



## **Manage key managers**

### **ONTAP 9.6 REST API reference**

NetApp  
August 29, 2024

# Table of Contents

- Manage key managers . . . . . 1
  - Security key-managers endpoint overview . . . . . 1
  - Retrieve key managers . . . . . 15
  - Create a key manager . . . . . 24
  - Delete key managers . . . . . 35
  - Retrieve key managers . . . . . 37
  - Update key managers . . . . . 43

# Manage key managers

## Security key-managers endpoint overview

### Overview

A key manager is a key management solution (software or dedicated hardware) that enables other ONTAP client modules to securely and persistently store keys for various uses. For example, WAFL uses the key management framework to store and retrieve the volume encryption keys that it uses to encrypt/decrypt data on NVE volumes. A key manager can be configured at both cluster scope and SVM, with one key manager allowed per SVM. The key management framework in ONTAP supports two mutually exclusive modes for persisting keys, external and onboard.

When an SVM is configured with external key management, the keys are stored on up to four key servers that are external to the system.

Once external key management is enabled for an SVM, key servers can be added or removed using the `/api/security/key-managers/{uuid}/key-servers` endpoint. See [POST `/security/key-managers/{uuid}/key-servers`] and [DELETE `/security/key-managers/{uuid}/key-servers/{server}`] for more details.

Setting up external key management dictates that the required certificates for securely communicating with the key server are installed prior to configuring the key manager. To install the required client and server\_ca certificates, use the `/api/security/certificates/` endpoint.

See [POST `/security/certificates`], [GET `/security/certificates/uuid`] and [DELETE `/security/certificates/{uuid}`] for more details.

When an SVM is configured with onboard key management, the keys are stored in ONTAP in wrapped format using a key hierarchy created using the salted hash of the passphrase entered when configuring onboard key management. This model fits well for customers who use ONTAP to store their own data.

### Examples

#### Creating an external key manager with 1 key server for a cluster

The example key manager is configured at the cluster-scope with one key server. Note that the UUIDs of the certificates are those that are already installed at the cluster-scope. Note the `return_records=true` query parameter is used to obtain the newly created key manager configuration

```
# The API:
POST /api/security/key-managers

# The call:
curl -X POST 'https://<mgmt-ip>/api/security/key-
managers?return_records=true' -H 'accept: application/hal+json' -d "{
\"external\": { \"client_certificate\": { \"uuid\": \"5fb1701a-d922-11e8-
bfe8-005056bb017d\" }, \"server_ca_certificates\": [ { \"uuid\":
\"827d7d31-d6c8-11e8-b5bf-005056bb017d\" } ],\"servers\": [ { \"server\":
\"10.225.89.33:5696\" } ] } }"

# The response:
{
  "num_records": 1,
  "records": [
    {
      "uuid": "815e9462-dc57-11e8-9b2c-005056bb017d",
      "external": {
        "client_certificate": {
          "uuid": "5fb1701a-d922-11e8-bfe8-005056bb017d"
        },
        "server_ca_certificates": [
          {
            "uuid": "827d7d31-d6c8-11e8-b5bf-005056bb017d"
          }
        ],
        "servers": [
          {
            "server": "10.225.89.33:5696"
          }
        ]
      },
      "_links": {
        "self": {
          "href": "/api/security/key-managers/815e9462-dc57-11e8-9b2c-
005056bb017d"
        }
      }
    }
  ]
}
```

## Creating an external key manager with 1 key server for an SVM

The example key manager is configured at the SVM-scope with one key server. Note that the UUIDs of the certificates are those that are already installed in that SVM. Note the *return\_records=true* query parameter is used to obtain the newly created key manager configuration

```

# The API:
POST /api/security/key-managers

# The call:
curl -X POST 'https://<mgmt-ip>/api/security/key-
managers?return_records=true' -H 'accept: application/hal+json' -d "{
 \"svm\": { \"uuid\": \"216e6c26-d6c6-11e8-b5bf-005056bb017d\" },
 \"external\": { \"client_certificate\": { \"uuid\": \"91dcaf7c-dbbd-11e8-
9b2c-005056bb017d\" }, \"server_ca_certificates\": [ { \"uuid\":
 \"a4d4b8ba-dbbd-11e8-9b2c-005056bb017d\" } ], \"servers\": [ { \"server\":
 \"10.225.89.34:5696\" } ] } }"

# The response:
{
  "num_records": 1,
  "records": [
    {
      "uuid": "80af63f2-dbbf-11e8-9b2c-005056bb017d",
      "svm": {
        "uuid": "216e6c26-d6c6-11e8-b5bf-005056bb017d"
      },
      "external": {
        "client_certificate": {
          "uuid": "91dcaf7c-dbbd-11e8-9b2c-005056bb017d"
        },
        "server_ca_certificates": [
          {
            "uuid": "a4d4b8ba-dbbd-11e8-9b2c-005056bb017d"
          }
        ],
        "servers": [
          {
            "server": "10.225.89.34:5696"
          }
        ]
      },
      "_links": {
        "self": {
          "href": "/api/security/key-managers/80af63f2-dbbf-11e8-9b2c-
005056bb017d"
        }
      }
    }
  ]
}

