



Manage keystores

REST API reference

NetApp

September 09, 2025

Table of Contents

Manage keystores	1
Security key-stores endpoint overview	1
Overview	1
Examples	1
Retrieve keystores	4
Related ONTAP commands	4
Parameters	4
Response	6
Error	7
Definitions	8
Delete an inactive keystore configuration	11
Related ONTAP commands	11
Parameters	12
Response	12
Error	12
Definitions	13
Retrieve keystore configuration details with the specified UUID	14
Related ONTAP commands	14
Parameters	14
Response	14
Error	16
Definitions	17
Enable a keystore configuration	19
Related ONTAP commands	19
Parameters	19
Request Body	20
Response	22
Response	22
Error	22
Definitions	24

Manage keystores

Security key-stores endpoint overview

Overview

A keystore describes a key-manager configuration, specifically the type of key-manager and whether the configuration is currently enabled for the configured SVM.

Examples

Retrieving information for all configured key managers

The following example shows how to retrieve information about all configured key managers.

```
# The API:  
GET /api/security/key-stores  
  
# The call:  
curl -X GET 'https://<mgmt-ip>/api/security/key-stores?fields=*' -H  
'accept: application/hal+json'  
  
# The response:  
{  
  "records": [  
    {  
      "type": "okm",  
      "configuration": {  
        "name": "default",  
        "uuid": "ec8711c9-4e9f-11ef-b477-005056bb677e"  
      },  
      "uuid": "ec8711c9-4e9f-11ef-b477-005056bb677e",  
      "enabled": true,  
      "location": "onboard",  
      "scope": "cluster",  
      "state": "active"  
    },  
    {  
      "type": "kmip",  
      "configuration": {  
        "name": "default",  
        "uuid": "d81f43cd-4e9f-11ef-b477-005056bb677e"  
      },  
      "uuid": "d81f43cd-4e9f-11ef-b477-005056bb677e",  
    }  
  ]  
}
```

```
        "enabled": false,
        "location": "external",
        "scope": "cluster"
    },
    {
        "type": "kmip",
        "configuration": {
            "name": "default",
            "uuid": "7da22185-4ea0-11ef-b477-005056bb677e"
        },
        "uuid": "7da22185-4ea0-11ef-b477-005056bb677e",
        "enabled": true,
        "location": "external",
        "scope": "svm",
        "svm": {
            "name": "vs0",
            "uuid": "3cbe691b-4ea0-11ef-b477-005056bb677e"
        },
        "state": "active"
    }
],
"num_records": 3
}
```

Retrieving a specific keystore by its UUID

The following example shows how to retrieve information about a specific keystore.

```

# The API:
GET /api/security/key-stores/{uuid}

# The call:
curl -X GET 'https://<mgmt-ip>/api/security/key-stores/33421d82-0a8d-11ec-
ae88-005056bb5955?fields=' -H 'accept: application/hal+json'

# The response:
{
  "type": "okm",
  "configuration": {
    "name": "default",
    "uuid": "ec8711c9-4e9f-11ef-b477-005056bb677e",
  },
  "uuid": "ec8711c9-4e9f-11ef-b477-005056bb677e",
  "enabled": true,
  "location": "onboard",
  "scope": "cluster",
  "state": "active"
}

```

Enabling a specific keystore configuration

The following example shows how to enable a specific keystore configuration.

```

# The API:
PATCH /api/security/key-stores/{uuid}

# The call:
curl -X PATCH 'https://<mgmt-ip>/api/security/key-stores/33421d82-0a8d-
11ec-ae88-005056bb5955' -H 'accept: application/hal+json' -d "{
  \"enabled\": true }"

```

Deleting a specific keystore configuration

The following example shows how to delete a specific keystore configuration. Only an inactive configuration can be deleted.

```
# The API:
DELETE /api/security/key-stores/{uuid}

# The call:
curl -X DELETE 'https://<mgmt-ip>/api/security/key-stores/33421d82-0a8d-11ec-ae88-005056bb5955' -H 'accept: application/hal+json'
```

Retrieve keystores

GET /security/key-stores

Introduced In: 9.10

Retrieves keystores.

