



Update user account password

ONTAP 9.11.1 REST API reference

NetApp
April 02, 2024

Table of Contents

- Update user account password 1
- Security authentication password endpoint overview 1
- Update the user account password 2

Update user account password

Security authentication password endpoint overview

Overview

This API changes the password for a local user account.

Only cluster administrators with the *"admin"* role can change the password for other cluster or SVM user accounts. If you are not a cluster administrator, you can only change your own password.

Examples

Changing the password of another cluster or SVM user account by a cluster administrator

Specify the user account name and the new password in the body of the POST request. The *owner.uuid* or *owner.name* are not required to be specified for a cluster-scoped user account.

For an SVM-scoped account, along with new password and user account name, specify either the SVM name as the *owner.name* or SVM uuid as the *owner.uuid* in the body of the POST request. These indicate the SVM for which the user account is created and can be obtained from the response body of a GET request performed on the */api/svm/svms* API.

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

```
# The call to change the password of another cluster user:  
curl -X POST "https://<mgmt-ip>/api/security/authentication/password" -d  
'{"name":"cluster_user1","password":"hello@1234"}'
```

```
# The call to change the password of another SVM user:  
curl -X POST "https://<mgmt-ip>/api/security/authentication/password" -d  
'{"owner.name":"svm1","name":"svm_user1","password":"hello@1234"}'
```

```
# The call to change the password hash algorithm of the cluster user:  
curl -X POST "https://<mgmt-ip>/api/security/authentication/password" -d  
'{"name":"cluster_user1","password":"hello@1234","password_hash_algorithm"  
:"sha256"}'
```

```
# The call to change the password hash algorithm of another SVM user:  
curl -X POST "https://<mgmt-ip>/api/security/authentication/password" -d  
'{"owner.name":"svm1","name":"svm_user1","password":"hello@1234","password  
_hash_algorithm":"sha256"}'
```

Changing the password of an SVM-scoped user



The IP address in the URI must be same as one of the interfaces owned by the SVM.

```
# The API:  
POST "/api/security/authentication/password"  
  
# The call:  
curl -X POST "https://<SVM-ip>/api/security/authentication/password" -d  
'{"name":"svm_user1","password":"new1@1234"}'
```

Update the user account password

POST /security/authentication/password

Introduced In: 9.6

Updates the password for a user account.

Required parameters

- `name` - User account name.
- `password` - New password for the user account.

Optional parameters

- `owner.name` or `owner.uuid` - Name or UUID of the SVM for an SVM-scoped user account.
- `password_hash_algorithm` - Optional property that specifies the password hash algorithm used to generate a hash of the user's password for password matching. Default value is "sha512".

Related ONTAP commands

- `security login password`

Learn more

- [DOC /security/authentication/password](#)
- [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
name	string	The user account name whose password is being modified.
owner	owner	Owner name and UUID that uniquely identifies the user account. This field is optional and valid only when a cluster administrator is executing the API to uniquely identify the account whose password is being modified. The "owner" field is not required to be specified for SVM user accounts trying to modify their password.
password	string	The password string
password_hash_algorithm	string	Optional property that specifies the password hash algorithm used to generate a hash of the user's password for password matching.

Example request

```
{
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "password_hash_algorithm": "sha512"
}
```

Response

Status: 201, Created

Error

Status: Default

ONTAP Error Response Codes

Error Code	Description
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.
7077940	The password exceeds maximum supported length.
7077941	Defined password composition exceeds the maximum password length of 128 characters.

Name	Type	Description
error	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	

owner

Owner name and UUID that uniquely identifies the user account. This field is optional and valid only when a cluster administrator is executing the API to uniquely identify the account whose password is being modified. The "owner" field is not required to be specified for SVM user accounts trying to modify their password.

Name	Type	Description
_links	_links	
name	string	The name of the SVM.
uuid	string	The unique identifier of the SVM.

account_password

The password object

Name	Type	Description
name	string	The user account name whose password is being modified.
owner	owner	Owner name and UUID that uniquely identifies the user account. This field is optional and valid only when a cluster administrator is executing the API to uniquely identify the account whose password is being modified. The "owner" field is not required to be specified for SVM user accounts trying to modify their password.
password	string	The password string

Name	Type	Description
password_hash_algorithm	string	Optional property that specifies the password hash algorithm used to generate a hash of the user's password for password matching.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

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 © 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.