```

## Creating an onboard key manager for a cluster

The following example shows how to create an onboard key manager for a cluster with the onboard key manager configured at the cluster-scope.

```
# The API:
POST /api/security/key-managers

# The call:
curl -X POST 'https://<mgmt-ip>/api/security/key-managers' -H 'accept:
application/hal+json' -d '{ "onboard": { "passphrase": "passphrase" } }'
```

## Retrieving the key manager configurations for all clusters and SVMs

The following example shows how to retrieve all configured key managers along with their configurations.

```
# The API:
GET /api/security/key-managers

# The call:
curl -X GET 'https://<mgmt-ip>/api/security/key-managers?fields=*' -H
'accept: application/hal+json'

# The response:
{
  "records": [
    {
      "uuid": "2345f09c-d6c9-11e8-b5bf-005056bb017d",
      "scope": "svm",
      "svm": {
        "uuid": "0f22f8f3-d6c6-11e8-b5bf-005056bb017d",
        "name": "vs0"
      },
      "external": {
        "client_certificate": {
          "uuid": "4cb15482-d6c8-11e8-b5bf-005056bb017d",
          "_links": {
            "self": {
              "href": "/api/security/certificates/4cb15482-d6c8-11e8-b5bf-
005056bb017d/"
            }
          }
        }
      },
      "server_ca_certificates": [
```

```

    {
      "uuid": "8a17c858-d6c8-11e8-b5bf-005056bb017d",
      "_links": {
        "self": {
          "href": "/api/security/certificates/8a17c858-d6c8-11e8-b5bf-005056bb017d/"
        }
      }
    }
  ],
  "servers": [
    {
      "server": "10.2.30.4:5696",
      "timeout": 25,
      "username": "",
      "_links": {
        "self": {
          "href": "/api/security/key-managers/2345f09c-d6c9-11e8-b5bf-005056bb017d/key-servers/10.2.30.4:5696/"
        }
      }
    },
    {
      "server": "vs0.local1:3678",
      "timeout": 25,
      "username": "",
      "_links": {
        "self": {
          "href": "/api/security/key-managers/2345f09c-d6c9-11e8-b5bf-005056bb017d/key-servers/vs0.local1:3678/"
        }
      }
    }
  ]
},
"_links": {
  "self": {
    "href": "/api/security/key-managers/2345f09c-d6c9-11e8-b5bf-005056bb017d"
  }
}
},
{
  "uuid": "815e9462-dc57-11e8-9b2c-005056bb017d",
  "scope": "cluster",
  "external": {

```



```
"client_certificate": {
  "uuid": "5fb1701a-d922-11e8-bfe8-005056bb017d",
  "_links": {
    "self": {
      "href": "/api/security/certificates/5fb1701a-d922-11e8-bfe8-005056bb017d/"
    }
  }
},
"server_ca_certificates": [
  {
    "uuid": "827d7d31-d6c8-11e8-b5bf-005056bb017d",
    "_links": {
      "self": {
        "href": "/api/security/certificates/827d7d31-d6c8-11e8-b5bf-005056bb017d/"
      }
    }
  }
],
"servers": [
  {
    "server": "10.225.89.33:5696",
    "timeout": 25,
    "username": "",
    "_links": {
      "self": {
        "href": "/api/security/key-managers/815e9462-dc57-11e8-9b2c-005056bb017d/key-servers/10.225.89.33:5696/"
      }
    }
  }
],
"_links": {
  "self": {
    "href": "/api/security/key-managers/815e9462-dc57-11e8-9b2c-005056bb017d"
  }
}
],
"num_records": 2,
"_links": {
  "self": {
    "href": "/api/security/key-managers?fields="
  }
}
```

```
}  
}  
}
```

