



Manage authentication keys (for admins)

ONTAP 9.15.1 REST API reference

NetApp
September 11, 2024

Table of Contents

- Manage authentication keys (for admins) 1
 - Security authentication publickeys endpoint overview 1
 - Retrieve public keys configured for user accounts 5
 - Create a public key for a user account 12

Manage authentication keys (for admins)

Security authentication publickeys endpoint overview

Overview

This API configures the public keys for user accounts.

For secure shell (SSH) access, public-private key pair based authentication is possible by associating the public key with a user account. Prerequisites: You must have generated the SSH key. You must be a cluster or SVM administrator to perform the user's public key.

Examples

Creating a public key for cluster-scoped user accounts

Specify the user account name, public key, index, comment, and optionally the certificate in the body of the POST request. The owner.uuid or owner.name are not required for a cluster-scoped user account.

```
# The API:
POST "/api/security/authentication/publickey"

# The call
curl -k https://<mgmt-ip>/api/security/authentication/publickeys --request
POST --data '{ "account": "pubuser2", "comment": "Cserver-
Creation", "index": 0, "certificate": "-----BEGIN CERTIFICATE-----
\nMIIFrTCCA5WgAwIBAgICEAMwDQYJKoZIhvcNAQELBQAwYDELMAkGA1UEBhMCVVMx\nCzAJBg
NVBAGMAk5DMQwwCgYDVQQHDANSVFAXDzANBgNVBAoMBk5FVEFQUDENMASG\nA1UECwwETlRBUD
EWMBQGA1UEAwwNTlRBUC1JTlRFUkNBmjaeFw0yMzAxMTkwOTE4\nMzBaFw0yMzAxMTkwOTE4Mz
BaMFcxZAJBgNVBAYTAk1OMQswCQYDVQQIDAJLQTEM\nMAoGA1UEBwwDQkxSMQ0wCwYDVQQKDA
ROVEFQM0wCwYDVQQLDAROVEFQM08wDQYD\nvVQDDAZNWU5UQVAggEiMA0GCSqGSIb3DQEBAQ
UAA4IBDwAwggEKAoIBAQDfkwQD\n4kQcInzLQh95eNMxOP6AK9DIzMe5V7350xTiWmrmiqREh
96Asms4RxOHTI4Q1ox\nghn3NugjWy/y9aCao+Uz6nIG8gAP+NIYb3TU/WeGJFKF6fRJgaZxIz
Bjla3x1QQ5\nnrCWZMPuEiKZeBtNyHnoz6g3d5Cz4Ahu2mmHUDbAah25nNuYA9vbroP4GptE4KQ
YQ\n2lKtXnw8UKvyTYBOU3Kz2MPP+1htNm31/rgFhx99x1P6x8I8c6xRRQIjfiHH9n\n8mLk
Elc3SMSerNLIQn8JSd9gly6FyHDF2jsPWdrjTlPvyGen+LNUsBrBgmeyuFvA\nTq0/7lavqoNi
wA4dAgMBAAGjggF4MIIBDdAJBgNVHRMEAjaAMBEGCWCsGAGG+EIB\nAQQEAWIGQDAzBglghkgB
hvhCAQ0EJhYkT3BlblNTTCBHZW5lcmF0ZWQgU2VydMvY\nIENlcuRzmljYXR1MB0GA1UdDgQW
BBQkJKGop1Kmp0D5jkb1SGk3nSGHf5jCBiwYD\nVR0jBIGDMIGAgBQqjApAoQETk23RqM0Fo7u6
0SsmL6FkpgIwYDELMAkGA1UEBhMC\nVVMxZAJBgNVBAGMAk5DMQwwCgYDVQQHDANSVFAXDzAN
BgNVBAoMBk5FVEFQUDEN\nMASGA1UECwwETlRBUDUdEWMBQGA1UEAwwNTlRBUC1JTlRFUkNBMYIC
EAAwDgYDVR0P\nAQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBME0GCCsGAQUFBwEBBEEw
PzA9\nnBggrBgEFBQcwAYYxaHR0cDovL3Njc3ByMjY5Mjc4OTAYMS5nZGwuZW5nGFILm5l\nndG
FwcC5jb206MjU2MDANBgkqhkiG9w0BAQsFAAOCAGeEASSs8BR96qNipv4X8ZS49\nnhW5MpkUqMH
g2E7ICXYPp+r0qHeAafVpstLoju7ICo1HyfswzlnC08X2V37cQsCB\nnMsMq1THVhKExPuAwUj
Tk6aP6kiun8Werr7rOqFKheZDkCxIMQ0E2mK+O5z6wZaqc\nOalo4jmaEDUvLBYLYxa0qXa1Eu
nLp0OJTg0fkCW8SOWGDT7CWhpk1AiqivnGnsaz\nhN54gPbinI6La9e1efbNJSOLQUGzvp9nhk
FGNssx5t10Ij+qzxV6DrzbY8qAeCH2\nnrZnasMILUGISQC1LvxxeGcZ7da4AX3V8/ixHeKoUsk
5kA+ucHEB+GP15L0KGU5xa\nY/Uy7Uoh1GRPmvILelxzf2jK+z4x8hudJ9TURskrLHkrsAm68e
W5IikIJmQsCBiM\nnioGib6tWl250etSiC9byQ48W99yOlyShe8EQStogOeshXJfMy7VZa0YA/
4Kmtvi\nO+fxF6LdeFMeu0qxvYLYnIbNPmc2ohGrZwffnL/Kc9s9RF5dk9bjchCKuL3+bdBm\n
IdcvjGilgGHZgvsG7W54/ctwFH/qW5N68SE7JCv0DtydjUht1U34I1RfrJD72L3X\nnLAb0K1LG
92Oun5psy49vpr143X7e01GB4TNjUsXW91NP/R8J3o1ZnNoZq7E32XI\nntsi/5Ttkq7aT975a
lerJoAU=\n-----END CERTIFICATE-----", "public_key": "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDfkwQD4kQcInzLQh95eNMxOP6AK9DIzMe5V7350xTiW
mrmiqREh96Asms4RxOHTI4Q1oxghn3NugjWy/y9aCao+Uz6nIG8gAP+NIYb3TU/WeGJFKF6fRJ
gaZxIzBjla3x1QQ5rCWZMPuEiKZeBtNyHnoz6g3d5Cz4Ahu2mmHUDbAah25nNuYA9vbroP4Gpt
E4KQYQ2lKtXnw8UKvyTYBOU3Kz2MPP+1htNm31/rgFhx99x1P6x8I8c6xRRQIjfiHH9n8mLk
Elc3SMSerNLIQn8JSd9gly6FyHDF2jsPWdrjTlPvyGen+LNUsBrBgmeyuFvATq0/7lavqoNi
wA4d" }'
```

