



Security

ONTAP 9.7 REST API reference

NetApp
May 08, 2024

Table of Contents

Security	1
Security overview	1
Manage security-related operations	1

Security

Security overview

Overview

You can use ONTAP security APIs to manage security settings for the cluster and SVMs.

SAML

Configure the SAML 2.0 SP (Service Provider) protocol inside ONTAP. Doing so redirects the authentication task to a third-party Identity Provider (IDP) that can utilize any number of approaches for multi-factor authentication. After SAML authentication is enabled, all interactive web access (System Manager, SPI) is authenticated via SAML and a third-party IDP.

Manage security-related operations

Security endpoint overview

Overview

This API returns an object 'onboard_key_manager_configurable_status' which details whether the Onboard Key Manager can be configured on the cluster or not.

Examples

Retrieving information about the security configured on the cluster

The following example shows how to retrieve the key manager configuration of the cluster.

```
# The API:
GET /api/security:

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

# The response:
{
  {
    "onboard_key_manager_configurable_status": {
      "supported": "false",
      "message": "Onboard Key Manager cannot be configured on the cluster.
There are no self-encrypting disks in the cluster, and the following nodes
do not support volume granular encryption: ntap-vsim2.",
      "code": 65537300
    },
  },
}
```

'''

```
[[ID5e142aafa89de296b82d5b3bc9190225]]
= Retrieve information about security configured on the cluster
```

```
[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security`#
```

Retrieves information about the security configured on the cluster.

== Learn more

* xref:{relative_path}security_overview.html[DOC /security]

== Parameters

```

[cols=5*,options=header]
|===

|Name
|Type
|In
|Required
|Description

|max_records
|integer
|query
|False
a|Limit the number of records returned.

|return_records
|boolean
|query
|False
a|The default is true for GET calls. When set to false, only the number
of records is returned.

|return_timeout
|integer
|query
|False
a|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.

|order_by
|array[string]
|query
|False
a|Order results by specified fields and optional [asc|desc] direction.
Default direction is 'asc' for ascending.

|fields
|array[string]
|query
|False
a|Specify the fields to return.

```

| ===

== Response

Status: 200, Ok

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|onboard_key_manager_configurable_status
|link:#onboard_key_manager_configurable_status[onboard_key_manager_configurable_status]
a|Indicates whether the Onboard Key Manager can be configured in the cluster.
```

```
|===
```

```
.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "onboard_key_manager_configurable_status": {
    "code": 65537300,
    "message": "No platform support for volume encryption in following nodes - node1, node2."
  }
}
=====

== Error
```

Status: Default, Error

```
[cols=3*,options=header]
|===
|Name
```

```

|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string

```



```

a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#onboard_key_manager_configurable_status]
[.api-collapsible-fifth-title]
onboard_key_manager_configurable_status

Indicates whether the Onboard Key Manager can be configured in the
cluster.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|integer
a|Code corresponding to the status message. Returns a 0 if the Onboard Key
Manager can be configured in the cluster.

|message
|string
a|Reason that Onboard Key Manager cannot be configured in the cluster.

```

```

|supported
|boolean
a|Set to true if the Onboard Key Manager can be configured in the cluster.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code

```

```
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
====
```

```
:leveloffset: -1
```

```
= Manage security-related accounts
```

```
:leveloffset: +1
```

```
[[ID2c7f4a897387bb2c7f171fd1f2f4dc53]]
= Security accounts endpoint overview
```

```
== Overview
```

A valid user account is required to login to and provision, monitor, and manage the cluster. The scope of the management operation can be at the cluster level or at an individual SVM level. There is a need to create user accounts with specific privileges apart from the default user accounts, "admin", for cluster and "vsadmin" for SVM. Custom user accounts can be configured to perform specific (scoped) operations. User accounts can either be created locally (on the Netapp system) or referenced from an external directory server (NIS, LDAP, or Active Directory). Apart from creation, modification, and deletion of a user account, locking and unlocking of a user account or resetting the password (for local

accounts only) is possible.

A user account must be associated with the following before it can become operational:

- . A management application (SSH, HTTP, console, shelf-processor, and such like) for user login. HTTP enables REST API access.
- . Scope - either cluster or SVM.
- . Authentication source - password (local, NIS/LDAP, Active Directory), public/private key pair-based, certificate based.
- . RBAC role - determines what operations are permitted for the user account.

=== Restrictions

A number of internal/restricted account names, such as admin, diag, autosupport, and root cannot be used.

There must be at least one console cluster administrator account. Any attempt to delete the last remaining administrator account fails.

Multi-factor authentication is only possible for SSH application and the only combination possible is password (local or NIS/LDAP) and public key.

All authentication sources are not supported by all applications. You must select a compatible authentication method based on the application. The following types of authentications methods are supported:

|===

Application	Supported Authentication Methods
-------------	----------------------------------

console	
password	

service-processor	
password	

HTTP	
password, domain, nsswitch, certificate	

ONTAPI	
password, domain, nsswitch, certificate	

SSH	
password, publickey (key pair), domain, nsswitch	

|===

NOTE: In this table, "certificate" means security certificate, "domain" means that the user directory server is an external Active Directory, "nsswitch" means the directory server is an external NIS or LDAP server. At login time, the user is authenticated with these external directory servers which must be provisioned separately.

== Examples

=== Creating a cluster-scoped user account

Specify the user account name, role name, and the tuples (of application and authentication methods) in the body of the POST request. The owner.uuid or owner.name are not required to be specified for a cluster-scoped user account.

NOTE: Each entry in the applications array must be for a different application.

The API:

POST "/api/security/accounts"

The call to create a cluster user account with applications ssh, http and password authentication scheme:

```
curl -X POST "https://<mgmt-ip>/api/security/accounts" -d
'{"name":"cluster_user1","applications":[{"application":"ssh","authentication_methods":["password"],"second_authentication_method":"none"}, {"application":"http","authentication_methods":["password"]}], "role":"admin","password":"p@ssw@rd123"}'
```

Note: The password is an optional parameter for creation and can be set later using a PATCH request. See the examples for modification of user account or password.

=== Creating an SVM-scoped user account

For an SVM-scoped account, specify either the SVM name as the owner.name or SVM uuid as the owner.uuid along with other parameters for the user account. These indicate the SVM for which the user account is being created and can be obtained from the response body of GET performed on the `_/api/svm/svms_` API.

The API:

POST "/api/security/accounts"

```
# The call:
curl -X POST "https://<mgmt-ip>/api/security/accounts" -d
'{"owner":{"uuid":"aaef7c38-4bd3-11e9-b238-0050568e2e25"},"name":"svm_user1","applications":[{"application":"ssh","authentication_methods":["password"],"second_authentication_method":"none"}],"role":"vsadmin","password":"p@ssw@rd123"}'
```

=== Retrieving the configured user accounts

Use the following API to retrieve all of the user accounts or a filtered list of user accounts (by name, for a specific SVM, and so on).

```
# The API:
GET "/api/security/accounts"
```

The call to retrieve all the user accounts configured in the cluster:

```
curl -X GET "https://<mgmt-ip>/api/security/accounts"
```

The response:

```
{
  "records": [
    {
      "owner": {
        "uuid": "2903de6f-4bd2-11e9-b238-0050568e2e25",
        "name": "cluster1",
        "_links": {
          "self": {
            "href": "/api/svm/svms/2903de6f-4bd2-11e9-b238-0050568e2e25"
          }
        }
      },
      "name": "admin",
      "_links": {
        "self": {
          "href": "/api/security/accounts/2903de6f-4bd2-11e9-b238-0050568e2e25/admin"
        }
      }
    },
    {
      "owner": {
        "uuid": "2903de6f-4bd2-11e9-b238-0050568e2e25",
```

```

    "name": "cluster1",
    "_links": {
      "self": {
        "href": "/api/svm/svms/2903de6f-4bd2-11e9-b238-0050568e2e25"
      }
    }
  },
  "name": "autosupport",
  "_links": {
    "self": {
      "href": "/api/security/accounts/2903de6f-4bd2-11e9-b238-0050568e2e25/autosupport"
    }
  }
},
{
  "owner": {
    "uuid": "2903de6f-4bd2-11e9-b238-0050568e2e25",
    "name": "cluster1",
    "_links": {
      "self": {
        "href": "/api/svm/svms/2903de6f-4bd2-11e9-b238-0050568e2e25"
      }
    }
  },
  "name": "cluster_user1",
  "_links": {
    "self": {
      "href": "/api/security/accounts/2903de6f-4bd2-11e9-b238-0050568e2e25/cluster_user1"
    }
  }
},
{
  "owner": {
    "uuid": "aaef7c38-4bd3-11e9-b238-0050568e2e25",
    "name": "svm1",
    "_links": {
      "self": {
        "href": "/api/svm/svms/aaef7c38-4bd3-11e9-b238-0050568e2e25"
      }
    }
  },
  "name": "svm_user1",
  "_links": {
    "self": {

```

```

        "href": "/api/security/accounts/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_user1"
    }
}
},
{
    "owner": {
        "uuid": "aaef7c38-4bd3-11e9-b238-0050568e2e25",
        "name": "svml",
        "_links": {
            "self": {
                "href": "/api/svm/svms/aaef7c38-4bd3-11e9-b238-0050568e2e25"
            }
        }
    },
    "name": "vsadmin",
    "_links": {
        "self": {
            "href": "/api/security/accounts/aaef7c38-4bd3-11e9-b238-0050568e2e25/vsadmin"
        }
    }
}
],
"num_records": 5,
"_links": {
    "self": {
        "href": "/api/security/accounts"
    }
}
}
}

```

```

# The scoped call to retrieve the configured cluster-scoped user accounts:
curl -X GET "https://<mgmt-ip>/api/security/accounts/?scope=cluster"

```

```

# The scoped call to retrieve the configured SVM-scoped user accounts:
curl -X GET "https://<mgmt-ip>/api/security/accounts/?scope=svm"

```

```

# The scoped call to retrieve the user accounts configured for the SVM
"svml":
curl -X GET "https://<mgmt-ip>/api/security/accounts/?owner.name=svml"

```

```

# The scoped call to retrieve the user accounts configured with the
"admin" role:
curl -X GET "https://<mgmt-ip>/api/security/accounts/?role=admin"
----

```



```
[[IDca5d287ef6b3cb1c73d1683aa694f572]]  
= Retrieve user accounts in the cluster
```

```
[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-  
block]#`/security/accounts`#
```

Retrieves a list of user accounts in the cluster.

== Related ONTAP commands

* `security login show`

== Learn more

* xref:{relative_path}security_accounts_endpoint_overview.html[DOC
/security/accounts]

== Parameters

```
[cols=5*,options=header]  
|===
```

```
|Name  
|Type  
|In  
|Required  
|Description
```

```
|owner.uuid  
|string  
|query  
|False  
a|Filter by owner.uuid
```

```
|owner.name  
|string  
|query  
|False  
a|Filter by owner.name
```

```
|scope
|string
|query
|False
a|Filter by scope
```

```
|role.name
|string
|query
|False
a|Filter by role.name
```

```
|applications.authentication_methods
|string
|query
|False
a|Filter by applications.authentication_methods
```

```
|applications.application
|string
|query
|False
a|Filter by applications.application
```

```
|applications.second_authentication_method
|string
|query
|False
a|Filter by applications.second_authentication_method
```

```
|comment
|string
|query
|False
a|Filter by comment
```

```
|locked
|boolean
|query
```

```

|False
a|Filter by locked

|name
|string
|query
|False
a|Filter by name

|fields
|array[string]
|query
|False
a|Specify the fields to return.

|max_records
|integer
|query
|False
a|Limit the number of records returned.

|return_records
|boolean
|query
|False
a|The default is true for GET calls. When set to false, only the number
of records is returned.

|return_timeout
|integer
|query
|False
a|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.

|order_by
|array[string]
|query
|False

```

a|Order results by specified fields and optional [asc|desc] direction.
Default direction is 'asc' for ascending.

|===

== Response

Status: 200, Ok

[cols=3*,options=header]

|===

|Name

|Type

|Description

|_links

|link:#_links[_links]

a|

|num_records

|integer

a|Number of records

|records

|array[link:#account[account]]

a|

|===

.Example response

[%collapsible%closed]

====

[source,json,subs=+macros]

{

 "_links": {

 "next": {

 "href": "/api/resourcelink"

 },

 "self": {

 "href": "/api/resourcelink"

 }

 },

 "records": {

 "_links": {

```

    "self": {
      "href": "/api/resourcelink"
    }
  },
  "applications": {
    "application": "console",
    "authentication_methods": {
    },
    "second_authentication_method": "none"
  },
  "comment": "string",
  "name": "joe.smith",
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "role": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "admin"
  },
  "scope": "cluster"
}
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error

```

```

|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

```

```

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|next
|link:#href[href]
a|

|self
|link:#href[href]
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#account_application]
[.api-collapsible-fifth-title]
account_application

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```
|application
|string
a|Applications
```

```
|authentication_methods
|array[string]
a|
```

```
|second_authentication_method
|string
a|An optional additional authentication method for MFA. This only works
with SSH as the application. It is ignored for all other applications.
```

```
|===
```

```
[#owner]
[.api-collapsible-fifth-title]
owner
```

Owner name and UUID that uniquely identifies the user account.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```



```

[#role]
[.api-collapsible-fifth-title]
role

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|Role name

|===

[#account]
[.api-collapsible-fifth-title]
account

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|applications
|array[link:#account_application[account_application]]
a|

|comment
|string
a|Optional comment for the user account.

```

```

|locked
|boolean
a|Locked status of the account.

|name
|string
a|User or group account name

|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the user account.

|password
|string
a|Password for the account. The password can contain a mix of lower and
upper case alphabetic characters, digits, and special characters.

|role
|link:#role[role]
a|

|scope
|string
a|Scope of the entity. Set to "cluster" for cluster owned objects and to
"svm" for SVM owned objects.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

```

```

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
=====

```

```
[[ID65152b31b211b01b35e54b808ec33202]]
```

= Create a new user account

```
[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-block]#`/security/accounts`#
```

Creates a new user account.

== Required parameters

- * `name` - Account name to be created.
- * `applications` - Array of one or more application tuples (of application and authentication methods).

== Optional parameters

- * `owner.name` or `owner.uuid` - Name or UUID of the SVM for an SVM-scoped user account. If not supplied, a cluster-scoped user account is created.
- * `role` - RBAC role for the user account. Defaulted to `admin` for cluster user account and to `vsadmin` for SVM-scoped account.
- * `password` - Password for the user account (if the authentication method is opted as password for one or more of applications).
- * `second_authentication_method` - Needed for MFA and only supported for ssh application. Defaults to `none` if not supplied.
- * `comment` - Comment for the user account (e.g purpose of this account).
- * `locked` - Locks the account after creation. Defaults to `false` if not supplied.

== Related ONTAP commands

- * `security login create`

== Learn more

- * xref:{relative_path}security_accounts_endpoint_overview.html[DOC /security/accounts]

== Parameters

```
[cols=5*,options=header]
|===
```

```

|Name
|Type
|In
|Required
|Description

|return_records
|boolean
|query
|False
a|The default is false. If set to true, the records are returned.

|===

== Request Body

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|applications
|array[link:#account_application[account_application]]
a|

|comment
|string
a|Optional comment for the user account.

|locked
|boolean
a|Locked status of the account.

|name
|string
a|User or group account name

```

```

|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the user account.

|password
|string
a|Password for the account. The password can contain a mix of lower and
upper case alphabetic characters, digits, and special characters.

|role
|link:#role[role]
a|

|scope
|string
a|Scope of the entity. Set to "cluster" for cluster owned objects and to
"svm" for SVM owned objects.

|===

.Example request
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "applications": {
    "application": "console",
    "authentication_methods": {
    },
    "second_authentication_method": "none"
  },
  "comment": "string",
  "name": "joe.smith",
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    }
  }
}

```

```

    }
  },
  "name": "svml",
  "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
},
"role": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "name": "admin"
},
"scope": "cluster"
}
=====

```

== Response

Status: 201, Created

```

== Error

```

Status: Default

ONTAP Error Response Codes

```

|===
| Error Code | Description
| 1261215
| The role was not found.
| 1263343
| Cannot lock user with password not set or non-password authentication
method.
| 5636099
| User creation with a non-admin role is not supported for service-
processor application.
| 5636121
| The user account name is reserved for use by the system.
| 5636126

```

| Cannot create a user with the username or role as AutoSupport because it is reserved by the system.

| 5636140
| Creating a login with application console for a data Vserver is not supported.

| 5636141
| Creating a login with application service-processor for a data Vserver is not supported.

| 5636154
| The second-authentication-method parameter is supported for ssh application.

| 5636155
| The second-authentication-method parameter can be specified only if the authentication-method password or public key nsswitch.

| 5636156
| The same value cannot be specified for the second-authentication-method and the authentication-method.

| 5636157
| If the authentication-method is domain, the second-authentication-method cannot be specified.

| 5636164
| If the value for either the authentication-method second-authentication-method is nsswitch or password, the other parameter must differ.

| 7077897
| Invalid character in username.

| 7077898
| The username must contain both letters and numbers.

| 7077899
| The username does not meet length requirements.

| 7077906
| A role with that name has not been defined for the Vserver.

| 7077918
| The password cannot contain the username.

| 7077919


```

| The minimum length for new password does not meet the policy.

| 7077920
| A new password must have both letters and numbers.

| 7077921
| The minimum number of special characters required do not meet the
policy.

| 7077929
| Cannot lock user with password not set or non-password authentication
method.

| 7077940
| The password exceeds the maximum supported length.

| 7077941
| The defined password composition exceeds the maximum password length of
128 characters.

| 7078900
| An admin password is not set. Set the password by including it in the
request.
|===

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {

```

```

        "code": "string",
        "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
}
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]

```

```

a|

|===

[#account_application]
[.api-collapsible-fifth-title]
account_application

[cols=3*,options=header]
|===
|Name
|Type
|Description

|application
|string
a|Applications

|authentication_methods
|array[string]
a|

|second_authentication_method
|string
a|An optional additional authentication method for MFA. This only works
with SSH as the application. It is ignored for all other applications.

|===

[#owner]
[.api-collapsible-fifth-title]
owner

Owner name and UUID that uniquely identifies the user account.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links

```

```
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#role]
[.api-collapsible-fifth-title]
role
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|Role name
```

```
|===
```

```
[#account]
[.api-collapsible-fifth-title]
account
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```

|_links
|link:#_links[_links]
a|

|applications
|array[link:#account_application[account_application]]
a|

|comment
|string
a|Optional comment for the user account.

|locked
|boolean
a|Locked status of the account.

|name
|string
a|User or group account name

|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the user account.

|password
|string
a|Password for the account. The password can contain a mix of lower and
upper case alphabetic characters, digits, and special characters.

|role
|link:#role[role]
a|

|scope
|string
a|Scope of the entity. Set to "cluster" for cluster owned objects and to
"svm" for SVM owned objects.

|===

```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
|string
a|Error code
```

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
=====
```

```
:leveloffset: -1
```

```
= Manage scoped user accounts
```

```
:leveloffset: +1
```

```
[[ID70fadffbe8f5417baa8431d513464c0a]]
= Security accounts owner.uuid name endpoint overview
```

```
== Overview
```

This API displays and manages the configuration of scoped user accounts.

Newly created user accounts might need to be updated for many reasons. For example, a user account might need to use a different application or its role might need to be modified. According to a policy, the password or authentication source of a user account might need to be changed, or a user account might need to be locked or deleted from the system. This API allows you to make these changes to user accounts.

Specify the owner UUID and the user account name in the URI path. The owner UUID corresponds to the UUID of the SVM for which the user account has been created and can be obtained from the response body of the GET request performed on one of the following APIs:

```
_/_api/security/accounts_ for all user accounts
/_api/security/accounts/?scope=cluster_ for cluster-scoped user accounts
/_api/security/accounts/?scope=svm_ for SVM-scoped accounts
/_api/security/accounts/?owner.name=\{svm-name}_ for a specific SVM
```

This API response contains the complete URI for each user account that can be used.

== Examples

=== Retrieving the user account details

The API:

GET "/api/security/accounts/{owner.uuid}/{name}"

The call:

curl -X GET "https://<mgmt-ip>/api/security/accounts/aef7c38-4bd3-11e9-b238-0050568e2e25/svm_user1"

The response:

```
{
  "owner": {
    "uuid": "aef7c38-4bd3-11e9-b238-0050568e2e25",
    "name": "svm1",
    "_links": {
      "self": {
        "href": "/api/svm/svms/aef7c38-4bd3-11e9-b238-0050568e2e25"
      }
    }
  },
  "name": "svm_user1",
  "applications": [
    {
      "application": "ssh",
      "authentication_methods": [
        "password"
      ],
      "second_authentication_method": "none"
    }
  ],
  "role": {
    "name": "vsadmin",
    "_links": {
      "self": {
        "href": "/api/svms/aef7c38-4bd3-11e9-b238-0050568e2e25/admin/roles/vsadmin"
      }
    }
  }
},
```



```

"locked": false,
"scope": "svm",
"_links": {
  "self": {
    "href": "/api/security/accounts/aaef7c38-4bd3-11e9-b238-
0050568e2e25/svm_user1"
  }
}
}
}
-----

```

=== Updating the applications and role in a user account

Specify the desired configuration in the form of tuples (of applications and authentication methods) and the role. All other previously configured applications that are not specified in the "applications" parameter of the PATCH request will be de-provisioned for the user account.

The API:

```
PATCH "/api/security/accounts/{owner.uuid}/{name}"
```

The call to update the applications and role:

```

curl -X PATCH "https://<mgmt-ip>/api/security/accounts/aaef7c38-4bd3-11e9-
b238-0050568e2e25/svm_user1" -d
'{"applications":[{"application":"http","authentication_methods":["domain"
]},{ "application":"ontapi","authentication_methods":["password"]}], "role":
"vsadmin-backup"}'

```

The call to update only the role:

```

curl -X PATCH "https://<mgmt-ip>/api/security/accounts/aaef7c38-4bd3-11e9-
b238-0050568e2e25/svm_user1" -d '{"role":"vsadmin-protocol"}'
-----

```

=== Updating the password for a user account

The API:

```
PATCH "/api/security/accounts/{owner.uuid}/{name}"
```

The call:

```

curl -X PATCH "https://<mgmt-ip>/api/security/accounts/aaef7c38-4bd3-11e9-
b238-0050568e2e25/svm_user1" -d '{"password":"newp@ssw@rd2"}'
-----

```

=== Locking a user account

The API:

PATCH "/api/security/accounts/{owner.uuid}/{name}"

The call:

curl -X PATCH "https://<mgmt-ip>/api/security/accounts/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_user1" -d '{"locked":"true"}'

=== Deleting a user account

The API:

DELETE "/api/security/accounts/{owner.uuid}/{name}"

The call:

curl -X DELETE "https://<mgmt-ip>/api/security/accounts/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_user1"

[[ID953c9d1dcad3fee6629178d3c4586a53]]

= Delete a user account

[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-block]#`/security/accounts/{owner.uuid}/{name}`#

Deletes a user account.

== Required parameters

* `name` - Account name to be deleted.

* `owner.uuid` - UUID of the SVM housing the user account to be deleted.

== Related ONTAP commands

* `security login delete`

== Learn more

```
*
xref:{relative_path}security_accounts_owner.uuid_name_endpoint_overview.ht
ml[DOC /security/accounts/{owner.uuid}/{name}]
* xref:{relative_path}security_accounts_endpoint_overview.html[DOC
/security/accounts]
```

== Parameters

[cols=5*,options=header]

|===

Name
Type
In
Required
Description

owner.uuid

string

path

True

a

name

string

path

True

a

|===

== Response

Status: 200, Ok

== Error

Status: Default

ONTAP Error Response Codes

|===

Error Code	Description
------------	-------------

5636098	
---------	--

```
| Last unlocked account that has an admin role cannot be deleted.
```

```
| 5636125
```

```
| The operation is not supported on system accounts.
```

```
| 5636146
```

```
| Cannot delete the last console account with admin role.
```

```
|===
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
```

```
{  
  "error": {  
    "arguments": {  
      "code": "string",  
      "message": "string"  
    },  
    "code": "4",  
    "message": "entry doesn't exist",  
    "target": "uuid"  
  }  
}
```

```
=====
```

```
== Definitions
```

```
[.api-def-first-level]
```

```
.See Definitions
```

```
[%collapsible%closed]
```

```
//Start collapsible Definitions block
```

```

====
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
=====
```

```
[[IDc0551700d9fed0012bb40e17dc9305db]]
= Retrieve a specific user account
```

```
[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/accounts/{owner.uuid}/{name}`#
```

Retrieves a specific user account.

== Related ONTAP commands

* `security login show`

== Learn more

```
*
xref:{relative_path}security_accounts_owner.uuid_name_endpoint_overview.ht
ml[DOC /security/accounts/{owner.uuid}/{name}]
* xref:{relative_path}security_accounts_endpoint_overview.html[DOC
/security/accounts]
```

== Parameters

```
[cols=5*,options=header]
|===
```

```
|Name
|Type
|In
|Required
```

```

|Description

|fields
|array[string]
|query
|False
a|Specify the fields to return.

|owner.uuid
|string
|path
|True
a|Account owner UUID

|name
|string
|path
|True
a|User account name

|===

== Response

```

Status: 200, Ok

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records

|records
|array[link:#account[account]]
a|

```

|===

.Example response

[%collapsible%closed]

====

[source,json,subs=+macros]

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "applications": {
      "application": "console",
      "authentication_methods": {
      },
      "second_authentication_method": "none"
    },
    "comment": "string",
    "name": "joe.smith",
    "owner": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "svm1",
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    },
    "role": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      }
    },
  },
}
```



```

    "name": "admin"
  },
  "scope": "cluster"
}
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]

```

```

//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|====
|Name
|Type
|Description

|href
|string
a|

|====

[#\_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|====
|Name
|Type
|Description

|next
|link:#href[href]
a|

|self
|link:#href[href]
a|

|====

[#\_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|====
|Name

```

```

|Type
|Description

|self
|link:#href[href]
a|

|===

[#account_application]
[.api-collapsible-fifth-title]
account_application

[cols=3*,options=header]
|===
|Name
|Type
|Description

|application
|string
a|Applications

|authentication_methods
|array[string]
a|

|second_authentication_method
|string
a|An optional additional authentication method for MFA. This only works
with SSH as the application. It is ignored for all other applications.

|===

[#owner]
[.api-collapsible-fifth-title]
owner

Owner name and UUID that uniquely identifies the user account.

[cols=3*,options=header]
|===

```

```

|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

|===

[#role]
[.api-collapsible-fifth-title]
role

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|Role name

|===

[#account]
[.api-collapsible-fifth-title]
account

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|applications
|array[link:#account_application[account_application]]
a|

|comment
|string
a|Optional comment for the user account.

|locked
|boolean
a|Locked status of the account.

|name
|string
a|User or group account name

|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the user account.

|password
|string
a|Password for the account. The password can contain a mix of lower and
upper case alphabetic characters, digits, and special characters.

|role
|link:#role[role]
a|

|scope
|string
a|Scope of the entity. Set to "cluster" for cluster owned objects and to

```

"svm" for SVM owned objects.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]

|===

|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]

|===

|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
====
```

```
[[ID96b46c94472d9021ffc7b6eb6b2c4cee]]
= Update a user account
```

```
[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-
block]#`/security/accounts/{owner.uuid}/{name}`#
```

Updates a user account. Locks or unlocks a user account and/or updates the role, applications, and/or password for the user account.

== Required parameters

- * `name` - Account name to be updated.
- * `owner.uuid` - UUID of the SVM housing the user account to be updated.

== Optional parameters

- * `applications` - Array of one or more tuples (of application and authentication methods).
- * `role` - RBAC role for the user account.
- * `password` - Password for the user account (if the authentication method is opted as password for one or more of applications).
- * `second_authentication_method` - Needed for MFA and only supported for ssh application. Defaults to `none` if not supplied.
- * `comment` - Comment for the user account (e.g purpose of this account).
- * `locked` - Set to true/false to lock/unlock the account.

== Related ONTAP commands

- * `security login create`
- * `security login modify`
- * `security login password`
- * `security login lock`
- * `security login unlock`

== Learn more

*

xref:{relative_path}security_accounts_owner.uuid_name_endpoint_overview.html[DOC /security/accounts/{owner.uuid}/{name}]

* xref:{relative_path}security_accounts_endpoint_overview.html[DOC /security/accounts]

== Parameters

[cols=5*,options=header]

|===

|Name

|Type

|In

|Required

|Description

|owner.uuid

|string

|path

|True

a|Account owner UUID

|name

|string

|path

|True

a|User account name

|===

== Request Body


```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|applications
|array[link:#account_application[account_application]]
a|

|comment
|string
a|Optional comment for the user account.

|locked
|boolean
a|Locked status of the account.

|name
|string
a|User or group account name

|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the user account.

|password
|string
a|Password for the account. The password can contain a mix of lower and
upper case alphabetic characters, digits, and special characters.

|role
|link:#role[role]
a|

|scope
|string

```

a|Scope of the entity. Set to "cluster" for cluster owned objects and to "svm" for SVM owned objects.

|===

.Example request

[%collapsible%closed]

====

[source,json,subs=+macros]

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "applications": {
    "application": "console",
    "authentication_methods": {
    },
    "second_authentication_method": "none"
  },
  "comment": "string",
  "name": "joe.smith",
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "role": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "admin"
  },
  "scope": "cluster"
}
```

====

== Response

Status: 200, Ok

== Error

Status: Default

ONTAP Error Response Codes

```
|===  
| Error Code | Description  
  
| 1261215  
| The role was not found.  
  
| 1261218  
| The user was not found.  
  
| 1263343  
| Cannot lock user with password not set or non-password authentication  
method.  
  
| 5636096  
| Cannot perform the operation for this user account since the password is  
not set.  
  
| 5636097  
| The operation for user account failed since user password is not set.  
  
| 5636100  
| User modification is not supported for service-processor application.  
  
| 5636125  
| The operation not supported on AutoSupport user account which is  
reserved.  
  
| 5636129  
| The role does not exist.  
  
| 5636154  
| The second-authentication-method parameter is supported for ssh  
application.  
  
| 5636155
```

| The second-authentication-method parameter can be specified only if the authentication-method password or public key nsswitch.

| 5636156

| Same value cannot be specified for the second-authentication-method and the authentication-method.

| 5636157

| If the authentication-method is domain, the second-authentication-method cannot be specified.

| 5636159

| For a given user and application, if the second-authentication-method is specified, only one such login entry is supported.

| 5636164

| If the value for either the authentication-method second-authentication-method is nsswitch or password, the other parameter must differ.

| 5636174

| You are not authorized to change the password for other users.

| 7077896

| Cannot lock the account of the last console admin user.

| 7077906

| A role with that name has not been defined for the Vserver.

| 7077911

| The user is not configured to use the password authentication method.

| 7077918

| The password cannot contain the username.

| 7077919

| The minimum length for new password does not meet the policy.

| 7077920

| The new password must have both letters and numbers.

| 7077921

| The minimum number of special characters required do not meet the policy.

| 7077924

| The new password must be different than last N passwords.

```
| 7077925
| The new password must be different to the old password.

| 7077929
| Cannot lock user with password not set or non-password authentication
method.

| 7077940
| The password exceeds maximum supported length.

| 7077941
| Defined password composition exceeds the maximum password length of 128
characters.

| 7078900
| An aAdmin password is not set. Set the password by including it in the
request.
|===
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
```

```
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

```

    }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#account_application]
[.api-collapsible-fifth-title]

```

account_application

[cols=3*,options=header]

|===

|Name

|Type

|Description

|application

|string

a|Applications

|authentication_methods

|array[string]

a|

|second_authentication_method

|string

a|An optional additional authentication method for MFA. This only works with SSH as the application. It is ignored for all other applications.

|===

[#owner]

[.api-collapsible-fifth-title]

owner

Owner name and UUID that uniquely identifies the user account.

[cols=3*,options=header]

|===

|Name

|Type

|Description

|_links

|link:#_links[_links]

a|

|name

|string

a|The name of the SVM.

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#role]
[.api-collapsible-fifth-title]
role
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|Role name
```

```
|===
```

```
[#account]
[.api-collapsible-fifth-title]
account
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|applications
|array[link:#account_application[account_application]]
```



```

a|

|comment
|string
a|Optional comment for the user account.

|locked
|boolean
a|Locked status of the account.

|name
|string
a|User or group account name

|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the user account.

|password
|string
a|Password for the account. The password can contain a mix of lower and
upper case alphabetic characters, digits, and special characters.

|role
|link:#role[role]
a|

|scope
|string
a|Scope of the entity. Set to "cluster" for cluster owned objects and to
"svm" for SVM owned objects.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===

```

```
|Name
|Type
|Description

|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
|===
```

```
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
|string
a|Error code
```

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```

|===

//end collapsible .Definitions block
====

:leveloffset: -1

= View and update audit settings

:leveloffset: +1

[[ID26edcb029a021dcd15832df6e6e7a667]]
= Security audit endpoint overview


== Overview

This API controls what is logged to the audit log files. All operations
that make changes are always logged and cannot be disabled. The PATCH
request updates administrative audit settings for GET requests. All fields
are optional for a PATCH request. A GET request retrieves administrative
audit settings for GET requests.
+

'''

== Examples

=== Retrieving administrative audit settings for GET requests

The following example shows the administrative audit settings for GET
requests.
+

'''

-----

# The API:
/api/security/audit

```

```

# The call:
curl -X GET "https://<cluster-ip>/api/security/audit"

# The response:
{
  "cli": false,
  "http": false,
  "ontapi": false,
  "_links": {
    "self": {
      "href": "/api/security/audit"
    }
  }
}
----

'''

=== Updating administrative audit settings for GET requests

The following example updates the administrative audit settings for GET
requests
+

'''

----

# The API:
/api/security/audit

# The call:
curl -X PATCH "https://<cluster-ip>/api/security/audit" -d
'{"cli": "false", "http": "true", "ontapi": "true"}'
----

'''

[[IDb78a5cfbelf78c3777667b86b87de1cc]]
= Retrieve administrative audit settings for GET requests

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/audit`#

```

Retrieves administrative audit settings for GET requests.