## Retrieving a specific key manager configuration

The following example shows how to retrieve a specific key manager configuration.

```
# The API:  
GET /api/security/key-managers/{uuid}  
  
# The call:  
curl -X GET 'https://<mgmt-ip>/api/security/key-managers/<uuid>?fields=*'  
-H 'accept: application/hal+json'  
  
# The response:  
{  
  "uuid": "2345f09c-d6c9-11e8-b5bf-005056bb017d",  
  "scope": "svm",  
  "svm": {  
    "uuid": "0f22f8f3-d6c6-11e8-b5bf-005056bb017d",  
    "name": "vs0"  
  },  
  "external": {  
    "client_certificate": {  
      "uuid": "4cb15482-d6c8-11e8-b5bf-005056bb017d",  
      "_links": {  
        "self": {  
          "href": "/api/security/certificates/4cb15482-d6c8-11e8-b5bf-  
005056bb017d/"  
        }  
      }  
    },  
    "server_ca_certificates": [  
      {  
        "uuid": "8a17c858-d6c8-11e8-b5bf-005056bb017d",  
        "_links": {  
          "self": {  
            "href": "/api/security/certificates/8a17c858-d6c8-11e8-b5bf-  
005056bb017d/"  
          }  
        }  
      }  
    ]  
  },  
}
```

```

"servers": [
  {
    "server": "10.2.30.4:5696",
    "timeout": 25,
    "username": "",
    "_links": {
      "self": {
        "href": "/api/security/key-managers/2345f09c-d6c9-11e8-b5bf-
005056bb017d/key-servers/10.2.30.4:5696/"
      }
    }
  },
  {
    "server": "vs0.local1:3678",
    "timeout": 25,
    "username": "",
    "_links": {
      "self": {
        "href": "/api/security/key-managers/2345f09c-d6c9-11e8-b5bf-
005056bb017d/key-servers/vs0.local1:3678/"
      }
    }
  }
],
"_links": {
  "self": {
    "href": "/api/security/key-managers/2345f09c-d6c9-11e8-b5bf-
005056bb017d"
  }
}
}

```

## Updating the configuration of an external key manager

The following example shows how to update the server-ca configuration of an external key manager.

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

# The call:
curl -X PATCH 'https://<mgmt-ip>/api/security/key-managers/<uuid>?' -H
'accept: application/hal+json' -d "{ \"external\": {
  \"server_ca_certificates\": [ { \"uuid\": \"23b05c58-d790-11e8-b5bf-
005056bb017d\" } ] } }"
```

---

### Updating the passphrase of an onboard key manager

The following example shows how to update the passphrase of a given key manager.

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

# The call:
curl -X PATCH 'https://<mgmt-ip>/api/security/key-managers/<uuid>?' -H
'accept: application/hal+json' -d "{ \"onboard\": {
  \"existing_passphrase\": \"existing_passphrase\", \"passphrase\":
  \"new_passphrase\" } }"
```

---

### Deleting a configured key manager

The following example shows how to delete a key manager given its UUID.

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

# The call:
curl -X DELETE 'https://<mgmt-ip>/api/security/key-managers/<uuid>?' -H
'accept: application/hal+json'
```

---

### Adding a key server to an external key manager

The following example shows how to add a key server to an external key manager.

```
# The API:
POST /api/security/key-managers/{uuid}/key-servers

# The call:
curl -X POST 'https://<mgmt-ip>/api/security/key-managers/<uuid>/key-
servers?return_records=true' -H 'accept: application/hal+json' -d "{
  \"server\": \"10.225.89.34:5696\" }"

# The response:
{
  "num_records": 1,
  "records": [
    {
      "server": "10.225.89.34:5696",
      "_links": {
        "self": {
          "href": "/api/security/key-managers/43e0c191-dc5c-11e8-9b2c-
005056bb017d/key-servers/10.225.89.34%3A5696"
        }
      }
    }
  ]
}
```

---

## Adding 2 key servers to an external key manager

The following example shows how to add 2 key servers to an external key manager. Note that the *records* property is used to add multiple key servers to the key manager in a single API call.

```
# The API:
POST /api/security/key-managers/{uuid}/key-servers

# The call:
curl -X POST 'https://<mgmt-ip>/api/security/key-managers/<uuid>/key-
servers?return_records=true' -H 'accept: application/hal+json' -d "{
\"records\": [ { \"server\": \"10.225.89.34:5696\" }, { \"server\":
\"10.225.89.33:5696\" } ] }"

# The response:
{
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/security/key-managers/43e0c191-dc5c-11e8-9b2c-
005056bb017d/key-servers/"
        }
      }
    }
  ]
}
```

---

### Retrieving all the key servers configured in an external key manager

The following example shows how to retrieve all key servers configured in an external key manager.