Related ONTAP commands

- `security key-manager show-key-store`
- `security key-manager keystore show`

Parameters

Name	Type	In	Required	Description
svm.name	string	query	False	Filter by svm.name
svm.uuid	string	query	False	Filter by svm.uuid
uuid	string	query	False	Filter by uuid
type	string	query	False	Filter by type
scope	string	query	False	Filter by scope <ul style="list-style-type: none"> • Introduced in: 9.14
state	string	query	False	Filter by state <ul style="list-style-type: none"> • Introduced in: 9.16
location	string	query	False	Filter by location

Name	Type	In	Required	Description
enabled	boolean	query	False	Filter by enabled <ul style="list-style-type: none"> Introduced in: 9.14
configuration.uuid	string	query	False	Filter by configuration.uuid <ul style="list-style-type: none"> Introduced in: 9.14
configuration.name	string	query	False	Filter by configuration.name <ul style="list-style-type: none"> Introduced in: 9.14
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
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. <ul style="list-style-type: none"> Default value: 1 Max value: 120 Min value: 0
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. <ul style="list-style-type: none"> Default value: 1

Name	Type	In	Required	Description
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[security_keystore]	

Example response

```
{  
  "_links": {  
    "next": {  
      "href": "/api/resourcelink"  
    },  
    "self": {  
      "href": "/api/resourcelink"  
    }  
  },  
  "num_records": 1,  
  "records": [  
    {  
      "configuration": {  
        "_links": {  
          "self": {  
            "href": "/api/resourcelink"  
          }  
        },  
        "name": "default",  
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563434"  
      },  
      "location": "string",  
      "scope": "string",  
      "state": "string",  
      "svm": {  
        "_links": {  
          "self": {  
            "href": "/api/resourcelink"  
          }  
        },  
        "name": "svml1",  
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"  
      },  
      "type": "string",  
      "uuid": "string"  
    }  
  ]  
}
```

Error

Status: Default

ONTAP Error Response Codes

Error Code	Description
13434920	SVM does not exist.

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
next	href	
self	href	

_links

Name	Type	Description
self	href	

configuration

Security keystore object reference.

Name	Type	Description
_links	_links	
name	string	Name of the configuration.
uuid	string	Keystore UUID.

svm

SVM, applies only to SVM-scoped objects.

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.

security_keystore

Name	Type	Description
configuration	configuration	Security keystore object reference.
enabled	boolean	Indicates whether the configuration is enabled.
location	string	Indicates whether the keystore is onboard or external. * 'onboard' - Onboard Key Database * 'external' - External Key Database, including KMIP and Cloud Key Management Systems
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".
state	string	State of the keystore: * 'active' - The key manager is active and serving new and existing keys. * 'mixed' - The key manager has a mixed configuration. New keys can't be created. * 'svm_kek_rekey' - An SVM key encryption key (KEK) rekey is in progress. New keys can't be created. * 'blocked' - The key manager is blocked and cannot serve new and existing keys. * 'switching' - Switching the enabled key manager keystore configuration. Some operations are blocked. * 'initializing' - The key manager is being initialized. All operations are blocked. * 'disabling' - The key manager is being disabled. All operations are blocked.
svm	svm	SVM, applies only to SVM-scoped objects.

Name	Type	Description
type	string	Type of keystore that is configured: * 'okm' - Onboard Key Manager * 'kmip' - External Key Manager * 'akv' - Azure Key Vault Key Management Service * 'gcp' - Google Cloud Platform Key Management Service * 'aws' - Amazon Web Service Key Management Service * 'ikp' - IBM Key Protect Key Management Service
uuid	string	

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.

Delete an inactive keystore configuration

DELETE /security/key-stores/{uuid}

Introduced In: 9.14

Deletes an inactive keystore configuration.

Related ONTAP commands

- `security key-manager keystore delete`

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	

Response

Status: 200, Ok

Error

Status: Default

ONTAP Error Response Codes

Error Code	Description
262155	This operation requires an effective cluster version of 9.14.0 or later.
65538905	The keystore configuration is currently enabled and cannot be deleted.
65538907	The method is not yet supported for deleting the given UUID's type of configuration.
65538908	The specified keystore configuration UUID either does not exist or corresponds to a keystore configuration that is not supported by this operation.
65539521	An effective cluster version of ONTAP 9.16.1 or later is required to delete an inactive key manager on the admin SVM.
65539522	This command does not support disabling key manager configurations with the specified keystore type on the admin SVM.
65539593	Cannot delete an inactive key manager configuration while the keystore is in the switching state.