Creating a public key for SVM-scoped user accounts

For a SVM-scoped account, specify either the SVM name as the owner.name or the SVM UUID as the

owner.uuid along with other parameters for the user account. These parameters indicate the SVM that contains the user account for the public key being created and can be obtained from the response body of the GET request performed on the API"/api/svm/svms".

```
# The API:
```

```
POST "/api/security/authentication/publickey"
```

```
# The call
```

```
curl -k https://<mgmt-ip>/api/security/authentication/publickeys --request  
POST --data '{ "account": "pubuser4", "comment": "Vserver-  
Creation", "index": 0, "certificate": "-----BEGIN CERTIFICATE-----  
\nMIIFrTCCA5WgAwIBAgICEAMwDQYJKoZIhvcNAQELBQAwYDELMAkGA1UEBhMCVVMx\nnCzAJBgNVBAGMAk5DMQwwCgYDVQQHDANSVFAXDzANBgNVBAoMBk5FVEFQUDENMA  
Sg\nnA1UECwwETlRBUD  
EWMBQGA1UEAwwNTlRBUC1JTlRFUknBMjAeFw0yMzAxMTkwOTE4\nnMzBaFw0yNDAxMjkwOTE4Mz  
BaMFcxZAJBgNVBAYTAk1OMQswCQYDVQQIDAJLQTEM\nnMAoGA1UEBwwDQkxSMQ0wCwYDVQQKDA  
ROVEFQM0wCwYDVQQLDAROVEFQM08wDQYD\nnVQDDAZNWU5UQVAggEiMA0GCSqGSIb3DQEBAQ  
UAA4IBDwAwggEKAoIBAQDfkwQD\nn4kQcInzLQh95eNMXOP6AK9DIzM1e5V7350xTiWmrm  
iqREh96Asms4RxOHTI4Q1ox\nngghn3NugjWy/y9aCao+Uz6nIG8gAP+NIYb3TU/WeGJFKF6fR  
JgaZxIzBjla3x1QQ5\n\nnrCWZMPuEiKZeBtNyHnoz6g3d5Cz4Ahu2mmH  
UDbAah25nNuYA9vbrop4GPT  
E4KQYQ2lKtXnw8UKvyTYBOU3Kz  
M2PP+lhtNmh3l/rgFhx99x1P6x8I8c6xRRQI  
jfhHH9n8mLkElc3SMSeRNL  
IQn8JSd9gly6FyHDF2jsPWdRjTlP  
yvGeN+LNUsBrBgmeyuFvATq0/7lavqoN  
iwa4d" }'
```