```
# The API:
GET /api/security/key-managers/{uuid}/key-servers

# The call:
curl -X GET 'https://<mgmt-ip>/api/security/key-managers/<uuid>/key-servers?fields=*' -H 'accept: application/hal+json'

# The response:
{
  "records": [
    {
      "uuid": "43e0c191-dc5c-11e8-9b2c-005056bb017d",
      "server": "10.225.89.33:5696",
      "timeout": 25,
      "username": "",
      "_links": {
        "self": {
          "href": "/api/security/key-managers/43e0c191-dc5c-11e8-9b2c-005056bb017d/key-servers/10.225.89.33%3A5696"
        }
      }
    },
    {
      "uuid": "43e0c191-dc5c-11e8-9b2c-005056bb017d",
      "server": "10.225.89.34:5696",
      "timeout": 25,
      "username": "",
      "_links": {
        "self": {
          "href": "/api/security/key-managers/43e0c191-dc5c-11e8-9b2c-005056bb017d/key-servers/10.225.89.34%3A5696"
        }
      }
    }
  ],
  "num_records": 2,
  "_links": {
    "self": {
      "href": "/api/security/key-managers/43e0c191-dc5c-11e8-9b2c-005056bb017d/key-servers?fields=*"
    }
  }
}
```

## Retrieving a specific key server configured in an external key manager

The following example shows how to retrieve a specific key server configured in an external key manager.

```
# The API:
GET /api/security/key-managers/{uuid}/key-servers/{server}

# The call:
curl -X GET 'https://<mgmt-ip>/api/security/key-managers/<uuid>/key-servers/{server}?fields=*' -H 'accept: application/hal+json'

# The response:
{
  "uuid": "43e0c191-dc5c-11e8-9b2c-005056bb017d",
  "server": "10.225.89.34:5696",
  "timeout": 25,
  "username": "",
  "_links": {
    "self": {
      "href": "/api/security/key-managers/43e0c191-dc5c-11e8-9b2c-005056bb017d/key-servers/10.225.89.34:5696"
    }
  }
}
```

---

## Updating a specific key server configuration configured in an external key manager

The following example shows how to update a specific key server configured in an external key manager.

```
# The API:
PATCH /api/security/key-managers/{uuid}/key-servers/{server}

# The call:
curl -X PATCH 'https://<mgmt-ip>/api/security/key-managers/<uuid>/key-servers/{server}' -H 'accept: application/hal+json' -d '{"timeout": 45}'
```

---

## Deleting a key server from an external key manager

The following example shows how to delete a key server from an external key manager.



```
# The API:
DELETE /api/security/key-managers/{uuid}/key-servers/{server}

# The call:
curl -X DELETE 'https://<mgmt-ip>/api/security/key-managers/<uuid>/key-servers/{server}' -H 'accept: application/hal+json'
```

## Retrieve key managers

GET /security/key-managers

Retrieves key managers.

### Related ONTAP commands

- `security key-manager show-keystore`
- `security key-manager external show`

### Learn more

- [DOC /security/key-managers](#)

### Parameters

Name	Type	In	Required	Description
onboard.enabled	boolean	query	False	Filter by onboard.enabled
external.server_ca_certificates.uuid	string	query	False	Filter by external.server_ca_certificates.uuid
external.client_certificate.uuid	string	query	False	Filter by external.client_certificate.uuid
external.servers.server	string	query	False	Filter by external.servers.server
external.servers.timeout	integer	query	False	Filter by external.servers.timeout

Name	Type	In	Required	Description
external.servers.user name	string	query	False	Filter by external.servers.use rname
uuid	string	query	False	Filter by uuid
svm.uuid	string	query	False	Filter by svm.uuid
svm.name	string	query	False	Filter by svm.name
scope	string	query	False	Filter by scope
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.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned.
order_by	array[string]	query	False	Order results by specified fields and optional [asc

## Response

```
Status: 200, Ok
```

Name	Type	Description
_links	<a href="#">_links</a>	
num_records	integer	Number of records
records	array[ <a href="#">security_key_manager</a> ]	

## Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "external": {
        "client_certificate": {
          "_links": {
            "self": {
              "href": "/api/resourcelink"
            }
          },
          "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
        },
        "server_ca_certificates": [
          {
            "_links": {
              "self": {
                "href": "/api/resourcelink"
              }
            },
            "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
          }
        ],
        "servers": [
          {
            "_links": {
              "self": {
                "href": "/api/resourcelink"
              }
            },
            "server": "keyserver1.com:5698",
            "timeout": 60,
          }
        ]
      }
    }
  ]
}
```

```

        "username": "username"
    }
  ]
},
"onboard": {
  "existing_passphrase": "The cluster password of length 32-256
ASCII characters.",
  "passphrase": "The cluster password of length 32-256 ASCII
characters."
},
"scope": "string",
"svm": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "name": "svm1",
  "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
},
"uuid": "string"
}
]
}

