Manage scoped user accounts

ONTAP 9.15.1 REST API reference

NetApp
September 11, 2024

Table of Contents

Manage scoped user accounts

Security accounts owner.uuid name endpoint overview

Overview

This API displays and manages the configuration of scoped user accounts.

Newly created user accounts might need to be updated for many reasons. For example, a user account might need to use a different application or its role might need to be modified. According to a policy, the password or authentication source of a user account might need to be changed, or a user account might need to be locked or deleted from the system. This API allows you to make these changes to user accounts.

Specify the owner UUID and the user account name in the URI path. The owner UUID corresponds to the UUID of the SVM for which the user account has been created and can be obtained from the response body of the GET request performed on one of the following APIs: /api/security/accounts for all user accounts /api/security/accounts/?scope=cluster for cluster-scoped user accounts /api/security/accounts/?scope=svm for SVM-scoped accounts /api/security/accounts/?owner.name=<svm-name></i> for a specific SVM This API response contains the complete URI for each user account that can be used.</svm-name>

Examples

Retrieving the user account details

```
# The API:
GET "/api/security/accounts/{owner.uuid}/{name}"

# The call:
curl -X GET "https://<mgmt-ip>/api/security/accounts/aef7c38-4bd3-11e9-
b238-0050568e2e25/svm_user1"

# The response:
{
"owner": {
  "uuid": "aaef7c38-4bd3-11e9-b238-0050568e2e25",
  "name": "svm1",
  "_links": {
    "self": {
      "href": "/api/svm/svms/aaef7c38-4bd3-11e9-b238-0050568e2e25"
    }
        }
},
"name": "svm_user1",
"applications": [
  {
    "application": "ssh",
    "authentication_methods": [
```

```
      "password"
    ],
    "second_authentication_method": "none"
  }
],
"role": {
  "name": "vsadmin",
  "_links": {
    "self": {
      "href": "/api/svms/aaef7c38-4bd3-11e9-b238-
0050568e2e25/admin/roles/vsadmin"
    }
  }
},
"locked": false,
"password_hash_algorithm": "sha512",
"scope": "svm",
"_links": {
  "self": {
    "href": "/api/security/accounts/aaef7c38-4bd3-11e9-b238-
0050568e2e25/svm_user1"
  }
}
}
```

Updating the applications and role in a user account

Specify the desired configuration in the form of tuples (of applications and authentication methods) and the role. All other previously configured applications that are not specified in the "applications" parameter of the PATCH request will be de-provisioned for the user account.

```
# The API:
PATCH "/api/security/accounts/{owner.uuid}/{name}"

# The call to update the applications and role:
curl -X PATCH "https://<mgmt-ip>/api/security/accounts/aaef7c38-4bd3-11e9-
b238-0050568e2e25/svm_user1" -d
'{"applications":[{"application":"http","authentication_methods":["domain"
]},{"application":"ontapi","authentication_methods":["password"]}],"role":
{"name": "vsadmin-backup"}}'

# The call to update only the role:
curl -X PATCH "https://<mgmt-ip>/api/security/accounts/aaef7c38-4bd3-11e9-
b238-0050568e2e25/svm_user1" -d '{"role":"vsadmin-protocol"}'
```

Updating the password for a user account

```
# The API:
PATCH "/api/security/accounts/{owner.uuid}/{name}"

# The call:
curl -X PATCH "https://<mgmt-ip>/api/security/accounts/aaef7c38-4bd3-11e9-
b238-0050568e2e25/svm_user1" -d '{"password":"newp@ssw@rd2"}'
```

Locking a user account

```
The API:
PATCH "/api/security/accounts/{owner.uuid}/{name}"
The call:
curl -X PATCH "https://<mgmt-ip>/api/security/accounts/aaef7c38-4bd3-11e9-
b238-0050568e2e25/svm_user1" -d '{"locked":"true"}'
```

Deleting a user account

```
# The API:
DELETE "/api/security/accounts/{owner.uuid}/{name}"

# The call:
curl -X DELETE "https://<mgmt-ip>/api/security/accounts/aaef7c38-4bd3-
11e9-b238-0050568e2e25/svm_user1"
```

Delete a user account

DELETE `/security/accounts/{owner.uuid}/{name}`

Introduced In: 9.6

Deletes a user account.

Required parameters

- `name` - Account name to be deleted.
- `owner.uuid` - UUID of the SVM housing the user account to be deleted.

