



Manage SAML default metadata configuration

REST API reference

NetApp
February 06, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap-restapi/security_authentication_cluster_saml-sp_default-metadata_endpoint_overview.html on February 06, 2026. Always check docs.netapp.com for the latest.

Table of Contents

- Manage SAML default metadata configuration 1
 - Manage SAML default metadata configuration 1
 - Overview 1
 - Examples 1
 - Delete the SAML default metadata configuration. 2
 - Response 2
 - Error 2
 - Definitions 3
 - Retrieve the SAML default metadata configuration 4
 - Parameters. 4
 - Response 5
 - Error 6
 - Definitions 7
 - Create the SAML default metadata configuration 9
 - Optional properties. 9
 - Parameters. 9
 - Request Body. 10
 - Response 11
 - Response 11
 - Error 12
 - Definitions 12

Manage SAML default metadata configuration

Manage SAML default metadata configuration

Overview

This API is used to manage relevant information about the SAML default metadata configuration in the cluster. The POST request creates a SAML default metadata configuration if there is none present. The DELETE request removes the SAML default metadata configuration. Various responses are shown in the examples below.

Examples

Retrieving the SAML default metadata configuration in the cluster

The following output shows the SAML default metadata configuration in the cluster.

```
# The API:
/api/security/authentication/cluster/saml-sp/default-metadata

# The call:
curl -X GET "https://<mgmt-ip>/api/security/authentication/cluster/saml-sp/default-metadata" -H "accept: application/hal+json"

# The response:
{
  "host": "172.21.74.181",
  "certificate": {
    "ca": "cluster-1",
    "serial_number": "180E3331A0DC5A19",
    "common_name": "cluster-1"
  },
  "scope": "cluster",
  "_links": {
    "self": {
      "href": "/api/security/authentication/cluster/saml-sp/default-metadata"
    }
  }
}
```

Creating the SAML default metadata configuration in the cluster

The following output shows how to create the SAML default metadata in the cluster.

```
# The API:
/api/security/authentication/cluster/saml-sp/default-metadata

# The call:
curl -X POST "https://<mgmt-ip>/api/security/authentication/cluster/saml-sp/default-metadata?return_records=true" -H "accept: application/hal+json" -d '{ "host": "172.21.74.181", "certificate": { "ca": "cluster1", "serial_number": "156F10C3EB4C51C1" } }'
```

Deleting the SAML default metadata configuration in the cluster

```
# The API:
/api/security/authentication/cluster/saml-sp/default-metadata

# The call:
curl -X DELETE "https://<mgmt-ip>/api/security/authentication/cluster/saml-sp/default-metadata/"
```

Delete the SAML default metadata configuration

DELETE /security/authentication/cluster/saml-sp/default-metadata

Introduced In: 9.17

Deletes the SAML default metadata configuration.

Response

```
Status: 200, Ok
```

Error

Status: Default

ONTAP Error Response Codes

Error Code	Description
12320817	Internal Error. The SAML service provider metadata configuration is being created, but is taking longer than expected to complete.
12320826	SAML configuration already exists. Cannot delete the metadata when SAML configuration is already present.
12320832	Internal Error. Failed to execute the command, web server setup is in progress. Retry after some time.

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 the SAML default metadata configuration

GET /security/authentication/cluster/saml-sp/default-metadata

Introduced In: 9.17

Retrieves the SAML default metadata configuration.

Parameters

Name	Type	In	Required	Description
host	string	query	False	Filter by host
certificate.common_name	string	query	False	Filter by certificate.common_name
certificate.serial_number	string	query	False	Filter by certificate.serial_number • maxLength: 40 • minLength: 1

Name	Type	In	Required	Description
certificate.ca	string	query	False	Filter by certificate.ca • maxLength: 256 • minLength: 1
scope	string	query	False	Filter by scope
fields	array[string]	query	False	Specify the fields to return.

Response

Status: 200, Ok

Name	Type	Description
_links	_links	
certificate	certificate	
host	string	The SAML service provider host.
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.

Example response

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "certificate": {
    "ca": "string",
    "common_name": "cluster1",
    "serial_number": "1506B24A94F566BA"
  },
  "host": "string",
  "scope": "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	

certificate

Name	Type	Description
ca	string	Server certificate issuing certificate authority (CA). This cannot be used with the server certificate common name.
common_name	string	Server certificate common name. This cannot be used with the certificate authority (CA) or serial_number.
serial_number	string	Server certificate serial number. This cannot be used with the server certificate common 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

Name	Type	Description
target	string	The target parameter that caused the error.

Create the SAML default metadata configuration

POST /security/authentication/cluster/saml-sp/default-metadata

Introduced In: 9.17

Creates the SAML default metadata configuration. Note that `common_name` is mutually exclusive with `serial_number` and `ca` in POST requests.

Optional properties

- `certificate`
- `host`

Parameters

Name	Type	In	Required	Description
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202. • Default value: 0 • Max value: 120 • Min value: 0

Request Body

Name	Type	Description
certificate	certificate	
host	string	The SAML service provider host.
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.

Example request

```
{
  "certificate": {
    "ca": "string",
    "common_name": "cluster1",
    "serial_number": "1506B24A94F566BA"
  },
  "host": "string",
  "scope": "string"
}
```

Response

Status: 202, Accepted

Name	Type	Description
job	job_link	

Example response

```
{
  "job": {
    "uuid": "string"
  }
}
```

Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Response

Status: 201, Created

Error

Status: Default

ONTAP Error Response Codes

Error Code	Description
12320794	Invalid host parameter for default metadata generation. The host parameter must be the cluster management interface's IP address. If the cluster management interface is not available, the node management interface's IP address must be used.
12320805	The certificate information provided does not match any installed certificates.
12320806	The certificate information entered does not match any installed certificates.
12320820	No certificate is installed with the specified <code>certificate.ca</code> and <code>certificate.serial</code> .
12320821	No certificate is installed with the specified <code>certificate.common_name</code> .
12320825	SAML configuration already exists. Cannot create the metadata when SAML configuration is already present.
12320831	Default metadata configuration already exists.

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

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

certificate

Name	Type	Description
ca	string	Server certificate issuing certificate authority (CA). This cannot be used with the server certificate common name.
common_name	string	Server certificate common name. This cannot be used with the certificate authority (CA) or serial_number.
serial_number	string	Server certificate serial number. This cannot be used with the server certificate common name.

security_saml_def_metadata

Name	Type	Description
certificate	certificate	
host	string	The SAML service provider host.
scope	string	Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.

job_link

Name	Type	Description
uuid	string	The UUID of the asynchronous job that is triggered by a POST, PATCH, or DELETE operation.

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

Copyright © 2026 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.