```

## Error

Status: Default, Error

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
next	<a href="#">href</a>	
self	<a href="#">href</a>	

\_links

Name	Type	Description
self	<a href="#">href</a>	

client\_certificate

Client certificate

Name	Type	Description
_links	<a href="#">_links</a>	
uuid	string	Certificate UUID

server\_ca\_certificates

Security certificate object reference

Name	Type	Description
_links	<a href="#">_links</a>	
uuid	string	Certificate UUID

key\_server\_readcreate

Name	Type	Description
_links	<a href="#">_links</a>	
server	string	External key server for key management. If no port is provided, a default port of 5696 is used.

Name	Type	Description
timeout	integer	I/O timeout in seconds for communicating with the key server.
username	string	Username credentials for connecting with the key server.

external

Configures external key management

Name	Type	Description
client_certificate	<a href="#">client_certificate</a>	Client certificate
server_ca_certificates	array[ <a href="#">server_ca_certificates</a> ]	The UUIDs of the server CA certificates already installed in the cluster or SVM. The array of certificates are common for all the key servers per SVM.
servers	array[ <a href="#">key_server_readcreate</a> ]	The set of external key servers.

onboard

Configures onboard key management. After configuring onboard key management, save the encrypted configuration data in a safe location so that you can use it if you need to perform a manual recovery operation.

Name	Type	Description
enabled	boolean	Is the onboard key manager enabled?
existing_passphrase	string	The cluster-wide passphrase. This is not audited.
passphrase	string	The cluster-wide passphrase. This is not audited.

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
_links	<a href="#">_links</a>	



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

#### security\_key\_manager

Name	Type	Description
_links	<a href="#">_links</a>	
external	<a href="#">external</a>	Configures external key management
onboard	<a href="#">onboard</a>	Configures onboard key management. After configuring onboard key management, save the encrypted configuration data in a safe location so that you can use it if you need to perform a manual recovery operation.
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".
svm	<a href="#">svm</a>	SVM, applies only to SVM-scoped objects.
uuid	string	

#### error\_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

#### error

Name	Type	Description
arguments	array[ <a href="#">error_arguments</a> ]	Message arguments
code	string	Error code
message	string	Error message

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

## Create a key manager

POST /security/key-managers

Creates a key manager.

### Required properties

- `svm.uuid` or `svm.name` - Existing SVM in which to create a key manager.
- `external.client_certificate` - Client certificate. Required only when creating an external key manager.
- `external.server_ca_certificates` - Server CA certificates. Required only when creating an external key manager.
- `external.servers.server` - Key servers. Required only when creating an external key manager.
- `onboard.passphrase` - Cluster-wide passphrase. Required only when creating an onboard key manager.

### Related ONTAP commands

- `security key-manager external enable`
- `security key-manager onboard enable`

### Learn more

- [DOC /security/key-managers](#)

### Request Body

Name	Type	Description
<code>_links</code>	<code>_links</code>	
<code>external</code>	<code>external</code>	Configures external key management
<code>onboard</code>	<code>onboard</code>	Configures onboard key management. After configuring onboard key management, save the encrypted configuration data in a safe location so that you can use it if you need to perform a manual recovery operation.

Name	Type	Description
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".
svm	svm	SVM, applies only to SVM-scoped objects.
uuid	string	

## Example request

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "external": {
    "client_certificate": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    },
    "server_ca_certificates": [
      {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      }
    ],
    "servers": [
      {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "server": "keyserver1.com:5698",
        "timeout": 60,
        "username": "username"
      }
    ]
  },
  "onboard": {
    "existing_passphrase": "The cluster password of length 32-256 ASCII characters.",
    "passphrase": "The cluster password of length 32-256 ASCII characters."
  },
}
```

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

## Response

Status: 201, Created

Name	Type	Description
<a href="#">_links</a>	<a href="#">_links</a>	
num_records	integer	Number of records
records	array[ <a href="#">security_key_manager</a> ]	

## Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "external": {
        "client_certificate": {
          "_links": {
            "self": {
              "href": "/api/resourcelink"
            }
          },
          "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
        },
        "server_ca_certificates": [
          {
            "_links": {
              "self": {
                "href": "/api/resourcelink"
              }
            },
            "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
          }
        ],
        "servers": [
          {
            "_links": {
              "self": {
                "href": "/api/resourcelink"
              }
            },
            "server": "keyserver1.com:5698",
            "timeout": 60,