== Learn more

* xref:{relative_path}security_audit_endpoint_overview.html[DOC
/security/audit]

== Parameters

[cols=5*,options=header]
|===

|Name
|Type
|In
|Required
|Description

|max_records
|integer
|query
|False
a|Limit the number of records returned.

|return_records
|boolean
|query
|False
a|The default is true for GET calls. When set to false, only the number of records is returned.

|return_timeout
|integer
|query
|False
a|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.

```
|order_by
|array[string]
|query
|False
a|Order results by specified fields and optional [asc|desc] direction.
Default direction is 'asc' for ascending.
```

```
|fields
|array[string]
|query
|False
a|Specify the fields to return.
```

```
|===
```

```
== Response
```

Status: 200, Ok

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|cli
```

```
|boolean
```

```
a|Enable auditing of CLI GET Operations. Valid in PATCH
```

```
|http
```

```
|boolean
```

```
a|Enable auditing of HTTP GET Operations. Valid in PATCH
```

```
|ontapi
```

```
|boolean
```

```
a|Enable auditing of ONTAP API GET operations. Valid in PATCH
```

```
|===
```

```
== Error
```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name

```

```

|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

```



```
//end collapsible .Definitions block
```

```
====
```

```
[[IDf3a1b7ed178475fa6606df43dd51deba]]
```

```
= Update administrative audit settings for GET requests
```

```
[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-  
block]#`/security/audit`#
```

Updates administrative audit settings for GET requests.

All of the fields are optional. An empty body will make no changes.

== Learn more

* xref:{relative_path}security_audit_endpoint_overview.html[DOC
/security/audit]

== Parameters

```
[cols=5*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|In
```

```
|Required
```

```
|Description
```

```
|return_records
```

```
|boolean
```

```
|query
```

```
|False
```

a|The default is false. If set to true, the records are returned.

```
|return_timeout
```

```
|integer
```

```
|query
```

```
|False
```

a|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.

|===

== Request Body

[cols=3*,options=header]

|===

|Name

|Type

|Description

|cli

|boolean

a|Enable auditing of CLI GET Operations. Valid in PATCH

|http

|boolean

a|Enable auditing of HTTP GET Operations. Valid in PATCH

|ontapi

|boolean

a|Enable auditing of ONTAP API GET operations. Valid in PATCH

|===

== Response

Status: 202, Accepted

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|cli
|boolean
a|Enable auditing of CLI GET Operations. Valid in PATCH

|http
|boolean
a|Enable auditing of HTTP GET Operations. Valid in PATCH

|ontapi
|boolean
a|Enable auditing of ONTAP API GET operations. Valid in PATCH

|===

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
=====
[source,json,subs=+macros]

```

```

{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#security_audit]
[.api-collapsible-fifth-title]
security_audit

[cols=3*,options=header]
|===
|Name
|Type
|Description

|cli
|boolean
a|Enable auditing of CLI GET Operations. Valid in PATCH

|http
|boolean
a|Enable auditing of HTTP GET Operations. Valid in PATCH

|ontapi
|boolean
a|Enable auditing of ONTAP API GET operations. Valid in PATCH

|===

```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
|string
a|Error code
```

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
====
```

```
:leveloffset: -1
```

```
= Forward audit logs to syslog/splunk servers
```

```
:leveloffset: +1
```

```
[[ID7eab19403530691b2484d1444b5b65a5]]
= Security audit destinations endpoint overview
```

```
== Overview
```

This API controls the forwarding of audit log information to remote syslog/splunk servers. Multiple destinations can be configured and all audit records are forwarded to all destinations.

A GET operation retrieves information about remote syslog/splunk server destinations.

A POST operation creates a remote syslog/splunk server destination.

A GET operation on /security/audit/destinations/{address}/{port} retrieves information about the syslog/splunk server destination given its address and port number.

A PATCH operation on /security/audit/destinations/{address}/{port} updates information about the syslog/splunk server destination given its address and port number.

A DELETE operation on /security/audit/destinations/{address}/{port} deletes a syslog/splunk server destination given its address and port number.

=== Overview of fields used for creating a remote syslog/splunk destination

The fields used for creating a remote syslog/splunk destination fall into the following categories

==== Required properties

All of the following fields are required for creating a remote syslog/splunk destination

- * `address`

==== Optional properties

All of the following fields are optional for creating a remote syslog/splunk destination

- * `port`
- * `protocol`
- * `facility`
- * `verify_server`
- +

'''

== Examples

=== Retrieving remote syslog/splunk server destinations

The following example shows remote syslog/splunk server destinations

- +

'''

The API:
/api/security/audit/destinations

The call:
curl -X GET "https://<cluster-ip>/api/security/audit/destinations"

The response:
{
"records": [
 {

```

    "address": "1.1.1.1",
    "port": 514,
    "_links": {
        "self": {
            "href": "/api/security/audit/destinations/1.1.1.1/514"
        }
    }
}
],
"num_records": 1,
"_links": {
    "self": {
        "href": "/api/security/audit/destinations"
    }
}
}
----

'''

=== Creating remote syslog/splunk server destinations

The following example creates remote syslog/splunk server destinations.
+

'''

----

# The API:
/api/security/audit/destinations

# The call:
curl -X POST "https://<cluster-
ip>/api/security/audit/destinations?force=true -d '{ "address":
"<destination-address>", "port": <destination-port>, "protocol":
"udp_unencrypted", "facility": "kern"}'"
----

'''

=== Retrieving a remote syslog/splunk server destination given its
destination address and port number

The following example retrieves a remote syslog/splunk server destination
given its destination address and port number.
+

```



```

'''

----

# The API:
/api/security/audit/destinations/{address}/{port}

# The call:
curl -X GET "https://<cluster-
ip>/api/security/audit/destinations/<destination-address>/<destination-
port>"

# The response:
{
  "address": "1.1.1.1",
  "port": 514,
  "protocol": "udp_unencrypted",
  "facility": "kern",
  "verify_server": false,
  "_links": {
    "self": {
      "href": "/api/security/audit/destinations/1.1.1.1/514"
    }
  }
}
'''

----

'''

=== Updating a remote syslog/splunk server destination given its
destination address and port number

The following example updates a remote syslog/splunk server destination
configuration given its destination address and port number.
+

'''

----

# The API:
/api/security/audit/destinations/{address}/{port}

# The call:
curl -X PATCH "https://<cluster-
ip>/api/security/audit/destinations/<destination-address>/<destination-

```

```

port> -d '{"facility": "kern"}'
----

'''

=== Deleting a remote syslog/splunk server destination given its
destination address and port number

The following example deletes a remote syslog/splunk server destination
configuration given its destination address and port number.
+

'''

----

# The API:
/api/security/audit/destinations/{address}/{port}

# The call:
curl -X DELETE "https://<cluster-
ip>/api/security/audit/destinations/<destination-address>/<destination-
port>"
----

'''

[[ID170f47c8de635aded26f150d98887150]]
= Define a remote syslog or splunk server to receive audit information

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/audit/destinations`#

Defines a remote syslog/splunk server for sending audit information to.

== Learn more

*
xref:{relative_path}security_audit_destinations_endpoint_overview.html[DOC
/security/audit/destinations]

```

== Parameters

```
[cols=5*,options=header]  
|===
```

```
|Name  
|Type  
|In  
|Required  
|Description
```

```
|order_by  
|array[string]  
|query  
|False
```

a|Order results by specified fields and optional [asc|desc] direction.
Default direction is 'asc' for ascending.

```
|facility  
|string  
|query  
|False  
a|Filter by facility
```

```
|address  
|string  
|query  
|False  
a|Filter by address
```

```
|port  
|integer  
|query  
|False  
a|Filter by port
```

```
|protocol  
|string  
|query  
|False  
a|Filter by protocol
```

```
|verify_server
|boolean
|query
|False
a|Filter by verify_server
```

```
|fields
|array[string]
|query
|False
a|Specify the fields to return.
```

```
|max_records
|integer
|query
|False
a|Limit the number of records returned.
```

```
|return_timeout
|integer
|query
|False
a|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
a|The default is true for GET calls.  When set to false, only the number
of records is returned.
```

```
|===
```

```
== Response
```

Status: 200, Ok

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records


|records
|array[link:#security_audit_log_forward[security_audit_log_forward]]
a|

|===

.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "facility": "kern",
    "protocol": "udp_unencrypted"
  }
}
=====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|next
|link:#href[href]
a|

|self
|link:#href[href]
a|

|===

[#security_audit_log_forward]
[.api-collapsible-fifth-title]
security_audit_log_forward

[cols=3*,options=header]
|===
|Name
|Type
|Description

|address
|string
a|Destination syslog\|splunk host to forward audit records to. This can be
an IP address (IPv4\|IPv6) or a hostname.

|facility
|string

```

a|This is the standard Syslog Facility value that is used when sending audit records to a remote server.

|port

|integer

a|Destination Port. The default port depends on the protocol chosen:

For un-encrypted destinations the default port is 514.

For encrypted destinations the default port is 6514.

|protocol

|string

a|Log forwarding protocol

|verify_server

|boolean

a|This is only applicable when the protocol is tcp_encrypted. This controls whether the remote server's certificate is validated. Setting "verify_server" to "true" will enforce validation of remote server's certificate. Setting "verify_server" to "false" will not enforce validation of remote server's certificate.

|===

[#error_arguments]

[.api-collapsible-fifth-title]

error_arguments

[cols=3*,options=header]

|===

|Name

|Type

|Description

|code

|string

a|Argument code

|message

|string

a|Message argument


```

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[ID89b605e5f7395e14db8f267a6634a448]]
= Define the remote syslog or splunk server information

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/audit/destinations`#

```

Configures remote syslog/splunk server information.

== Required properties

All of the following fields are required for creating a remote syslog/splunk destination

- * `address`

== Optional properties

All of the following fields are optional for creating a remote syslog/splunk destination

- * `port`

- * `protocol`

- * `facility`

- * `verify_server` (Can only be "true" when protocol is "tcp_encrypted")

== Learn more

*

xref:{relative_path}security_audit_destinations_endpoint_overview.html[DOC /security/audit/destinations]

== Parameters

[cols=5*,options=header]

|===

|Name

|Type

|In

|Required

|Description

|return_timeout

|integer

|query

|False

a|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: 1

|return_records
|boolean
|query
|False

a|The default is false. If set to true, the records are returned.

* Default value: 1

|force
|boolean
|query
|False

a|Skip the Connectivity Test

* Default value:

|===

== Request Body

[cols=3*,options=header]

|===

|Name
|Type
|Description

|address
|string

a|Destination syslog\|splunk host to forward audit records to. This can be an IP address (IPv4\|IPv6) or a hostname.

|facility
|string

a|This is the standard Syslog Facility value that is used when sending audit records to a remote server.

```

|port
|integer
a|Destination Port. The default port depends on the protocol chosen:
For un-encrypted destinations the default port is 514.
For encrypted destinations the default port is 6514.

|protocol
|string
a|Log forwarding protocol

|verify_server
|boolean
a|This is only applicable when the protocol is tcp_encrypted. This
controls whether the remote server's certificate is validated. Setting
"verify_server" to "true" will enforce validation of remote server's
certificate. Setting "verify_server" to "false" will not enforce
validation of remote server's certificate.

|===

.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "facility": "kern",
  "protocol": "udp_unencrypted"
}
====

== Response

```

Status: 202, Accepted

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records


|records
|array[link:#security_audit_log_forward[security_audit_log_forward]]
a|

|===

.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "facility": "kern",
    "protocol": "udp_unencrypted"
  }
}
=====

== Error

```

Status: Default

ONTAP Error Response Codes

|===

| Error Code | Description

| 15661

| The object specified could not be found

| 13114

| Internal error

| 13115

| Invalid input

| 4522285

| Server verification cannot be enabled because it requires a protocol with encryption. Encryption can be selected using the protocol field.

| 9240603

| Cannot ping destination host. Verify connectivity to desired host or skip the connectivity check with the -force parameter.

| 327698

| Failed to create RPC client to destination host

| 9240609

| Cannot connect to destination host.

| 9240604

| Cannot resolve the destination host.

|===

[cols=3*,options=header]

|===

|Name

|Type

|Description

|error

|link:#error[error]

a|

|===

```
.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
=====
```

== Definitions

```
[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
=====
[#security_audit_log_forward]
[.api-collapsible-fifth-title]
security_audit_log_forward

[cols=3*,options=header]
|===
|Name
|Type
|Description

|address
|string
a|Destination syslog\|splunk host to forward audit records to. This can be
an IP address (IPv4\|IPv6) or a hostname.

|facility
|string
a|This is the standard Syslog Facility value that is used when sending
audit records to a remote server.
```

```

|port
|integer
a|Destination Port. The default port depends on the protocol chosen:
For un-encrypted destinations the default port is 514.
For encrypted destinations the default port is 6514.

|protocol
|string
a|Log forwarding protocol

|verify_server
|boolean
a|This is only applicable when the protocol is tcp_encrypted. This
controls whether the remote server's certificate is validated. Setting
"verify_server" to "true" will enforce validation of remote server's
certificate. Setting "verify_server" to "false" will not enforce
validation of remote server's certificate.

|===

[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===

```



```

|Name
|Type
|Description

|next
|link:#href[href]
a|

|self
|link:#href[href]
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
|string
a|Error code
```

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
=====
```

```
[[IDda41ec6c0baa9a686a3f2a3b12cdcc0a]]
= Delete the remote syslog or splunk server information
```

```
[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-
block]#`/security/audit/destinations/{address}/{port}`#
```

Deletes remote syslog/splunk server information.

== Learn more

*

xref:{relative_path}security_audit_destinations_endpoint_overview.html[DOC
/security/audit/destinations]

== Parameters

```
[cols=5*,options=header]
|===
|Name
|Type
|In
|Required
|Description

|address
|string
|path
|True
a|

|port
|integer
|path
|True
a|
|===

== Response
```

Status: 200, Ok

```
== Error
```

Status: Default, Error

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
```

```

[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]

```

```

[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[ID6690373c9cfe7d86450ca40968cf3ac9]]
= Retrieve the remote syslog or splunk server information

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/audit/destinations/{address}/{port}`#

Defines a remote syslog/splunk server for sending audit information to.

```

== Learn more

*

xref:{relative_path}security_audit_destinations_endpoint_overview.html[DOC
/security/audit/destinations]

== Parameters

[cols=5*,options=header]

|===

|Name

|Type

|In

|Required

|Description

|address

|string

|path

|True

a|IP address of remote syslog/splunk server.

|port

|integer

|path

|True

a|Port number of remote syslog/splunk server.

|fields

|array[string]

|query

|False

a|Specify the fields to return.

|===

== Response

Status: 200, Ok

[cols=3*,options=header]

|===

```

|Name
|Type
|Description

|address
|string
a|Destination syslog\|splunk host to forward audit records to. This can be
an IP address (IPv4\|IPv6) or a hostname.

|facility
|string
a|This is the standard Syslog Facility value that is used when sending
audit records to a remote server.

|port
|integer
a|Destination Port. The default port depends on the protocol chosen:
For un-encrypted destinations the default port is 514.
For encrypted destinations the default port is 6514.

|protocol
|string
a|Log forwarding protocol

|verify_server
|boolean
a|This is only applicable when the protocol is tcp_encrypted. This
controls whether the remote server's certificate is validated. Setting
"verify_server" to "true" will enforce validation of remote server's
certificate. Setting "verify_server" to "false" will not enforce
validation of remote server's certificate.

|===

.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "facility": "kern",
  "protocol": "udp_unencrypted"
}

```

```

}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#error_arguments]
[.api-collapsible-fifth-title]

```


error_arguments

[cols=3*,options=header]

|===

|Name

|Type

|Description

|code

|string

a|Argument code

|message

|string

a|Message argument

|===

[#error]

[.api-collapsible-fifth-title]

error

[cols=3*,options=header]

|===

|Name

|Type

|Description

|arguments

|array[link:#error_arguments[error_arguments]]

a|Message arguments

|code

|string

a|Error code

|message

|string

a|Error message

|target

```

|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
=====

[[ID2eff8743f9cfcabd83192d664ad1c702]]
= Update the remote syslog or splunk server information

[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-
block]#`/security/audit/destinations/{address}/{port}`#

Updates remote syslog/splunk server information.

== Learn more

*
xref:{relative_path}security_audit_destinations_endpoint_overview.html[DOC
/security/audit/destinations]

== Parameters

[cols=5*,options=header]
|===

|Name
|Type
|In
|Required
|Description

|address
|string
|path
|True
a|IP address of remote syslog/splunk server.

```

```

|port
|integer
|path
|True
a|Port number of remote syslog/splunk server.

|===

== Request Body

[cols=3*,options=header]
|===
|Name
|Type
|Description

|address
|string
a|Destination syslog\|splunk host to forward audit records to. This can be
an IP address (IPv4\|IPv6) or a hostname.

|facility
|string
a|This is the standard Syslog Facility value that is used when sending
audit records to a remote server.

|port
|integer
a|Destination Port. The default port depends on the protocol chosen:
For un-encrypted destinations the default port is 514.
For encrypted destinations the default port is 6514.

|protocol
|string
a|Log forwarding protocol

|verify_server
|boolean
a|This is only applicable when the protocol is tcp_encrypted. This
controls whether the remote server's certificate is validated. Setting
"verify_server" to "true" will enforce validation of remote server's

```

certificate. Setting "verify_server" to "false" will not enforce validation of remote server's certificate.

|===

.Example request

[%collapsible%closed]

====

[source,json,subs=+macros]

```
{
  "facility": "kern",
  "protocol": "udp_unencrypted"
}
```

====

== Response

Status: 200, Ok

[cols=3*,options=header]

|===

|Name

|Type

|Description

|address

|string

a|Destination syslog\|splunk host to forward audit records to. This can be an IP address (IPv4\|IPv6) or a hostname.

|facility

|string

a|This is the standard Syslog Facility value that is used when sending audit records to a remote server.

|port

|integer

a|Destination Port. The default port depends on the protocol chosen: For un-encrypted destinations the default port is 514. For encrypted destinations the default port is 6514.

```

|protocol
|string
a|Log forwarding protocol

|verify_server
|boolean
a|This is only applicable when the protocol is tcp_encrypted. This
controls whether the remote server's certificate is validated. Setting
"verify_server" to "true" will enforce validation of remote server's
certificate. Setting "verify_server" to "false" will not enforce
validation of remote server's certificate.

|===

.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "facility": "kern",
  "protocol": "udp_unencrypted"
}
=====

== Error

```

Status: Default, Default

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]

```

```

=====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
=====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
=====
[#security_audit_log_forward]
[.api-collapsible-fifth-title]
security_audit_log_forward

[cols=3*,options=header]
|==
|Name
|Type
|Description

|address
|string
a|Destination syslog\|splunk host to forward audit records to. This can be
an IP address (IPv4\|IPv6) or a hostname.

|facility
|string
a|This is the standard Syslog Facility value that is used when sending
audit records to a remote server.

|port
|integer

```

a|Destination Port. The default port depends on the protocol chosen:

For un-encrypted destinations the default port is 514.

For encrypted destinations the default port is 6514.

|protocol

|string

a|Log forwarding protocol

|verify_server

|boolean

a|This is only applicable when the protocol is tcp_encrypted. This controls whether the remote server's certificate is validated. Setting "verify_server" to "true" will enforce validation of remote server's certificate. Setting "verify_server" to "false" will not enforce validation of remote server's certificate.

|===

[#error_arguments]

[.api-collapsible-fifth-title]

error_arguments

[cols=3*,options=header]

|===

|Name

|Type

|Description

|code

|string

a|Argument code

|message

|string

a|Message argument

|===

[#error]

[.api-collapsible-fifth-title]

```

error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments


|code
|string
a|Error code


|message
|string
a|Error message


|target
|string
a|The target parameter that caused the error.


|===


//end collapsible .Definitions block
====

:leveloffset: -1

= View administrative audit logs

:leveloffset: +1


[[ID07e6ea2c98bf6ec4c58668eee81cc46f]]
= Security audit messages endpoint overview

```


== Overview

These APIs return audit log records. The GET requests retrieves all audit log records. An audit log record contains information such as timestamp, node name, index and so on.

+

'''

== Example

=== Retrieving audit log records

The following example shows the audit log records.

+

'''

The API:

/api/security/audit/messages

The call:

```
curl -X GET "https://<cluster-ip>/api/security/audit/messages"
```

The response:

```
{
  "records": [
    {
      "timestamp": "2019-03-08T11:03:32-05:00",
      "node": {
        "name": "node1",
        "uuid": "bc9af9da-41bb-11e9-a3db-005056bb27cf",
        "_links": {
          "self": {
            "href": "/api/cluster/nodes/bc9af9da-41bb-11e9-a3db-005056bb27cf"
          }
        }
      },
      "index": 4294967299,
      "application": "http",
      "location": "172.21.16.89",
      "user": "admin",
```

```

    "input": "GET /api/security/audit/destinations/",
    "state": "pending",
    "scope": "cluster"
  }
],
"num_records": 1,
"_links": {
  "self": {
    "href": "/api/security/audit/messages"
  }
}
}
}

```

'''

[[ID06fc4dcde4487f0a888f2ea1421400bc]]
 = Retrieve the administrative audit log viewer

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-block]#`/security/audit/messages`#

Retrieves the administrative audit log viewer.

== Learn more

* xref:{relative_path}security_audit_messages_endpoint_overview.html[DOC /security/audit/messages]

== Parameters

```

[cols=5*,options=header]
|===

```

```

|Name
|Type
|In
|Required
|Description

```

```
|index
|integer
|query
|False
a|Filter by index
```

```
|timestamp
|string
|query
|False
a|Filter by timestamp
```

```
|state
|string
|query
|False
a|Filter by state
```

```
|scope
|string
|query
|False
a|Filter by scope
```

```
|application
|string
|query
|False
a|Filter by application
```

```
|user
|string
|query
|False
a|Filter by user
```

```
|node.uuid
|string
|query
|False
a|Filter by node.uuid
```

```
|node.name  
|string  
|query  
|False  
a|Filter by node.name
```

```
|location  
|string  
|query  
|False  
a|Filter by location
```

```
|session_id  
|string  
|query  
|False  
a|Filter by session_id
```

```
|command_id  
|string  
|query  
|False  
a|Filter by command_id
```

```
|message  
|string  
|query  
|False  
a|Filter by message
```

```
|input  
|string  
|query  
|False  
a|Filter by input
```

```
|svm.name  
|string  
|query
```

```

|False
a|Filter by svm.name


|fields
|array[string]
|query
|False
a|Specify the fields to return.


|max_records
|integer
|query
|False
a|Limit the number of records returned.


|return_timeout
|integer
|query
|False
a|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
a|The default is true for GET calls. When set to false, only the number
of records is returned.


|order_by
|array[string]
|query
|False
a|Order results by specified fields and optional [asc|desc] direction.
Default direction is 'asc' for ascending.


|===

== Response

```

Status: 200, Ok

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records

|records
|array[link:#security_audit_log[security_audit_log]]
a|

|===
```

```
.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    },
  "application": "internal",
  "command_id": "string",
  "index": 0,
```

```

    "input": "string",
    "location": "string",
    "message": "string",
    "node": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "node1",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    },
    "scope": "svm",
    "session_id": "string",
    "state": "pending",
    "timestamp": "string",
    "user": "string"
  }
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {

```

```

        "code": "string",
        "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
}
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|next
|link:#href[href]

```



```

a|

|self
|link:#href[href]
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#node]
[.api-collapsible-fifth-title]
node

Node where the audit message resides.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|

```

```
|uuid
|string
a|
```

```
|===
```

```
[#svm]
[.api-collapsible-fifth-title]
svm
```

This is the SVM through which the user connected.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|name
|string
a|
```

```
|===
```

```
[#security_audit_log]
[.api-collapsible-fifth-title]
security_audit_log
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|application
|string
a|This identifies the "application" by which the request was processed.
```

```
|command_id
```

```

|string
a|This is the command ID for this request.
Each command received on a CLI session is assigned a command ID. This
enables you to correlate a request and response.

|index
|integer
a|Internal index for accessing records with same time/node. This is a 64
bit unsigned value.

|input
|string
a|The request.

|location
|string
a|This identifies the location of the remote user. This is an IP address
or "console".

|message
|string
a|This is an optional field that might contain "error" or "additional
information" about the status of a command.

|node
|link:#node[node]
a|Node where the audit message resides.

|scope
|string
a|Set to "svm" when the request is on a data SVM; otherwise set to
"cluster".

|session_id
|string
a|This is the session ID on which the request is received. Each SSH
session is assigned a session ID.
Each http/ontapi/snmp request is assigned a unique session ID.

```

```

|state
|string
a|State of of this request.

|svm
|link:#svm[svm]
a|This is the SVM through which the user connected.

|timestamp
|string
a|Log entry timestamp. Valid in URL

|user
|string
a|Username of the remote user.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]

```

```

[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

:leveloffset: -1

= Manage data SVM account information

:leveloffset: +1

[[ID7cd60d9f0a9424a13ca57b2fa58490b8]]
= Security authentication cluster ad-proxy endpoint overview

```

== Overview

This API configures data SVM account information at the Active Directory. For Active Directory domain-based authentication for cluster accounts, a data SVM must be configured and registered as a machine account at the Active Directory. All authentication requests are proxied through this SVM.

== Examples

=== Creating a data SVM proxy for domain-based authentication for cluster accounts

The API:

POST "/api/security/authentication/cluster/ad-proxy"

The call:

curl -X POST "https://<mgmt-ip>/api/security/authentication/cluster/ad-proxy" -d '{"svm.uuid":"13f87d78-70c7-11e9-b722-0050568ec89f"}'

=== Updating a data SVM proxy for domain-based authentication for cluster accounts

The API:

PATCH "/api/security/authentication/cluster/ad-proxy"

The call:

curl -X PATCH "https://<mgmt-ip>/api/security/authentication/cluster/ad-proxy" -d '{"svm.uuid":"13f87d78-70c7-11e9-b722-0050568ec89f"}'

=== Retrieving a data SVM proxy for domain-based authentication for cluster accounts

The API:

GET "/api/security/authentication/cluster/ad-proxy"

```
# The call:
curl -X GET "https://<mgmt-ip>/api/security/authentication/cluster/ad-proxy"

# The response:
{
  "svm": {
    "uuid": "512eab7a-6bf9-11e9-a896-005056bb9ce1",
    "name": "vs2",
    "_links": {
      "self": {
        "href": "/api/svm/svms/512eab7a-6bf9-11e9-a896-005056bb9ce1"
      }
    }
  },
  "_links": {
    "self": {
      "href": "/api/security/authentication/cluster/ad-proxy"
    }
  }
}
----
```

```
[[ID0cb1116cea9faad808b8b8182c7e0f69]]
= Delete a data SVM configured as a tunnel
```

```
[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-block]#`/security/authentication/cluster/ad-proxy`#
```

Deletes the data SVM configured as a tunnel for Active Directory-based authentication for cluster user accounts.

== Learn more

```
* xref:{relative_path}security_authentication_cluster_ad-proxy_endpoint_overview.html[DOC /security/authentication/cluster/ad-proxy]
```

== Response

Status: 200, Ok

```
== Error
```

Status: Default, Error

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#error_arguments]
[.api-collapsible-fifth-title]
```


error_arguments

[cols=3*,options=header]

|===

|Name

|Type

|Description

|code

|string

a|Argument code

|message

|string

a|Message argument

|===

[#error]

[.api-collapsible-fifth-title]

error

[cols=3*,options=header]

|===

|Name

|Type

|Description

|arguments

|array[link:#error_arguments[error_arguments]]

a|Message arguments

|code

|string

a|Error code

|message

|string

a|Error message

|target

```

|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
=====

[[ID7b03bd5154a83cb1378e29c865073077]]
= Retrieve SVM information configured as an Active Directory domain-tunnel

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/authentication/cluster/ad-proxy`#

Retrieves SVM information configured as an Active Directory domain-tunnel.

== Learn more

* xref:{relative_path}security_authentication_cluster_ad-
proxy_endpoint_overview.html[DOC /security/authentication/cluster/ad-
proxy]

== Response

```

Status: 200, Ok

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|svm
|link:#svm[svm]
a|
```

```
|===
```

.Example response

[%collapsible%closed]

====

[source,json,subs=+macros]

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

====

== Error

Status: Default, Error

```
[cols=3*,options=header]
|===
```

```

|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href

```

```

|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#svm]
[.api-collapsible-fifth-title]
svm

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

```

```
|===
```

```
[#error_arguments]  
[.api-collapsible-fifth-title]  
error_arguments
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name  
|Type  
|Description
```

```
|code  
|string  
a|Argument code
```

```
|message  
|string  
a|Message argument
```

```
|===
```

```
[#error]  
[.api-collapsible-fifth-title]  
error
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name  
|Type  
|Description
```

```
|arguments  
|array[link:#error_arguments[error_arguments]]  
a|Message arguments
```

```
|code  
|string  
a|Error code
```

```
|message
```

```

|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
=====

[[ID16aa4f63717c50634aeabd4f8e775e42]]
= Update a data SVM configured as a tunnel

[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-
block]#`/security/authentication/cluster/ad-proxy`#

Updates the data SVM configured as a tunnel for Active Directory-based
authentication for cluster user accounts.

== Learn more

* xref:{relative_path}security_authentication_cluster_ad-
proxy_endpoint_overview.html[DOC /security/authentication/cluster/ad-
proxy]

== Parameters

[cols=5*,options=header]
|===

|Name
|Type
|In
|Required
|Description

|return_records

```

```
|boolean
|query
|False
a|The default is false. If set to true, the records are returned.
```

```
|===
```

```
== Request Body
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|svm
```

```
|link:#svm[svm]
```

```
a|
```

```
|===
```

```
.Example request
```

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
```

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



```
}  
====  
  
== Response
```

Status: 200, Ok

```
== Error
```

Status: Default, Error

```
[cols=3*,options=header]  
|===  
|Name  
|Type  
|Description  
  
|error  
|link:#error[error]  
a|  
  
|===  
  
.Example error  
[%collapsible%closed]  
====  
[source,json,subs=+macros]  
{  
  "error": {  
    "arguments": {  
      "code": "string",  
      "message": "string"  
    },  
    "code": "4",  
    "message": "entry doesn't exist",  
    "target": "uuid"  
  }  
}  
====  
  
== Definitions  
  
[.api-def-first-level]  
.See Definitions
```

```

[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#svm]
[.api-collapsible-fifth-title]
svm

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#cluster_ad_proxy]
[.api-collapsible-fifth-title]
cluster_ad_proxy
```

The SVM configured as proxy for Active Directory authentication of cluster accounts.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|svm
|link:#svm[svm]
a|
```

```
|===
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
```

```

|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

```

```
|===
```

```
//end collapsible .Definitions block  
=====
```

```
[[ID6deffca1ef6b29cd69fe37e3a7583a8b]]  
= Configure a data SVM as a proxy
```

```
[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-  
block]#`/security/authentication/cluster/ad-proxy`#
```

Configures a data SVM as a proxy for Active Directory-based authentication for cluster user accounts.

== Learn more

```
* xref:{relative_path}security_authentication_cluster_ad-  
proxy_endpoint_overview.html[DOC /security/authentication/cluster/ad-  
proxy]
```

== Parameters

```
[cols=5*,options=header]  
|===
```

```
|Name  
|Type  
|In  
|Required  
|Description
```

```
|return_records  
|boolean  
|query  
|False  
a|The default is false. If set to true, the records are returned.
```

```
|===
```

== Request Body

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|svm
```

```
|link:#svm[svm]
```

```
a|
```

```
|===
```

.Example request

[%collapsible%closed]

====

```
[source,json,subs=+macros]
```

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

====

== Response

Status: 201, Created

```
== Error
```

Status: Default, Error

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href
```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#svm]
[.api-collapsible-fifth-title]
svm

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

```



```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#cluster_ad_proxy]
[.api-collapsible-fifth-title]
cluster_ad_proxy
```

The SVM configured as proxy for Active Directory authentication of cluster accounts.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|svm
|link:#svm[svm]
a|
```

```
|===
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|code
|string
```

```

a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
=====

```

```
:leveloffset: -1
```

```
= Manage LDAP server configuration
```

```
:leveloffset: +1
```

```
[[ID43e27165bedb082cbbe638a77b6672e6]]
```

```
= Security authentication cluster LDAP endpoint overview
```

```
== Overview
```

LDAP servers are used to centrally maintain user information. LDAP configurations must be set up to look up information stored in the LDAP directory on the external LDAP servers. This API is used to retrieve and manage cluster LDAP server configurations.

```
== Examples
```

```
=== Retrieving the cluster LDAP information
```

The cluster LDAP GET request retrieves the LDAP configuration of the cluster.