Retrieving the configured public key for user accounts

Retrieves all public keys associated with the user accounts or a filtered list (for a specific user account name, a specific SVM and so on) of public keys.

```
# The API:
GET "/api/security/authentication/publickeys"

# The call to retrieve all the user accounts configured in the cluster:
curl -k https://<mgmt-ip>/api/security/authentication/publickeys
```

Retrieve public keys configured for user accounts

GET /security/authentication/publickeys

Introduced In: 9.7

Retrieves the public keys configured for user accounts.

Related ONTAP commands

- `security login publickey show`

Learn more

- [DOC /security/authentication/publickeys](#)
- [DOC /security/accounts](#)

Parameters

Name	Type	In	Required	Description
certificate_expired	string	query	False	Filter by certificate_expired <ul style="list-style-type: none">• Introduced in: 9.13
obfuscated_fingerprint	string	query	False	Filter by obfuscated_fingerprint
certificate_details	string	query	False	Filter by certificate_details <ul style="list-style-type: none">• Introduced in: 9.13

Name	Type	In	Required	Description
comment	string	query	False	Filter by comment
owner.uuid	string	query	False	Filter by owner.uuid
owner.name	string	query	False	Filter by owner.name
account.name	string	query	False	Filter by account.name
certificate	string	query	False	Filter by certificate <ul style="list-style-type: none"> • Introduced in: 9.13
index	integer	query	False	Filter by index <ul style="list-style-type: none"> • Max value: 99 • Min value: 0
public_key	string	query	False	Filter by public_key
scope	string	query	False	Filter by scope
sha_fingerprint	string	query	False	Filter by sha_fingerprint
certificate_revoked	string	query	False	Filter by certificate_revoked <ul style="list-style-type: none"> • Introduced in: 9.13
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. <ul style="list-style-type: none"> • Default value: 1

Name	Type	In	Required	Description
return_timeout	integer	query	False	<p>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.</p> <ul style="list-style-type: none"> • 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	
num_records	integer	Number of records
records	array[publickey]	

Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_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": "svml",
        "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
next	href	
self	href	

_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.

publickey

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

Name	Type	Description
_links	_links	

Name	Type	Description
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).

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.

Create a public key for a user account

POST `/security/authentication/publickeys`

Introduced In: 9.7

Creates a public key along with an optional certificate for a user account.

Required properties

- `owner.uuid` - UUID of the account owner.
- `name` - User account name.
- `index` - Index number for the public key (where there are multiple keys for the same account).
- `public_key` - The publickey details for the creation of the user account.

Optional properties

- `comment` - Comment text for the public key.
- `certificate` - The certificate in PEM format.

Related ONTAP commands

- `security login publickey create`

Learn more

- [DOC /security/authentication/publickeys](#)
- [DOC /security/accounts](#)

Parameters

Name	Type	In	Required	Description
return_records	boolean	query	False	<p>The default is false. If set to true, the records are returned.</p> <ul style="list-style-type: none"> • Default value:

Request Body

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.

Name	Type	Description
sha_fingerprint	string	The SHA fingerprint for the public key (READONLY).

Example request

```
{
  "_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"
}
```

Response

Status: 201, Created

Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Error

Status: Default

ONTAP Error Response Codes

Error Code	Description
5832705	Public key already exists for the given user and application.
5832707	Failed to generate fingerprint for the public key.
5832722	The public key cannot be associated with this user on the SVM because a login method using the given application and authentication method does not exist for this user.

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

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.

publickey

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

Name	Type	Description
_links	_links	
account	account_reference	
certificate	string	Optional certificate for the public key.

Name	Type	Description
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).

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.

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.