```

```

        "username": "username"
    }
  ]
},
"onboard": {
  "existing_passphrase": "The cluster password of length 32-256
ASCII characters.",
  "passphrase": "The cluster password of length 32-256 ASCII
characters."
},
"scope": "string",
"svm": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "name": "svm1",
  "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
},
"uuid": "string"
}
]
}

```

## Error

Status: Default

### ONTAP Error Response Codes

Error Code	Description
65536822	Multitenant key management is not supported in the current cluster version.
65536823	The SVM has key manager already configured.
65536878	External key management cannot be configured as one or more volume encryption keys of the SVM are stored in cluster key management server.
65536824	Multitenant key management is not supported in MetroCluster configurations.
65536038	A maximum of 4 active key servers are allowed.

Error Code	Description
65536876	External key management requires client and server CA certificates installed and with one or more key servers provided.
65536920	Onboard key manager passphrase length is incorrect.
65536871	Duplicate key management servers exist.
65536834	Failed to get existing key-server details for the SVM.
65536870	Key management servers already configured.
65536821	Certificate is not installed.
65536852	Failed to query supported KMIP protocol versions.
65536895	External key manager cannot be configured since this cluster is part of a MetroCluster configuration and the partner site of this MetroCluster configuration has onboard key manager configured.
65536916	Onboard key management is only supported for an admin SVM.
65536906	Onboard key management has already been configured at the partner site. Use the CLI to sync the onboard key management with the same passphrase.
65536907	Onboard key management is already configured. Use the CLI to sync any nodes with onboard key management configuration.
65536508	The platform does not support data at rest encryption.
65536310	Failed to setup onboard key management because the MetroCluster peer is unhealthy.
65536900	Onboard key management cannot be configured because this cluster is part of a MetroCluster configuration and the partner site has the external key manager configured.
65536903	Onboard key management has failed to configure on some nodes in the cluster. Use the CLI to sync the onboard key management configuration on failed nodes.
65536214	Failed to generate cluster key encryption key.
65536216	Failed to add cluster key encryption key.
66060338	Failed to establish secure connection for a key management server due to incorrect server_ca certificates.
66060339	Failed to establish secure connection for a key management server due to incorrect client certificates.
66060340	Failed to establish secure connection for a key management server due to Cryptsoft error.



Error Code	Description
66060341	Failed to establish secure connection for a key management server due to network configuration issues.

Name	Type	Description
error	<a href="#">error</a>	

### 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	<a href="#">href</a>	

client\_certificate

Client certificate

Name	Type	Description
_links	<a href="#">_links</a>	
uuid	string	Certificate UUID

server\_ca\_certificates

Security certificate object reference

Name	Type	Description
_links	<a href="#">_links</a>	
uuid	string	Certificate UUID

key\_server\_readcreate

Name	Type	Description
_links	<a href="#">_links</a>	
server	string	External key server for key management. If no port is provided, a default port of 5696 is used.
timeout	integer	I/O timeout in seconds for communicating with the key server.
username	string	Username credentials for connecting with the key server.

external

Configures external key management

Name	Type	Description
client_certificate	<a href="#">client_certificate</a>	Client certificate
server_ca_certificates	array[ <a href="#">server_ca_certificates</a> ]	The UUIDs of the server CA certificates already installed in the cluster or SVM. The array of certificates are common for all the key servers per SVM.
servers	array[ <a href="#">key_server_readcreate</a> ]	The set of external key servers.

onboard

Configures onboard key management. After configuring onboard key management, save the encrypted configuration data in a safe location so that you can use it if you need to perform a manual recovery operation.

Name	Type	Description
enabled	boolean	Is the onboard key manager enabled?
existing_passphrase	string	The cluster-wide passphrase. This is not audited.
passphrase	string	The cluster-wide passphrase. This is not audited.

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
<a href="#">_links</a>	<a href="#">_links</a>	
name	string	The name of the SVM.
uuid	string	The unique identifier of the SVM.

security\_key\_manager

Name	Type	Description
<a href="#">_links</a>	<a href="#">_links</a>	

Name	Type	Description
external	<a href="#">external</a>	Configures external key management
onboard	<a href="#">onboard</a>	Configures onboard key management. After configuring onboard key management, save the encrypted configuration data in a safe location so that you can use it if you need to perform a manual recovery operation.
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".
svm	<a href="#">svm</a>	SVM, applies only to SVM-scoped objects.
uuid	string	

#### \_links

Name	Type	Description
next	<a href="#">href</a>	
self	<a href="#">href</a>	

#### error\_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

#### error

Name	Type	Description
arguments	array[ <a href="#">error_arguments</a> ]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

# Delete key managers

DELETE /security/key-managers/{uuid}

Deletes a key manager.