The following example shows how a GET request is used to retrieve the cluster LDAP information:

```
----
```

```
# The API:
```

```
/api/security/authentication/cluster/ldap
```

```
# The call:
```

```
curl -X GET "https://<mgmt-ip>/api/security/authentication/cluster/ldap"  
-H "accept: application/hal+json"
```

```
# The response:
```

```
{  
  "servers": [  
    "10.10.10.10",  
    "domainB.example.com"
```

```

],
"schema": "ad_idmu",
"port": 389,
"min_bind_level": "anonymous",
"bind_dn": "cn=Administrators,cn=users,dc=domainA,dc=example,dc=com",
"base_dn": "dc=domainA,dc=example,dc=com",
"base_scope": "subtree",
"use_start_tls": true,
"session_security": "none",
"_links": {
  "self": {
    "href": "/api/security/authentication/cluster/ldap"
  }
}
}
}
----

```

=== Creating the cluster LDAP configuration

The cluster LDAP POST operation creates an LDAP configuration for the cluster.

The following example shows how to issue a POST request with all of the fields specified:

```

----

# The API:
/api/security/authentication/cluster/ldap

# The call:
curl -X POST "https://<mgmt-ip>/api/security/authentication/cluster/ldap"
-H "accept: application/hal+json" -H "Content-Type: application/json" -d
"{ \"servers\": [ \"10.10.10.10\\\", \"domainB.example.com\" ], \"schema\":
\"ad_idmu\", \"port\": 389, \"min_bind_level\": \"anonymous\",
\"bind_dn\": \"cn=Administrators,cn=users,dc=domainA,dc=example,dc=com\",
\"bind_password\": \"abc\", \"base_dn\": \"dc=domainA,dc=example,dc=com\",
\"base_scope\": \"subtree\", \"use_start_tls\": false,
\"session_security\": \"none\"}"
----

```

The following example shows how to issue a POST request with a number of optional fields not specified:

```

----

```

```
# The API:
/api/security/authentication/cluster/ldap

# The call:
curl -X POST "https://<mgmt-ip>/api/security/authentication/cluster/ldap"
-H "accept: application/hal+json" -H "Content-Type: application/json" -d
"{ \"port\": 389, \"bind_dn\":
\"cn=Administrators,cn=users,dc=domainA,dc=example,dc=com\",
\"bind_password\": \"abc\", \"base_dn\": \"dc=domainA,dc=example,dc=com\",
\"session_security\": \"none\"}"
----
```

=== Updating the cluster LDAP configuration

The cluster LDAP PATCH request updates the LDAP configuration of the cluster.

The following example shows how a PATCH request is used to update the cluster LDAP configuration:

```
-----

# The API:
/api/security/authentication/cluster/ldap

# The call:
curl -X PATCH "https://<mgmt-ip>/api/security/authentication/cluster/ldap"
-H "accept: application/json" -H "Content-Type: application/json" -d "{
\"servers\": [ \"55.55.55.55\" ], \"schema\": \"ad_idmu\", \"port\": 636,
\"use_start_tls\": false }"
-----
```

=== Deleting the cluster LDAP configuration

The cluster LDAP DELETE request deletes the LDAP configuration of the cluster.

The following example shows how a DELETE request is used to delete the cluster LDAP configuration:

```
-----

# The API:
/api/security/authentication/cluster/ldap

# The call:
curl -X DELETE "https://<mgmt-
```

```
ip>/api/security/authentication/cluster/ldap" -H "accept:
application/hal+json"
```

```
[[ID12d26bbbbc7d35a2fa4e49cbf10c3646]]
```

```
= Delete the LDAP configuration for the cluster
```

```
[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-
block]#`/security/authentication/cluster/ldap`#
```

Deletes the LDAP configuration of the cluster.

== Learn more

*

```
xref:{relative_path}security_authentication_cluster_ldap_endpoint_overview
.html[DOC /security/authentication/cluster/ldap]
```

== Response

Status: 200, Ok

== Error

Status: Default, Error

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

```

```

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[IDb6b6d68a9fa0406e548e565a564d7e8b]]
= Retrieve the LDAP configuration for the cluster

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/authentication/cluster/ldap`#

```


Retrieves the cluster LDAP configuration.

== Learn more

*

xref:{relative_path}security_authentication_cluster_ldap_endpoint_overview.html[DOC /security/authentication/cluster/ldap]

== Parameters

[cols=5*,options=header]

|===

|Name

|Type

|In

|Required

|Description

|max_records

|integer

|query

|False

a|Limit the number of records returned.

|return_records

|boolean

|query

|False

a|The default is true for GET calls. When set to false, only the number of records is returned.

|return_timeout

|integer

|query

|False

a|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.

|order_by

|array[string]

```
|query
|False
a|Order results by specified fields and optional [asc|desc] direction.
Default direction is 'asc' for ascending.

|fields
|array[string]
|query
|False
a|Specify the fields to return.

|===

== Response
```

Status: 200, Ok

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|base_dn
|string
a|Specifies the default base DN for all searches.

|base_scope
|string
a|Specifies the default search scope for LDAP queries:

* base - search the named entry only
* onelevel - search all entries immediately below the DN
* subtree - search the named DN entry and the entire subtree below the DN

|bind_dn
|string
a|Specifies the user that binds to the LDAP servers.
```

```

|bind_password
|string
a|Specifies the bind password for the LDAP servers.

|min_bind_level
|string
a|The minimum bind authentication level. Possible values are:

* anonymous - anonymous bind
* simple - simple bind
* sasl - Simple Authentication and Security Layer (SASL) bind

|port
|integer
a|The port used to connect to the LDAP Servers.

|schema
|string
a|The name of the schema template used by the SVM.

* AD-IDMU - Active Directory Identity Management for UNIX
* AD-SFU - Active Directory Services for UNIX
* MS-AD-BIS - Active Directory Identity Management for UNIX
* RFC-2307 - Schema based on RFC 2307
* Custom schema

|servers
|array[string]
a|

|session_security
|string
a|Specifies the level of security to be used for LDAP communications:

* none - no signing or sealing
* sign - sign LDAP traffic
* seal - seal and sign LDAP traffic

|use_start_tls
|boolean
a|Specifies whether or not to use Start TLS over LDAP connections.

```

```
|===
```

```
.Example response
```

```
[%collapsible%closed]
```

```
====
```

```
[source,json,subs=+macros]
```

```
{  
  "_links": {  
    "self": {  
      "href": "/api/resourcelink"  
    }  
  },  
  "base_scope": "base",  
  "min_bind_level": "anonymous",  
  "port": 389,  
  "servers": {  
  },  
  "session_security": "none"  
}
```

```
====
```

```
== Error
```

Status: Default, Error

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
====
```

```
[source,json,subs=+macros]
```

```
{
```

```

"error": {
  "arguments": {
    "code": "string",
    "message": "string"
  },
  "code": "4",
  "message": "entry doesn't exist",
  "target": "uuid"
}
}

```

====

== Definitions

```

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block

```

====

```

[#href]
[.api-collapsible-fifth-title]
href

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|href
|string
a|

```

|===

```

[#_links]
[.api-collapsible-fifth-title]
_links

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|self
|link:#href[href]
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string

```

a|Error code

|message

|string

a|Error message

|target

|string

a|The target parameter that caused the error.

|===

//end collapsible .Definitions block

====

[[ID7a96eda297a3c2a2b2f9189d3ee055b2]]

= Update the LDAP configuration for the cluster

[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-block]#`/security/authentication/cluster/ldap`#

Both mandatory and optional parameters of the LDAP configuration can be updated.

IPv6 must be enabled if IPv6 family addresses are specified. Configuring more than one LDAP server is recommended to avoid a single point of failure. Both FQDNs and IP addresses are supported for the `servers` property.

The LDAP servers are validated as part of this operation. LDAP validation fails in the following scenarios:

- . The server does not have LDAP installed.
- . The server is invalid.
- . The server is unreachable.

== Learn more

*

xref:{relative_path}security_authentication_cluster_ldap_endpoint_overview.html[DOC /security/authentication/cluster/ldap]

== Parameters

[cols=5*,options=header]

|===

|Name

|Type

|In

|Required

|Description

|return_records

|boolean

|query

|False

a|The default is false. If set to true, the records are returned.

|===

== Request Body

[cols=3*,options=header]

|===

|Name

|Type

|Description

|_links

|link:#_links[_links]

a|

|base_dn

|string

a|Specifies the default base DN for all searches.

|base_scope

|string

a|Specifies the default search scope for LDAP queries:

* base - search the named entry only

* onelevel - search all entries immediately below the DN

* subtree - search the named DN entry and the entire subtree below the DN


```

|bind_dn
|string
a|Specifies the user that binds to the LDAP servers.

|bind_password
|string
a|Specifies the bind password for the LDAP servers.

|min_bind_level
|string
a|The minimum bind authentication level. Possible values are:

* anonymous - anonymous bind
* simple - simple bind
* sasl - Simple Authentication and Security Layer (SASL) bind

|port
|integer
a|The port used to connect to the LDAP Servers.

|schema
|string
a|The name of the schema template used by the SVM.

* AD-IDMU - Active Directory Identity Management for UNIX
* AD-SFU - Active Directory Services for UNIX
* MS-AD-BIS - Active Directory Identity Management for UNIX
* RFC-2307 - Schema based on RFC 2307
* Custom schema

|servers
|array[string]
a|

|session_security
|string
a|Specifies the level of security to be used for LDAP communications:

* none - no signing or sealing
* sign - sign LDAP traffic

```

```
* seal - seal and sign LDAP traffic
```

```
|use_start_tls
```

```
|boolean
```

```
a|Specifies whether or not to use Start TLS over LDAP connections.
```

```
|===
```

```
.Example request
```

```
[%collapsible%closed]
```

```
====
```

```
[source,json,subs=+macros]
```

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "base_scope": "base",
  "min_bind_level": "anonymous",
  "port": 389,
  "servers": {
  },
  "session_security": "none"
}
```

```
====
```

```
== Response
```

Status: 200, Ok

```
== Error
```

Status: Default

ONTAP Error Response Codes

```
|===
```

```
| Error Code | Description
```

```
| 4915203
```

```
| The specified LDAP schema does not exist.
```

```

| 4915208
| The specified LDAP servers contain duplicate server entries.

| 4915229
| DNS resolution failed due to an internal error. Contact technical
support if this issue persists.

| 4915231
| DNS resolution failed for one or more of the specified LDAP servers.
Verify that a valid DNS server is configured.

| 23724132
| DNS resolution failed for all the specified LDAP servers. Verify that a
valid DNS server is configured.

| 4915234
| Specified LDAP server is not supported because it is one of the
following: multicast, loopback, 0.0.0.0, or broadcast.

| 4915248
| LDAP servers cannot be empty or "-". Specified FQDN is not valid because
it is empty or "-" or it contains either special characters or "-" at the
start or end of the domain.

| 4915251
| STARTTLS and LDAPS cannot be used together

| 4915257
| The LDAP configuration is not valid. Verify that the Distinguished Names
and bind password are correct.

| 4915258
| The LDAP configuration is not valid. Verify that the servers are
reachable and that the network configuration is correct.

| 23724130
| Cannot use an IPv6 name server address because there are no IPv6
interfaces.
|===

[cols=3*,options=header]
|===
|Name
|Type

```

```

|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
=====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
=====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

```

```

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#cluster_ldap]
[.api-collapsible-fifth-title]
cluster_ldap

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|base_dn
|string
a|Specifies the default base DN for all searches.

|base_scope
|string
a|Specifies the default search scope for LDAP queries:

* base - search the named entry only
* onelevel - search all entries immediately below the DN
* subtree - search the named DN entry and the entire subtree below the DN

```

```

|bind_dn
|string
a|Specifies the user that binds to the LDAP servers.

|bind_password
|string
a|Specifies the bind password for the LDAP servers.

|min_bind_level
|string
a|The minimum bind authentication level. Possible values are:

* anonymous - anonymous bind
* simple - simple bind
* sasl - Simple Authentication and Security Layer (SASL) bind

|port
|integer
a|The port used to connect to the LDAP Servers.

|schema
|string
a|The name of the schema template used by the SVM.

* AD-IDMU - Active Directory Identity Management for UNIX
* AD-SFU - Active Directory Services for UNIX
* MS-AD-BIS - Active Directory Identity Management for UNIX
* RFC-2307 - Schema based on RFC 2307
* Custom schema

|servers
|array[string]
a|

|session_security
|string
a|Specifies the level of security to be used for LDAP communications:

* none - no signing or sealing
* sign - sign LDAP traffic
* seal - seal and sign LDAP traffic

```

```
|use_start_tls
|boolean
a|Specifies whether or not to use Start TLS over LDAP connections.
```

```
|===
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

```

```

|===

```

```

//end collapsible .Definitions block
====

```

```

[[IDde01b6f3fc8ca554282aa6419461fd33]]
= Create the LDAP configuration for the cluster

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/authentication/cluster/ldap`#

```

A cluster can have only one LDAP configuration. IPv6 must be enabled if IPv6 family addresses are specified.

== Required properties

- * `servers` - List of LDAP servers used for this client configuration.
- * `bind_dn` - Specifies the user that binds to the LDAP servers.
- * `base_dn` - Specifies the default base DN for all searches.

== Recommended optional properties

- * `schema` - Schema template name.
- * `port` - Port used to connect to the LDAP Servers.
- * `min_bind_level` - Minimum bind authentication level.
- * `bind_password` - Specifies the bind password for the LDAP servers.

- * ``base_scope`` - Specifies the default search scope for LDAP queries.
- * ``use_start_tls`` - Specifies whether or not to use Start TLS over LDAP connections.
- * ``session_security`` - Specifies the level of security to be used for LDAP communications.

== Default property values

- * ``schema`` - `_RFC-2307_`
- * ``port`` - `_389_`
- * ``min_bind_level`` - `_simple_`
- * ``base_scope`` - `_subtree_`
- * ``use_start_tls`` - `_false_`
- * ``session_security`` - `_none_`

Configuring more than one LDAP server is recommended to avoid a single point of failure. Both FQDNs and IP addresses are supported for the ``servers`` property.

The LDAP servers are validated as part of this operation. LDAP validation fails in the following scenarios:

- . The server does not have LDAP installed.
- . The server is invalid.
- . The server is unreachable.

== Learn more

*
[xref:{relative_path}security_authentication_cluster_ldap_endpoint_overview.html](#)[DOC /security/authentication/cluster/ldap]

== Parameters

[cols=5*,options=header]
|==

Name
Type
In
Required
Description

return_records
boolean
query
False

```

a|The default is false. If set to true, the records are returned.

|===

== Request Body

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|base_dn
|string
a|Specifies the default base DN for all searches.

|base_scope
|string
a|Specifies the default search scope for LDAP queries:

* base - search the named entry only
* onelevel - search all entries immediately below the DN
* subtree - search the named DN entry and the entire subtree below the DN

|bind_dn
|string
a|Specifies the user that binds to the LDAP servers.

|bind_password
|string
a|Specifies the bind password for the LDAP servers.

|min_bind_level
|string
a|The minimum bind authentication level. Possible values are:

* anonymous - anonymous bind

```

```

* simple - simple bind
* sasl - Simple Authentication and Security Layer (SASL) bind

|port
|integer
a|The port used to connect to the LDAP Servers.

|schema
|string
a|The name of the schema template used by the SVM.

* AD-IDMU - Active Directory Identity Management for UNIX
* AD-SFU - Active Directory Services for UNIX
* MS-AD-BIS - Active Directory Identity Management for UNIX
* RFC-2307 - Schema based on RFC 2307
* Custom schema

|servers
|array[string]
a|

|session_security
|string
a|Specifies the level of security to be used for LDAP communications:

* none - no signing or sealing
* sign - sign LDAP traffic
* seal - seal and sign LDAP traffic

|use_start_tls
|boolean
a|Specifies whether or not to use Start TLS over LDAP connections.

|===

.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {

```

```

    "self": {
      "href": "/api/resourcelink"
    },
    "base_scope": "base",
    "min_bind_level": "anonymous",
    "port": 389,
    "servers": {
    },
    "session_security": "none"
  }
====

== Response

```

Status: 201, Created

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of LDAP records.

|records
|array[link:#ldap_service[ldap_service]]
a|

|===

.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "next": {

```

```

    "href": "/api/resourcelink"
  },
  "self": {
    "href": "/api/resourcelink"
  }
},
"records": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "base_scope": "base",
  "min_bind_level": "anonymous",
  "port": 389,
  "preferred_ad_servers": {
  },
  "servers": {
  },
  "session_security": "none",
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
}
====

== Error

```

Status: Default

ONTAP Error Response Codes

```

|===
| Error Code | Description
| 4915203
| The specified LDAP schema does not exist.

```

```
| 4915207
| The specified LDAP servers contain duplicate server entries.

| 4915229
| DNS resolution failed due to an internal error. Contact technical
support if this issue persists.

| 4915231
| DNS resolution failed for one or more of the specified LDAP servers.
Verify that a valid DNS server is configured.

| 23724132
| DNS resolution failed for all the specified LDAP servers. Verify that a
valid DNS server is configured.

| 4915234
| The specified LDAP server is not supported because it is one of the
following: multicast, loopback, 0.0.0.0, or broadcast.

| 4915248
| LDAP servers cannot be empty or "-". Specified FQDN is invalid because
it is empty or "-" or it contains either special characters or "-" at the
start or end of the domain.

| 4915251
| STARTTLS and LDAPS cannot be used together.

| 4915257
| The LDAP configuration is invalid. Verify that bind-dn and bind password
are correct.

| 4915258
| The LDAP configuration is invalid. Verify that the servers are reachable
and that the network configuration is correct.

| 23724130
| Cannot use an IPv6 name server address because there are no IPv6
interfaces.
|===
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|error
|link:#error[error]
a|
```

```
|===
```

```
.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
```

```
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

```
== Definitions
```

```
[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
```

```
====
```

```
[#href]
[.api-collapsible-fifth-title]
href
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|href
|string
a|
```

```

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#cluster_ldap]
[.api-collapsible-fifth-title]
cluster_ldap

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|base_dn
|string
a|Specifies the default base DN for all searches.

|base_scope
|string
a|Specifies the default search scope for LDAP queries:

* base - search the named entry only
* onelevel - search all entries immediately below the DN
* subtree - search the named DN entry and the entire subtree below the DN

```



```
|bind_dn
|string
a|Specifies the user that binds to the LDAP servers.

|bind_password
|string
a|Specifies the bind password for the LDAP servers.

|min_bind_level
|string
a|The minimum bind authentication level. Possible values are:

* anonymous - anonymous bind
* simple - simple bind
* sasl - Simple Authentication and Security Layer (SASL) bind

|port
|integer
a|The port used to connect to the LDAP Servers.

|schema
|string
a|The name of the schema template used by the SVM.

* AD-IDMU - Active Directory Identity Management for UNIX
* AD-SFU - Active Directory Services for UNIX
* MS-AD-BIS - Active Directory Identity Management for UNIX
* RFC-2307 - Schema based on RFC 2307
* Custom schema

|servers
|array[string]
a|

|session_security
|string
a|Specifies the level of security to be used for LDAP communications:

* none - no signing or sealing
* sign - sign LDAP traffic
* seal - seal and sign LDAP traffic
```

```
|use_start_tls
|boolean
a|Specifies whether or not to use Start TLS over LDAP connections.
```

```
|===
```

```
[#_links]
[.api-collapsible-fifth-title]
_links
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|next
|link:#href[href]
```

```
a|
```

```
|self
|link:#href[href]
```

```
a|
```

```
|===
```

```
[#svm]
[.api-collapsible-fifth-title]
svm
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
```

```
a|
```

```
|name
|string
```

a|The name of the SVM.

|uuid

|string

a|The unique identifier of the SVM.

|===

[#ldap_service]

[.api-collapsible-fifth-title]

ldap_service

[cols=3*,options=header]

|===

|Name

|Type

|Description

|_links

|link:#_links[_links]

a|

|ad_domain

|string

a|This parameter specifies the name of the Active Directory domain used to discover LDAP servers for use by this client.

This is mutually exclusive with `servers` during POST and PATCH.

|base_dn

|string

a|Specifies the default base DN for all searches.

|base_scope

|string

a|Specifies the default search scope for LDAP queries:

- * base - search the named entry only
- * onelevel - search all entries immediately below the DN
- * subtree - search the named DN entry and the entire subtree below the DN

|bind_dn

```

|string
a|Specifies the user that binds to the LDAP servers.

|bind_password
|string
a|Specifies the bind password for the LDAP servers.

|min_bind_level
|string
a|The minimum bind authentication level. Possible values are:

* anonymous - anonymous bind
* simple - simple bind
* sasl - Simple Authentication and Security Layer (SASL) bind

|port
|integer
a|The port used to connect to the LDAP Servers.

|preferred_ad_servers
|array[string]
a|

|schema
|string
a|The name of the schema template used by the SVM.

* AD-IDMU - Active Directory Identity Management for UNIX
* AD-SFU - Active Directory Services for UNIX
* MS-AD-BIS - Active Directory Identity Management for UNIX
* RFC-2307 - Schema based on RFC 2307
* Custom schema

|servers
|array[string]
a|

|session_security
|string
a|Specifies the level of security to be used for LDAP communications:

* none - no signing or sealing

```

```
* sign - sign LDAP traffic
* seal - seal and sign LDAP traffic
```

```
|svm
|link:#svm[svm]
a|
```

```
|use_start_tls
|boolean
a|Specifies whether or not to use Start TLS over LDAP connections.
```

```
|===
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
|===
|Name
|Type
```

```

|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments


|code
|string
a|Error code


|message
|string
a|Error message


|target
|string
a|The target parameter that caused the error.


|===

//end collapsible .Definitions block
====

:leveloffset: -1

= Manage NIS configuration

:leveloffset: +1

[[ID5395f23068f06a9232c611616700c365]]
= Security authentication cluster NIS endpoint overview

== Overview

```

NIS servers are used to authenticate user and client computers. NIS domain name and NIS server information is required to configure NIS. This API

retrieves and manages NIS server configurations.

== Examples

=== Retrieving cluster NIS information

The cluster NIS GET request retrieves the NIS configuration of the cluster.

The following example shows how a GET request is used to retrieve the cluster NIS configuration:

The API:

/security/authentication/cluster/nis

The call:

```
curl -X GET "https://<mgmt-ip>/api/security/authentication/cluster/nis" -H  
"accept: application/hal+json"
```

The response:

```
{  
  "domain": "domainA.example.com",  
  "servers": [  
    "10.10.10.10",  
    "example.com"  
  ]  
  "bound_servers": [  
    "10.10.10.10"  
  ]  
}
```

=== Creating the cluster NIS configuration

The cluster NIS POST request creates a NIS configuration for the cluster.

The following example shows how a POST request is used to create a cluster NIS configuration:

The API:

/security/authentication/cluster/nis

The call:

```
curl -X POST "https://<mgmt-ip>/api/security/authentication/cluster/nis"
-H "accept: application/json" -H "Content-Type: application/json" -d "{
\"domain\": \"domainA.example.com\", \"servers\": [
\"10.10.10.10\", \"example.com\" ]}"
```

=== Updating the cluster NIS configuration

The cluster NIS PATCH request updates the NIS configuration of the cluster.

The following example shows how to update the domain:

The API:

/security/authentication/cluster/nis

The call:

```
curl -X PATCH "https://<mgmt-ip>/api/security/authentication/cluster/nis"
-H "accept: application/json" -H "Content-Type: application/json" -d "{
\"domain\": \"domainC.example.com\", \"servers\": [ \"13.13.13.13\" ]}"
```

The following example shows how to update the server:

The API:

/security/authentication/cluster/nis

The call:

```
curl -X PATCH "https://<mgmt-ip>/api/security/authentication/cluster/nis"
-H "accept: application/json" -H "Content-Type: application/json" -d "{
\"servers\": [ \"14.14.14.14\" ]}"
```

== Deleting the cluster NIS configuration

The cluster NIS DELETE request deletes the NIS configuration of the cluster.

The following example shows how a DELETE request is used to delete the cluster NIS configuration:

```
# The API:
/security/authentication/cluster/nis

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

'''

[[ID19a728c993595fd08643392f17b8a279]]
= Delete the NIS configuration for the cluster

[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-
block]#`/security/authentication/cluster/nis`#

Deletes the NIS configuration of the cluster. NIS can be removed as a
source from ns-switch if NIS is not used for lookups.

== Learn more

*
xref:{relative_path}security_authentication_cluster_nis_endpoint_overview.
html[DOC /security/authentication/cluster/nis]
```

== Response

Status: 200, Ok

== Error

Status: Default, Error

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|error
|link:#error[error]
a|
```

```
|===
```

```
.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
```

```
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

```
== Definitions
```

```
[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[IDdb3eea81539c5c41ef47d3826dbb8099]]

```

= Retrieve the NIS configuration for the cluster

```
[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-  
block]#`/security/authentication/cluster/nis`#
```

Retrieves the NIS configuration of the cluster. Both NIS domain and servers are displayed by default.

The `bound_servers` property indicates the successfully bound NIS servers.

== Learn more

*

```
xref:{relative_path}security_authentication_cluster_nis_endpoint_overview.  
html[DOC /security/authentication/cluster/nis]
```

== Parameters

```
[cols=5*,options=header]  
|==
```

```
|Name  
|Type  
|In  
|Required  
|Description
```

```
|max_records  
|integer  
|query  
|False  
a|Limit the number of records returned.
```

```
|return_records  
|boolean  
|query  
|False  
a|The default is true for GET calls. When set to false, only the number  
of records is returned.
```

```
|return_timeout  
|integer  
|query
```

```
|False
a|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.
```

```
|order_by
|array[string]
|query
|False
a|Order results by specified fields and optional [asc|desc] direction.
Default direction is 'asc' for ascending.
```

```
|fields
|array[string]
|query
|False
a|Specify the fields to return.
```

```
|===
```

```
== Response
```

Status: 200, Ok

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|bound_servers
|array[string]
a|

|domain
|string
a|The NIS domain to which this configuration belongs.

|servers
|array[string]
a|A list of hostnames or IP addresses of NIS servers used
by the NIS domain configuration.

|===

.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "bound_servers": {
  },
  "servers": {
  }
}
====

== Error

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name

```

```

|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

```



```

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[IDff5f7cb0407f843935256667d767cd6b]]
= Update the NIS configuration for the cluster

[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-
block]#`/security/authentication/cluster/nis`#

```

Both NIS domain and servers can be updated. Domains and servers cannot be empty. Both FQDNs and IP addresses are supported for the 'servers' field. If the domain is updated, NIS servers must also be specified. IPv6 must be enabled if IPv6 family addresses are specified for the `servers` property.

== Learn more

*

xref:{relative_path}security_authentication_cluster_nis_endpoint_overview.
html[DOC /security/authentication/cluster/nis]

== Parameters

[cols=5*,options=header]

|===

|Name

|Type

|In

|Required

|Description

|return_records

|boolean

|query

|False

a|The default is false. If set to true, the records are returned.

|===

== Request Body

[cols=3*,options=header]

|===

|Name

|Type

|Description

|_links

|link:#_links[_links]

a|

```
|bound_servers
|array[string]
a|

|domain
|string
a|The NIS domain to which this configuration belongs.

|servers
|array[string]
a|A list of hostnames or IP addresses of NIS servers used
by the NIS domain configuration.
```

|===

.Example request

[%collapsible%closed]

====

[source,json,subs=+macros]

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "bound_servers": {
  },
  "servers": {
  }
}
```

====

== Response

Status: 200, Ok

== Error

Status: Default

ONTAP Error Response Codes

```

|===
| Error Code | Description

| 1966253
| IPv6 is not enabled in the cluster .

| 3276964
| The NIS domain name or NIS server domain is too long. The maximum
supported for domain name is 64 characters and the maximum supported for
NIS server domain is 255 characters.

| 3276933
| A maximum of 10 NIS servers can be configured per SVM.

| 23724109
| DNS resolution failed for one or more specified servers.

| 23724112
| DNS resolution failed due to an internal error. Contact technical
support if this issue persists.

| 23724132
| DNS resolution failed for all the specified servers.

| 23724130
| Cannot use an IPv6 name server address because there are no IPv6
interfaces
|===

```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
=====
```

```

[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type

```

```

|Description

|self
|link:#href[href]
a|

|===

[#cluster_nis_service]
[.api-collapsible-fifth-title]
cluster_nis_service

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|bound_servers
|array[string]
a|

|domain
|string
a|The NIS domain to which this configuration belongs.

|servers
|array[string]
a|A list of hostnames or IP addresses of NIS servers used
by the NIS domain configuration.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===

```

```
|Name
|Type
|Description

|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
|===
```

```
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
|string
a|Error code
```

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
```

```
=====
```

```
[[IDd0f4aaa86d9c639e62fda0be8db55525]]
```

```
= Create the NIS configuration for the cluster
```

```
[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-  
block]#`/security/authentication/cluster/nis`#
```

The cluster can have one NIS server configuration. Specify the NIS domain and NIS servers as input. Domain name and servers fields cannot be empty. Both FQDNs and IP addresses are supported for the `server` property. IPv6 must be enabled if IPv6 family addresses are specified in the `server` property. A maximum of ten NIS servers are supported.

```
== Required properties
```

* `domain` - NIS domain to which this configuration belongs.

* `servers` - List of hostnames or IP addresses of NIS servers used by the NIS domain configuration.

```
== Learn more
```

*

```
xref:{relative_path}security_authentication_cluster_nis_endpoint_overview.  
html[DOC /security/authentication/cluster/nis]
```

```
== Parameters
```

```
[cols=5*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|In
```

```
|Required
```

```
|Description
```

```
|return_records
```



```
|boolean
|query
|False
a|The default is false. If set to true, the records are returned.
```

```
|===
```

```
== Request Body
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|bound_servers
```

```
|array[string]
```

```
a|
```

```
|domain
```

```
|string
```

```
a|The NIS domain to which this configuration belongs.
```

```
|servers
```

```
|array[string]
```

```
a|A list of hostnames or IP addresses of NIS servers used  
by the NIS domain configuration.
```

```
|===
```

```
.Example request
```

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
```

```
{
```

```
  "_links": {
```

```
    "self": {
```

```
      "href": "/api/resourcelink"
```

```

    }
  },
  "bound_servers": {
  },
  "servers": {
  }
}
====

```

```

== Response

```

Status: 201, Created

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of NIS domain records.

|records
|array[link:#cluster_nis_service[cluster_nis_service]]
a|

|===

```

```

.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  }
}

```

```

    }
  },
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "bound_servers": {
    },
    "servers": {
    }
  }
}
====

== Error

```

Status: Default

ONTAP Error Response Codes

```

|====
| Error Code | Description
|
| 1966253
| IPv6 is not enabled in the cluster.
|
| 3276964
| The NIS domain name or NIS server domain is too long. The maximum
supported for domain name is 64 characters and the maximum supported for
NIS server domain is 255 characters.
|
| 3276933
| A maximum of 10 NIS servers can be configured per SVM.
|
| 23724109
| DNS resolution failed for one or more specified servers.
|
| 23724112
| DNS resolution failed due to an internal error. Contact technical
support if this issue persists.
|
| 23724132
| DNS resolution failed for all the specified servers.

```

```

| 23724130
| Cannot use an IPv6 name server address because there are no IPv6
interfaces.
|===

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]

```

```

href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:href[href]
a|

|===

[#cluster_nis_service]
[.api-collapsible-fifth-title]
cluster_nis_service

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:_links[_links]
a|

|bound_servers

```

```

|array[string]
a|

|domain
|string
a|The NIS domain to which this configuration belongs.

|servers
|array[string]
a|A list of hostnames or IP addresses of NIS servers used
by the NIS domain configuration.

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|next
|link:#href[href]
a|

|self
|link:#href[href]
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
|string
a|Error code
```

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
=====

:leveloffset: -1

= Manage SAML service

:leveloffset: +1

[[ID7d21cd8c4b46af3807d7b0b113306085]]
= Security authentication cluster saml-sp endpoint overview

== Overview

This API is used to retrieve and display relevant information pertaining
to the SAML service provider configuration in the cluster. The POST
request creates a SAML service provider configuration if there is none
present. The DELETE request removes the SAML service provider
configuration. The PATCH request enables and disables SAML in the
cluster. Various responses are shown in the examples below.
+

'''

== Examples

=== Retrieving the SAML service provider configuration in the cluster

The following output shows the SAML service provider configuration in the
cluster.
+

'''

-----

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

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



```
sp" -H "accept: application/hal+json"
```

```
# The response:
```

```
{
  "idp_uri": "https://examplelab.customer.com/idp/Metadata",
  "enabled": true,
  "host": "172.21.74.181",
  "certificate": {
    "ca": "cluster1",
    "serial_number": "156F10C3EB4C51C1",
    "common_name": "cluster1"
  },
  "_links": {
    "self": {
      "href": "/api/security/authentication/cluster/saml-sp"
    }
  }
}
```

```
----
```

```
'''
```

```
=== Creating the SAML service provider configuration
```

The following output shows how to create a SAML service provider configuration in the cluster.

```
+
```

```
'''
```

```
----
```

```
# The API:
```

```
/api/security/authentication/cluster/saml-sp
```

```
# The call:
```

```
curl -X POST "https://<mgmt-ip>/api/security/authentication/cluster/saml-sp?return_records=true" -H "accept: application/hal+json" -d '{ "idp_uri": "https://examplelab.customer.com/idp/Metadata", "host": "172.21.74.181", "certificate": { "ca": "cluster1", "serial_number": "156F10C3EB4C51C1" } }'
```

```
----
```

```
'''
```

```
=== Updating the SAML service provider configuration
```

The following output shows how to enable a SAML service provider

configuration in the cluster.

