View and delete an OAuth 2.0 configuration

ONTAP 9.14.1 REST API reference

NetApp
April 02, 2024

This PDF was generated from https://docs.netapp.com/us-en/ontap-restapi/ontap/security_authentication_cluster_oauth2_clients_name_endpoint_overview.html on April 02, 2024. Always check docs.netapp.com for the latest.

Table of Contents

View and delete an OAuth 2.0 configuration 1
Security authentication cluster oauth2 clients name endpoint overview 1
Delete an OAuth 2.0 configuration 3
Retrieve an OAuth 2.0 configuration with the specified name 5

View and delete an OAuth 2.0 configuration

Security authentication cluster oauth2 clients name endpoint overview

Overview

This API is used to retrieve and delete the OAuth 2.0 configuration in the cluster. The GET request retrieves the OAuth 2.0 configuration. The DELETE request removes the OAuth 2.0 configuration. Various responses are shown in the examples below.

Examples

Retrieving the OAuth 2.0 configuration in the cluster

The following output shows the OAuth 2.0 configuration in the cluster.

```
# The API:
/api/security/authentication/cluster/oauth2/clients/{name}

# The call:
curl -X GET "https://<mgmt-
ip>/api/security/authentication/cluster/oauth2/clients/auth0" -H "accept:
application/hal+json"

# The response:
{
"name": "auth0",
"application": "http",
"issuer": "https://examplelab.customer.com",
"audience": "aud",
"client_id": "client_id",
"hashed_client_secret":
"a019c4d5f3815b50f5e9267d3ee80e8d8008308b83705c57206a1f5984dd0b26",
"introspection": {
  "endpoint_uri": "https://examplelab.customer.com/server/endpoint",
  "interval": "PT1H"
},
"remote_user_claim": "user_claim",
"jwks": {
  "provider_uri": "https://examplelab.customer.com/pf/JWKS",
  "refresh_interval": "PT1H"
},
"use_local_roles_if_present": false,
"outgoing_proxy": "https://johndoe:secretpass@proxy.example.com:8080",
"_links": {
  "self": {
    "href": "/api/security/authentication/cluster/oauth2/clients"
  }
},
"use_mutual_tls": "required"
}
```

Deleting the OAuth 2.0 configuration

```
# The API:
/api/security/authentication/cluster/oauth2/clients/{name}

# The call:
curl -X DELETE "https://<mgmt-
ip>/api/security/authentication/cluster/oauth2/clients/auth0"
```

Delete an OAuth 2.0 configuration

DELETE `/security/authentication/cluster/oauth2/clients/{name}`

Introduced In: 9.14

Deletes the OAuth 2.0 configuration with the specified name.

Required properties

- `config_name`

Related ONTAP commands

- `security oauth2 client delete`

Parameters

Name	Type	In	Required	Description
name	string	path	True	OAuth 2.0 configuration name.

Response

```
Status: 200, Ok
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
203816995	OAuth 2.0 must be disabled before the configuration can be removed.

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 an OAuth 2.0 configuration with the specified name

GET `/security/authentication/cluster/oauth2/clients/{name}`

Introduced In: 9.14

Retrieves the OAuth 2.0 configuration with the specified name.

Related ONTAP commands

- `security oauth2 client show`

Parameters

Name	Type	In	Required	Description
name	string	path	True	OAuth 2.0 configuration name.
use_mutual_tls	string	query	False	Filter by use_mutual_tls

Name	Type	In	Required	Description
introspection.endpoint_uri	string	query	False	Filter by introspection.endpoint_uri
introspection.interval	string	query	False	Filter by introspection.interval
jwks.refresh_interval	string	query	False	Filter by jwks.refresh_interval
jwks.provider_uri	string	query	False	Filter by jwks.provider_uri
audience	string	query	False	Filter by audience
application	string	query	False	Filter by application
issuer	string	query	False	Filter by issuer
outgoing_proxy	string	query	False	Filter by outgoing_proxy
hashed_client_secret	string	query	False	Filter by hashed_client_secret
use_local_roles_if_present	boolean	query	False	Filter by use_local_roles_if_present
client_id	string	query	False	Filter by client_id
remote_user_claim	string	query	False	Filter by remote_user_claim
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
application	string	The name of the application using OAuth 2.0. Required for POST operations.
audience	string	The OAuth 2.0 Audience.
client_id	string	The OAuth 2.0 client ID. Required in POST operations for remote introspection.
client_secret	string	The OAuth 2.0 client secret. Required in POST operations for remote introspection.
hashed_client_secret	string	The OAuth 2.0 client secret as a SHA256 HMAC hashed value created with the cluster UUID as its HMAC secret key.
introspection	introspection	
issuer	string	The OAuth 2.0 Issuer.
jwks	jwks	
name	string	The configuration name. Required for POST operations.
outgoing_proxy	string	Outgoing proxy to access external identity providers (IdPs). If not specified, no proxy is configured.
remote_user_claim	string	The remote user claim.
skip_uri_validation	boolean	Indicates whether or not to validate the input URIs. Default value is false.
use_local_roles_if_present	boolean	Indicates whether or not to use locally confgiured roles, if present. Default value is false.

Name	Type	Description
use_mutual_tls	string	OAuth 2.0 mutual TLS authentication setting. Set this value to "none" to disable mutual TLS authentication. Set this value to "required" to enforce mutual TLS authentication for all access tokens and reject any token that does not have x5t#S256 property in the cnf section. The default value is "request" which means mutual TLS authentication is enforced only if the x5t#S256 property is present in the cnf section of the access token.

Example response


```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "application": "http",
  "hashed_client_secret": "string",
  "introspection": {
    "endpoint_uri": "https://examplelab.customer.com/token/introspect",
    "interval": "PT1H"
  },
  "issuer": "https://examplelab.customer.com",
  "jwks": {
    "provider_uri": "https://examplelab.customer.com/pf/JWKS",
    "refresh_interval": "PT2H"
  },
  "name": "auth0",
  "outgoing_proxy":
"https://johndoe:secretpass@proxy.example.com:8080",
  "use_mutual_tls": "none"
}
```


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	

introspection

Name	Type	Description
endpoint_uri	string	The token introspection endpoint URI.
interval	string	The refresh interval for caching tokens, in ISO-8601 format. This can be set to the value "disabled" to disable caching of tokens. When set to 0, tokens are cached according to the expiry period in them. Otherwise, it can be set to a value from 1 second to 2147483647 seconds.

jwks

Name	Type	Description
provider_uri	string	The URI on which the JSON Web Key Set (JWKS) are hosted.
refresh_interval	string	The refresh interval for the JSON Web Key Set (JWKS), in ISO-8601 format. This can be set to a value from 300 seconds to 2147483647 seconds.

error_arguments

Name	Type	Description
code	string	Argument code

Name	Type	Description
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 © 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.