Related ONTAP commands

- `security login delete`

Learn more

- DOC /security/accounts/{owner.uuid}/{name}
- DOC /security/accounts

Parameters

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

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
5636098	Last unlocked account that has an admin role cannot be deleted.
5636125	The operation is not supported on system accounts.
5636146	Cannot delete the last console account with admin role.

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

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 a specific user account

GET `/security/accounts/{owner.uuid}/{name}`

Introduced In: 9.6

Retrieves a specific user account.

Related ONTAP commands

- `security login show`

Learn more

- DOC /security/accounts/{owner.uuid}/{name}
- DOC /security/accounts

Parameters

Name	Type	In	Required	Description
owner.uuid	string	path	True	Account owner UUID
name	string	path	True	User account name
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
applications	array[account_application]	
authentication_methods	array[string]	
comment	string	Optional comment for the user account.
locked	boolean	Locked status of the account.
name	string	User or group account name

Name	Type	Description
owner	owner	Owner name and UUID that uniquely identifies the user account.
password	string	Password for the account. The password can contain a mix of lower and upper case alphabetic characters, digits, and special characters.
password_hash_algorithm	string	Password hash algorithm used to generate a hash of the user's password for password matching.To modify "password_hash_algorithm", use REST API "/api/security/authentication/password".
public_key	string	Public key for SSH.
role	role	
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.
ssl_ca_certificate	string	SSL certificate for the chain of certificate authorities (CA) that have signed this user's client certificate.

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "applications": [
    {
      "application": "string",
      "authentication_methods": [
        "string"
      ],
      "second_authentication_method": "string"
    }
  ],
  "authentication_methods": [
    "string"
  ],
  "comment": "string",
  "name": "joe.smith",
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "password": "string",
  "password_hash_algorithm": "sha512",
  "public_key": "string",
  "role": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "admin"
  },
  "scope": "string",
  "ssl_ca_certificate": "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_application

Name	Type	Description
application	string	Applications
authentication_methods	array[string]	
is_ldap_fastbind	boolean	Optional property that specifies the mode of authentication as LDAP Fastbind.
is_ns_switch_group	boolean	Optional property that specifies whether the user is an LDAP or NIS group.
second_authentication_method	string	An optional additional authentication method for multifactor authentication (MFA). This property is only supported for SSH (*ssh*) and Service Processor (*service_processor*) applications. It is ignored for all other applications. Time-based One-Time Passwords (TOTPs) are only supported with the authentication method password or public key. For the Service Processor (*service_processor*) application, *none* and *publickey* are the only supported enum values.

owner

Owner name and UUID that uniquely identifies the user account.

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.

role

Name	Type	Description
_links	_links	
name	string	Role name

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 a user account

PATCH `/security/accounts/{owner.uuid}/{name}`

Introduced In: 9.6

Updates a user account. Locks or unlocks a user account and/or updates the role, applications, and/or

password for the user account.

Required parameters

- `name` - Account name to be updated.
- `owner.uuid` - UUID of the SVM housing the user account to be updated.

Optional parameters

- `applications` - Array of one or more tuples (of application and authentication methods).
- `role` - RBAC role for the user account.
- `password` - Password for the user account (if the authentication method is opted as password for one or more of applications).
- `second_authentication_method` - Needed for MFA and only supported for *ssh* and *service_processor* applications. Defaults to *none* if not supplied.
- `comment` - Comment for the user account (e.g purpose of this account).
- `locked` - Set to true/false to lock/unlock the account.
- `is_ldap_fastbind` - Set to true/false to enable LDAP Fastbind Authentication.
- `is_ns_switch_group` - Set to true/false to specify whether the user is an LDAP or NIS group.

Related ONTAP commands

- `security login create`
- `security login modify`
- `security login password`
- `security login lock`
- `security login unlock`

Learn more

- DOC /security/accounts/{owner.uuid}/{name}
- DOC /security/accounts

Parameters

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

Request Body

Name	Type	Description
_links	_links	
applications	array[account_application]	
authentication_methods	array[string]	
comment	string	Optional comment for the user account.
locked	boolean	Locked status of the account.
name	string	User or group account name
owner	owner	Owner name and UUID that uniquely identifies the user account.
password	string	Password for the account. The password can contain a mix of lower and upper case alphabetic characters, digits, and special characters.
password_hash_algorithm	string	Password hash algorithm used to generate a hash of the user's password for password matching.To modify "password_hash_algorithm", use REST API "/api/security/authentication/password".
public_key	string	Public key for SSH.
role	role	
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.
ssl_ca_certificate	string	SSL certificate for the chain of certificate authorities (CA) that have signed this user's client certificate.