Disabling the configuration requires the client to be authenticated through SAML prior to performing the operation.

+

'''

The API:

/api/security/authentication/cluster/saml-sp

The call:

```
curl -X PATCH "https://<mgmt-ip>/api/security/authentication/cluster/saml-sp/" -d '{ "enabled": true }'
```

'''

=== Deleting the SAML service provider configuration

'''

The API:

/api/security/authentication/cluster/saml-sp

The call:

```
curl -X DELETE "https://<mgmt-ip>/api/security/authentication/cluster/saml-sp/"
```

'''

[[ID0f5fc85bacc673af7d8fa23ed2aa29da]]

= Delete a SAML service provider configuration

[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-block]#`/security/authentication/cluster/saml-sp`#

Deletes a SAML service provider configuration.

== Learn more

* xref:{relative_path}security_authentication_cluster_saml-sp_endpoint_overview.html[DOC /security/authentication/cluster/saml-sp]

== Response

Status: 200, Ok

== Error

Status: Default

ONTAP Error Response Codes

```
|===
| Error Code | Description
| 12320803
| SAML must be disabled before the configuration can be removed.
|===
```

[cols=3*,options=header]

```
|===
|Name
|Type
|Description
```

```
|error
|link:#error[error]
a|
```

```
|===
```

```
.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
```

```

{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}

```

====

== Definitions

```

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block

```

====

```

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|code
|string
a|Argument code

```

```

|message
|string
a|Message argument

```

|===

```

[#error]
[.api-collapsible-fifth-title]
error

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[ID3295470f324197490be5dfb0b4414b2e]]
= Retrieve a SAML service provider configuration

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/authentication/cluster/saml-sp`#

Retrieves a SAML service provider configuration.

== Learn more

* xref:{relative_path}security_authentication_cluster_saml-

```

== Parameters

[cols=5*,options=header]

|===

|Name

|Type

|In

|Required

|Description

|max_records

|integer

|query

|False

a|Limit the number of records returned.

|return_records

|boolean

|query

|False

a|The default is true for GET calls. When set to false, only the number of records is returned.

|return_timeout

|integer

|query

|False

a|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.

|order_by

|array[string]

|query

|False

a|Order results by specified fields and optional [asc|desc] direction. Default direction is 'asc' for ascending.

```
|certificate.common_name
|string
|query
|False
a|Filter by certificate.common_name
```

```
|certificate.serial_number
|string
|query
|False
a|Filter by certificate.serial_number
```

```
|certificate.ca
|string
|query
|False
a|Filter by certificate.ca
```

```
|idp_uri
|string
|query
|False
a|Filter by idp_uri
```

```
|enabled
|boolean
|query
|False
a|Filter by enabled
```

```
|host
|string
|query
|False
a|Filter by host
```

```
|fields
|array[string]
|query
|False
a|Specify the fields to return.
```

```
|===
```

```
== Response
```

Status: 200, Ok

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|certificate
|link:#certificate[certificate]
a|

|enabled
|boolean
a|The SAML service provider is enabled. Valid for PATCH and GET
operations only.

|host
|string
a|The SAML service provider host.

|idp_uri
|string
a|The identity provider (IdP) metadata location. Required for POST
operations.

|===

.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
```



```

    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "certificate": {
      "common_name": "cluster1",
      "serial_number": "1506B24A94F566BA"
    },
    "idp_uri": "https://idp.example.com/FederationMetadata/2007-
06/FederationMetadata.xml"
  }
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}

```

```

}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#certificate]
[.api-collapsible-fifth-title]
certificate

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|ca
|string
a|Server certificate issuing certificate authority (CA). This cannot be
used with the server certificate common name.

|common_name
|string
a|Server certificate common name. This cannot be used with the
certificate authority (CA) or serial_number.

|serial_number
|string
a|Server certificate serial number. This cannot be used with the server
certificate common name.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

```

```

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[IDde946f7e842619b4e11acfdc9edc8e65]]
= Update a SAML service provider configuration

[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-
block]#`/security/authentication/cluster/saml-sp`#

```

Updates a SAML service provider configuration.

== Learn more

* xref:{relative_path}security_authentication_cluster_saml-sp_endpoint_overview.html[DOC /security/authentication/cluster/saml-sp]

== Parameters

[cols=5*,options=header]
|===

|Name
|Type
|In
|Required
|Description

|return_records
|boolean
|query
|False

a|The default is false. If set to true, the records are returned.

|===

== Request Body

[cols=3*,options=header]
|===

|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|certificate
|link:#certificate[certificate]
a|

```

|enabled
|boolean
a|The SAML service provider is enabled. Valid for PATCH and GET
operations only.

|host
|string
a|The SAML service provider host.

|idp_uri
|string
a|The identity provider (IdP) metadata location. Required for POST
operations.

|===

.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "certificate": {
    "common_name": "cluster1",
    "serial_number": "1506B24A94F566BA"
  },
  "idp_uri": "https://idp.example.com/FederationMetadata/2007-
06/FederationMetadata.xml"
}
====

== Response

```

Status: 200, Ok

```
== Error
```

ONTAP Error Response Codes

|===

| Error Code | Description

| 12320791

| SAML can only be disabled using the console or a SAML-authenticated application.

|===

[cols=3*,options=header]

|===

|Name

|Type

|Description

|error

|link:#error[error]

a|

|===

.Example error

[%collapsible%closed]

=====

[source,json,subs=+macros]

```

{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}

```

=====

== Definitions

```

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#certificate]
[.api-collapsible-fifth-title]
certificate

[cols=3*,options=header]
|===
|Name
|Type

```



```

|Description

|ca
|string
a|Server certificate issuing certificate authority (CA). This cannot be
used with the server certificate common name.

|common_name
|string
a|Server certificate common name. This cannot be used with the
certificate authority (CA) or serial_number.

|serial_number
|string
a|Server certificate serial number. This cannot be used with the server
certificate common name.

|===

[#security_saml_sp]
[.api-collapsible-fifth-title]
security_saml_sp

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|certificate
|link:#certificate[certificate]
a|

|enabled
|boolean
a|The SAML service provider is enabled. Valid for PATCH and GET
operations only.

```

```

|host
|string
a|The SAML service provider host.

|idp_uri
|string
a|The identity provider (IdP) metadata location. Required for POST
operations.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
|string
a|Error code
```

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
=====
```

```
[[ID95c46d0ba08955d07e8e38ec8171502d]]
= Create a SAML service provider configuration
```

```
[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/authentication/cluster/saml-sp`#
```

Creates a SAML service provider configuration. Note that "common_name" is mutually exclusive with "serial_number" and "ca" in POST. SAML will initially be disabled, requiring a patch to set "enabled" to "true", so that the user has time to complete the setup of the IdP.

== Required properties

* `idp_uri`

== Optional properties

```

* `certificate`
* `enabled`
* `host`

== Learn more

* xref:{relative_path}security_authentication_cluster_saml-
sp_endpoint_overview.html[DOC /security/authentication/cluster/saml-sp]

== Parameters

[cols=5*,options=header]
|===
|Name
|Type
|In
|Required
|Description

|return_timeout
|integer
|query
|False
a|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: 1

|return_records
|boolean
|query
|False
a|The default is false. If set to true, the records are returned.

* Default value: 1

|verify_metadata_server
|boolean

```

```

|query
|False
a|Verify IdP metadata server identity.

* Default value: 1

|===

== Request Body

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|certificate
|link:#certificate[certificate]
a|

|enabled
|boolean
a|The SAML service provider is enabled. Valid for PATCH and GET
operations only.

|host
|string
a|The SAML service provider host.

|idp_uri
|string
a|The identity provider (IdP) metadata location. Required for POST
operations.

|===

.Example request

```

```
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "certificate": {
    "common_name": "cluster1",
    "serial_number": "1506B24A94F566BA"
  },
  "idp_uri": "https://idp.example.com/FederationMetadata/2007-
06/FederationMetadata.xml"
}
====

== Response
```

Status: 202, Accepted

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|job
|link:#job_link[job_link]
a|

|===

.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "string"
  }
}
====

== Error

```

Status: Default

ONTAP Error Response Codes

```

|===
| Error Code | Description

| 12320789
| Failed to download data file from specified URI.

| 12320794
| The host parameter provided 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.

```

```
| 12320795
| A valid cluster or node management interface IP address must be
provided.

| 12320805
| The certificate information provided does not match any installed
certificates.

| 12320806
| The certificate information entered does not match any installed
certificates.

| 12320814
| An invalid IDP URI has been entered.

| 12320815
| An IDP URI must be an HTTPS or FTPS URI.
|===
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
```

```
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
```



```

    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#certificate]

```

```

[.api-collapsible-fifth-title]
certificate

[cols=3*,options=header]
|===
|Name
|Type
|Description

|ca
|string
a|Server certificate issuing certificate authority (CA). This cannot be
used with the server certificate common name.

|common_name
|string
a|Server certificate common name. This cannot be used with the
certificate authority (CA) or serial_number.

|serial_number
|string
a|Server certificate serial number. This cannot be used with the server
certificate common name.

|===

[#security_saml_sp]
[.api-collapsible-fifth-title]
security_saml_sp

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|certificate
|link:#certificate[certificate]
a|

```

```

|enabled
|boolean
a|The SAML service provider is enabled. Valid for PATCH and GET
operations only.

|host
|string
a|The SAML service provider host.

|idp_uri
|string
a|The identity provider (IdP) metadata location. Required for POST
operations.

|===

[#job_link]
[.api-collapsible-fifth-title]
job_link

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

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

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|code
```

```
|string
```

```
a|Argument code
```

```
|message
```

```
|string
```

```
a|Message argument
```

```
|===
```

```
[#error]
```

```
[.api-collapsible-fifth-title]
```

```
error
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|arguments
```

```
|array[link:#error_arguments[error_arguments]]
```

```
a|Message arguments
```

```
|code
```

```
|string
```

```
a|Error code
```

```
|message
```

```
|string
```

```
a|Error message
```

```
|target
```

```
|string
```

a|The target parameter that caused the error.

|===

//end collapsible .Definitions block

====

:leveloffset: -1

= Update the user account password

:leveloffset: +1

[[ID7c72ae76b7fb85a953158f35e697e54e]]

= Security authentication password endpoint overview

== Overview

This API changes the password for a local user account.

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

== Examples

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

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

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

```

-----

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

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

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

```

=== Changing the password of an SVM-scoped user

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

```

-----

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

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

```

'''

```

[[IDc95a4a6b00afff87791843881ca16107]]
= Update the user account password

```

```

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/authentication/password`#

```

Updates the password for a user account.

== Required parameters

```

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

== Optional parameters

* `owner.name` or `owner.uuid` - Name or UUID of the SVM for an SVM-scoped
user account.

== Related ONTAP commands

* `security login password`

== Learn more

*
xref:{relative_path}security_authentication_password_endpoint_overview.htm
l[DOC /security/authentication/password]
* xref:{relative_path}security_accounts_endpoint_overview.html[DOC
/security/accounts]

== Parameters

[cols=5*,options=header]
|===
|Name
|Type
|In
|Required
|Description

|return_records
|boolean
|query
|False
a|The default is false. If set to true, the records are returned.

|===

== Request Body

[cols=3*,options=header]
|===
|Name

```

```

|Type
|Description

|name
|string
a|The user account name whose password is being modified.

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

|password
|string
a|The password string

|===

.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  }
}
====

== Response

```

Status: 201, Created


```
== Error
```

Status: Default

ONTAP Error Response Codes

```
|===  
| Error Code | Description  
  
| 7077918  
| The password cannot contain the username.  
  
| 7077919  
| The minimum length for new password does not meet the policy.  
  
| 7077920  
| The new password must have both letters and numbers.  
  
| 7077921  
| The minimum number of special characters required do not meet the  
policy.  
  
| 7077924  
| The new password must be different than last N passwords.  
  
| 7077925  
| The new password must be different to the old password.  
  
| 7077940  
| The password exceeds maximum supported length.  
  
| 7077941  
| Defined password composition exceeds the maximum password length of 128  
characters.  
|===
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```

|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

```

```
[#_links]
[.api-collapsible-fifth-title]
_links
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|self
|link:#href[href]
a|
```

```
|===
```

```
[#owner]
[.api-collapsible-fifth-title]
owner
```

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

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#account_password]  
[.api-collapsible-fifth-title]  
account_password
```

The password object

```
[cols=3*,options=header]
```

```
|===
```

```
|Name  
|Type  
|Description
```

```
|name
```

```
|string
```

a|The user account name whose password is being modified.

```
|owner
```

```
|link:#owner[owner]
```

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

```
|password
```

```
|string
```

a|The password string

```
|===
```

```
[#error_arguments]  
[.api-collapsible-fifth-title]  
error_arguments
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name  
|Type
```

```

|Description

|code
|string
a|Argument code


|message
|string
a|Message argument


|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments


|code
|string
a|Error code


|message
|string
a|Error message


|target
|string
a|The target parameter that caused the error.


|===

```

```
//end collapsible .Definitions block
```

```
====
```

```
:leveloffset: -1
```

```
= Manage authentication keys (for admins)
```

```
:leveloffset: +1
```

```
[[ID97a3dcfde12c7dc30c4ef96f37c3e02c]]
```

```
= Security authentication publickeys endpoint overview
```

```
== Overview
```

This API configures the public keys for user accounts.

For secure shell (SSH) access, public-private key pair based authentication is possible by associating the public key with a user account.

Prerequisites:

You must have generated the SSH key.

You must be a cluster or SVM administrator to perform the user's public key.

```
== Examples
```

```
=== Creating a public key for cluster-scoped user accounts
```

Specify the user account name, public key, index, and comment in the body of the POST request. The owner.uuid or owner.name are not required for a cluster-scoped user account.

```
----
```

```
# The API:
```

```
POST "/api/security/authentication/publickey"
```

```
# The call
```

```
curl -k https://<mgmt-ip>/api/security/authentication/publickeys --request  
POST --data '{ "account": "pubuser2","comment": "Cserver-
```

```
Creation", "index": 0, "public_key": "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDWTerk2xXi3Lkrqrm6Q67aNmNDNKgpezwzl9Ap+DxtM
xmocHC52CuWecJjIUel21uAi0myscaJmC5Y0BzSnYuwcJ3/82kconFUwtK0h6QUTGqbc0vb4MZ
39yIiiItCOBWTot3msJYfZB+dgCcxMZ+0bl9YwZXrWMWP6XDJw/ai/EfWTZHC7e8Xe1mfp+C0c
GMhlxRvgfeGjhZqU85DBfdGD5Tu/67vD13Q+817Jf8iBxgrEFiqirnkWNX5dj+jkMlEVC3s6dY
ciJNBEiMxNkSFGTnkG74S61pvZNFD6mSznV/28hl3zSjwWiuacsP3BelydeG8nEcCRN5Ap7vMd
Vd" }'
```

=== Creating a public key for SVM-scoped user accounts

For a SVM-scoped account, specify either the SVM name as the owner.name or the SVM UUID as the owner.uuid along with other parameters for the user account. These parameters indicate the SVM that contains the user account for the public key being created and can be obtained from the response body of the GET request performed on the API"/api/svm/svms".

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

```
# The call
curl -k https://<mgmt-ip>/api/security/authentication/publickeys --request
POST --data '{ "account": "pubuser4", "comment": "Vserver-
Creation", "index": 0, "owner.uuid": "513a78c7-8c13-11e9-8f78-
005056bbf6ac", "owner.name": "vs0", "public_key": "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDWTerk2xXi3Lkrqrm6Q67aNmNDNKgpezwzl9Ap+DxtM
xmocHC52CuWecJjIUel21uAi0myscaJmC5Y0BzSnYuwcJ3/82kconFUwtK0h6QUTGqbc0vb4MZ
39yIiiItCOBWTot3msJYfZB+dgCcxMZ+0bl9YwZXrWMWP6XDJw/ai/EfWTZHC7e8Xe1mfp+C0c
GMhlxRvgfeGjhZqU85DBfdGD5Tu/67vD13Q+817Jf8iBxgrEFiqirnkWNX5dj+jkMlEVC3s6dY
ciJNBEiMxNkSFGTnkG74S61pvZNFD6mSznV/28hl3zSjwWiuacsP3BelydeG8nEcCRN5Ap7vMd
Vd" }'
```

=== Retrieving the configured public key for user accounts

Retrieves all public keys associated with the user accounts or a filtered list (for a specific user account name, a specific SVM and so on) of public keys.

```
# The API:
GET "/api/security/authentication/publickeys"
```

```
# The call to retrieve all the user accounts configured in the cluster:
```

```
curl -k https://<mgmt-ip>/api/security/authentication/publickeys
```

```
----
```

```
[[ID25c24cbd68949f747e9e144b0cee0739]]
```

```
= Retrieve public keys configured for user accounts
```

```
[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-  
block]#`/security/authentication/publickeys`#
```

Retrieves the public keys configured for user accounts.

== Learn more

*

```
xref:{relative_path}security_authentication_publickeys_endpoint_overview.h  
tml[DOC /security/authentication/publickeys]
```

== Parameters

```
[cols=5*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|In
```

```
|Required
```

```
|Description
```

```
|sha_fingerprint
```

```
|string
```

```
|query
```

```
|False
```

```
a|Filter by sha_fingerprint
```

```
|obfuscated_fingerprint
```

```
|string
```

```
|query
```

```
|False
```

```
a|Filter by obfuscated_fingerprint
```



```
|scope
|string
|query
|False
a|Filter by scope
```

```
|public_key
|string
|query
|False
a|Filter by public_key
```

```
|index
|integer
|query
|False
a|Filter by index
```

```
|comment
|string
|query
|False
a|Filter by comment
```

```
|account.name
|string
|query
|False
a|Filter by account.name
```

```
|owner.uuid
|string
|query
|False
a|Filter by owner.uuid
```

```
|owner.name
|string
|query
```

```

|False
a|Filter by owner.name

|fields
|array[string]
|query
|False
a|Specify the fields to return.

|max_records
|integer
|query
|False
a|Limit the number of records returned.

|return_records
|boolean
|query
|False
a|The default is true for GET calls. When set to false, only the number
of records is returned.

|return_timeout
|integer
|query
|False
a|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.

|order_by
|array[string]
|query
|False
a|Order results by specified fields and optional [asc|desc] direction.
Default direction is 'asc' for ascending.

|===

== Response

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records

|records
|array[link:#publickey[publickey]]
a|

|===

.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "account": {
      "_links": {
        "self": {

```

```

        "href": "/api/resourcelink"
      }
    },
    "name": "joe.smith"
  },
  "comment": "string",
  "obfuscated_fingerprint": "string",
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "scope": "cluster",
  "sha_fingerprint": "string"
}
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {

```

```

    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

```

== Definitions

```

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====

```

```

[#href]
[.api-collapsible-fifth-title]
href

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|href
|string
a|

```

```

|===

```

```

[#_links]
[.api-collapsible-fifth-title]
_links

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|next

```

```

|link:#href[href]
a|

|self
|link:#href[href]
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#account_reference]
[.api-collapsible-fifth-title]
account_reference

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|User account

|===

```

```
[#owner]
[.api-collapsible-fifth-title]
owner
```

Owner name and UUID that uniquely identifies the public key.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#publickey]
[.api-collapsible-fifth-title]
publickey
```

The public key for the user account (to access SSH).

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
```

```

a|

|account
|link:#account_reference[account_reference]
a|

|comment
|string
a|Optional comment for the public key.

|index
|integer
a|Index number for the public key (where there are multiple keys for the
same account).

|obfuscated_fingerprint
|string
a|The obfuscated fingerprint for the public key (READONLY).

|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the public key.

|public_key
|string
a|The public key

|scope
|string
a|Scope of the entity. Set to "cluster" for cluster owned objects and to
"svm" for SVM owned objects.

|sha_fingerprint
|string
a|The SHA fingerprint for the public key (READONLY).

|===

[#error_arguments]

```



```
[.api-collapsible-fifth-title]
```

```
error_arguments
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|code
```

```
|string
```

```
a|Argument code
```

```
|message
```

```
|string
```

```
a|Message argument
```

```
|===
```

```
[#error]
```

```
[.api-collapsible-fifth-title]
```

```
error
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|arguments
```

```
|array[link:#error_arguments[error_arguments]]
```

```
a|Message arguments
```

```
|code
```

```
|string
```

```
a|Error code
```

```
|message
```

```
|string
```

```
a|Error message
```

```

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
=====

[[IDcf1193539e8a1b8e818ab8f82e293851]]
= Create a public key for a user account

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/authentication/publickeys`#

Creates a public key for a user account.

== Learn more

*
xref:{relative_path}security_authentication_publickeys_endpoint_overview.h
tml[DOC /security/authentication/publickeys]

== Parameters

[cols=5*,options=header]
|===

|Name
|Type
|In
|Required
|Description

|return_records
|boolean
|query
|False
a|The default is false. If set to true, the records are returned.

```

```

|===

== Request Body

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|account
|link:#account_reference[account_reference]
a|

|comment
|string
a|Optional comment for the public key.

|index
|integer
a|Index number for the public key (where there are multiple keys for the
same account).

|obfuscated_fingerprint
|string
a|The obfuscated fingerprint for the public key (READONLY).

|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the public key.

|public_key
|string
a|The public key

|scope

```

```
|string
a|Scope of the entity. Set to "cluster" for cluster owned objects and to
"svm" for SVM owned objects.
```

```
|sha_fingerprint
|string
a|The SHA fingerprint for the public key (READONLY).
```

```
|===
```

```
.Example request
```

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "account": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "joe.smith"
  },
  "comment": "string",
  "obfuscated_fingerprint": "string",
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "scope": "cluster",
  "sha_fingerprint": "string"
}
=====
```

== Response

Status: 201, Created

== Error

Status: Default, Error

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
=====
```

```

[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#account_reference]
[.api-collapsible-fifth-title]
account_reference

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

```

```
|name
|string
a|User account
```

```
|===
```

```
[#owner]
[.api-collapsible-fifth-title]
owner
```

Owner name and UUID that uniquely identifies the public key.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#publickey]
[.api-collapsible-fifth-title]
publickey
```

The public key for the user account (to access SSH).

```
[cols=3*,options=header]
```

```

|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|account
|link:#account_reference[account_reference]
a|

|comment
|string
a|Optional comment for the public key.

|index
|integer
a|Index number for the public key (where there are multiple keys for the
same account).

|obfuscated_fingerprint
|string
a|The obfuscated fingerprint for the public key (READONLY).

|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the public key.

|public_key
|string
a|The public key

|scope
|string
a|Scope of the entity. Set to "cluster" for cluster owned objects and to
"svm" for SVM owned objects.

|sha_fingerprint
|string

```


a|The SHA fingerprint for the public key (READONLY).

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]

|===

|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]

|===

|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
=====
```

```
:leveloffset: -1
```

```
= Manage authentication keys (end-users)
```

```
:leveloffset: +1
```

```
[[ID38ae5e302483e41cc21c71cee632aa30]]
= Security authentication publickeys owner.uuid account.name index
endpoint overview
```

```
== Overview
```

This API configures the public keys for end-user (non-cluster admin) accounts.

Specify the owner UUID, the user account name, and the index in the URI path. The owner UUID corresponds to the UUID of the SVM containing the user account associated with the public key and can be obtained from the response body of the GET request performed on the API `"/api/svm/svms"`.

The index value corresponds to the public key that needs to be modified or deleted (it is possible to create more than one public key for the same user account).

== Examples

=== Retrieving the specific configured public key for user accounts

The API:

GET

"/api/security/authentication/publickeys/{owner.uuid}/{account.name}/{index}"

The call:

curl -k https://<mgmt-ip>/api/security/authentication/publickeys/513a78c7-8c13-11e9-8f78-005056bbf6ac/pubuser4/0

=== Updating the public key and comment for user accounts

The API:

PATCH

"/api/security/authentication/publickeys/{owner.uuid}/{account.name}/{index}"

The call:

curl -k https://<mgmt-ip>/api/security/authentication/publickeys/d49de271-8c11-11e9-8f78-005056bbf6ac/pubuser1/0 --request PATCH --data '{
"comment": "Cserver-modification", "public_key": "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQCMsLP/FeiT1J4Fb4GNVO4ioa1NIUHWeG08+anDbFke3J
cFT5JqBn0QZiG0uF0bqepken/moVKZg8iQng1arjP4ULhhje/LwDuUbaB7kvtPL2gyzAX1qFYn
BJ5R1LXja25Z4xeeaXUBJjhUmvpfque0TxbvpaG5V9rFTzVg9ccjBnkBchg3EkHF4VtHmrZNpT
DAUOBaz69FRYXYZ2ExoCHWqElHBjEp9D0DLN0XtzQA0IF9hJck6xja5RcAQ6f9pLMCol9vJiqp
cBAjkUmg1qH5ZNHsgDQ7dtGNGJw45zqXHPAy9z8yKJuIsdK2/4iVYLDL8mlHFEIgeADn6OSxui
j1" }'

=== Deleting the public key for user accounts

The API:

DELETE

"/api/security/authentication/publickeys/{owner.uuid}/{account.name}/{index}"

The call:

```
curl -k https://<mgmt-ip>/api/security/authentication/publickeys/d49de271-8c11-11e9-8f78-005056bbf6ac/pubuser1/0 --request DELETE
```

```
[[IDea829bdd3815a61e5b367499726ae438]]  
= Delete a public key for a user account
```

```
[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-  
block]#`/security/authentication/publickeys/{owner.uuid}/{account.name}/{i  
ndex}`#
```

Deletes the public key for a user account.

== Learn more

*

```
xref:{relative_path}security_authentication_publickeys_owner.uuid_account.  
name_index_endpoint_overview.html[DOC  
/security/authentication/publickeys/{owner.uuid}/{account.name}/{index}]
```

== Parameters

```
[cols=5*,options=header]  
|===
```

```
|Name  
|Type  
|In  
|Required  
|Description
```

```
|owner.uuid  
|string  
|path  
|True  
a|Account owner UUID
```

```
|account.name  
|string
```

```

|path
|True
a|User account name

|index
|integer
|path
|True
a|Index number for the public key (where there are multiple keys for the
same account).

* Max value: 99
* Min value: 0

|===

== Response

```

Status: 200, Ok

```

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {

```

```

        "code": "string",
        "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
}
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name

```

```

|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[ID06609d7578ab1d7ed432e02eaa6a5afb]]
= Retrieve public keys configured for a user account

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/authentication/publickeys/{owner.uuid}/{account.name}/{i
ndex}`#

Retrieves the public keys configured for a user account.

== Learn more

*
xref:{relative_path}security_authentication_publickeys_owner.uuid_account.
name_index_endpoint_overview.html[DOC

```

```
/security/authentication/publickeys/{owner.uuid}/{account.name}/{index}]
```

== Parameters

```
[cols=5*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|In
```

```
|Required
```

```
|Description
```

```
|owner.uuid
```

```
|string
```

```
|path
```

```
|True
```

```
a|Account owner UUID
```

```
|account.name
```

```
|string
```

```
|path
```

```
|True
```

```
a|User account name
```

```
|index
```

```
|integer
```

```
|path
```

```
|True
```

```
a|Index number for the public key (where there are multiple keys for the same account).
```

```
* Max value: 99
```

```
* Min value: 0
```

```
|fields
```

```
|array[string]
```

```
|query
```

```
|False
```

```
a|Specify the fields to return.
```

```
|max_records
```



```

|integer
|query
|False
a|Limit the number of records returned.

|return_records
|boolean
|query
|False
a|The default is true for GET calls. When set to false, only the number
of records is returned.

|return_timeout
|integer
|query
|False
a|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.

* Max value: 120
* Min value: 0

|order_by
|array[string]
|query
|False
a|Order results by specified fields and optional [asc|desc] direction.
Default direction is 'asc' for ascending.

|===

== Response

```

Status: 200, Ok

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|_links
|link:#_links[_links]
a|

|account
|link:#account_reference[account_reference]
a|

|comment
|string
a|Optional comment for the public key.

|index
|integer
a|Index number for the public key (where there are multiple keys for the
same account).

|obfuscated_fingerprint
|string
a|The obfuscated fingerprint for the public key (READONLY).

|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the public key.

|public_key
|string
a|The public key

|scope
|string
a|Scope of the entity. Set to "cluster" for cluster owned objects and to
"svm" for SVM owned objects.

|sha_fingerprint
|string
a|The SHA fingerprint for the public key (READONLY).

|===

```

```
.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "account": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "joe.smith"
  },
  "comment": "string",
  "obfuscated_fingerprint": "string",
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "scope": "cluster",
  "sha_fingerprint": "string"
}
====

== Error
```

Status: Default, Error

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

```

```
[#_links]
[.api-collapsible-fifth-title]
_links
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|self
|link:#href[href]
a|
```

```
|===
```

```
[#account_reference]
[.api-collapsible-fifth-title]
account_reference
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|User account
```

```
|===
```

```
[#owner]
[.api-collapsible-fifth-title]
owner
```

Owner name and UUID that uniquely identifies the public key.

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]

```

```

[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments


|code
|string
a|Error code


|message
|string
a|Error message


|target
|string
a|The target parameter that caused the error.


|===

//end collapsible .Definitions block
====

[[ID37444d6b845836e97b13019ace48c327]]
= Update a public key for a user account

[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-
block]#`/security/authentication/publickeys/{owner.uuid}/{account.name}/{i
ndex}`#

Updates the public key for a user account.

```

== Learn more

*

xref:{relative_path}security_authentication_publickeys_owner.uuid_account.
name_index_endpoint_overview.html[DOC
/security/authentication/publickeys/{owner.uuid}/{account.name}/{index}]

== Parameters

[cols=5*,options=header]
|==

|Name
|Type
|In
|Required
|Description

|owner.uuid
|string
|path
|True
a|Account owner UUID

|account.name
|string
|path
|True
a|User account name

|index
|integer
|path
|True
a|Index number for the public key (where there are multiple keys for the
same account).

* Max value: 99
* Min value: 0

|==

== Request Body


```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|account
|link:#account_reference[account_reference]
a|

|comment
|string
a|Optional comment for the public key.

|index
|integer
a|Index number for the public key (where there are multiple keys for the
same account).

|obfuscated_fingerprint
|string
a|The obfuscated fingerprint for the public key (READONLY).

|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the public key.

|public_key
|string
a|The public key

|scope
|string
a|Scope of the entity. Set to "cluster" for cluster owned objects and to
"svm" for SVM owned objects.

```

```
|sha_fingerprint
|string
a|The SHA fingerprint for the public key (READONLY).
```

```
|===
```

```
.Example request
```

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
```

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "account": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "joe.smith"
  },
  "comment": "string",
  "obfuscated_fingerprint": "string",
  "owner": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "scope": "cluster",
  "sha_fingerprint": "string"
}
```

```
=====
```

```
== Response
```

Status: 200, Ok

```
== Error
```

Status: Default, Error

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
=====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
=====
[#href]
[.api-collapsible-fifth-title]
```

```

href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:href[href]
a|

|===

[#account_reference]
[.api-collapsible-fifth-title]
account_reference

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:_links[_links]
a|

|name

```

```
|string
a|User account
```

```
|===
```

```
[#owner]
[.api-collapsible-fifth-title]
owner
```

Owner name and UUID that uniquely identifies the public key.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#publickey]
[.api-collapsible-fifth-title]
publickey
```

The public key for the user account (to access SSH).

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```

|Type
|Description

|_links
|link:#_links[_links]
a|

|account
|link:#account_reference[account_reference]
a|

|comment
|string
a|Optional comment for the public key.

|index
|integer
a|Index number for the public key (where there are multiple keys for the
same account).

|obfuscated_fingerprint
|string
a|The obfuscated fingerprint for the public key (READONLY).

|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the public key.

|public_key
|string
a|The public key

|scope
|string
a|Scope of the entity. Set to "cluster" for cluster owned objects and to
"svm" for SVM owned objects.

|sha_fingerprint
|string
a|The SHA fingerprint for the public key (READONLY).

```

|===

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
```

|===

```
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

|===

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
```

|===

```
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
|string
a|Error code
```

```
|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
=====
```

```
:leveloffset: -1
```

```
= Manage Azure Key Vaults
```

```
:leveloffset: +1
```

```
[[IDe3a495cb2c5b9c6da6d2713f1275f64c]]
= Security azure-key-vaults endpoint overview
```

```
== Overview
```

Azure Key Vault (AKV) is a cloud key management service (KMS) that provides a secure store for secrets. This feature allows ONTAP to securely store its encryption keys using AKV. In order to use AKV with ONTAP, you must first deploy an Azure application with the appropriate access to an AKV and then provide ONTAP with the necessary details, such as key vault name, application ID so that ONTAP can communicate with the deployed Azure application.