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 keystore configuration details with the specified UUID

GET /security/key-stores/{uuid}

Introduced In: 9.14

Retrieves details of the keystore configuration with the specified UUID.

Related ONTAP commands

- `security key-manager keystore show`

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	Keystore configuration UUID
fields	array[string]	query	False	Specify the fields to return.

Response

Status: 200, Ok

Name	Type	Description
configuration	configuration	Security keystore object reference.
enabled	boolean	Indicates whether the configuration is enabled.
location	string	Indicates whether the keystore is onboard or external. * 'onboard' - Onboard Key Database * 'external' - External Key Database, including KMIP and Cloud Key Management Systems
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".

Name	Type	Description
state	string	State of the keystore: * 'active' - The key manager is active and serving new and existing keys. * 'mixed' - The key manager has a mixed configuration. New keys can't be created. * 'svm_kek_rekey' - An SVM key encryption key (KEK) rekey is in progress. New keys can't be created. * 'blocked' - The key manager is blocked and cannot serve new and existing keys. * 'switching' - Switching the enabled key manager keystore configuration. Some operations are blocked. * 'initializing' - The key manager is being initialized. All operations are blocked. * 'disabling' - The key manager is being disabled. All operations are blocked.
svm	svm	SVM, applies only to SVM-scoped objects.
type	string	Type of keystore that is configured: * 'okm' - Onboard Key Manager * 'kmip' - External Key Manager * 'akv' - Azure Key Vault Key Management Service * 'gcp' - Google Cloud Platform Key Management Service * 'aws' - Amazon Web Service Key Management Service * 'ikp' - IBM Key Protect Key Management Service
uuid	string	

Example response

```
{  
  "configuration": {  
    "_links": {  
      "self": {  
        "href": "/api/resourcelink"  
      }  
    },  
    "name": "default",  
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563434"  
  },  
  "location": "string",  
  "scope": "string",  
  "state": "string",  
  "svm": {  
    "_links": {  
      "self": {  
        "href": "/api/resourcelink"  
      }  
    },  
    "name": "svml1",  
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"  
  },  
  "type": "string",  
  "uuid": "string"  
}
```

Error

Status: Default

ONTAP Error Response Codes

Error Code	Description
65539523	Internal error. The keymanager_config table is missing.

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	

configuration

Security keystore object reference.

Name	Type	Description
_links	_links	
name	string	Name of the configuration.
uuid	string	Keystore UUID.

svm

SVM, applies only to SVM-scoped objects.

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.

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.

Enable a keystore configuration

PATCH /security/key-stores/{uuid}

Introduced In: 9.14

Enables a keystore configuration

Related ONTAP commands

- `security key-manager keystore enable`

Parameters

Name	Type	In	Required	Description
uuid	string	path	True	Keystore configuration UUID

Name	Type	In	Required	Description
return_timeout	integer	query	False	<p>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.</p> <ul style="list-style-type: none"> • Default value: 1 • Max value: 120 • Min value: 0

Request Body

Name	Type	Description
configuration	configuration	Security keystore object reference.
enabled	boolean	Indicates whether the configuration is enabled.
location	string	Indicates whether the keystore is onboard or external. * 'onboard' - Onboard Key Database * 'external' - External Key Database, including KMIP and Cloud Key Management Systems

Name	Type	Description
state	string	State of the keystore: <ul style="list-style-type: none"> * 'active' - The key manager is active and serving new and existing keys. * 'mixed' - The key manager has a mixed configuration. New keys can't be created. * 'svm_kek_rekey' - An SVM key encryption key (KEK) rekey is in progress. New keys can't be created. * 'blocked' - The key manager is blocked and cannot serve new and existing keys. * 'switching' - Switching the enabled key manager keystore configuration. Some operations are blocked. * 'initializing' - The key manager is being initialized. All operations are blocked. * 'disabling' - The key manager is being disabled. All operations are blocked.
svm	svm	SVM, applies only to SVM-scoped objects.
type	string	Type of keystore that is configured: <ul style="list-style-type: none"> * 'okm' - Onboard Key Manager * 'kmip' - External Key Manager * 'akv' - Azure Key Vault Key Management Service * 'gcp' - Google Cloud Platform Key Management Service * 'aws' - Amazon Web Service Key Management Service * 'ikp' - IBM Key Protect Key Management Service
uuid	string	