Example request

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "applications": [
    {
      "application": "string",
      "authentication_methods": [
        "string"
      ],
      "second_authentication_method": "string"
    }
  ],
  "authentication_methods": [
    "string"
  ],
  "comment": "string",
  "name": "joe.smith",
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "password": "string",
  "password_hash_algorithm": "sha512",
  "public_key": "string",
  "role": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "admin"
  },
  "scope": "string",
  "ssl_ca_certificate": "string"
}
```

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
1261215	The role was not found.
1261218	The user was not found.
1263343	Cannot lock user with password not set or non-password authentication method.
5636096	Cannot perform the operation for this user account since the password is not set.
5636097	The operation for user account failed since user password is not set.
5636100	Modification of a service-processor user’s role to a non-admin role is not supported.
5636125	The operation not supported on AutoSupport user account which is reserved.
5636129	The role does not exist.
5636136	Specifying "is_ns_switch_group" as "true" is supported only for authentication method "nsswitch".
5636154	The second authentication method parameter is supported for SSH and Service Processor (SP) applications only.
5636155	The second-authentication-method parameter can be specified only if the authentication-method password or public key nsswitch.
5636156	Same value cannot be specified for the second-authentication-method and the authentication-method.
5636159	For a given user and application, if the second-authentication-method is specified, only one such login entry is supported.
5636164	If the value for either the authentication-method second-authentication-method is nsswitch or password, the other parameter must differ.

Error Code	Description
5636165	Second authentication method is not supported for NIS or LDAP group based accounts.
5636197	LDAP fastbind combination for application and authentication method is not supported.
5636198	LDAP fastbind authentication is supported only for nsswitch.
5636210	User creation failed because LDAP is not configured for the SVM or the LDAP connection is not secure.
5636212	TOTP is supported only when the primary authentication method is password or public key.
5636214	Configuring the user with TOTP as secondary authentication method requires an effective cluster version of 9.13.1 or later
5636223	Specifying "is_ns_switch_group" as "true" is supported only for SSH, ONTAPI and HTTP applications.
5636224	Configuring a Service Processor (SP) user with two-factor authentication requires an effective cluster version of 9.15.1 or later.
5636225	For a Service Processor (SP) user, the second factor of authentication must be one of publickey or none.
5636226	Internal error. Failed to check for ONTAP capability.
7077896	Cannot lock the account of the last console admin user.
7077906	A role with that name has not been defined for the Vserver.
7077911	The user is not configured to use the password authentication method.
7077918	The password cannot contain the username.
7077919	The minimum length for new password does not meet the policy.
7077920	The new password must have both letters and numbers.
7077921	The minimum number of special characters required do not meet the policy.
7077924	The new password must be different than last N passwords.
7077925	The new password must be different to the old password.
7077929	Cannot lock user with password not set or non-password authentication method.

Error Code	Description
7077940	The password exceeds maximum supported length.
7077941	Defined password composition exceeds the maximum password length of 128 characters.
7078900	An aAdmin password is not set. Set the password by including it in the request.

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_application

Name	Type	Description
application	string	Applications
authentication_methods	array[string]	
is_ldap_fastbind	boolean	Optional property that specifies the mode of authentication as LDAP Fastbind.
is_ns_switch_group	boolean	Optional property that specifies whether the user is an LDAP or NIS group.
second_authentication_method	string	An optional additional authentication method for multifactor authentication (MFA). This property is only supported for SSH (*ssh*) and Service Processor (*service_processor*) applications. It is ignored for all other applications. Time-based One-Time Passwords (TOTPs) are only supported with the authentication method password or public key. For the Service Processor (*service_processor*) application, *none* and *publickey* are the only supported enum values.

owner

Owner name and UUID that uniquely identifies the user account.

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.

role

Name	Type	Description
_links	_links	
name	string	Role name

account

Name	Type	Description
_links	_links	
applications	array[account_application]	
authentication_methods	array[string]	
comment	string	Optional comment for the user account.
locked	boolean	Locked status of the account.
name	string	User or group account name
owner	owner	Owner name and UUID that uniquely identifies the user account.
password	string	Password for the account. The password can contain a mix of lower and upper case alphabetic characters, digits, and special characters.

Name	Type	Description
password_hash_algorithm	string	Password hash algorithm used to generate a hash of the user's password for password matching.To modify "password_hash_algorithm", use REST API "/api/security/authentication/password".
public_key	string	Public key for SSH.
role	role	
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.
ssl_ca_certificate	string	SSL certificate for the chain of certificate authorities (CA) that have signed this user's client certificate.

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

Trademark information