```
== Examples
```

```
=== Creating an AKV for a cluster
```

The example AKV is configured 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/azure-key-vaults

The call:

```
curl -X POST 'https://<mgmt-ip>/api/security/azure-key-  
vaults?return_records=true' -H 'accept: application/hal+json' -d "{  
  \"client_id\": \"client1\", \"tenant_id\": \"tenant1\", \"name\":  
  \"https://mykeyvault.azure.vault.net/\", \"key_id\": \"https://keyvault-  
test.vault.azure.net/keys/key1/a8e619fd8f234db3b0b95c59540e2a74\",  
  \"client_secret\" : \"myclientPwd\" }"
```

The response:

```
{  
  "num_records": 1,  
  "records": [  
    {  
      "uuid": "85619643-9a06-11ea-8d52-005056bbeba5",  
      "client_id": "client1",  
      "tenant_id": "tenant1",  
      "name": "https://mykeyvault.azure.vault.net/",  
      "key_id": "https://keyvault-  
test.vault.azure.net/keys/key1/a8e619fd8f234db3b0b95c59540e2a74",  
      "_links": {  
        "self": {  
          "href": "/api/security/azure-key-vaults/85619643-9a06-11ea-8d52-  
005056bbeba5"  
        }  
      }  
    }  
  ]  
}
```

'''

=== Creating an AKV for an SVM

The example AKV is configured for a specific SVM. Note the `_return_records=true_` query parameter is used to obtain the newly created key manager configuration.

```

# The API:
POST /api/security/azure-key-vaults

# The call:
curl -X POST 'https://<mgmt-ip>/api/security/azure-key-
vaults?return_records=true' -H 'accept: application/hal+json' -d "{
  \"svm\": { \"uuid\": \"4f7abf4c-9a07-11ea-8d52-005056bbeba5\" },
  \"client_id\": \"client1\", \"tenant_id\": \"tenant1\", \"name\":
  \"https://mykeyvault.azure.vault.net/\", \"key_id\": \"https://keyvault-
test.vault.azure.net/keys/key1/a8e619fd8f234db3b0b95c59540e2a74\",
  \"client_secret\" : \"myclientPwd\" }"

# The response:
{
  "num_records": 1,
  "records": [
    {
      "uuid": "024cd3cf-9a08-11ea-8d52-005056bbeba5",
      "svm": {
        "uuid": "4f7abf4c-9a07-11ea-8d52-005056bbeba5",
        "name": "vs0"
      },
      "client_id": "client1",
      "tenant_id": "tenant1",
      "name": "https://mykeyvault.azure.vault.net/",
      "key_id": "https://keyvault-
test.vault.azure.net/keys/key1/a8e619fd8f234db3b0b95c59540e2a74",
      "_links": {
        "self": {
          "href": "/api/security/azure-key-vaults/024cd3cf-9a08-11ea-8d52-
005056bbeba5"
        }
      }
    }
  ]
}
----

'''

=== Retrieving the AKVs configured for all clusters and SVMs

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

----

```

```

# The API:
GET /api/security/azure-key-vaults

# The call:
curl -X GET 'https://<mgmt-ip>/api/security/azure-key-vaults?fields=*'

# The response:
{
  "records": [
    {
      "uuid": "024cd3cf-9a08-11ea-8d52-005056bbeba5",
      "scope": "svm",
      "svm": {
        "uuid": "4f7abf4c-9a07-11ea-8d52-005056bbeba5",
        "name": "vs0"
      },
      "client_id": "client1",
      "tenant_id": "tenant1",
      "name": "https://mykeyvault.azure.vault.net/",
      "key_id": "https://keyvault-
test.vault.azure.net/keys/key1/a8e619fd8f234db3b0b95c59540e2a74",
      "state": {
        "cluster_state": true,
        "message": "",
        "code": 0
      },
      "_links": {
        "self": {
          "href": "/api/security/azure-key-vaults/024cd3cf-9a08-11ea-8d52-
005056bbeba5"
        }
      }
    },
    {
      "uuid": "85619643-9a06-11ea-8d52-005056bbeba5",
      "scope": "cluster",
      "client_id": "client1",
      "tenant_id": "tenant1",
      "name": "https://mykeyvault.azure.vault.net/",
      "key_id": "https://keyvault-
test.vault.azure.net/keys/key1/a8e619fd8f234db3b0b95c59540e2a74",
      "state": {
        "cluster_state": true,
        "message": "",
        "code": 0
      },
    },
  ]
}

```

```

    "_links": {
      "self": {
        "href": "/api/security/azure-key-vaults/85619643-9a06-11ea-8d52-005056bbeba5"
      }
    }
  ],
  "num_records": 2,
  "_links": {
    "self": {
      "href": "/api/security/azure-key-vaults?fields=*"
    }
  }
}
----

'''

```

=== Retrieving the AKV configured for a specific SVM

The following example retrieves a configured AKV for a specific SVM.

```

----

# The API:
GET /api/security/azure-key-vaults

# The call:
curl -X GET 'https://<mgmt-ip>/api/security/azure-key-vaults/85619643-9a06-11ea-8d52-005056bbeba5?fields=*'

# The response:
{
  "uuid": "85619643-9a06-11ea-8d52-005056bbeba5",
  "scope": "cluster",
  "client_id": "client1",
  "tenant_id": "tenant1",
  "name": "https://mykeyvault.azure.vault.net/",
  "key_id": "https://keyvault-test.vault.azure.net/keys/key1/a8e619fd8f234db3b0b95c59540e2a74",
  "state": {
    "cluster_state": true,
    "message": "",
    "code": 0
  }
},

```

```
"_links": {
  "self": {
    "href": "/api/security/azure-key-vaults/85619643-9a06-11ea-8d52-005056bbeba5"
  }
}
}
```

'''

=== Updating the client password of a specific SVM

The following example updates the client password of a configured AKV for a specific SVM.

```
# The API:
PATCH /api/security/azure-key-vaults
```

```
# The call:
curl -X PATCH 'https://<mgmt-ip>/api/security/azure-key-vaults/85619643-9a06-11ea-8d52-005056bbeba5' -d "{ \"client_secret\": \"newSecret\" }"
----
```

'''

=== Deleting an AKV configuration for a specific SVM

The following example deletes a configured AKV for a specific SVM.

```
# The API:
DELETE /api/security/azure-key-vaults
```

```
# The call:
curl -X DELETE 'https://<mgmt-ip>/api/security/azure-key-vaults/85619643-9a06-11ea-8d52-005056bbeba5'
----
```

'''

=== Restoring the keys for a specific SVM configured with an AKV

The following example restores all the keys of a specific SVM configured

with an AKV.

The API:

POST security/azure-key-vaults/{azure_key_vault.uuid}/restore

The call:

curl -X POST 'https://<mgmt-ip>/api/security/azure-key-vaults/85619643-9a06-11ea-8d52-005056bbeba5/restore'

The response:

```
{
  "job": {
    "uuid": "6ab6946f-9a0c-11ea-8d52-005056bbeba5",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/6ab6946f-9a0c-11ea-8d52-005056bbeba5"
      }
    }
  }
}
```

'''

[[ID66747c8b72bb7a0808eed1e81f65f72]]

= Retrieve AKVs configured for all clusters and SVMs

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-block]#`/security/azure-key-vaults`#

Retrieves AKVs configured for all clusters and SVMs.

== Related ONTAP commands

* `security key-manager external azure show`

== Learn more

* xref:{relative_path}security_azure-key-vaults_endpoint_overview.html[DOC

```
/security/azure-key-vaults]
```

```
== Parameters
```

```
[cols=5*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|In
```

```
|Required
```

```
|Description
```

```
|key_id
```

```
|string
```

```
|query
```

```
|False
```

```
a|Filter by key_id
```

```
|svm.uuid
```

```
|string
```

```
|query
```

```
|False
```

```
a|Filter by svm.uuid
```

```
|svm.name
```

```
|string
```

```
|query
```

```
|False
```

```
a|Filter by svm.name
```

```
|client_id
```

```
|string
```

```
|query
```

```
|False
```

```
a|Filter by client_id
```

```
|tenant_id
```

```
|string
```

```
|query
```

```
|False
```

```
a|Filter by tenant_id
```

```
|uuid
|string
|query
|False
a|Filter by uuid
```

```
|name
|string
|query
|False
a|Filter by name
```

```
|state.message
|string
|query
|False
a|Filter by state.message
```

```
|state.cluster_state
|boolean
|query
|False
a|Filter by state.cluster_state
```

```
|state.code
|integer
|query
|False
a|Filter by state.code
```

```
|scope
|string
|query
|False
a|Filter by scope
```

```
|fields
|array[string]
|query
```



```

|False
a|Specify the fields to return.

|max_records
|integer
|query
|False
a|Limit the number of records returned.

|return_timeout
|integer
|query
|False
a|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
a|The default is true for GET calls.  When set to false, only the number
of records is returned.

|order_by
|array[string]
|query
|False
a|Order results by specified fields and optional [asc|desc] direction.
Default direction is 'asc' for ascending.

|===

== Response

```

Status: 200, Ok

```

[cols=3*,options=header]
|===
|Name
|Type

```

|Description

|_links

|link:#_links[_links]

a|

|num_records

|integer

a|Number of records

|records

|array[link:#azure_key_vault[azure_key_vault]]

a|

|===

.Example response

[%collapsible%closed]

====

[source,json,subs=+macros]

{

 "_links": {

 "next": {

 "href": "/api/resourcelink"

 },

 "self": {

 "href": "/api/resourcelink"

 }

 },

 "records": {

 "_links": {

 "self": {

 "href": "/api/resourcelink"

 }

 },

 "client_id": "aaaaaaaa-bbbb-aaaa-bbbb-aaaaaaaaaaaaa",

 "client_secret": "abcdef",

 "key_id":

 "https://keyvault1.vault.azure.net/keys/key1/a8e619fd8f234db3b0b95c59540e2a74",

 "name": "https://kmip-akv-keyvault.vault.azure.net/",

 "scope": "svm",

 "state": {

 "code": 346758,

```

    "message": "AKV key protection is unavailable in following nodes -
node1, node2."
  },
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "tenant_id": "zzzzzzzz-yyy-zzzz-yyy-zzzzzzzzzzzz",
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
}
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },

```

```

    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

```

== Definitions

```

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====

```

```

[#href]
[.api-collapsible-fifth-title]
href

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|href
|string
a|

```

```

|===

```

```

[#_links]
[.api-collapsible-fifth-title]
_links

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|next
|link:#href[href]
a|

```

```

|self
|link:#href[href]

```

```

a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#state]
[.api-collapsible-fifth-title]
state

Indicates whether the AKV key protection is available cluster wide.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|cluster_state
|boolean
a|Set to true when AKV key protection is available on all nodes of the
cluster.

|code
|integer
a|Code corresponding to the status message. Returns a 0 if AKV key
protection is available in all nodes of the cluster.

```

```
|message
|string
a|Error message set when cluster availability is false.
```

```
|===
```

```
[#svm]
[.api-collapsible-fifth-title]
svm
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#azure_key_vault]
[.api-collapsible-fifth-title]
azure_key_vault
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
```

```

a|

|client_id
|string
a|Application client ID of the deployed Azure application with appropriate
access to an AKV.

|client_secret
|string
a|Password used by the application to prove its identity to AKV.

|key_id
|string
a|Key Identifier of AKV key encryption key.

|name
|string
a|Name of the deployed AKV that will be used by ONTAP for storing keys.

* example: https://kmip-akv-keyvault.vault.azure.net/
* format: uri

|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

|state
|link:#state[state]
a|Indicates whether the AKV key protection is available cluster wide.

|svm
|link:#svm[svm]
a|

|tenant_id
|string
a|Directory (tenant) ID of the deployed Azure application with appropriate
access to an AKV.

```

```
|uuid
|string
a|A unique identifier for the Azure Key Vault (AKV).
```

```
|===
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
```



```

|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[ID3fc16aa7f803cf59734098ccc03e923e]]
= Create an AKV configuration for all clusters and SVMs

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/azure-key-vaults`#

Configures the AKV configuration for all clusters and SVMs.

== Required properties

* `svm.uuid` or `svm.name` - Existing SVM in which to create a AKV.
* `client_id` - Application (client) ID of the deployed Azure application
with appropriate access to an AKV.
* `tenant_id` - Directory (tenant) ID of the deployed Azure application
with appropriate access to an AKV.
* `client_secret` - Password used by the application to prove its identity
to AKV.
* `key_id` - Key Identifier of AKV encryption key.
* `name` - Name of the deployed AKV used by ONTAP for storing keys.

== Related ONTAP commands

* `security key-manager external azure enable`

```

== Learn more

* xref:{relative_path}security_azure-key-vaults_endpoint_overview.html[DOC /security/azure-key-vaults]

== Parameters

[cols=5*,options=header]

|===

|Name

|Type

|In

|Required

|Description

|return_records

|boolean

|query

|False

a|The default is false. If set to true, the records are returned.

|===

== Request Body

[cols=3*,options=header]

|===

|Name

|Type

|Description

|_links

|link:#_links[_links]

a|

|client_id

|string

a|Application client ID of the deployed Azure application with appropriate access to an AKV.

|client_secret

```

|string
a|Password used by the application to prove its identity to AKV.

|key_id
|string
a|Key Identifier of AKV key encryption key.

|name
|string
a|Name of the deployed AKV that will be used by ONTAP for storing keys.

* example: https://kmip-akv-keyvault.vault.azure.net/
* format: uri

|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

|state
|link:#state[state]
a|Indicates whether the AKV key protection is available cluster wide.

|svm
|link:#svm[svm]
a|

|tenant_id
|string
a|Directory (tenant) ID of the deployed Azure application with appropriate
access to an AKV.

|uuid
|string
a|A unique identifier for the Azure Key Vault (AKV).

|===

```

.Example request

```
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "client_id": "aaaaaaaa-bbbb-aaaa-bbbb-aaaaaaaaaaaaa",
  "client_secret": "abcdef",
  "key_id":
"https://keyvault1.vault.azure.net/keys/key1/a8e619fd8f234db3b0b95c59540e2a74",
  "name": "https://kmip-akv-keyvault.vault.azure.net/",
  "scope": "svm",
  "state": {
    "code": 346758,
    "message": "AKV key protection is unavailable in following nodes -
node1, node2."
  },
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "tenant_id": "zzzzzzzz-yyyy-zzzz-yyyy-zzzzzzzzzzzzz",
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
}
====

== Response
```

Status: 201, Created

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records

|records
|array[link:#azure_key_vault[azure_key_vault]]
a|

|===

```

.Example response

[%collapsible%closed]

====

[source,json,subs=+macros]

```

{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "client_id": "aaaaaaaa-bbbb-aaaa-bbbb-aaaaaaaaaaaa",
    "client_secret": "abcdef",
    "key_id":
"https://keyvault1.vault.azure.net/keys/key1/a8e619fd8f234db3b0b95c59540e2a74",
    "name": "https://kmip-akv-keyvault.vault.azure.net/",
    "scope": "svm",
    "state": {
      "code": 346758,
      "message": "AKV key protection is unavailable in following nodes -
node1, node2."
    }
  }
}

```

```

    },
    "svm": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "svm1",
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    },
    "tenant_id": "zzzzzzzz-yyy-zzzz-yyy-zzzzzzzzzzzz",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  }
}
====

```

== Error

Status: Default

ONTAP Error Response Codes

```

|====
| Error Code | Description
|
| 3735553
| Failed to create self-signed certificate.
|
| 3735664
| The specified key size is not supported in FIPS mode.
|
| 3735665
| The specified hash function is not supported in FIPS mode.
|
| 3735700
| The specified key size is not supported.
|
| 52559972
| The certificates start date is later than the current date.
|
| 65537500
| A key manager has already been configured for this SVM.
|
| 65537503
| Passwords do not match.

```

```
| 65537504
| Internal error. Failed to store configuration in internal database.

| 65537505
| One or more volume encryption keys of the given SVM are stored on a key
manager configured for the admin SVM.

| 65537506
| AKV is not supported in MetroCluster configurations.

| 65537512
| AKV cannot be configured for the given SVM as not all nodes in the
cluster have the azure.key.vault capability needed to enable the feature.

| 65537514
| Failed to check or update the azure.key.vault feature capability.

| 65537518
| Failed to find an interface with Cluster role.
|===
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
```

```
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
```

```

    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

```



```

[#state]
[.api-collapsible-fifth-title]
state

Indicates whether the AKV key protection is available cluster wide.


[cols=3*,options=header]
|===
|Name
|Type
|Description

|cluster_state
|boolean
a|Set to true when AKV key protection is available on all nodes of the
cluster.


|code
|integer
a|Code corresponding to the status message. Returns a 0 if AKV key
protection is available in all nodes of the cluster.


|message
|string
a|Error message set when cluster availability is false.


|===


[#svm]
[.api-collapsible-fifth-title]
svm

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#azure_key_vault]
[.api-collapsible-fifth-title]
azure_key_vault
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|client_id
|string
a|Application client ID of the deployed Azure application with appropriate
access to an AKV.
```

```
|client_secret
|string
a|Password used by the application to prove its identity to AKV.
```

```
|key_id
|string
a|Key Identifier of AKV key encryption key.
```

```
|name
|string
a|Name of the deployed AKV that will be used by ONTAP for storing keys.
```

```

* example: https://kmip-akv-keyvault.vault.azure.net/
* format: uri

|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

|state
|link:#state[state]
a|Indicates whether the AKV key protection is available cluster wide.

|svm
|link:#svm[svm]
a|

|tenant_id
|string
a|Directory (tenant) ID of the deployed Azure application with appropriate
access to an AKV.

|uuid
|string
a|A unique identifier for the Azure Key Vault (AKV).

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|next
|link:#href[href]
a|

```

```

|self
|link:#href[href]
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string

```

```

a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[ID1bc5f4032b77844d6638f9b54240f009]]
= Restore keys for an SVM from a configured AKV

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/azure-key-vaults/{azure_key_vault.uuid}/restore`#

Restore the keys for an SVM from a configured AKV.

== Related ONTAP commands

* `security key-manager external azure restore`

== Parameters

[cols=5*,options=header]
|===

|Name
|Type
|In
|Required
|Description

```

```
|return_timeout
|integer
|query
|False
```

a|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.

```
|return_records
|boolean
|query
|False
```

a|The default is false. If set to true, the records are returned.

```
|azure_key_vault.uuid
|string
|path
|True
```

a|UUID of the existing AKV configuration.

```
|===
```

== Response

Status: 202, Accepted

== Error

Status: Default

ONTAP Error Response Codes

```
|===
```

```
| Error Code | Description
```

```
| 65537511
```

```
| AKV is not configured for the given SVM.
```

```
| 65537515
```

```
| Failed to restore keys on some nodes in the cluster.
```

```
|===
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
```

```
{
```

```
  "error": {
```

```
    "arguments": {
```

```
      "code": "string",
```

```
      "message": "string"
```

```
    },
```

```
    "code": "4",
```

```
    "message": "entry doesn't exist",
```

```
    "target": "uuid"
```

```
  }
```

```
}
```

```
=====
```

```
== Definitions
```

```
[.api-def-first-level]
```

```
.See Definitions
```

```
[%collapsible%closed]
```

```
//Start collapsible Definitions block
```

```
=====
```

```
[#error_arguments]
```

```
[.api-collapsible-fifth-title]
```

```
error_arguments
```

```
[cols=3*,options=header]
```

```

|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

```



```
|===
```

```
//end collapsible .Definitions block
```

```
=====
```

```
[[ID92a8013e47c390ea6659b1ddf9282e6a]]
```

```
= Delete an AKV configuration
```

```
[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-  
block]#`/security/azure-key-vaults/{uuid}`#
```

Deletes an AKV configuration.

== Related ONTAP commands

* `security key-manager external azure disable`

== Learn more

* xref:{relative_path}security_azure-key-vaults_endpoint_overview.html[DOC
/security/azure-key-vaults]

== Parameters

```
[cols=5*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|In
```

```
|Required
```

```
|Description
```

```
|uuid
```

```
|string
```

```
|path
```

```
|True
```

```
a|
```

```
|===
```

== Response

Status: 200, Ok

== Error

Status: Default

ONTAP Error Response Codes

|===

Error Code	Description
------------	-------------

65536242	One or more Storage Encryption devices are assigned an authentication key.
----------	--

65536817	Internal error. Failed to determine if key manager is safe to disable.
----------	--

65536827	Internal error. Failed to determine if the given SVM has any encrypted volumes.
----------	---

65536834	Internal error. Failed to get existing key-server details for the given SVM.
----------	--

65536867	Volume encryption keys (VEK) for one or more encrypted volumes are stored on the key manager configured for the given SVM.
----------	--

65536883	Internal error. Volume encryption key is missing for a volume.
----------	--

65536884	Internal error. Volume encryption key is invalid for a volume.
----------	--

65536924	Cannot remove key manager that still contains one or more NSE authentication keys.
----------	--

65537511	AKV is not configured for the given SVM.
----------	--

```
| 196608301
| Internal error. Failed to get encryption type.
```

```
| 196608305
| NAE aggregates found in the cluster.
|===
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|error
|link:#error[error]
a|
```

```
|===
```

```
.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
```

```
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

```
====
```

```
== Definitions
```

```
[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#error_arguments]
```

[.api-collapsible-fifth-title]

error_arguments

[cols=3*,options=header]

|===

|Name

|Type

|Description

|code

|string

a|Argument code

|message

|string

a|Message argument

|===

[#error]

[.api-collapsible-fifth-title]

error

[cols=3*,options=header]

|===

|Name

|Type

|Description

|arguments

|array[link:#error_arguments[error_arguments]]

a|Message arguments

|code

|string

a|Error code

|message

|string

a|Error message

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
=====
```

```
[[ID98dd63f7b3bf9e83d20d3322183138d5]]
= Retrieve AKV configuration for an SVM specified by the UUID
```

```
[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/azure-key-vaults/{uuid}`#
```

Retrieves the AKV configuration for the SVM specified by the UUID.

== Related ONTAP commands

* `security key-manager external azure show`

== Learn more

* xref:{relative_path}security_azure-key-vaults_endpoint_overview.html[DOC
/security/azure-key-vaults]

== Parameters

```
[cols=5*,options=header]
|===
```

```
|Name
|Type
|In
|Required
|Description
```

```
|uuid
|string
|path
```

```

|True
a|AKV UUID

|fields
|array[string]
|query
|False
a|Specify the fields to return.

|===

== Response

```

Status: 200, Ok

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|client_id
|string
a|Application client ID of the deployed Azure application with appropriate
access to an AKV.

|client_secret
|string
a|Password used by the application to prove its identity to AKV.

|key_id
|string
a|Key Identifier of AKV key encryption key.

|name
|string
a|Name of the deployed AKV that will be used by ONTAP for storing keys.

```

```

* example: https://kmip-akv-keyvault.vault.azure.net/
* format: uri

|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

|state
|link:#state[state]
a|Indicates whether the AKV key protection is available cluster wide.

|svm
|link:#svm[svm]
a|

|tenant_id
|string
a|Directory (tenant) ID of the deployed Azure application with appropriate
access to an AKV.

|uuid
|string
a|A unique identifier for the Azure Key Vault (AKV).

|===

.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "client_id": "aaaaaaaa-bbbb-aaaa-bbbb-aaaaaaaaaaaaa",
  "client_secret": "abcdef",
  "key_id":
"https://keyvault1.vault.azure.net/keys/key1/a8e619fd8f234db3b0b95c59540e2

```

```

a74",
  "name": "https://kmip-akv-keyvault.vault.azure.net/",
  "scope": "svm",
  "state": {
    "code": 346758,
    "message": "AKV key protection is unavailable in following nodes -
node1, node2."
  },
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "tenant_id": "zzzzzzzz-yyy-zzzz-yyy-zzzzzzzzzzzz",
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {

```



```

    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

```

== Definitions

```

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====

```

```

[#href]
[.api-collapsible-fifth-title]
href

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|href
|string
a|

```

```

|===

```

```

[#_links]
[.api-collapsible-fifth-title]
_links

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|self

```

|link:#href[href]

a|

|===

[#state]

[.api-collapsible-fifth-title]

state

Indicates whether the AKV key protection is available cluster wide.

[cols=3*,options=header]

|===

|Name

|Type

|Description

|cluster_state

|boolean

a|Set to true when AKV key protection is available on all nodes of the cluster.

|code

|integer

a|Code corresponding to the status message. Returns a 0 if AKV key protection is available in all nodes of the cluster.

|message

|string

a|Error message set when cluster availability is false.

|===

[#svm]

[.api-collapsible-fifth-title]

svm

[cols=3*,options=header]

|===

|Name

|Type

```

|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]

```

```

|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments


|code
|string
a|Error code


|message
|string
a|Error message


|target
|string
a|The target parameter that caused the error.


|===


//end collapsible .Definitions block
====

[[ID8c7e66404b604aa11d0f911a029e95a4]]
= Update the AKV configuration

[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-
block]#`/security/azure-key-vaults/{uuid}`#


Updates the AKV configuration.


== Required properties


* `client_secret` - New password used to prove the application's identity
to the AKV.

```

== Related ONTAP commands

* `security key-manager external azure modify`

== Learn more

* xref:{relative_path}security_azure-key-vaults_endpoint_overview.html[DOC /security/azure-key-vaults]

== Parameters

[cols=5*,options=header]

|===

|Name

|Type

|In

|Required

|Description

|uuid

|string

|path

|True

a|AKV UUID

|===

== Request Body

[cols=3*,options=header]

|===

|Name

|Type

|Description

|_links

|link:#_links[_links]

a|

|client_id

|string

a|Application client ID of the deployed Azure application with appropriate

access to an AKV.

|client_secret

|string

a|Password used by the application to prove its identity to AKV.

|key_id

|string

a|Key Identifier of AKV key encryption key.

|name

|string

a|Name of the deployed AKV that will be used by ONTAP for storing keys.

* example: <https://kmip-akv-keyvault.vault.azure.net/>

* format: uri

|scope

|string

a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".

|state

|link:#state[state]

a|Indicates whether the AKV key protection is available cluster wide.

|svm

|link:#svm[svm]

a|

|tenant_id

|string

a|Directory (tenant) ID of the deployed Azure application with appropriate access to an AKV.

|uuid

|string

a|A unique identifier for the Azure Key Vault (AKV).

|===

.Example request

[%collapsible%closed]

====

[source,json,subs=+macros]

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "client_id": "aaaaaaaa-bbbb-aaaa-bbbb-aaaaaaaaaaaaa",
  "client_secret": "abcdef",
  "key_id":
"https://keyvault1.vault.azure.net/keys/key1/a8e619fd8f234db3b0b95c59540e2a74",
  "name": "https://kmip-akv-keyvault.vault.azure.net/",
  "scope": "svm",
  "state": {
    "code": 346758,
    "message": "AKV key protection is unavailable in following nodes -
node1, node2."
  },
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "tenant_id": "zzzzzzzz-yyyy-zzzz-yyyy-zzzzzzzzzzzzz",
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
}
```

====

== Response

Status: 200, Ok

== Error

ONTAP Error Response Codes

|===

| Error Code | Description

| 65537503

| Passwords do not match.

| 65537504

| Internal error. Failed to store configuration in internal database.

| 65537511

| AKV is not configured for the given SVM.

| 65537517

| The field "new_client_secret" must be specified.

|===

[cols=3*,options=header]

|===

|Name

|Type

|Description

|error

|link:#error[error]

a|

|===

.Example error

[%collapsible%closed]

=====

[source,json,subs=+macros]

```
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
```



```

    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

```

```

[#state]
[.api-collapsible-fifth-title]
state

Indicates whether the AKV key protection is available cluster wide.


[cols=3*,options=header]
|===
|Name
|Type
|Description

|cluster_state
|boolean
a|Set to true when AKV key protection is available on all nodes of the
cluster.


|code
|integer
a|Code corresponding to the status message. Returns a 0 if AKV key
protection is available in all nodes of the cluster.


|message
|string
a|Error message set when cluster availability is false.


|===


[#svm]
[.api-collapsible-fifth-title]
svm

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#azure_key_vault]
[.api-collapsible-fifth-title]
azure_key_vault
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|client_id
|string
a|Application client ID of the deployed Azure application with appropriate
access to an AKV.
```

```
|client_secret
|string
a|Password used by the application to prove its identity to AKV.
```

```
|key_id
|string
a|Key Identifier of AKV key encryption key.
```

```
|name
|string
a|Name of the deployed AKV that will be used by ONTAP for storing keys.
```

```

* example: https://kmip-akv-keyvault.vault.azure.net/
* format: uri

|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

|state
|link:#state[state]
a|Indicates whether the AKV key protection is available cluster wide.

|svm
|link:#svm[svm]
a|

|tenant_id
|string
a|Directory (tenant) ID of the deployed Azure application with appropriate
access to an AKV.

|uuid
|string
a|A unique identifier for the Azure Key Vault (AKV).

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

```

```

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
=====

```

```
:leveloffset: -1
```

= Manage security certificates

```
:leveloffset: +1
```

```
[[ID49dc7c2f1559b4f0e5c8cf3da8750b34]]
```

= Security certificates endpoint overview

== Overview

This API displays security certificate information and manages the certificates in ONTAP.

== Installing certificates in ONTAP

The security certificates GET request retrieves all of the certificates in the cluster.

