name}/{index}`

Introduced In: 9.7

Retrieves the public keys configured for a user account.

Related ONTAP commands

- `security login publickey show`

Learn more

- DOC /security/authentication/publickeys/{owner.uuid}/{account.name}/{index}
- DOC /security/accounts

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	Account owner UUID

Name	Type	In	Required	Description
account.name	string	path	True	User account name
index	integer	path	True	Index number for the public key (where there are multiple keys for the same account). • Max value: 99 • Min value: 0
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Max value: 120 • Min value: 0 • Default value: 1
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
account	account_reference	
certificate	string	Optional certificate for the public key.
certificate_details	string	The details present in the certificate (READONLY).
certificate_expired	string	The expiration details of the certificate (READONLY).
certificate_revoked	string	The revocation details of the certificate (READONLY).
comment	string	Optional comment for the public key.
index	integer	Index number for the public key (where there are multiple keys for the same account).
obfuscated_fingerprint	string	The obfuscated fingerprint for the public key (READONLY).
owner	owner	Owner name and UUID that uniquely identifies the public key.
public_key	string	The public key
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.
sha_fingerprint	string	The SHA fingerprint for the public key (READONLY).

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "account": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "joe.smith"
  },
  "certificate": "string",
  "certificate_details": "string",
  "certificate_expired": "string",
  "certificate_revoked": "string",
  "comment": "string",
  "obfuscated_fingerprint": "string",
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "public_key": "string",
  "scope": "string",
  "sha_fingerprint": "string"
}
```


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	

account_reference

Name	Type	Description
_links	_links	
name	string	User account

owner

Owner name and UUID that uniquely identifies the public key.

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

Name	Type	Description
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Update a public key for a user account

PATCH `/security/authentication/publickeys/{owner.uuid}/{account.name}/{index}`

Introduced In: 9.7

Updates the public key and/or certificate for a user account.

Related ONTAP commands

- `security login publickey modify`

Learn more

- DOC /security/authentication/publickeys/{owner.uuid}/{account.name}/{index}
- DOC /security/accounts

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	Account owner UUID
account.name	string	path	True	User account name
index	integer	path	True	Index number for the public key (where there are multiple keys for the same account). • Max value: 99 • Min value: 0

Request Body

Name	Type	Description
certificate	string	Optional certificate for the public key.
certificate_details	string	The details present in the certificate (READONLY).
certificate_expired	string	The expiration details of the certificate (READONLY).
certificate_revoked	string	The revocation details of the certificate (READONLY).
comment	string	Optional comment for the public key.
obfuscated_fingerprint	string	The obfuscated fingerprint for the public key (READONLY).
public_key	string	The public key
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.
sha_fingerprint	string	The SHA fingerprint for the public key (READONLY).

Example request

```
{
  "certificate": "string",
  "certificate_details": "string",
  "certificate_expired": "string",
  "certificate_revoked": "string",
  "comment": "string",
  "obfuscated_fingerprint": "string",
  "public_key": "string",
  "scope": "string",
  "sha_fingerprint": "string"
}
```

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
5832707	Failed to generate fingerprint for the public key.

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

account_reference

Name	Type	Description
name	string	User account

owner

Owner name and UUID that uniquely identifies the public key.

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.

publickey

The public key for the user account (to access SSH).

Name	Type	Description
certificate	string	Optional certificate for the public key.
certificate_details	string	The details present in the certificate (READONLY).
certificate_expired	string	The expiration details of the certificate (READONLY).
certificate_revoked	string	The revocation details of the certificate (READONLY).
comment	string	Optional comment for the public key.

Name	Type	Description
obfuscated_fingerprint	string	The obfuscated fingerprint for the public key (READONLY).
public_key	string	The public key
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.
sha_fingerprint	string	The SHA fingerprint for the public key (READONLY).

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.