Example request

```
{  
  "configuration": {  
    "name": "default",  
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563434"  
  },  
  "location": "string",  
  "state": "string",  
  "svm": {  
    "name": "svml",  
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"  
  },  
  "type": "string",  
  "uuid": "string"  
}
```

Response

Status: 200, Ok

Name	Type	Description
job	job_link	

Example response

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

Response

Status: 202, Accepted

Error

Status: Default

ONTAP Error Response Codes

Error Code	Description
262155	This operation requires an effective cluster version of 9.14.0 or later.
65537605	Failed to establish connectivity with the cloud key management service.
65538908	The specified keystore configuration UUID either does not exist or corresponds to a keystore configuration that is not supported by this operation.
65538909	A value for enabled is required.
65538910	Disabling an enabled configuration through this method is currently not supported.
65539206	The SVM associated with the supplied keystore UUID already has a keystore configuration enabled. This command does not support migrating from configurations of that keystore type".
65539212	Cannot switch the enabled keystore configuration when it is not in the 'active' or 'switching' state.
65539513	An effective cluster version of ONTAP 9.16.1 or later is required to enable an inactive key manager on the admin SVM.
65539514	This command does not support enabling key manager configurations with the specified keystore type on the admin SVM.
65539515	Cannot switch keystore types on the admin SVM. The keystore type for the invalid configuration must be OKM and the enabled configuration must be KMIP, or vice versa.
65539518	Internal error. Cannot find the enabled configuration.
65539520	Cannot enable the Onboard Key Manager on the admin SVM because an inactive Onboard Key Manager already exists on the admin SVM.
65539534	Cannot switch admin SVM Key Manager when system root volumes are present.
65539583	Cannot switch to the Onboard Key Manager when the external key manager has a policy associated with it
65539585	Cannot enable an external key manager on the admin SVM because an inactive external key manager already exists on the admin SVM.

Error Code	Description
65539590	Cannot switch to the Onboard Key Manager if there are more than two NSE-AKs in the cluster.
65539591	Cannot switch to the Onboard Key Manager if there are fewer than two NSE-AKs in the cluster.

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

configuration

Security keystore object reference.

Name	Type	Description
name	string	Name of the configuration.
uuid	string	Keystore UUID.

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
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.

security_keystore

Name	Type	Description
configuration	configuration	Security keystore object reference.
enabled	boolean	Indicates whether the configuration is enabled.
location	string	Indicates whether the keystore is onboard or external. * 'onboard' - Onboard Key Database * 'external' - External Key Database, including KMIP and Cloud Key Management Systems

Name	Type	Description
state	string	<p>State of the keystore:</p> <ul style="list-style-type: none"> * 'active' - The key manager is active and serving new and existing keys. * 'mixed' - The key manager has a mixed configuration. New keys can't be created. * 'svm_kek_rekey' - An SVM key encryption key (KEK) rekey is in progress. New keys can't be created. * 'blocked' - The key manager is blocked and cannot serve new and existing keys. * 'switching' - Switching the enabled key manager keystore configuration. Some operations are blocked. * 'initializing' - The key manager is being initialized. All operations are blocked. * 'disabling' - The key manager is being disabled. All operations are blocked.
svm	svm	SVM, applies only to SVM-scoped objects.
type	string	Type of keystore that is configured: <ul style="list-style-type: none"> * 'okm' - Onboard Key Manager * 'kmip' - External Key Manager * 'akv' - Azure Key Vault Key Management Service * 'gcp' - Google Cloud Platform Key Management Service * 'aws' - Amazon Web Service Key Management Service * 'ikp' - IBM Key Protect Key Management Service
uuid	string	

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 © 2025 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.