== Examples

=== Retrieving all certificates installed in the cluster with their common-names

```
# The API:
/api/security/certificates
```

```
# The call:
curl -X GET "https://<mgmt-
ip>/api/security/certificates?fields=common_name" -H "accept:
application/hal+json"
```

```
# The response:
{
  "records": [
    {
      "svm": {
        "name": "vs0"
      },
      "uuid": "dad2363b-8ac0-11e8-9058-005056b482fc",
      "common_name": "vs0",
```

```

    "_links": {
      "self": {
        "href": "/api/security/certificates/dad2363b-8ac0-11e8-9058-005056b482fc"
      }
    },
    {
      "uuid": "1941e048-8ac1-11e8-9058-005056b482fc",
      "common_name": "ROOT",
      "_links": {
        "self": {
          "href": "/api/security/certificates/1941e048-8ac1-11e8-9058-005056b482fc"
        }
      }
    },
    {
      "uuid": "5a3a77a8-892d-11e8-b7da-005056b482fc",
      "common_name": "gshanccluster-4",
      "_links": {
        "self": {
          "href": "/api/security/certificates/5a3a77a8-892d-11e8-b7da-005056b482fc"
        }
      }
    }
  ],
  "num_records": 3,
  "_links": {
    "self": {
      "href": "/api/security/certificates?fields=common_name"
    }
  }
}
-----
'''

```

=== Retrieving all certificates installed at cluster-scope with their common-names

```

'''
-----

```

```

# The API:
/api/security/certificates

# The call:
curl -X GET "https://<mgmt-
ip>/api/security/certificates?scope=cluster&fields=common_name" -H
"accept: application/hal+json"

# The response:
{
  "records": [
    {
      "uuid": "1941e048-8ac1-11e8-9058-005056b482fc",
      "scope": "cluster",
      "common_name": "ROOT",
      "_links": {
        "self": {
          "href": "/api/security/certificates/1941e048-8ac1-11e8-9058-
005056b482fc"
        }
      }
    },
    {
      "uuid": "5a3a77a8-892d-11e8-b7da-005056b482fc",
      "scope": "cluster",
      "common_name": "gshancluster-4",
      "_links": {
        "self": {
          "href": "/api/security/certificates/5a3a77a8-892d-11e8-b7da-
005056b482fc"
        }
      }
    }
  ],
  "num_records": 2,
  "_links": {
    "self": {
      "href": "/api/security/certificates?scope=cluster&fields=common_name"
    }
  }
}
----

'''

=== Retrieving all certificates installed on a specific SVM with their

```



```

common-names

'''

----

# The API:
/api/security/certificates

# The call:
curl -X GET "https://<mgmt-
ip>/api/security/certificates?svm.name=vs0&fields=common_name" -H "accept:
application/hal+json"

# The response:
{
"records": [
  {
    "svm": {
      "name": "vs0"
    },
    "uuid": "dad2363b-8ac0-11e8-9058-005056b482fc",
    "common_name": "vs0",
    "_links": {
      "self": {
        "href": "/api/security/certificates/dad2363b-8ac0-11e8-9058-
005056b482fc"
      }
    }
  },
  ],
"num_records": 1,
"_links": {
  "self": {
    "href": "/api/security/certificates?svm.name=vs0&fields=common_name"
  }
}
}

'''

=== Retrieving a certificate using its UUID for all fields

'''

```



```

}
}
}
----

```

=== Creating a certificate in a cluster

These certificates can be used to help administrators enable certificate-based authentication and to enable SSL-based communication to the cluster.

```
----
```

```

# The API:
/api/security/certificates

```

```

# The call:
curl -X POST "https://<mgmt-ip>/api/security/certificates" -H "accept:
application/hal+json" -H "Content-Type: application/json" -d "{
\"common_name\": \"TEST-SERVER\", \"type\": \"server\" }"
----

```

=== Installing a certificate in a cluster

These certificates can be used to help administrators enable certificate-based authentication and to enable-SSL based communication to the cluster.

```
----
```

```

# The API:
/api/security/certificates

```

```

# The call:
curl -X POST "https://<mgmt-ip>/api/security/certificates" -H "accept:
application/json" -H "Content-Type: application/json" -d "{ \"type\":
\"server-ca\", \"public_certificate\": \"-----BEGIN CERTIFICATE-----
\nMIIFYDCCA0igAwIBAgIQCgFCgAAAAUjyES1AAAAjANBgkqhkiG9w0BAQsFADBKMQswCQYD
VQQG\nEwJVUzESMBAGA1UEChMJSWRlb1RydXN0MScwJQYDVQQDEx5JZGVuVHJ1c3QgQ29tbWVY
Y2lhbCBS\nb290IENBIDEwHhcNMTQwMTE2MTg0MjIzWhcNMzQwMTE2MTg0MjIzWjBKMQswCQYD
VQQGEwJVUzES\nMBAGA1UEChMJSWRlb1RydXN0MScwJQYDVQQDEx5JZGVuVHJ1c3QgQ29tbWVY
Y2lhbCBSb290IENB\nIDEwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCnUBneP5k9
1DNG8W9RYYKyqU+PZ4ld\nhNlT3Qwo2dfw/66VQ3KZ+bVdfIrBQuExUHTRgQ18zZshq0PirK1e
hm7zCYofWjK9ouuU+ehcCuz/\nmNKvcbo0U590h++SvL3sTzIwiEsXXlfEU8L2ApeN2WIrVYQf
Yo3fw7gpS014PJNgiCL8mdo2yMKi\nlCcxUAGclbnO/AljwpN3lsKImesrgNqUZfVx9t++uP0D1
bVoE/c40yiTcdCMbXTMTE13EASX2MN0C\nXZ/g1Ue9tOsbobtJSdifWwLziuQkkORiT0/Br4sO
dBeo0XKIanoBScy0RnnGF7HamB4HWfp1IYVl\n3ZBWzvurpWCdxJ35UrCLvYf5jysjCiN2O/cz
4ckA82n5S6LgTrx+kzmEB/dEcH7+B1rlsazRGMzy\nNeVJSQjKVsk9+w8YfYs7wRPCTY/JTw43
6R+hDmrfYi7LNQZReSzIJTj0+kuniVyc0uMNOYZKdHzV\nWYfCP04MXFL0PfdSgvHqo6z9STQa

```

```
KPNBiDoT7uje/5kdX7rL6B7yuVBgwDHTc+XvvqDtMwt0viAg\nxGds8AgDelWAF0Z0lqf0Hj7h
9tgJ4TNkK2PXMl6f+cB7D3hvl7yTmvmcEpB4eoCHFddydJxVdHix\nnuuFucAS6T6C6aMN7/zHw
cz09lCqxCOEOoP5NiGVreTO0lwIDAQABo0IwQDAOBgNVHQ8BAf8EBAMC\nAQYwDwYDVR0TAQH/
BAUwAwEB/zAdBgNVHQ4EFgQU7UQZwNPwBovupHu+QucmVMiONnYwDQYJKoZI\nnhvcNAQELBQAD
ggIBAA2ukDL2pkt8RHYZYR4nKMleVO8lvOMIkPkp165oCOGUAFjvLi5+U1KMtLwH\nn6oi6mYtQ
lNeCgN9hCQCTrQ0U5s7B8jeUeLBfnLOic7iPBZM4zY0+sLj7wM+x8uwtLRvM7Kqas6pg\nnghst
O8OEPVeKlh6cdbjTMMlgCIOQ045U8U1mwF10A0Cj7oV+wh93nAbowacYXVKV7cndJZ5t+qnt\nn
ozo00F172ulQ8zW/7esUTTHHYPTa8Yec4kjixsU3+wYQ+nVZZjFHKdp2mhZpgq7vmrlR94gjmm
mV\nYjzLVYA211QC//G5Xc7UI2/YRYRKW2XviQzdFKcgyxilJbQN+QHwotL0AMh0jqEqSI512x
PE4iUX\nnfeu+hlsXIFRRk0pTAWvsXcoz7WL9RccvW9xYoIA55vrX/hMUpu09lEpCdNTDd1lzzY
9GvLU47/ro\nnkTLqllgEIt44w8y8bckzOmoKaT+gyOpyj4xjhi09bTyWnpXgSUyqorkqG5w2gX
jtw+hG4iZZRHUE\nn2XWJUc0QhJ1hYMTd+ZciTY6Y5uN/9lu7rs3KSoFrXgVzUeF0K+l+J6fZmU
lO+KWA2yUPHGNiiskz\nnZ2s8EIPGrd6ozRaOjfAHN3Gf8qv8QfXBi+wAN10J5U6A7/qxXDgGpR
tK4dw4LTzcx+QGtVKnO7R\nncGzM7vRX+Bi6hG6H\n-----END CERTIFICATE-----\n\"
}"
```

'''

=== Installing a certificate on a specific SVM

'''

```
# The API:
/api/security/certificates
```

```
# The call:
```

```
curl -X POST "https://<mgmt-ip>/api/security/certificates" -H "accept:
application/json" -H "Content-Type: application/json" -d "{  \"svm\" : {
\"name\" : \"vs0\" }, \"type\": \"server-ca\", \"public_certificate\":
\"-----BEGIN CERTIFICATE-----
\nMIIFDYCCA0igAwIBAgIQCGFCgAAAAUjyES1AAAAjANBgkqhkiG9w0BAQsFADBKMQswCQYD
VQQG\nnEwJVUzESMBAGA1UEChMJSWRlblRydXN0MScwJQYDVQQDEx5JZGVuVHJlc3QgQ29tbWV5
Y2lhbCBS\nnb290IENBIDEwHhcNMTQwMTE2MTgxmjIzWhcNMzQwMTE2MTgxmjIzWjBKMQswCQYD
VQQGEwJVUzES\nnMBAGA1UEChMJSWRlblRydXN0MScwJQYDVQQDEx5JZGVuVHJlc3QgQ29tbWV5
Y2lhbCBS\nsb290IENB\nnIDEwggiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCnUBneP5k9
1DNG8W9RYYKYqU+PZ4ld\nnhNlT3Qwo2dfw/66VQ3KZ+bVdfIrBQuExUHTRgQl8zZshq0PirK1e
hm7zCYofWjK9ouuU+ehcCuz/\n\nnmNKvcbO0U59Oh++SvL3sTzIwiEsXXlfEU8L2ApeN2WIrVYQf
Yo3fw7gps014PJNgicL8mdo2yMKi\nn1CxUAGclbnO/AljwpN3lsKImesrgNqUZFvX9t++uP0D1
bVoE/c40yiTcdCMbXTMTEl3EASX2MN0C\nnXZ/g1Ue9tOsbobTJSdifWwLziuQkkORiT0/Br4sO
dBeo0XKianoBSgy0RnnGF7HamB4HWfp1IYVl\nn3ZBWzvurpWCdxJ35UrCLvYf5jysjCiN2O/cz
4ckA82n5S6LgTrx+kzmEB/dEcH7+B1rlsazRGMzy\nnNeVJSQjKVsk9+w8YfYs7wRPCTY/JTw43
6R+hDmrfYi7LNQZReSzIJTj0+kuniVyc0uMNOYZKdHzV\nnWYfCP04MXFL0PfdSgvHqo6z9STQa
KPNBiDoT7uje/5kdX7rL6B7yuVBgwDHTc+XvvqDtMwt0viAg\nxGds8AgDelWAF0Z0lqf0Hj7h
```

```

9tgJ4TNkK2PXm16f+cB7D3hvl7yTmvmcEpB4eoCHFddyJxVdHix\nuuFucAS6T6C6aMN7/zHw
cz09lCqxCOEOoP5NiGVreTO0lwIDAQABo0IwQDAOBgNVHQ8BAf8EBAMC\nAQYwDwYDVR0TAQH/
BAUwAwEB/zAdBgNVHQ4EFgQU7UQZwNPwBovupHu+QucmVMiONnYwDQYJKoZI\nhvcNAQELBQAD
ggIBAA2ukDL2pkt8RHYZYR4nKM1eVO8lvOMIkPkp165oCOGUAFjvLi5+U1KMtLwH\n6oi6mYtQ
lNeCgN9hCQCTrQ0U5s7B8jeUeLBfnLOic7iPBZM4zY0+sLj7wM+x8uwtLRvM7Kqas6pg\nnghst
O8OEPVeKlh6cdbjTMM1gCIOQ045U8U1mwF10A0Cj7oV+wh93nAbowacYXVKV7cndJZ5t+qnt\n
ozo00F172u1Q8zW/7esUTTHHYPTa8Yec4kjixsU3+wYQ+nVZZjFHKdp2mhZpgq7vmr1R94gJmm
mV\nYjz1VYA211QC//G5Xc7UI2/YRYRKW2XviQzdFKcgyxilJbQN+QHwotL0AMh0jqEqSI512x
PE4iUX\nnfeu+h1sXIFRRk0pTAwvsXcoz7WL9RccvW9xYoIA55vrX/hMUpu091EpCdNTDd11zzY
9GvlU47/ro\nnkTLq11gEIt44w8y8bckzOmoKaT+gyOpyj4xjhi09bTyWnpXgSUyqorkqG5w2gX
jtw+hG4iZZRHUe\n2XWJUc0QhJ1hYMTd+ZciTY6Y5uN/9lu7rs3KSoFrXgvzUeF0K+l+J6fZmU
lO+KWA2yUPHGNiiskz\nZ2s8EIPGrd6ozRaOjfAHN3Gf8qv8QfXBi+wAN10J5U6A7/qxXDgGpR
tK4dw4LTzcqx+QGtVKnO7R\ncGzM7vRX+Bi6hG6H\n-----END CERTIFICATE-----\n\"
}

```

```
----
```

```
'''
```

```
=== Deleting a certificate using its UUID
```

```
'''
```

```
----
```

```
# The API:
```

```
/api/security/certificates/{uuid}
```

```
# The call:
```

```
curl -X DELETE "https://<mgmt-ip>/api/security/certificates/dad2363b-8ac0-
11e8-9058-005056b482fc?fields=*" -H "accept: application/hal+json"
```

```
----
```

```
=== Signing a new certificate signing request using an existing CA
certificate UUID
```

Once you have created a certificate of type "root_ca", you can use that certificate to act as a local Certificate Authority to sign new certificate signing requests. The following example signs a new certificate signing request using an existing CA certificate UUID. If successful, the API returns a signed certificate.

```
----
```

```
# The API:
```

```
/api/security/certificates/{ca.uuid}/sign
```

```
# The call:
```

```
curl -X POST "https://<mgmt-ip>/api/security/certificates/253add53-8ac9-11e8-9058-005056b482fc/sign" -H "accept: application/json" -H "Content-Type: application/json" -d "{ \"signing_request\": \"-----BEGIN CERTIFICATE REQUEST-----\nMIICYTCCAUKCAQAwhDENMASGA1UEAxMEVEVTVDELMAkGA1UEBhMCVVMwgGgEiMA0G\nb3DQEBAQUAA4IBDwAwggEKAoIBAQCIBCuVfbYHNdOO7vjRQja4JqL2cHqK\\ndrlTj5hz9RVqFKZ7VPh8DSP9LoTbYWsvrTkbuD0Wi715MVQCsbkq/mHos+Y5lfqs\\nNP5K92fc6EhBzBDYFgZGFntZYJjEG5MPerIUE7CfVy7o6sjWOlxeY33pjefObyvP\\nBcJkBHg6SFJK/TDLvIYJkonLkJEOJoTI6++a3I/1bCMfUeuRtLU9ThWlna1kMMYK\\n4T16/Bxgm4bha2U2jtosc0Wltnld/capc+eqRV07WVbMmEOTtop3cv0h3N0S6lbn\\nFkd96DXzeGWbSHFHckeCZ9bOHhnVbfEa/efkPLx7ziMC8GtRHHlwbNk7AgMBAAAGg\\nADANBgkqhkiG9w0BAQsFAAOCAQEaf+rs1i5PHaOSI2HtTM+Hcv/p71yzgoLL+aeU\\ntB0V4iuoXdqY8oQeWoPI92ci0K08JuSpu6D0DwCK1stfwuGkAA2b0Wr7ZDRonTUq\\nmJ4j3O47MLysW4Db2LbGws/AuDsCIRBJDWHMPHaqsvRbpMx2xQ/V5oagUw5eGGpN\\ne4fg/E2k9mGkpxwkUzT7w1RZirpND4xL+XTzpzeZqgalpXug4yjIXlI5hpRESZ9/\\nAkGJSCWxI15IZdxxFVXlBcmm6WpJnnboqkcKeXz95GM6Re+oBy9tlgvwv1Vd5s8uHX+bycFiZp09Wsm8Ev727MziZ+0II9nxwkDKsdPvam+KLI9hLQ==\\n-----END CERTIFICATE REQUEST-----\\n\", \"hash_function\": \"sha256\\\"}"
```

The response:

```
{
  "public_certificate": "-----BEGIN CERTIFICATE-----\nMIIDBzCCAe+gAwIBAgIIFUKQpcqeaUAWDQYJKoZIhvcNAQELBQAwHdENMASGA1UE\nFDWDELMAkGA1UEBhMCVVMwHhcNMTgWnZe4MjAzMTA1WhcNMTkwNze4MjAz\\nMTA1WjAcMQ0wCwYDVQQDEwRURVNUMQswCQYDVQQGEwJVUzCCASIwDQYJKoZIhvcN\\nAQEBBQADggEPADCCAQoCggEBAKIEK5V9tgc1047u+NFCNrgmovZweop2uVOPmHP1\\nFWoUpntU+HwNI/0uhNthay+tORu4PRaLvXkxVAKxuSr+Yeiz5jmV+qw0/kr3Z9zo\\nSEHMENgWBkYWellgmMQbkW96shQTSJ9XLujqyNY6XF5jFemN585vK88FwmQEeDpI\\nUkr9MMu8hgmSicuQkQ4mhMjr75rcj/VsIx9R65G0tT10FaWdrWQwxgrhPXR8HGcb\\nhuFrZTa02ixzRaW2eV39xqlz56pFXTtZVsyYQ502indy/SHc3RLqVucWR33oNfN4\\nZZtIcUdyR4Jn1s4eGdVt8Rr95+Q8vHvOIwLwa1EceXBucrsCAwEAaANNMEswCQYD\\nVR0TBAlwADAdBgNVHQ4EFgQUJMPxjeW1G76TbbD2tXB8dwSpI3MwHwYDVR0jBBgw\\nu5aH0mWR4cFoN9i7k96d2op3sPwwDQYJKoZIhvcNAQELBQADggEBAl5ai+Zi\\nFQZUXRTqJCgHsgBThARneVWQYkYpyAXmTR7QeLfld4ZHL33i4xWCqX3uvW7SFJLe\\nZajT2AVmgiDbaWIHtDtvqz1BY78PSgUwPH/IyARTEOBeikp6KdwMPraehDIBMAcc\\nANY58wXiTBbsl8UMD6tGecgnzw6sxlMmadGvrfJeJmgY4zert6NNvgtTPhcZQdLS\\ne0fGzHS6+3ajCCfEEhPNPer9D0e5Me81i9EsQGENrnJzTci8rzXPuF4bC3gghrK1\\nI1+kmJQ1kLYVUcsntcrIiHmNvtPFJY6stjDgQKS9aDd/THhPpokPtZoCmE6PDxh6\\nR+dO6C0hcDKHFzA=\\n-----END CERTIFICATE-----\\n"
```

'''

[[ID95b83ba50a81c815b20a27ae4983a7cc]]

= Retrieve security certificates

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-block]#`/security/certificates`#

Retrieves security certificates.

== Related ONTAP commands

* `security certificate show`

== Learn more

* xref:{relative_path}security_certificates_endpoint_overview.html[DOC /security/certificates]

== Parameters

[cols=5*,options=header]

|===

|Name

|Type

|In

|Required

|Description

|scope

|string

|query

|False

a|Filter by scope

|svm.name

|string

|query

|False

a|Filter by svm.name

|svm.uuid

|string

|query

```
|False  
a|Filter by svm.uuid
```

```
|common_name  
|string  
|query  
|False  
a|Filter by common_name
```

```
|serial_number  
|string  
|query  
|False  
a|Filter by serial_number
```

```
|ca  
|string  
|query  
|False  
a|Filter by CA
```

```
|type  
|string  
|query  
|False  
a|Filter by certificate type
```

```
|key_size  
|string  
|query  
|False  
a|Filter by key_size
```

```
|expiry_time  
|string  
|query  
|False  
a|Filter by expiry_time
```

```
|hash_function
```



```
|string
|query
|False
a|Filter by hash_function
```

```
|fields
|array[string]
|query
|False
a|Specify the fields to return.
```

```
|max_records
|integer
|query
|False
a|Limit the number of records returned.
```

```
|return_timeout
|integer
|query
|False
a|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
a|The default is true for GET calls.  When set to false, only the number
of records is returned.
```

```
|order_by
|array[string]
|query
|False
a|Order results by specified fields and optional [asc|desc] direction.
Default direction is 'asc' for ascending.
```

```
|===
```

== Response

Status: 200, Ok

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records

|records
|array[link:#security_certificate[security_certificate]]
a|

|===

.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "ca": "string",
```

```

    "common_name": "test.domain.com",
    "hash_function": "sha1",
    "intermediate_certificates": {
    },
    "private_key": "-----BEGIN PRIVATE KEY-----
MIIBVAIBADANBgkqhkiG9w0BAQEFAASCAT4wggE6AgEAAkEAu1/a8f3G47cZ6pel
Hd3aONMNkGJ8vSCH5QjicuDm92VtVwkAACEjIoZSLYlJvPD+odL+lFzVQSmkneW7
VCGqYQIDAQABAkAcfNpg6GCQxoneLOghvlUrRotNZGvqpUOEAvHK3X7AJhz5SU4V
an36qvsAt5ghFMVM2iGvGaXbj0dAd+Jg64pxAiEA32Eh9mPtFSmZhTIUMeGcPmPk
qIYCEuP8a/ZLmI9s4TsCIQDWvLQuvjSVfwPhi0TFAb5wqAET8X5LBFqtGX5QlUep
EwIgFnqM02Gc4wtLoqa2d4qPkYu13+uUW9hLd4XSd6i/OS8CIQDT3elU+Rt+qIwW
u0cFrVvNYSV3HNzDfS9N/IoxTagfewIgpVxAdE5c2EWbhCUkhN+ZCf38AKewK9TW
lQcDy4L+f14= -----END PRIVATE KEY-----",
    "public_certificate": "-----BEGIN CERTIFICATE-----
MIIBuzCCAWWgAwIBAgIIFTZBrqZwUUMwDQYJKoZIhvcNAQELBQAwhDENMAsGA1UE
AxMEVEVTVDELMAkGA1UEBhMCVVMwHhcNMTgwNjA4MTgwOTAxWhcNMTkwNjA4MTgw
OTAxWjAcMQ0wCwYDVQQDEwRURVNUMQswCQYDVQQGEwJVUzBcMA0GCSqGSIb3DQEB
AQUAA0sAMEgCQQDaPvbqUJJFJ6NNTyK3Yb+ytSjJ9aa3yUmYTD9uMiP+6ycjxHWB
e8u9z6yCHsW03ync+dnhe5c5z8wuDAY0fv15AgMBAAGjgYowgYcwDAYDVR0TBAUw
AwEB/zALBgNVHQ8EBAMCAQYwHQYDVR0OBBYEFMJ7Ev/o/3+YNzYh5XNlqqjnw4zm
MEsGA1UdIwREMEKAQFMJ7Ev/o/3+YNzYh5XNlqqjnw4zmoSCkHjAcMQ0wCwYDVQQD
EwRURVNUMQswCQYDVQQGEwJVU4IIFTZBrqZwUUMwDQYJKoZIhvcNAQELBQADQQA
vDovYeyGNknkjGI+TVNX6nDbyzf7zUPqnri0KuvObEeybrbPW45sgsnT5dyeE/32U
9Yr6lklkBtVBDTmLnrc -----END CERTIFICATE-----",
    "scope": "svm",
    "serial_number": "string",
    "svm": {
        "_links": {
            "self": {
                "href": "/api/resourcelink"
            }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    },
    "type": "client",
    "uuid": "string"
}
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|next
|link:href[href]
a|

|self
|link:href[href]
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:href[href]
a|

|===

[#svm]
[.api-collapsible-fifth-title]

```

svm

[cols=3*,options=header]

|===

|Name

|Type

|Description

|_links

|link:#_links[_links]

a|

|name

|string

a|The name of the SVM.

|uuid

|string

a|The unique identifier of the SVM.

|===

[#security_certificate]

[.api-collapsible-fifth-title]

security_certificate

[cols=3*,options=header]

|===

|Name

|Type

|Description

|_links

|link:#_links[_links]

a|

|ca

|string

a|Certificate authority

|common_name

|string

a|FQDN or custom common name. Provide on POST when creating a self-signed

certificate.

|expiry_time

|string

a|Certificate expiration time. Can be provided on POST if creating self-signed certificate. The expiration time range is between 1 day to 10 years.

|hash_function

|string

a|Hashing function. Can be provided on POST when creating a self-signed certificate. Hash functions md5 and sha1 are not allowed on POST.

|intermediate_certificates

|array[string]

a|Chain of intermediate Certificates in PEM format. Only valid in POST when installing a certificate.

|key_size

|integer

a|Key size of requested Certificate in bits. One of 512, 1024, 1536, 2048, 3072. Can be provided on POST if creating self-signed certificate. Key size of 512 is not allowed on POST.

|private_key

|string

a|Private key Certificate in PEM format. Only valid for create when installing a CA-signed certificate. This is not audited.

|public_certificate

|string

a|Public key Certificate in PEM format. If this is not provided in POST, a self-signed certificate is created.

|scope

|string

a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".

```

|serial_number
|string
a|Serial number of certificate.

|svm
|link:#svm[svm]
a|

|type
|string
a|Type of Certificate. The following types are supported:

* client - a certificate and its private key used by an SSL client in
ONTAP.
* server - a certificate and its private key used by an SSL server in
ONTAP.
* client_ca - a Certificate Authority certificate used by an SSL server in
ONTAP to verify an SSL client certificate.
* server_ca - a Certificate Authority certificate used by an SSL client in
ONTAP to verify an SSL server certificate.
* root_ca - a self-signed certificate used by ONTAP to sign other
certificates by acting as a Certificate Authority.
* enum: ["client", "server", "client_ca", "server_ca", "root_ca"]

|uuid
|string
a|Unique ID that identifies a certificate.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

```



```

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
=====

```

```
[[ID89e0f9d619f797ddeec94f6568ac9c20]]  
= Create or install security certificates
```

```
[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-  
block]#`/security/certificates`#
```

Creates or installs a certificate.

== Required properties

- * `svm.uuid` or `svm.name` - Existing SVM in which to create or install the certificate.
- * `common_name` - Common name of the certificate. Required when creating a certificate.
- * `type` - Type of certificate.
- * `public_certificate` - Public key certificate in PEM format. Required when installing a certificate.
- * `private_key` - Private key certificate in PEM format. Required when installing a CA-signed certificate.

== Recommended optional properties

- * `expiry_time` - Certificate expiration time. Specifying an expiration time is recommended when creating a certificate.
- * `key_size` - Key size of the certificate in bits. Specifying a strong key size is recommended when creating a certificate.

== Default property values

If not specified in POST, the following default property values are assigned:

- * `key_size` - `_2048_`
- * `expiry_time` - `_P365DT_`
- * `hash_function` - `_sha256_`

== Related ONTAP commands

- * `security certificate create``
- * `security certificate install``

== Learn more

* `xref:{relative_path}security_certificates_endpoint_overview.html`[DOC

```
/security/certificates]
```

```
== Parameters
```

```
[cols=5*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|In
```

```
|Required
```

```
|Description
```

```
|return_records
```

```
|boolean
```

```
|query
```

```
|False
```

```
a|The default is false. If set to true, the records are returned.
```

```
|===
```

```
== Request Body
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
 |_links
```

```
 |link:#_links[_links]
```

```
a|
```

```
 |ca
```

```
 |string
```

```
a|Certificate authority
```

```
 |common_name
```

```
 |string
```

```
a|FQDN or custom common name. Provide on POST when creating a self-signed certificate.
```

|expiry_time
|string
a|Certificate expiration time. Can be provided on POST if creating self-signed certificate. The expiration time range is between 1 day to 10 years.

|hash_function
|string
a|Hashing function. Can be provided on POST when creating a self-signed certificate. Hash functions md5 and sha1 are not allowed on POST.

|intermediate_certificates
|array[string]
a|Chain of intermediate Certificates in PEM format. Only valid in POST when installing a certificate.

|key_size
|integer
a|Key size of requested Certificate in bits. One of 512, 1024, 1536, 2048, 3072. Can be provided on POST if creating self-signed certificate. Key size of 512 is not allowed on POST.

|private_key
|string
a|Private key Certificate in PEM format. Only valid for create when installing a CA-signed certificate. This is not audited.

|public_certificate
|string
a|Public key Certificate in PEM format. If this is not provided in POST, a self-signed certificate is created.

|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".

|serial_number
|string
a|Serial number of certificate.

```
|svm
|link:#svm[svm]
a|
```

```
|type
|string
```

a|Type of Certificate. The following types are supported:

- * client - a certificate and its private key used by an SSL client in ONTAP.
- * server - a certificate and its private key used by an SSL server in ONTAP.
- * client_ca - a Certificate Authority certificate used by an SSL server in ONTAP to verify an SSL client certificate.
- * server_ca - a Certificate Authority certificate used by an SSL client in ONTAP to verify an SSL server certificate.
- * root_ca - a self-signed certificate used by ONTAP to sign other certificates by acting as a Certificate Authority.
- * enum: ["client", "server", "client_ca", "server_ca", "root_ca"]

```
|uuid
|string
a|Unique ID that identifies a certificate.
```

```
|===
```

.Example request

[%collapsible%closed]

====

```
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "ca": "string",
  "common_name": "test.domain.com",
  "hash_function": "sha1",
  "intermediate_certificates": {
  },

```

```

"private_key": "-----BEGIN PRIVATE KEY-----
MIIBVAIBADANBgkqhkiG9w0BAQEFAASCAT4wggE6AgEAAkEAu1/a8f3G47cZ6pel
Hd3aONMNkGJ8vSCH5QjicuDm92VtVwkAACEjIoZSLYlJvPD+odL+lFzVQSmkneW7
VCGqYQIDAQABAkAcfNpg6GCQxoneLOghvlUrRotNZGvqpUOEAvHK3X7AJhz5SU4V
an36qvsAt5ghFMVM2iGvGaXbj0dAd+Jg64pxAiEA32Eh9mPtFSmZhTIUMeGcPmPk
qIYCEuP8a/ZLmI9s4TsCIQDWvLQuvjSVfwPhi0TFab5wqAET8X5LBFqtGX5QlUep
EwIgFnqM02Gc4wtLoqa2d4qPkYul3+uUW9hLd4XSd6i/OS8CIQDT3elU+Rt+qIwW
u0cFrVvNYSV3HNzDfS9N/IoxTagfewIgpVxAdE5c2EWbhCUkhN+ZCf38AKewK9TW
lQcDy4L+f14= -----END PRIVATE KEY-----",
"public_certificate": "-----BEGIN CERTIFICATE-----
MIIBuzCCAWWgAwIBAgIIIFTZBrqZwUUMwDQYJKoZIhvcNAQELBQAWhDENMAsGA1UE
AxMEVEVETVDELMAkGA1UEBhMCMVVMwHhcNMTgwNjA4MTgwOTAxWhcNMTkwNjA4MTgw
OTAxWjAcMQ0wCwYDVQQDEwRURVNUMQswCQYDVQQGEwJVUzBcMA0GCSqGSIb3DQEB
AQUAA0sAMEgCQQDaPvbqUJJFJ6NNTyK3Yb+ytSjJ9aa3yUmYTD9uMiP+6ycjxHWB
e8u9z6yCHsW03ync+dnhE5c5z8wuDAY0fv15AgMBAAGjgYowgYcwDAYDVR0TBAUw
AwEB/zALBgNVHQ8EBAMCAQYwHQYDVR0OBBYEFMJ7Ev/o/3+YNzYh5XNlqqjnw4zm
MEsGA1UdIwREMEKAFMJ7Ev/o/3+YNzYh5XNlqqjnw4zmoSCkHjAcMQ0wCwYDVQQD
EwRURVNUMQswCQYDVQQGEwJVU4IIIFTZBrqZwUUMwDQYJKoZIhvcNAQELBQADQQAv
DovYeyGNknjGI+TVNX6nDbyzf7zUPqnri0KuvObEeybrbPW45sgsnT5dyeE/32U
9Yr6lklkBtVBDTmLnrc -----END CERTIFICATE-----",
"scope": "svm",
"serial_number": "string",
"svm": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "name": "svm1",
  "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
},
"type": "client",
"uuid": "string"
}
=====

```

== Response

Status: 201, Created

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records

|records
|array[link:#security_certificate[security_certificate]]
a|

|===

```

.Example response

[%collapsible%closed]

====

[source,json,subs=+macros]

```

{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "ca": "string",
    "common_name": "test.domain.com",
    "hash_function": "sha1",
    "intermediate_certificates": {
    },
    "private_key": "-----BEGIN PRIVATE KEY-----
MIIBVAIBADANBgkqhkiG9w0BAQEFAASCAT4wggE6AgEAAkEAu1/a8f3G47cZ6pel
Hd3aONMNkGJ8vSCH5QjicuDm92VtVwkAAACEjIoZSLYlJvPD+odL+lFzVQSmkneW7
VCGqYQIDAQABAkAcfNpg6GCQxoneLOghvlUrRotNZGvqpUOEAvHK3X7AJhz5SU4V
an36qvsAt5ghFMVM2iGvGaXbj0dAd+Jg64pxAiEA32Eh9mPtFSmZhTIUMeGcPmPk
qIYCEuP8a/ZLmI9s4TsCIQDWvLQuvjSVfwPhi0TFab5wqAET8X5LBFqtGX5QlUep

```

```

EwIgFnqM02Gc4wtLoqa2d4qPkYu13+uUW9hLd4XSd6i/OS8CIQDT3elU+Rt+qIwW
u0cFrVvNYSV3HNzDfS9N/IoxTagfewIgPvXADe5c2EWbhCUkhN+ZCf38AKewK9TW
lQcDy4L+f14= -----END PRIVATE KEY-----",
  "public_certificate": "-----BEGIN CERTIFICATE-----
MIIBuzCCAWWgAwIBAgIIIFTZBrqZwUUMwDQYJKoZIhvcNAQELBQAwhDENMAsgA1UE
AxMEVEVTVDELMAkGA1UEBhMCVVMwHhcNMTgwNjA4MTgwOTAxWhcNMTkwNjA4MTgw
OTAxWjAcMQ0wCwYDVQQDEwRURVNUMQswCQYDVQQGEwJVUzBcMA0GCSqGSIb3DQEB
AQUAA0sAMEgCQQDaPvbqUJJFJ6NNTyK3Yb+ytSjJ9aa3yUmYTD9uMiP+6ycjxHWB
e8u9z6yCHsW03ync+dnhE5c5z8wuDAY0fv15AgMBAAGjgYowgYcwDAYDVDR0TBAUw
AwEB/zALBgNVHQ8EBAMCAQYwHQYDVR0OBBYEFMJ7Ev/o/3+YNzYh5XNlqqjnw4zm
MESGA1UdIwREMEKAQFMJ7Ev/o/3+YNzYh5XNlqqjnw4zmoSCkHjAcMQ0wCwYDVQQD
EwRURVNUMQswCQYDVQQGEwJVU4IIIFTZBrqZwUUMwDQYJKoZIhvcNAQELBQADQQA
vDovYeyGNknjGI+TVNX6nDbyzf7zUPqnri0KuvObEeybrbPW45sgsnT5dyeE/32U
9Yr6lklkBtVBDTmLnrc -----END CERTIFICATE-----",
  "scope": "svm",
  "serial_number": "string",
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "type": "client",
  "uuid": "string"
}
}
====

== Error

```

Status: Default

ONTAP Error Response Codes

===	
Error Code	Description
3735645	Cannot specify a value for serial. It is generated automatically.
3735622	The certificate type is not supported.

| 3735664
| The specified key size is not supported in FIPS mode.

| 3735665
| The specified hash function is not supported in FIPS mode.

| 3735553
| Failed to create self-signed Certificate.

| 3735646
| Failed to store the certificates.

| 3735693
| The certificate installation failed as private key was empty.

| 3735618
| Cannot accept private key for server-ca or client-ca.

| 52363365
| Failed to allocate memory.

| 52559975
| Failed to read the certificate due to incorrect formatting.

| 52363366
| Unsupported key type.

| 52560123
| Failed to read the key due to incorrect formatting.

| 52559972
| The certificates start date is later than the current date.

| 52559976
| The certificate and private key do not match.

| 52559973
| The certificate has expired.

| 52363366
| Logic error: use of a dead object.

| 3735696
| Intermediate certificates are not supported with client-ca and server-ca type certificates.

| 52559974

```
| The certificate is not supported in FIPS mode.

| 3735676
| Cannot continue the installation without a value for the common name.
Since the subject field in the certificate is empty, the field
"common_name" must have a value to continue with the installation.

| 3735558
| Failed to extract information about Common Name from the certificate.

| 3735588
| The common name (CN) extracted from the certificate is not valid.

| 3735632
| Failed to extract Certificate Authority Information from the
certificate.
|===
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
```

```
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

```

}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#svm]
[.api-collapsible-fifth-title]
svm

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

|===

[#security_certificate]
[.api-collapsible-fifth-title]
security_certificate

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|ca
|string
a|Certificate authority

|common_name
|string
a|FQDN or custom common name. Provide on POST when creating a self-signed
certificate.

```

|expiry_time

|string

a|Certificate expiration time. Can be provided on POST if creating self-signed certificate. The expiration time range is between 1 day to 10 years.

|hash_function

|string

a|Hashing function. Can be provided on POST when creating a self-signed certificate. Hash functions md5 and sha1 are not allowed on POST.

|intermediate_certificates

|array[string]

a|Chain of intermediate Certificates in PEM format. Only valid in POST when installing a certificate.

|key_size

|integer

a|Key size of requested Certificate in bits. One of 512, 1024, 1536, 2048, 3072. Can be provided on POST if creating self-signed certificate. Key size of 512 is not allowed on POST.

|private_key

|string

a|Private key Certificate in PEM format. Only valid for create when installing a CA-signed certificate. This is not audited.

|public_certificate

|string

a|Public key Certificate in PEM format. If this is not provided in POST, a self-signed certificate is created.

|scope

|string

a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".

|serial_number

```

|string
a|Serial number of certificate.

|svm
|link:#svm[svm]
a|

|type
|string
a|Type of Certificate. The following types are supported:

* client - a certificate and its private key used by an SSL client in
ONTAP.
* server - a certificate and its private key used by an SSL server in
ONTAP.
* client_ca - a Certificate Authority certificate used by an SSL server in
ONTAP to verify an SSL client certificate.
* server_ca - a Certificate Authority certificate used by an SSL client in
ONTAP to verify an SSL server certificate.
* root_ca - a self-signed certificate used by ONTAP to sign other
certificates by acting as a Certificate Authority.
* enum: ["client", "server", "client_ca", "server_ca", "root_ca"]

|uuid
|string
a|Unique ID that identifies a certificate.