## Related ONTAP commands

- security key-manager external disable
- security key-manager onboard disable

## Learn more

- [DOC /security/key-managers](#)

## Parameters

Name	Type	In	Required	Description
uuid	string	path	True	

## Response

Status: 200, Ok

## Error

Status: Default

## ONTAP Error Response Codes

Error Code	Description
65536822	Multitenant key management is not supported in the current cluster version.
65536828	External key management is not enabled for the SVM.
65536242	One or more Storage Encryption devices are assigned an authentication key.
65536813	Encrypted kernel core files found.
65536817	Failed to determine if key manager is safe to disable.
65536827	Failed to determine if the SVM has any encrypted volumes.
65536867	Encrypted volumes are found for the SVM.
65536239	Encrypted volumes are found for the SVM.

Error Code	Description
196608301	Failed to determine the type of encryption.
196608305	NAE aggregates are found in the cluster.
65536242	One or more Storage Encryption devices are assigned an authentication key.
65536800	Failed to lookup onboard keys.
65536208	Failed to delete the SVM Key ID.
65536233	Internal error. Deletion of km_wrapped_kdb key database has failed for onboard key management.
65536234	Internal error. Deletion of cluster_kdb key database has failed for onboard key management.

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

error\_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

error

Name	Type	Description
arguments	array[ <a href="#">error_arguments</a> ]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

## Retrieve key managers

GET /security/key-managers/{uuid}

Retrieves key managers.

### Related ONTAP commands

- `security key-manager show-keystore`
- `security key-manager external show`

### Learn more

- [DOC /security/key-managers](#)

### Parameters

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

## Response

Status: 200, Ok

Name	Type	Description
_links	<a href="#">_links</a>	
external	<a href="#">external</a>	Configures external key management
onboard	<a href="#">onboard</a>	Configures onboard key management. After configuring onboard key management, save the encrypted configuration data in a safe location so that you can use it if you need to perform a manual recovery operation.
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".
svm	<a href="#">svm</a>	SVM, applies only to SVM-scoped objects.
uuid	string	



## Example response

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "external": {
    "client_certificate": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    },
    "server_ca_certificates": [
      {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      }
    ],
    "servers": [
      {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "server": "keyserver1.com:5698",
        "timeout": 60,
        "username": "username"
      }
    ]
  },
  "onboard": {
    "existing_passphrase": "The cluster password of length 32-256 ASCII characters.",
    "passphrase": "The cluster password of length 32-256 ASCII characters."
  },
}
```

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

## Error

Status: Default, Error

Name	Type	Description
error	<a href="#">error</a>	

## 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	<a href="#">href</a>	

client\_certificate

Client certificate

Name	Type	Description
_links	<a href="#">_links</a>	
uuid	string	Certificate UUID

server\_ca\_certificates

Security certificate object reference

Name	Type	Description
_links	<a href="#">_links</a>	
uuid	string	Certificate UUID

key\_server\_readcreate

Name	Type	Description
_links	<a href="#">_links</a>	
server	string	External key server for key management. If no port is provided, a default port of 5696 is used.
timeout	integer	I/O timeout in seconds for communicating with the key server.
username	string	Username credentials for connecting with the key server.

## external

Configures external key management

Name	Type	Description
client_certificate	<a href="#">client_certificate</a>	Client certificate
server_ca_certificates	array[ <a href="#">server_ca_certificates</a> ]	The UUIDs of the server CA certificates already installed in the cluster or SVM. The array of certificates are common for all the key servers per SVM.
servers	array[ <a href="#">key_server_readcreate</a> ]	The set of external key servers.

## onboard

Configures onboard key management. After configuring onboard key management, save the encrypted configuration data in a safe location so that you can use it if you need to perform a manual recovery operation.

Name	Type	Description
enabled	boolean	Is the onboard key manager enabled?
existing_passphrase	string	The cluster-wide passphrase. This is not audited.
passphrase	string	The cluster-wide passphrase. This is not audited.

## svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
<a href="#">_links</a>	<a href="#">_links</a>	
name	string	The name of the SVM.
uuid	string	The unique identifier of the SVM.

## error\_arguments

Name	Type	Description
code	string	Argument code

Name	Type	Description
message	string	Message argument

error

Name	Type	Description
arguments	array[ <a href="#">error_arguments</a> ]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

## Update key managers

PATCH /security/key-managers/{uuid}

Updates a key manager.

### Related ONTAP commands

- `security key-manager external modify`
- `security key-manager onboard update-passphrase`

### Learn more

- [DOC /security/key-managers](#)

### Parameters

Name	Type	In	Required	Description
uuid	string	path	True	Key manager UUID

### Request Body

Name	Type	Description
_links	<a href="#">_links</a>	
external	<a href="#">external</a>	Configures external key management

Name	Type	Description
onboard	onboard	Configures onboard key management. After configuring onboard key management, save the encrypted configuration data in a safe location so that you can use it if you need to perform a manual recovery operation.
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".
svm	svm	SVM, applies only to SVM-scoped objects.
uuid	string	

## Example request

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "external": {
    "client_certificate": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    },
    "server_ca_certificates": [
      {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      }
    ],
    "servers": [
      {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "server": "keyserver1.com:5698",
        "timeout": 60,
        "username": "username"
      }
    ]
  },
  "onboard": {
    "existing_passphrase": "The cluster password of length 32-256 ASCII characters.",
    "passphrase": "The cluster password of length 32-256 ASCII characters."
  },
}
```

```

"scope": "string",
"svm": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "name": "svm1",
  "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
},
"uuid": "string"
}

