Manage authentication keys (for admins)

ONTAP 9.14.1 REST API reference

NetApp
May 23, 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\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" }'
```

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\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-----", "owner.uuid":"513a78c7-8c13-11e9-
8f78-005056bbf6ac","owner.name":"vs0","public_key": "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDfkWQD4kQcInzLQh95eNMXOP6AK9DIzM1e5V7350xTiW
mrmiqREh96Asms4RxOHTI4Q1oxghn3NugjWy/y9aCao+Uz6nIG8gAP+NIYb3TU/WeGJFKF6fRJ
gaZxIzBjla3x1QQ5rCWZMPuEiKZeBtnyHnoz6g3d5Cz4Ahu2mmHUDbAah25nNuYA9vbroP4GPt
E4KQYQ2lKtXnw8UKvyTYBOU3KzM2PP+lhtNmh3l/rgFhx99x1P6x8I8c6xRRQIjfIhHH9n8mLk
Elc3SMSeRNLIQn8JSd9gly6FyHDF2jsPWdRjTlPyvGeN+LNUsBrBgmeyuFvATq0/7lavqoNiwA
4d" }'
```

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_revoked	string	query	False	Filter by certificate_revoked • Introduced in: 9.13
index	integer	query	False	Filter by index • Max value: 99 • Min value: 0
certificate_expired	string	query	False	Filter by certificate_expired • Introduced in: 9.13

Name	Type	In	Required	Description
certificate_details	string	query	False	Filter by certificate_details • Introduced in: 9.13
obfuscated_fingerprint	string	query	False	Filter by obfuscated_fingerprint
sha_fingerprint	string	query	False	Filter by sha_fingerprint
certificate	string	query	False	Filter by certificate • Introduced in: 9.13
owner.uuid	string	query	False	Filter by owner.uuid
owner.name	string	query	False	Filter by owner.name
comment	string	query	False	Filter by comment
scope	string	query	False	Filter by scope
public_key	string	query	False	Filter by public_key
account.name	string	query	False	Filter by account.name
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

Name	Type	In	Required	Description
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	
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_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"
    },
    "scope": "cluster",
    "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	The default is false. If set to true, the records are returned. • 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_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"
  },
  "scope": "cluster",
  "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

Trademark information