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|next
|link:#href[href]
a|

```

```

|self
|link:#href[href]
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string

```

```
a|Error code
```

```
|message
```

```
|string
```

```
a|Error message
```

```
|target
```

```
|string
```

```
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
```

```
====
```

```
[[ID6011f58f6f1bcael47579493fb11fab8]]
```

```
= Sign security certificates
```

```
[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-  
block]#`/security/certificates/{ca.uuid}/sign`#
```

Signs a certificate.

== Required properties

* `signing_request` - Certificate signing request to be signed by the given certificate authority.

== Recommended optional properties

* `expiry_time` - Certificate expiration time. Specifying an expiration time for a signed certificate is recommended.

* `hash_function` - Hashing function. Specifying a strong hashing function is recommended when signing a certificate.

== Default property values

If not specified in POST, the following default property values are assigned:


```
* `expiry_time` - _P365DT_  
* `hash_function` - _sha256_
```

== Related ONTAP commands

```
* `security certificate sign`
```

This API is used to sign a certificate request using a pre-existing self-signed root certificate. The self-signed root certificate acts as a certificate authority within its scope and maintains the records of its signed certificates.

The root certificate can be created for a given SVM or for the cluster using [`POST security/certificates`].

== Parameters

```
[cols=5*,options=header]  
|===
```

```
|Name  
|Type  
|In  
|Required  
|Description
```

```
|return_records  
|boolean  
|query  
|False
```

a|The default is false. If set to true, the records are returned.

```
|ca.uuid  
|string  
|path  
|True  
a|UUID of the existing certificate authority certificate
```

```
|===
```

== Request Body

```
[cols=3*,options=header]
```

```

|===
|Name
|Type
|Description

|expiry_time
|string
a|Certificate expiration time. The allowed expiration time range is
between 1 day to 10 years.

|hash_function
|string
a|Hashing function

|signing_request
|string
a|Certificate signing request to be signed by the given certificate
authority. Request should be in X509 PEM format.

|===

.Example request
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
    "hash_function": "sha256",
    "signing_request": "'-----BEGIN CERTIFICATE REQUEST-----
MIICYDCCAUGCAQAwGzEMMAoGA1UEAxMDQUJDMQswCQYDVQQGEwJVUzCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAPF+82SlqT3Vyu3Jx4IAwHcO5EGwLOxy
zQ6KNjz71Fca0n1/A1CbCPyOsSupGVObvdWxX7xLVMJ2Sxb7h43GCqYyX6FXJO4F
HOpmLvB+jxdeiW7SDbiZyLUlsvA+oRO/uNlcug773QZdKLjJD64erZZMRUNbUJB8
bARxAUi0FPvgTraSQ0UW5sRLiGKeAyKA4wekYe1VgjHRTBizFbD4dI3njfva/2Bl
jf+kkulgcLJTUJNtkgeimqMKYraYuleYcYk2K+C//0NuNOuPbDfTXCM7O61vik09
Szi8nLN70XE9KoAA93U/BCpSfpl8XIb4cGnEr8hgVHOotZSo+KZBFxMCAwEAAaAA
MA0GCSqGSIB3DQEBChUAA4IBAQC2vFYpvgsFrm5GnPx8tOBD1xsTyYjbWJMD8hAF
lFrvF9Sw9QGCTdyacxkwgJhQx8l8JiIS5GOY6WWLB19FMkLQNAhDL9xF3WF7vfYq
RKgrz3bd/Vg96fsRZNYIPLGmoEaqLOh3FOCGc2VbdsR9PwOn3fwthxkIRd6ds6/q
jc5cpSmVsCOgu+OKcpRXikYDbkWXftZ1AhSfn6njBYFdZ9+PNAu/0JRQh5bX60nO
5heniTcAJLwUZP/CQ8nxHY0Wqy+1rAtM33d5cVmHULBXQSIru/0ZkA/b9fK5Zv8E
ZMADYUoEvIG59VxhyCi8lzYf+Mxl8qBSF+ZdC4yWhzDqZtM9 -----END CERTIFICATE
REQUEST-----'"

```

```
}  
====  
  
== Response
```

Status: 200, Ok

```
[cols=3*,options=header]  
|===  
|Name  
|Type  
|Description  
  
|public_certificate  
|string  
a|CA signed public key Certificate  
  
|===  
  
== Error
```

Status: Default

```
ONTAP Error Response Codes  
  
|===  
| Error Code | Description  
  
| 3735628  
| Failed to use CA certificate for signing.  
  
| 3735665  
| The specified hash function is not supported in FIPS mode.  
  
| 52559974  
| The certificate is not supported in FIPS mode.  
  
| 3735626  
| Failed to generate signed Certificate.  
  
| 3735558  
| Failed to extract information about Common Name from the certificate.
```

```
| 3735588
| The common name (CN) extracted from the certificate is not valid.

| 3735632
| Failed to extract Certificate Authority Information from the
certificate.

| 3735629
| Failed to sign the certificate because Common Name of signing
certificate and Common Name of CA certificate are same.

| 3735630
| Failed to sign the certificate because expiry date of signing
certificate exceeds the expiry date of CA certificate.
|===
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
```

```
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

```
=====
```

== Definitions

```
[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#security_certificate_sign]
[.api-collapsible-fifth-title]
security_certificate_sign

[cols=3*,options=header]
|===
|Name
|Type
|Description

|expiry_time
|string
a|Certificate expiration time. The allowed expiration time range is
between 1 day to 10 years.

|hash_function
|string
a|Hashing function

|signing_request
|string
a|Certificate signing request to be signed by the given certificate
authority. Request should be in X509 PEM format.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
|string
a|Error code
```

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
====

[[ID1cb2a75942a913422a4576dc09340cef]]
= Delete security certificates

[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-
block]#`/security/certificates/{uuid}`#

Deletes a security certificate.

== Related ONTAP commands

* `security certificate delete`

== Learn more

* xref:{relative_path}security_certificates_endpoint_overview.html[DOC
/security/certificates]

== Parameters

[cols=5*,options=header]
|===
|Name
|Type
|In
|Required
|Description

|uuid
|string
|path
|True
a|
|===

== Response
```

Status: 200, Ok

```
== Error
```

Status: Default

ONTAP Error Response Codes

```
|===  
| Error Code | Description  
  
| 3735644  
| Cannot delete server-chain certificate. Reason: There is a corresponding  
server certificate for it.  
  
| 3735679  
| Cannot delete pre-installed server-ca certificates through REST. Use CLI  
or ZAPI.  
  
| 3735650  
| Deleting this client-ca certificate directly is not supported. Delete  
the corresponding root-ca certificate using type `root_ca` to delete the  
root, client, and server certificates.  
  
| 3735627  
| Deleting this server-ca certificate directly is not supported. Delete  
the corresponding root-ca certificate using type `root_ca` to delete the  
root, client, and server certificates.  
  
| 3735589  
| Cannot delete certificate.  
  
| 3735590  
| Cannot delete certificate. Failed to remove SSL configuration for the  
certificate.  
  
| 3735683  
| Cannot remove this certificate while external key manager is configured.  
|===
```

```
[cols=3*,options=header]
```

```
|===  
|Name  
|Type  
|Description
```



```
|error
|link:#error[error]
a|
```

```
|===
```

```
.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
```

```
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

```
== Definitions
```

```
[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
```

```
====
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[IDa5f63f1932e8e999f1ace238bbfdcf4]]

```

= Retrieve security certificates

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-block]#`/security/certificates/{uuid}`#

Retrieves security certificates.

== Related ONTAP commands

* `security certificate show`

== Learn more

* xref:{relative_path}security_certificates_endpoint_overview.html[DOC /security/certificates]

== Parameters

[cols=5*,options=header]

|===

|Name

|Type

|In

|Required

|Description

|uuid

|string

|path

|True

a|Certificate UUID

|fields

|array[string]

|query

|False

a|Specify the fields to return.

|===

== Response

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|ca
|string
a|Certificate authority

|common_name
|string
a|FQDN or custom common name. Provide on POST when creating a self-signed
certificate.

|expiry_time
|string
a|Certificate expiration time. Can be provided on POST if creating self-
signed certificate. The expiration time range is between 1 day to 10
years.

|hash_function
|string
a|Hashing function. Can be provided on POST when creating a self-signed
certificate. Hash functions md5 and sha1 are not allowed on POST.

|intermediate_certificates
|array[string]
a|Chain of intermediate Certificates in PEM format. Only valid in POST
when installing a certificate.

|key_size
|integer
a|Key size of requested Certificate in bits. One of 512, 1024, 1536, 2048,
3072. Can be provided on POST if creating self-signed certificate. Key
```

size of 512 is not allowed on POST.

|private_key

|string

a|Private key Certificate in PEM format. Only valid for create when installing a CA-signed certificate. This is not audited.

|public_certificate

|string

a|Public key Certificate in PEM format. If this is not provided in POST, a self-signed certificate is created.

|scope

|string

a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".

|serial_number

|string

a|Serial number of certificate.

|svm

|link:#svm[svm]

a|

|type

|string

a|Type of Certificate. The following types are supported:

* client - a certificate and its private key used by an SSL client in ONTAP.

* server - a certificate and its private key used by an SSL server in ONTAP.

* client_ca - a Certificate Authority certificate used by an SSL server in ONTAP to verify an SSL client certificate.

* server_ca - a Certificate Authority certificate used by an SSL client in ONTAP to verify an SSL server certificate.

* root_ca - a self-signed certificate used by ONTAP to sign other certificates by acting as a Certificate Authority.

* enum: ["client", "server", "client_ca", "server_ca", "root_ca"]

```
|uuid
|string
a|Unique ID that identifies a certificate.
```

```
|===
```

```
.Example response
```

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
```

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "ca": "string",
  "common_name": "test.domain.com",
  "hash_function": "sha1",
  "intermediate_certificates": {
  },
  "private_key": "-----BEGIN PRIVATE KEY-----
MIIBVAIBADANBgkqhkiG9w0BAQEFAASCAT4wggE6AgEAAkEAu1/a8f3G47cZ6pel
Hd3aONMNkGJ8vSCH5QjicuDm92VtVwkAACEjIoZSLYlJvPD+odL+lFzVQSmkneW7
VCGqYQIDAQABAkAcfNpg6GCQxoneLOghvlUrRotNZGvqpUOEAvHK3X7AJhz5SU4V
an36qvsAt5ghFMVM2iGvGaXbj0dAd+Jg64pxAiEA32Eh9mPtFSmZhTIUMeGcPmPk
qIYCEuP8a/ZLmI9s4TsCIQDWvLQuvjSVfwPhi0TFAb5wqAET8X5LBFqtGX5QlUep
EwIgFnqM02Gc4wtLoqa2d4qPkYul3+uUW9hLd4XSd6i/OS8CIQDT3elU+Rt+qIwW
u0cFrVvNYSV3HNzDfS9N/IoxTagfewIgpVxAdE5c2EWbhCUkhN+ZCf38AKewK9TW
lQcDy4L+f14= -----END PRIVATE KEY-----",
  "public_certificate": "-----BEGIN CERTIFICATE-----
MIIBuzCCAWWgAwIBAgIIFTZBrqZwUUMwDQYJKoZIhvcNAQELBQAWhDENMAsGA1UE
AxMEVEVTVDELMAkGA1UEBhMCVVMwHhcNMTgwNjA4MTgwOTAxWhcNMTkwNjA4MTgw
OTAxWjAcMQ0wCwYDVQQDEwRURVNUMQswCQYDVQQGEwJVUzBcMA0GCSqGSIb3DQEB
AQUAA0sAMEgCQQDaPvbqUJJFJ6NNTyK3Yb+ytSjJ9aa3yUmYTD9uMiP+6ycjxHWB
e8u9z6yCHsW03ync+dnhE5c5z8wuDAY0fv15AgMBAAGjgYowgYcwDAYDVR0TBAUw
AwEB/zALBgNVHQ8EBAMCAQYwHQYDVR0OBBYEFMJ7Ev/o/3+YNzYh5XNlqqjnw4zm
MEsGA1UdIwREMEKAUFMJ7Ev/o/3+YNzYh5XNlqqjnw4zmoSCkHjAcMQ0wCwYDVQQD
EwRURVNUMQswCQYDVQQGEwJVU4IIFTZBrqZwUUMwDQYJKoZIhvcNAQELBQADQQAv
DovYeyGNknkjGI+TVNX6nDbyzf7zUPqnri0KuvObEeybrbPW45sgsnT5dyeE/32U
9Yr6lklknbTbVBDTmLnrc -----END CERTIFICATE-----",
  "scope": "svm",
  "serial_number": "string",
  "svm": {
```

```

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

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}

```

```

====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====

[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#svm]
[.api-collapsible-fifth-title]
svm

```



```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]

```

```

[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

:leveloffset: -1

= View and update IPsec configuration

:leveloffset: +1

[[ID61fd85a6988f082e28bbbc354e917a68]]
= Security IPsec endpoint overview

```

== Overview

The following operations are supported:

- * GET to retrieve the IPsec status: GET security/ipsec
- * Patch to update IPsec status: PATCH security/ipsec

[[IDb2a75cc1408fcfd4c44a521dca1502f9]]

= Retrieve IPsec configuration

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-block]#`/security/ipsec`#

Retrieves IPsec configuration via REST APIs.

== Related ONTAP commands

- * 'security ipsec config show'

== Learn more

- * xref:{relative_path}security_ipsec_endpoint_overview.html[DOC /security/ipsec]

== Parameters

[cols=5*,options=header]

|==

|Name

|Type

|In

|Required

|Description

|max_records

|integer

```
|query
|False
a|Limit the number of records returned.

|return_records
|boolean
|query
|False
a|The default is true for GET calls. When set to false, only the number
of records is returned.

|return_timeout
|integer
|query
|False
a|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.

|order_by
|array[string]
|query
|False
a|Order results by specified fields and optional [asc|desc] direction.
Default direction is 'asc' for ascending.

|fields
|array[string]
|query
|False
a|Specify the fields to return.

|===

== Response
```

Status: 200, Ok

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#self_link[self_link]
a|

|enabled
|boolean
a|Indicates whether or not IPsec is enabled.

|===

.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  }
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

```

```

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#self_link]
[.api-collapsible-fifth-title]

```

```

self_link

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
|string
a|Error code
```

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
====
```

```
[[ID53a299c83d0e71dc8817c13cb94fa42e]]
= Update IPsec configuration
```

```
[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-
block]#`/security/ipsec`#
```

Updates IPsec configuration via REST APIs.

== Related ONTAP commands

* 'security ipsec config modify'

== Learn more

* xref:{relative_path}security_ipsec_endpoint_overview.html[DOC
/security/ipsec]

== Parameters

[cols=5*,options=header]

|===

|Name

|Type

|In

|Required

|Description

|return_records

|boolean

|query

|False

a|The default is false. If set to true, the records are returned.

|===

== Request Body

[cols=3*,options=header]

|===

|Name

|Type

|Description

|_links

|link:#self_link[self_link]

a|

|enabled

|boolean

a|Indicates whether or not IPsec is enabled.

|===

.Example request

[%collapsible%closed]

====

[source,json,subs=+macros]

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  }
}
```

```
====
```

```
== Response
```

Status: 200, Ok

```
== Error
```

Status: Default

ONTAP Error Response Codes

```
|===
```

```
| Error Code | Description
```

```
| 66256898
```

```
| Internal error. Failed to enable IPsec.
```

```
| 66256899
```

```
| Internal error. Failed to disable IPsec.
```

```
| 66257199
```

```
| IPsec is not supported in the current cluster version.
```

```
|===
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#self_link]
[.api-collapsible-fifth-title]
self_link

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#ipsec]
[.api-collapsible-fifth-title]
ipsec

Manages IPsec configuration via REST APIs.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#self_link[self_link]
a|

|enabled
|boolean
a|Indicates whether or not IPsec is enabled.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
|string
a|Error code
```

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
```

```
====
```

```
:leveloffset: -1
```

```
= Manage IPsec policies
```

```
:leveloffset: +1
```

```
[[IDac59deb96d4943d8b7dc3f216f4d552b]]
```

```
= Security IPsec policies endpoint overview
```

```
== Overview
```

The following operations are supported:

- * Collection Get: GET security/ipsec/policies
- * Creation Post: POST security/ipsec/policies
- * Instance Get: GET security/ipsec/policies/uuid
- * Instance Patch: PATCH security/ipsec/policies/uuid
- * Instance Delete: DELETE security/ipsec/policies/uuid

```
[[ID2fc577d2859e407ba1e20e3737435818]]
```

```
= Retrieve IPsec policies
```

```
[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-block]#`/security/ipsec/policies`#
```

Retrieves the collection of IPsec policies.

```
== Related ONTAP commands
```

```
* `security ipsec policy show`
```

```
== Learn more
```

```
* xref:{relative_path}security_ipsec_policies_endpoint_overview.html[DOC
/security/ipsec/policies]
```

```
== Parameters
```

```
[cols=5*,options=header]
|==
```

```
|Name
|Type
|In
|Required
|Description
```

```
|local_endpoint.family
|string
|query
|False
a|Filter by local_endpoint.family
```

```
|local_endpoint.port
|string
|query
|False
a|Filter by local_endpoint.port
```

```
|local_endpoint.netmask
|string
|query
|False
a|Filter by local_endpoint.netmask
```

```
|local_endpoint.address
|string
|query
|False
a|Filter by local_endpoint.address
```

```
|svm.uuid
|string
|query
```

```
|False
a|Filter by svm.uuid

|svm.name
|string
|query
|False
a|Filter by svm.name

|enabled
|boolean
|query
|False
a|Filter by enabled

|remote_endpoint.family
|string
|query
|False
a|Filter by remote_endpoint.family

|remote_endpoint.port
|string
|query
|False
a|Filter by remote_endpoint.port

|remote_endpoint.netmask
|string
|query
|False
a|Filter by remote_endpoint.netmask

|remote_endpoint.address
|string
|query
|False
a|Filter by remote_endpoint.address

|uuid
```



```
|string
|query
|False
a|Filter by uuid
```

```
|name
|string
|query
|False
a|Filter by name
```

```
|scope
|string
|query
|False
a|Filter by scope
```

```
|protocol
|string
|query
|False
a|Filter by protocol
```

```
|fields
|array[string]
|query
|False
a|Specify the fields to return.
```

```
|max_records
|integer
|query
|False
a|Limit the number of records returned.
```

```
|return_records
|boolean
|query
|False
a|The default is true for GET calls. When set to false, only the number
of records is returned.
```

```

|return_timeout
|integer
|query
|False
a|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.

|order_by
|array[string]
|query
|False
a|Order results by specified fields and optional [asc|desc] direction.
Default direction is 'asc' for ascending.

|===

== Response

```

Status: 200, Ok

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|error
|link:#error[error]
a|

|num_records
|integer
a|Number of records

|records
|array[link:#records[records]]

```

```

a|

|===

.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  },
  "num_records": 1,
  "records": {
    "action": "bypass",
    "local_endpoint": {
      "address": "10.10.10.7",
      "family": "ipv4",
      "netmask": "24",
      "port": "23"
    },
    "protocol": "17",
    "remote_endpoint": {
      "address": "10.10.10.7",
      "family": "ipv4",
      "netmask": "24",
      "port": "23"
    },
    "scope": "svm",
    "svm": {
      "_links": {

```

```

        "self": {
            "href": "/api/resourcelink"
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    },
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
}
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

```

```

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|next
|link:#href[href]
a|

|self
|link:#href[href]
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]

```

error_arguments

[cols=3*,options=header]

|===

|Name

|Type

|Description

|code

|string

a|Argument code

|message

|string

a|Message argument

|===

[#error]

[.api-collapsible-fifth-title]

error

[cols=3*,options=header]

|===

|Name

|Type

|Description

|arguments

|array[link:#error_arguments[error_arguments]]

a|Message arguments

|code

|string

a|Error code

|message

|string

a|Error message

|target

```

|string
a|The target parameter that caused the error.

|===

[#local_endpoint]
[.api-collapsible-fifth-title]
local_endpoint

Local endpoint for the IPsec policy.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|address
|string
a|IPv4 or IPv6 address

|family
|string
a|IPv4 or IPv6

|netmask
|string
a|Input as netmask length (16) or IPv4 mask (255.255.0.0). For IPv6, you
must set the netmask length. The default value is 64. Output is always
netmask length.

|port
|string
a|Application port to be covered by the IPsec policy

|===

[#remote_endpoint]
[.api-collapsible-fifth-title]

```

remote_endpoint

Remote endpoint for the IPsec policy.

[cols=3*,options=header]

|===

|Name

|Type

|Description

|address

|string

a|IPv4 or IPv6 address

|family

|string

a|IPv4 or IPv6

|netmask

|string

a|Input as netmask length (16) or IPv4 mask (255.255.0.0). For IPv6, you must set the netmask length. The default value is 64. Output is always netmask length.

|port

|string

a|Application port to be covered by the IPsec policy

|===

[#_links]

[.api-collapsible-fifth-title]

_links

[cols=3*,options=header]

|===

|Name

|Type

|Description

|self


```
|link:#href[href]
a|

|===

[#svm]
[.api-collapsible-fifth-title]
svm

SVM, applies only to SVM-scoped objects.
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#records]
[.api-collapsible-fifth-title]
records
```

IPsec policy object.

```
[cols=3*,options=header]
|===
|Name
|Type
```

```

|Description

|action
|string
a|Action for the IPsec policy.

|enabled
|boolean
a|Indicates whether or not the policy is enabled.

|local_endpoint
|link:#local_endpoint[local_endpoint]
a|Local endpoint for the IPsec policy.

|name
|string
a|IPsec policy name.

|protocol
|string
a|Lower layer protocol to be covered by the IPsec policy.

|remote_endpoint
|link:#remote_endpoint[remote_endpoint]
a|Remote endpoint for the IPsec policy.

|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

|secret_key
|string
a|Pre-shared key for IKE negotiation.

|svm
|link:#svm[svm]
a|SVM, applies only to SVM-scoped objects.

```

```
|uuid
|string
a|Unique identifier of the IPsec policy.
```

```
|===
```

```
//end collapsible .Definitions block
=====
```

```
[[ID066875bbbaa1e151d614ae1362ea3c6a]]
= Create an IPsec policy
```

```
[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/ipsec/policies`#
```

Creates an IPsec policy.

== Related ONTAP commands

* `security ipsec policy create`

== Learn more

* xref:{relative_path}security_ipsec_policies_endpoint_overview.html[DOC
/security/ipsec/policies]

== Parameters

```
[cols=5*,options=header]
|===
```

```
|Name
|Type
|In
|Required
|Description
```

```
|return_records
|boolean
```

```

|query
|False
a|The default is false. If set to true, the records are returned.

|===

== Request Body

[cols=3*,options=header]
|===
|Name
|Type
|Description

|action
|string
a|Action for the IPsec policy.

|enabled
|boolean
a|Indicates whether or not the policy is enabled.

|local_endpoint
|link:#local_endpoint[local_endpoint]
a|Local endpoint for the IPsec policy.

|name
|string
a|IPsec policy name.

|protocol
|string
a|Lower layer protocol to be covered by the IPsec policy.

|remote_endpoint
|link:#remote_endpoint[remote_endpoint]
a|Remote endpoint for the IPsec policy.

|scope

```

```

|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

|secret_key
|string
a|Pre-shared key for IKE negotiation.

|svm
|link:#svm[svm]
a|

|uuid
|string
a|Unique identifier of the IPsec policy.

|===

.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "action": "bypass",
  "local_endpoint": {
    "address": "10.10.10.7",
    "family": "ipv4",
    "netmask": "24",
    "port": "23"
  },
  "protocol": "17",
  "remote_endpoint": {
    "address": "10.10.10.7",
    "family": "ipv4",
    "netmask": "24",
    "port": "23"
  },
  "scope": "svm",
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"

```

```

    }
  },
  "name": "svm1",
  "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
},
"uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
}
====

== Response

```

Status: 201, Created

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|error
|link:#error[error]
a|

|num_records
|integer
a|Number of records

|records
|array[link:#records[records]]
a|

|===

.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "next": {

```

```

    "href": "/api/resourcelink"
  },
  "self": {
    "href": "/api/resourcelink"
  }
},
"error": {
  "arguments": {
    "code": "string",
    "message": "string"
  },
  "code": "4",
  "message": "entry doesn't exist",
  "target": "uuid"
},
"num_records": 1,
"records": {
  "action": "bypass",
  "local_endpoint": {
    "address": "10.10.10.7",
    "family": "ipv4",
    "netmask": "24",
    "port": "23"
  },
  "protocol": "17",
  "remote_endpoint": {
    "address": "10.10.10.7",
    "family": "ipv4",
    "netmask": "24",
    "port": "23"
  },
  "scope": "svm",
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
}
}
=====

```

Status: Default

ONTAP Error Response Codes

```
|===  
| Error Code | Description  
  
| 66257099  
| Only one protocol can be specified.  
  
| 66257100  
| Only one local port can be specified.  
  
| 66257101  
| Only one remote port can be specified.  
  
| 66257103  
| IPsec policy with same name already exists in this SVM.  
  
| 66257107  
| The specified pre-shared key is not a valid hexadecimal string.  
  
| 66257109  
| The specified pre-shared key is not a valid Base64 encoded binary  
string.  
  
| 66257110  
| Failed to a create policy sequencing value.  
  
| 66257111  
| The IPsec policy with action ESP TRANSPORT provides packet protection  
and requires a secret key for authentication.  
  
| 66257112  
| The IPsec policy with the action specified does not provide packet  
protection and the authentication method provided for the policy will be  
ignored.  
  
| 66257113  
| Only one local IP subnet can be specified.  
  
| 66257114  
| Only one remote IP subnet can be specified.
```



```

| 66257115
| Port ranges containing more than one port are not supported.

| 66257117
| IPsec is not supported on the SVM specified in the policy, IPsec is
supported on data SVMs only.

| 66257120
| The subnet selector must be a host address (An IPv4 address with a 32-
bit netmask or an IPv6 address with a 128-bit netmask).

| 66257121
| The maximum limit of IPsec Policies has reached for the specified SVM.

| 66257125
| The local_endpoint.address must be specified with
local_endpoint.netmask.

| 66257126
| The remote_endpoint.address must be specified with
remote_endpoint.netmask.
|===

```

```

[cols=3*,options=header]

```

```

|===

```

```

|Name

```

```

|Type

```

```

|Description

```

```

|error

```

```

|link:#error[error]

```

```

a|

```

```

|===

```

```

.Example error

```

```

[%collapsible%closed]

```

```

====

```

```

[source,json,subs=+macros]

```

```

{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    }
  }
}

```

```

    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

```

== Definitions

```

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====

```

```

[#local_endpoint]
[.api-collapsible-fifth-title]
local_endpoint

```

Local endpoint for the IPsec policy.

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|address
|string
a|IPv4 or IPv6 address

```

```

|family
|string
a|IPv4 or IPv6

```

```

|netmask
|string
a|Input as netmask length (16) or IPv4 mask (255.255.0.0). For IPv6, you
must set the netmask length. The default value is 64. Output is always
netmask length.

```

```

|port
|string

```

a|Application port to be covered by the IPsec policy

|===

[#remote_endpoint]

[.api-collapsible-fifth-title]

remote_endpoint

Remote endpoint for the IPsec policy.

[cols=3*,options=header]

|===

|Name

|Type

|Description

|address

|string

a|IPv4 or IPv6 address

|family

|string

a|IPv4 or IPv6

|netmask

|string

a|Input as netmask length (16) or IPv4 mask (255.255.0.0). For IPv6, you must set the netmask length. The default value is 64. Output is always netmask length.

|port

|string

a|Application port to be covered by the IPsec policy

|===

[#href]

[.api-collapsible-fifth-title]

href

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:href[href]
a|

|===

[#svm]
[.api-collapsible-fifth-title]
svm

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string

```

a|The name of the SVM.

|uuid

|string

a|The unique identifier of the SVM.

|===

[#ipsec_policy]

[.api-collapsible-fifth-title]

ipsec_policy

IPsec policy object.

[cols=3*,options=header]

|===

|Name

|Type

|Description

|action

|string

a|Action for the IPsec policy.

|enabled

|boolean

a|Indicates whether or not the policy is enabled.

|local_endpoint

|link:#local_endpoint[local_endpoint]

a|Local endpoint for the IPsec policy.

|name

|string

a|IPsec policy name.

|protocol

|string

a|Lower layer protocol to be covered by the IPsec policy.

```
|remote_endpoint
|link:#remote_endpoint[remote_endpoint]
a|Remote endpoint for the IPsec policy.
```

```
|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".
```

```
|secret_key
|string
a|Pre-shared key for IKE negotiation.
```

```
|svm
|link:#svm[svm]
a|
```

```
|uuid
|string
a|Unique identifier of the IPsec policy.
```

```
|===
```

```
[#_links]
[.api-collapsible-fifth-title]
_links
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|next
|link:#href[href]
a|
```

```
|self
|link:#href[href]
a|
```

|===

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
```

|===

```
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

|===

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
```

|===

```
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
|string
a|Error code
```

```
|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
[#svm]
[.api-collapsible-fifth-title]
svm
```

SVM, applies only to SVM-scoped objects.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#records]
[.api-collapsible-fifth-title]
records
```


IPsec policy object.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|action
```

```
|string
```

```
a|Action for the IPsec policy.
```

```
|enabled
```

```
|boolean
```

```
a|Indicates whether or not the policy is enabled.
```

```
|local_endpoint
```

```
|link:#local_endpoint[local_endpoint]
```

```
a|Local endpoint for the IPsec policy.
```

```
|name
```

```
|string
```

```
a|IPsec policy name.
```

```
|protocol
```

```
|string
```

```
a|Lower layer protocol to be covered by the IPsec policy.
```

```
|remote_endpoint
```

```
|link:#remote_endpoint[remote_endpoint]
```

```
a|Remote endpoint for the IPsec policy.
```

```
|scope
```

```
|string
```

```
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to  
"cluster".
```

```
|secret_key
```

```
|string
```

a|Pre-shared key for IKE negotiation.

|svm

|link:#svm[svm]

a|SVM, applies only to SVM-scoped objects.

|uuid

|string

a|Unique identifier of the IPsec policy.

|===

//end collapsible .Definitions block

====

[[ID2f46d2b0ec8acee13c987f31ec661137]]

= Delete an IPsec policy

[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-block]#`/security/ipsec/policies/{uuid}`#

Deletes a specific IPsec policy.

== Related ONTAP commands

* `security ipsec policy delete`

== Learn more

* xref:{relative_path}security_ipsec_policies_endpoint_overview.html[DOC /security/ipsec/policies]

== Parameters

[cols=5*,options=header]

|===

|Name

```
|Type
|In
|Required
|Description

|uuid
|string
|path
|True
a|
|===

== Response
```

Status: 200, Ok

```
== Error
```

Status: Default

ONTAP Error Response Codes

```
|===
| Error Code | Description

| 66257096
| Internal error. Failed to purge connections associated with the IPsec
policy.

| 66257116
| IPsec policy with the specified UUID was not found.
|===
```

```
[cols=3*,options=header]
```

```
|===
|Name
|Type
|Description
```

```
|error
|link:#error[error]
a|
```

```

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

```

```

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[ID155d01adac2622b969710501d704f0d4]]
= Retrieve an IPsec policy

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/ipsec/policies/{uuid}`#

```

Retrieves a specific IPsec policy.