```

## Response

Status: 200, Ok

## Error

Status: Default

### ONTAP Error Response Codes

Error Code	Description
65536822	Multitenant key management is not supported in the current cluster version.
65536828	External key management is not enabled for the SVM.
65536821	Certificate is not installed.
65536850	The new client certificate public or private keys are different from the existing client certificate.
65536852	Failed to query supported KMIP protocol versions.
65536917	Updating an onboard passphrase requires both new and existing cluster passphrase.
65536150	New passphrase is same as old passphrase.
65536139	The existing passphrase value provided does not match the configured passphrase.
65536404	Passphrase does not match the accepted length.
65536802	Passphrase does not match the accepted length in common criteria mode.



Error Code	Description
65536408	Passphrase update failed on some nodes.
65536407	Passphrase update failed on some nodes.
65536406	Change of passphrase failed.
66060338	Failed to establish secure connection for a key management server due to incorrect server_ca certificates.
66060339	Failed to establish secure connection for a key management server due to incorrect client certificates.
66060340	Failed to establish secure connection for a key management server due to Cryptsoft error.
66060341	Failed to establish secure connection for a key management server due to network configuration issues.

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	<a href="#">href</a>	

client\_certificate

Client certificate

Name	Type	Description
_links	<a href="#">_links</a>	
uuid	string	Certificate UUID

server\_ca\_certificates

Security certificate object reference

Name	Type	Description
_links	<a href="#">_links</a>	
uuid	string	Certificate UUID

key\_server\_readcreate

Name	Type	Description
_links	<a href="#">_links</a>	
server	string	External key server for key management. If no port is provided, a default port of 5696 is used.
timeout	integer	I/O timeout in seconds for communicating with the key server.
username	string	Username credentials for connecting with the key server.

external

Configures external key management

Name	Type	Description
client_certificate	<a href="#">client_certificate</a>	Client certificate
server_ca_certificates	array[ <a href="#">server_ca_certificates</a> ]	The UUIDs of the server CA certificates already installed in the cluster or SVM. The array of certificates are common for all the key servers per SVM.
servers	array[ <a href="#">key_server_readcreate</a> ]	The set of external key servers.

onboard

Configures onboard key management. After configuring onboard key management, save the encrypted configuration data in a safe location so that you can use it if you need to perform a manual recovery operation.

Name	Type	Description
enabled	boolean	Is the onboard key manager enabled?
existing_passphrase	string	The cluster-wide passphrase. This is not audited.
passphrase	string	The cluster-wide passphrase. This is not audited.

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
<a href="#">_links</a>	<a href="#">_links</a>	
name	string	The name of the SVM.
uuid	string	The unique identifier of the SVM.

security\_key\_manager

Name	Type	Description
<a href="#">_links</a>	<a href="#">_links</a>	

Name	Type	Description
external	<a href="#">external</a>	Configures external key management
onboard	<a href="#">onboard</a>	Configures onboard key management. After configuring onboard key management, save the encrypted configuration data in a safe location so that you can use it if you need to perform a manual recovery operation.
scope	string	Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".
svm	<a href="#">svm</a>	SVM, applies only to SVM-scoped objects.
uuid	string	

#### error\_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

#### error

Name	Type	Description
arguments	array[ <a href="#">error_arguments</a> ]	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.