== Related ONTAP commands

* `security ipsec policy show`

== Learn more

* [xref:{relative_path}security_ipsec_policies_endpoint_overview.html\[DOC /security/ipsec/policies\]](#)

== Parameters

[cols=5*,options=header]

|===

|Name

|Type

|In

|Required

|Description

|uuid

|string

|path

|True

a|IPsec policy UUID

|fields

|array[string]

|query

|False

a|Specify the fields to return.

|===

== Response

Status: 200, Ok

[cols=3*,options=header]

|===

```

|Name
|Type
|Description

|action
|string
a|Action for the IPsec policy.

|enabled
|boolean
a|Indicates whether or not the policy is enabled.

|local_endpoint
|link:#local_endpoint[local_endpoint]
a|Local endpoint for the IPsec policy.

|name
|string
a|IPsec policy name.

|protocol
|string
a|Lower layer protocol to be covered by the IPsec policy.

|remote_endpoint
|link:#remote_endpoint[remote_endpoint]
a|Remote endpoint for the IPsec policy.

|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

|secret_key
|string
a|Pre-shared key for IKE negotiation.

|svm
|link:#svm[svm]

```

```

a|

|uuid
|string
a|Unique identifier of the IPsec policy.

|===

.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "action": "bypass",
  "local_endpoint": {
    "address": "10.10.10.7",
    "family": "ipv4",
    "netmask": "24",
    "port": "23"
  },
  "protocol": "17",
  "remote_endpoint": {
    "address": "10.10.10.7",
    "family": "ipv4",
    "netmask": "24",
    "port": "23"
  },
  "scope": "svm",
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
}
=====

== Error

```

Status: Default

ONTAP Error Response Codes

|===

| Error Code | Description

| 66257116

| IPsec policy with the specified UUID was not found.

|===

[cols=3*,options=header]

|===

|Name

|Type

|Description

|error

|link:#error[error]

a|

|===

.Example error

[%collapsible%closed]

====

[source,json,subs=+macros]

```
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

====

== Definitions

[.api-def-first-level]

.See Definitions

[%collapsible%closed]

```
//Start collapsible Definitions block
====
[#local_endpoint]
[.api-collapsible-fifth-title]
local_endpoint

Local endpoint for the IPsec policy.


[cols=3*,options=header]
|===
|Name
|Type
|Description

|address
|string
a|IPv4 or IPv6 address

|family
|string
a|IPv4 or IPv6

|netmask
|string
a|Input as netmask length (16) or IPv4 mask (255.255.0.0). For IPv6, you
must set the netmask length. The default value is 64. Output is always
netmask length.

|port
|string
a|Application port to be covered by the IPsec policy

|===

[#remote_endpoint]
[.api-collapsible-fifth-title]
remote_endpoint

Remote endpoint for the IPsec policy.
```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|address
|string
a|IPv4 or IPv6 address

|family
|string
a|IPv4 or IPv6

|netmask
|string
a|Input as netmask length (16) or IPv4 mask (255.255.0.0). For IPv6, you
must set the netmask length. The default value is 64. Output is always
netmask length.

|port
|string
a|Application port to be covered by the IPsec policy

|===

[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

```

```

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#svm]
[.api-collapsible-fifth-title]
svm

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

|===

[#error_arguments]
[.api-collapsible-fifth-title]

```

error_arguments

[cols=3*,options=header]

|===

|Name

|Type

|Description

|code

|string

a|Argument code

|message

|string

a|Message argument

|===

[#error]

[.api-collapsible-fifth-title]

error

[cols=3*,options=header]

|===

|Name

|Type

|Description

|arguments

|array[link:#error_arguments[error_arguments]]

a|Message arguments

|code

|string

a|Error code

|message

|string

a|Error message

|target

```

|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
=====

[[ID220728fe800551cb46784d511d5f7fdd]]
= Update an IPsec policy

[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-
block]#`/security/ipsec/policies/{uuid}`#

Updates a specific IPsec policy.

== Related ONTAP commands

* `security ipsec policy modify`

== Learn more

* xref:{relative_path}security_ipsec_policies_endpoint_overview.html[DOC
/security/ipsec/policies]

== Parameters

[cols=5*,options=header]
|===

|Name
|Type
|In
|Required
|Description

|uuid
|string
|path
|True

```

a|IPsec policy UUID

|===

== Request Body

[cols=3*,options=header]

|===

|Name

|Type

|Description

|action

|string

a|Action for the IPsec policy.

|enabled

|boolean

a|Indicates whether or not the policy is enabled.

|local_endpoint

|link:#local_endpoint[local_endpoint]

a|Local endpoint for the IPsec policy.

|name

|string

a|IPsec policy name.

|protocol

|string

a|Lower layer protocol to be covered by the IPsec policy.

|remote_endpoint

|link:#remote_endpoint[remote_endpoint]

a|Remote endpoint for the IPsec policy.

|scope

|string

a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to

```

"cluster".

|secret_key
|string
a|Pre-shared key for IKE negotiation.

|svm
|link:#svm[svm]
a|

|uuid
|string
a|Unique identifier of the IPsec policy.

```

```

|===

```

```

.Example request
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "action": "bypass",
  "local_endpoint": {
    "address": "10.10.10.7",
    "family": "ipv4",
    "netmask": "24",
    "port": "23"
  },
  "protocol": "17",
  "remote_endpoint": {
    "address": "10.10.10.7",
    "family": "ipv4",
    "netmask": "24",
    "port": "23"
  },
  "scope": "svm",
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    }
  },
}

```



```
"name": "svm1",
"uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
},
"uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
}
====

== Response
```

Status: 200, Ok

```
== Error
```

Status: Default

ONTAP Error Response Codes

```
|===
| Error Code | Description

| 66257097
| Internal error. Failed to update the IPsec policy.

| 66257099
| Only one protocol can be specified.

| 66257100
| Only one local port can be specified.

| 66257101
| Only one remote port can be specified.

| 66257110
| Failed to create a policy sequencing value.

| 66257113
| Only one local IP subnet can be specified.

| 66257114
| Only one remote IP subnet can be specified.

| 66257115
| Port ranges containing more than one port are not supported.

| 66257116
```

```

| IPsec policy with the specified UUID was not found.

| 66257120
| The subnet selector must be a host address (An IPv4 address with a 32-
bit netmask or an IPv6 address with a 128-bit netmask).
|===

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#local_endpoint]

```

[.api-collapsible-fifth-title]

local_endpoint

Local endpoint for the IPsec policy.

[cols=3*,options=header]

|===

|Name

|Type

|Description

|address

|string

a|IPv4 or IPv6 address

|family

|string

a|IPv4 or IPv6

|netmask

|string

a|Input as netmask length (16) or IPv4 mask (255.255.0.0). For IPv6, you must set the netmask length. The default value is 64. Output is always netmask length.

|port

|string

a|Application port to be covered by the IPsec policy

|===

[#remote_endpoint]

[.api-collapsible-fifth-title]

remote_endpoint

Remote endpoint for the IPsec policy.

[cols=3*,options=header]

|===

|Name

```

|Type
|Description

|address
|string
a|IPv4 or IPv6 address


|family
|string
a|IPv4 or IPv6


|netmask
|string
a|Input as netmask length (16) or IPv4 mask (255.255.0.0). For IPv6, you
must set the netmask length. The default value is 64. Output is always
netmask length.


|port
|string
a|Application port to be covered by the IPsec policy


|===

[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]

```

```

_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#svm]
[.api-collapsible-fifth-title]
svm

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

|===

[#ipsec_policy]
[.api-collapsible-fifth-title]
ipsec_policy

IPsec policy object.

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|action
|string
a|Action for the IPsec policy.

|enabled
|boolean
a|Indicates whether or not the policy is enabled.

|local_endpoint
|link:#local_endpoint[local_endpoint]
a|Local endpoint for the IPsec policy.

|name
|string
a|IPsec policy name.

|protocol
|string
a|Lower layer protocol to be covered by the IPsec policy.

|remote_endpoint
|link:#remote_endpoint[remote_endpoint]
a|Remote endpoint for the IPsec policy.

|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

|secret_key
|string
a|Pre-shared key for IKE negotiation.

```

```
|svm
|link:#svm[svm]
a|

|uuid
|string
a|Unique identifier of the IPsec policy.
```

```
|===
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

:leveloffset: -1

= View IPsec security associations

:leveloffset: +1

[[ID28af7f57702c8a04f7ac439df5bb05d9]]
= Security IPsec security-associations endpoint overview

== Overview

* Collection Get: GET security/ipsec/security-associations
* Instance Get: GET security/ipsec/security-associations/uuid

```



```
[[IDe535aea98cle8af177065fd559cc78ea]]  
= Retrieve IPsec and IKE security associations
```

```
[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-  
block]#`/security/ipsec/security-associations`#
```

Retrieves the IPsec and IKE (Internet Key Exchange) security associations.

== Related ONTAP commands

```
* `security ipsec show-ipseca`  
* `security ipsec show-ikesa`
```

== Learn more

```
* xref:{relative_path}security_ipsec_security-  
associations_endpoint_overview.html[DOC /security/ipsec/security-  
associations]
```

== Parameters

```
[cols=5*,options=header]  
|===
```

```
|Name  
|Type  
|In  
|Required  
|Description
```

```
|local_address  
|string  
|query  
|False  
a|Filter by local_address
```

```
|node.uuid  
|string  
|query  
|False
```

```
a|Filter by node.uuid
```

```
|node.name
```

```
|string
```

```
|query
```

```
|False
```

```
a|Filter by node.name
```

```
|uuid
```

```
|string
```

```
|query
```

```
|False
```

```
a|Filter by uuid
```

```
|svm.uuid
```

```
|string
```

```
|query
```

```
|False
```

```
a|Filter by svm.uuid
```

```
|svm.name
```

```
|string
```

```
|query
```

```
|False
```

```
a|Filter by svm.name
```

```
|type
```

```
|string
```

```
|query
```

```
|False
```

```
a|Filter by type
```

```
|ike.responder_security_parameter_index
```

```
|integer
```

```
|query
```

```
|False
```

```
a|Filter by ike.responder_security_parameter_index
```

```
|ike.state
```

```
|string
```

```
|query
|False
a|Filter by ike.state

ike.authentication
|string
|query
|False
a|Filter by ike.authentication

ike.initiator_security_parameter_index
|integer
|query
|False
a|Filter by ike.initiator_security_parameter_index

ike.version
|string
|query
|False
a|Filter by ike.version

remote_address
|string
|query
|False
a|Filter by remote_address

ipsec.outbound.security_parameter_index
|integer
|query
|False
a|Filter by ipsec.outbound.security_parameter_index

ipsec.outbound.bytes
|integer
|query
|False
a|Filter by ipsec.outbound.bytes
```

```
|ipsec.outbound.packets
|integer
|query
|False
a|Filter by ipsec.outbound.packets

|ipsec.inbound.security_parameter_index
|integer
|query
|False
a|Filter by ipsec.inbound.security_parameter_index

|ipsec.inbound.bytes
|integer
|query
|False
a|Filter by ipsec.inbound.bytes

|ipsec.inbound.packets
|integer
|query
|False
a|Filter by ipsec.inbound.packets

|ipsec.action
|string
|query
|False
a|Filter by ipsec.action

|ipsec.state
|string
|query
|False
a|Filter by ipsec.state

|lifetime
|integer
|query
|False
a|Filter by lifetime
```

```
|name
|string
|query
|False
a|Filter by name
```

```
|cipher_suite
|string
|query
|False
a|Filter by cipher_suite
```

```
|fields
|array[string]
|query
|False
a|Specify the fields to return.
```

```
|max_records
|integer
|query
|False
a|Limit the number of records returned.
```

```
|return_records
|boolean
|query
|False
a|The default is true for GET calls. When set to false, only the number
of records is returned.
```

```
|return_timeout
|integer
|query
|False
a|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.
```

```

|order_by
|array[string]
|query
|False
a|Order results by specified fields and optional [asc|desc] direction.
Default direction is 'asc' for ascending.

|===

== Response

```

Status: 200, Ok

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|error
|link:#error[error]
a|

|num_records
|integer
a|Number of records

|records
|array[link:#records[records]]
a|

|===

.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {

```

```

    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  },
  "num_records": 1,
  "records": {
    "cipher_suite": "aescbc",
    "ike": {
      "authentication": "none",
      "state": "none"
    },
    "ipsec": {
      "action": "bypass"
    },
    "node": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "node1",
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    },
    "svm": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "svm1",
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    },
    "type": "ipsec"
  }
}

```

```

}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]

```



```

href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|next
|link:href[href]
a|

|self
|link:href[href]
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code

```

```

|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

[#ike]
[.api-collapsible-fifth-title]

```

ike

Objects containing parameters specific to IKE (Internet Key Exchange) security association.

[cols=3*,options=header]

|===

|Name

|Type

|Description

|authentication

|string

a|Authentication method for internet key exchange protocol.

|initiator_security_parameter_index

|integer

a|Initiator's security parameter index for the IKE security association.

|responder_security_parameter_index

|integer

a|Responder's security parameter index for the IKE security association.

|state

|string

a|State of the IKE connection.

|version

|string

a|Internet key exchange protocol version.

|===

[#inbound]

[.api-collapsible-fifth-title]

inbound

Status for inbound parameters for the IPsec security association.

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|bytes
|integer
a|Number of inbound bytes for the IPsec security association.

|packets
|integer
a|Number of inbound packets for the IPsec security association.

|security_parameter_index
|integer
a|Inbound security parameter index for the IPSec security association.

|===

[#outbound]
[.api-collapsible-fifth-title]
outbound

Status for outbound parameters for the IPsec security association.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|bytes
|integer
a|Number of outbound bytes for the IPsec security association.

|packets
|integer
a|Number of outbound packets for the IPsec security association.

```

```

|security_parameter_index
|integer
a|Outbound security parameter index for the IPsec security association.

|===

[#ipsec]
[.api-collapsible-fifth-title]
ipsec

Objects containing parameters specific to IPsec security association.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|action
|string
a|Action for the IPsec security association.

|inbound
|link:#inbound[inbound]
a|Status for inbound parameters for the IPsec security association.

|outbound
|link:#outbound[outbound]
a|Status for outbound parameters for the IPsec security association.

|state
|string
a|State of the IPsec security association.

|===

[#_links]
[.api-collapsible-fifth-title]
_links

```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#node]
[.api-collapsible-fifth-title]
node

Node with the security association.
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|

|uuid
|string
a|

|===
```

```
[#svm]
[.api-collapsible-fifth-title]
svm
```

SVM, applies only to SVM-scoped objects.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|name
```

```
|string
```

```
a|The name of the SVM.
```

```
|uuid
```

```
|string
```

```
a|The unique identifier of the SVM.
```

```
|===
```

```
[#records]
```

```
[.api-collapsible-fifth-title]
```

```
records
```

Security association object for IPsec security association and IKE (Internet Key Exchange) security association.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|cipher_suite
```

```
|string
```

```
a|Cipher suite for the security association.
```

```
|ike
```

```
|link:#ike[ike]
```

```
a|Objects containing parameters specific to IKE (Internet Key Exchange)
```

security association.

|ipsec

|link:#ipsec[ipsec]

a|Objects containing parameters specific to IPsec security association.

|lifetime

|integer

a|Lifetime for the security association in seconds.

|local_address

|string

a|Local address of the security association.

|name

|string

a|Policy name for the security association.

|node

|link:#node[node]

a|Node with the security association.

|remote_address

|string

a|Remote address of the security association.

|svm

|link:#svm[svm]

a|SVM, applies only to SVM-scoped objects.

|type

|string

a|Type of security association, it can be IPsec or IKE (Internet Key Exchange).

|uuid

|string

a|Unique identifier of the security association.

|===

//end collapsible .Definitions block

====

[[IDaaa6c9674ddd8a705900fdf246b35517]]

= Retrieve an IPsec or IKE security association

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-block]#`/security/ipsec/security-associations/{uuid}`#

Retrieves a specific IPsec or IKE (Internet Key Exchange) security association.

== Related ONTAP commands

* `security ipsec show-ipsecsa`

* `security ipsec show-ikesa`

== Learn more

* xref:{relative_path}security_ipsec_security-associations_endpoint_overview.html[DOC /security/ipsec/security-associations]

== Parameters

[cols=5*,options=header]

|===

|Name

|Type

|In

|Required

|Description

|uuid

|string

|path

```
|True
a|UUID of IPsec or IKE security association.

|fields
|array[string]
|query
|False
a|Specify the fields to return.

|===

== Response
```

Status: 200, Ok

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|cipher_suite
|string
a|Cipher suite for the security association.

|ike
|link:#ike[ike]
a|Objects containing parameters specific to IKE (Internet Key Exchange)
security association.

|ipsec
|link:#ipsec[ipsec]
a|Objects containing parameters specific to IPsec security association.

|lifetime
|integer
a|Lifetime for the security association in seconds.

|local_address
|string
a|Local address of the security association.
```

```

|name
|string
a|Policy name for the security association.

|node
|link:#node[node]
a|Node with the security association.

|remote_address
|string
a|Remote address of the security association.

|svm
|link:#svm[svm]
a|

|type
|string
a|Type of security association, it can be IPsec or IKE (Internet Key
Exchange).

|uuid
|string
a|Unique identifier of the security association.

|===

```

```

.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "cipher_suite": "aescbc",
  "ike": {
    "authentication": "none",
    "state": "none"
  },
  "ipsec": {
    "action": "bypass"
  }
}

```

```

},
"node": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "name": "node1",
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
},
"svm": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "name": "svm1",
  "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
},
"type": "ipsec"
}
====

== Error

```

Status: Default

ONTAP Error Response Codes

```

|===
| Error Code | Description
| 66257118
| IPsec SA with the specified UUID was not found.
| 66257119
| IPsec SA with the specified UUID was not found.
|===

```

[cols=3*,options=header]

```

|===
|Name
|Type
|Description

```

```
|error
|link:#error[error]
a|
```

```
|===
```

```
.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

```
== Definitions
```

```
[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#ike]
[.api-collapsible-fifth-title]
ike
```

Objects containing parameters specific to IKE (Internet Key Exchange) security association.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```

|authentication
|string
a|Authentication method for internet key exchange protocol.

|initiator_security_parameter_index
|integer
a|Initiator's security parameter index for the IKE security association.

|responder_security_parameter_index
|integer
a|Responder's security parameter index for the IKE security association.

|state
|string
a|State of the IKE connection.

|version
|string
a|Internet key exchange protocol version.

|===

[#inbound]
[.api-collapsible-fifth-title]
inbound

Status for inbound parameters for the IPsec security association.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|bytes
|integer
a|Number of inbound bytes for the IPsec security association.

|packets

```

```

|integer
a|Number of inbound packets for the IPsec security association.

|security_parameter_index
|integer
a|Inbound security parameter index for the IPsec security association.

|===

[#outbound]
[.api-collapsible-fifth-title]
outbound

Status for outbound parameters for the IPsec security association.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|bytes
|integer
a|Number of outbound bytes for the IPsec security association.

|packets
|integer
a|Number of outbound packets for the IPsec security association.

|security_parameter_index
|integer
a|Outbound security parameter index for the IPsec security association.

|===

[#ipsec]
[.api-collapsible-fifth-title]
ipsec

```

Objects containing parameters specific to IPsec security association.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|action
```

```
|string
```

```
a|Action for the IPsec security association.
```

```
|inbound
```

```
|link:#inbound[inbound]
```

```
a|Status for inbound parameters for the IPsec security association.
```

```
|outbound
```

```
|link:#outbound[outbound]
```

```
a|Status for outbound parameters for the IPsec security association.
```

```
|state
```

```
|string
```

```
a|State of the IPsec security association.
```

```
|===
```

```
[#href]
```

```
[.api-collapsible-fifth-title]
```

```
href
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|href
```

```
|string
```

```
a|
```

```
|===
```



```

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#node]
[.api-collapsible-fifth-title]
node

Node with the security association.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|

|uuid
|string
a|

|===

```

```

[#svm]
[.api-collapsible-fifth-title]
svm

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

```

```

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

:leveloffset: -1

= Manage key managers

:leveloffset: +1

```

```
[[ID46ce59e16ff23355e6df4a3dd08f5426]]
= 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 the key manager configurations for all clusters and SVMs (showing Onboard Key Manager)

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": "8ba52e0f-ae22-11e9-b747-005056bb7636",
    "scope": "cluster",
    "onboard": {
        "enabled": true,
        "key_backup": "-----BEGIN
BACKUP-----\n <Backup Data>
\n-----END BACKUP-----\n"
    },
    "volume_encryption": {
        "supported": false,
        "message": "The following nodes do not support volume granular
encryption: ntap-vsim2.",
        "code": 65536935
    },
    "is_default_data_at_rest_encryption_disabled": false
}
],
"num_records": 1
}
----

'''

```

=== Retrieving expensive fields such as, status.code and status.message, associated with a key manager.

These values are not retrieved by default with the 'fields=*' option. The following example shows how to retrieve the expensive objects associated with a key manager.

```

----

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

# The call:
curl -X GET "https://<mgmt-ip>/api/security/key-
managers?fields=status.message,status.code" -H 'accpt:
application/hal+json'

# The response:
{
"records": [
{
    "uuid": "ac305d46-aef4-11e9-ad3c-005056bb7636",
    "status": {

```

```

    "message": "No action needed at this time.",
    "code": 65537200
  },
  "_links": {
    "self": {
      "href": "/api/security/key-managers/ac305d46-aef4-11e9-ad3c-
005056bb7636"
    }
  }
},
"num_records": 1,
"_links": {
  "self": {
    "href": "/api/security/key-managers?fields=status.message,status.code"
  }
}
----

'''

```

=== 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.local11:3678",
        "timeout": 25,
        "username": "",
        "_links": {
          "self": {
            "href": "/api/security/key-managers/2345f09c-d6c9-11e8-b5bf-005056bb017d/key-servers/vs0.local11:3678/"
          }
        }
      }
    ],
    "_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\" } }"
```

```
----
```

```
'''
```

=== Synchronizing the passphrase of the Onboard Key Manager on a cluster

The following example shows how to synchronize the passphrase on a cluster where the Onboard Key Manager is already configured.

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\",    \"synchronize\": true
}}"
```

'''

=== Configuring the Onboard Key Manager on a cluster

The following example shows how to configure the Onboard Key Manager on a cluster where the Onboard Key Manager is not configured, but is configured on an MetroCluster partner cluster.

The API:

POST /api/security/key-managers

The call:

```
curl -X POST 'https://<mgmt-ip>/api/security/key-
managers?return_records=false' -H 'accept: application/hal+json' -H
"Content-Type: application/json" -d "{  \"onboard\": {    \"passphrase\":
\"passphrase\",    \"synchronize\": true  }}"
```

'''

=== 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'
----
```

'''

```
[[ID99e864e50009277ff819a6fc33998c4f]]
= Retrieve key managers
```

```
[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-block]#`/security/key-managers`#
```

Retrieves key managers.

== Expensive properties

There is an added cost to retrieving values for these properties. They are not included by default in GET results and must be explicitly requested using the ``fields`` query parameter. See [xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Requesting_specific_fields\[DOC Requesting specific fields\]](#) to learn more.

- * ``connectivity``
- * ``status.message``
- * ``status.code``

== Related ONTAP commands

- * ``security key-manager show-keystore``
- * ``security key-manager external show``
- * ``security key-manager external show-status``
- * ``security key-manager onboard show-backup``

== Learn more

- * [xref:{relative_path}security_key-managers_endpoint_overview.html\[DOC /security/key-managers\]](#)

```

== Parameters

[cols=5*,options=header]
|===

|Name
|Type
|In
|Required
|Description

|svm.uuid
|string
|query
|False
a|Filter by svm.uuid

|svm.name
|string
|query
|False
a|Filter by svm.name

|uuid
|string
|query
|False
a|Filter by uuid

|volume_encryption.code
|integer
|query
|False
a|Filter by volume_encryption.code

|volume_encryption.supported
|boolean
|query
|False
a|Filter by volume_encryption.supported

```

```
|volume_encryption.message
|string
|query
|False
a|Filter by volume_encryption.message
```

```
|is_default_data_at_rest_encryption_disabled
|boolean
|query
|False
a|Filter by is_default_data_at_rest_encryption_disabled
```

```
|external.servers.username
|string
|query
|False
a|Filter by external.servers.username
```

```
|external.servers.server
|string
|query
|False
a|Filter by external.servers.server
```

```
|external.servers.connectivity.cluster_availability
|boolean
|query
|False
a|Filter by external.servers.connectivity.cluster_availability
```

```
|external.servers.connectivity.records.state
|string
|query
|False
a|Filter by external.servers.connectivity.records.state
```

```
|external.servers.connectivity.records.node.uuid
|string
|query
|False
```

```
a|Filter by external.servers.connectivity.records.node.uuid
```

```
|external.servers.connectivity.records.node.name
```

```
|string
```

```
|query
```

```
|False
```

```
a|Filter by external.servers.connectivity.records.node.name
```

```
|external.servers.timeout
```

```
|integer
```

```
|query
```

```
|False
```

```
a|Filter by external.servers.timeout
```

```
|external.server_ca_certificates.uuid
```

```
|string
```

```
|query
```

```
|False
```

```
a|Filter by external.server_ca_certificates.uuid
```

```
|external.client_certificate.uuid
```

```
|string
```

```
|query
```

```
|False
```

```
a|Filter by external.client_certificate.uuid
```

```
|onboard.enabled
```

```
|boolean
```

```
|query
```

```
|False
```

```
a|Filter by onboard.enabled
```

```
|onboard.key_backup
```

```
|string
```

```
|query
```

```
|False
```

```
a|Filter by onboard.key_backup
```

```
|status.message
```

```
|string
```

```
|query
|False
a|Filter by status.message
```

```
|status.code
|integer
|query
|False
a|Filter by status.code
```

```
|scope
|string
|query
|False
a|Filter by scope
```

```
|fields
|array[string]
|query
|False
a|Specify the fields to return.
```

```
|max_records
|integer
|query
|False
a|Limit the number of records returned.
```

```
|return_timeout
|integer
|query
|False
a|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
```


a|The default is true for GET calls. When set to false, only the number of records is returned.

```
|order_by
|array[string]
|query
|False
```

a|Order results by specified fields and optional [asc|desc] direction. Default direction is 'asc' for ascending.

```
|===
```

== Response

Status: 200, Ok

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
```

a|

```
|num_records
|integer
a|Number of records
```

```
|records
|array[link:#security_key_manager[security_key_manager]]
a|
```

```
|===
```

.Example response

[%collapsible%closed]

=====

```
[source,json,subs=+macros]
```

```
{
  "_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"
        }
      },
      "connectivity": {
        "records": {
          "node": {
            "_links": {
              "self": {
                "href": "/api/resourcelink"
              }
            },
            "name": "node1",
            "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
          },

```



```

    "status": {
      "code": 346758,
      "message": "This cluster is part of a MetroCluster configuration.
Use the REST API POST method security/key_managers/ with the synchronize
option and the same passphrase on the partner cluster before proceeding
with any key manager operations. Failure to do so could lead to
switchover or switchback failure."
    },
    "svm": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "svm1",
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    },
    "uuid": "string",
    "volume_encryption": {
      "code": 346758,
      "message": "No platform support for volume encryption in following
nodes - node1, node2."
    }
  }
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error

```

```

[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===

```

```

|Name
|Type
|Description

|next
|link:#href[href]
a|

|self
|link:#href[href]
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#client_certificate]
[.api-collapsible-fifth-title]
client_certificate

Client certificate

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]

```

```

a|

|uuid
|string
a|Certificate UUID

|===

[#server_ca_certificates]
[.api-collapsible-fifth-title]
server_ca_certificates

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|uuid
|string
a|Certificate UUID

|===

[#self_link]
[.api-collapsible-fifth-title]
self_link

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

```

```
[#node]
[.api-collapsible-fifth-title]
node
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|name
```

```
|string
```

```
a|
```

```
|uuid
```

```
|string
```

```
a|
```

```
|===
```

```
[#key_server_state]
```

```
[.api-collapsible-fifth-title]
```

```
key_server_state
```

The state of the key server for a specific node.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|node
```

```
|link:#node[node]
```

```
a|
```

```
|state
```

```
|string
```

```
a|Key server connectivity state
```


|===

```
[#connectivity]
[.api-collapsible-fifth-title]
connectivity
```

This property returns the key server connectivity state on all nodes of the cluster. The state is returned for a node only if the connectivity is not in an available state on that node.

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```
[cols=3*,options=header]
```

|===

```
|Name
|Type
|Description
```

```
|cluster_availability
|boolean
```

a|Set to true when key server connectivity state is available on all nodes of the cluster.

```
|records
```

```
|array[link:#key_server_state[key_server_state]]
```

a|An array of key server connectivity states for each node.

|===

```
[#key_server_readcreate]
[.api-collapsible-fifth-title]
key_server_readcreate
```

```
[cols=3*,options=header]
```

|===

```
|Name
|Type
|Description
```

```

|_links
|link:#self_link[self_link]
a|

|connectivity
|link:#connectivity[connectivity]
a|This property returns the key server connectivity state on all nodes of
the cluster. The state is returned for a node only if the connectivity is
not in an available state on that node.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.

|server
|string
a|External key server for key management. If no port is provided, a
default port of 5696 is used.

|timeout
|integer
a|I/O timeout in seconds for communicating with the key server.

|username
|string
a|Username credentials for connecting with the key server.

|===

[#external]
[.api-collapsible-fifth-title]
external

Configures external key management

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```
|client_certificate
|link:#client_certificate[client_certificate]
a|Client certificate
```

```
|server_ca_certificates
|array[link:#server_ca_certificates[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 keyservers per
SVM.
```

```
|servers
|array[link:#key_server_readcreate[key_server_readcreate]]
a|The set of external key servers.
```

```
|===
```

```
[#onboard]
[.api-collapsible-fifth-title]
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.

```
[cols=3*,options=header]
|===
```

```
|Name
|Type
|Description
```

```
|enabled
|boolean
a|Is the onboard key manager enabled?
```

```
|existing_passphrase
|string
a|The cluster-wide passphrase. This is not audited.
```

```
|key_backup
```

```
|string
a|Backup of the onboard key manager's key hierarchy. It is required to
save this backup after configuring the onboard key manager to help in the
recovery of the cluster in case of catastrophic failures.
```

```
|passphrase
|string
a|The cluster-wide passphrase. This is not audited.
```

```
|synchronize
|boolean
a|Synchronizes missing onboard keys on any node in the cluster. If a node
is added to a cluster that has onboard key management configured, the
synchronize operation needs to be performed in a PATCH operation. In a
MetroCluster configuration, if onboard key management is enabled on one
site, then the synchronize operation needs to be run as a POST operation
on the remote site providing the same passphrase.
```

```
|===
```

```
[#status]
[.api-collapsible-fifth-title]
status
```

Optional status information on the current state of the key manager indicating if it is fully setup or requires more action.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|code
|integer
```

a|Code corresponding to the status message. Returns 0 if the setup is complete. This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```
|message
|string
a|Current state of the key manager indicating any additional steps to
perform to finish the setup. This is an advanced property; there is an
added cost to retrieving its value. The property is not populated for
either a collection GET or an instance GET unless it is explicitly
requested using the `fields` query parameter or GET for all advanced
properties is enabled.
```

```
|===
```

```
[#svm]
[.api-collapsible-fifth-title]
svm
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#volume_encryption]
[.api-collapsible-fifth-title]
volume_encryption
```

Indicates whether volume encryption is supported in the cluster.

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|integer
a|Code corresponding to the status message. Returns a 0 if volume
encryption is supported in all nodes of the cluster.

|message
|string
a|Reason for not supporting volume encryption.

|supported
|boolean
a|Set to true when volume encryption support is available on all nodes of
the cluster.

|===

[#security_key_manager]
[.api-collapsible-fifth-title]
security_key_manager

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|external
|link:#external[external]
a|Configures external key management

|is_default_data_at_rest_encryption_disabled

```

```

|boolean
a|Indicates whether default data-at-rest encryption is disabled in the
cluster.

|onboard
|link:#onboard[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
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

|status
|link:#status[status]
a|Optional status information on the current state of the key manager
indicating if it is fully setup or requires more action.

|svm
|link:#svm[svm]
a|

|uuid
|string
a|

|volume_encryption
|link:#volume_encryption[volume_encryption]
a|Indicates whether volume encryption is supported in the cluster.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name

```

```

|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

```



```
//end collapsible .Definitions block
====
```

```
[[ID1a0db32a134a4c561a8ca5c90268870c]]
= Create a key manager
```

```
[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/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.
- * `synchronize` - Synchronizes missing onboard keys on any node in the cluster. Required only when creating an Onboard Key Manager at the partner site of a MetroCluster configuration.

== Related ONTAP commands

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

== Learn more

* [xref:{relative_path}security_key-managers_endpoint_overview.html\[DOC /security/key-managers\]](#)

== Parameters

```

[cols=5*,options=header]
|===

|Name
|Type
|In
|Required
|Description

|return_records
|boolean
|query
|False
a|The default is false. If set to true, the records are returned.

|===

== Request Body

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|external
|link:#external[external]
a|Configures external key management

|is_default_data_at_rest_encryption_disabled
|boolean
a|Indicates whether default data-at-rest encryption is disabled in the
cluster.

|onboard
|link:#onboard[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
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

|status
|link:#status[status]
a|Optional status information on the current state of the key manager
indicating if it is fully setup or requires more action.

|svm
|link:#svm[svm]
a|

|uuid
|string
a|

|volume_encryption
|link:#volume_encryption[volume_encryption]
a|Indicates whether volume encryption is supported in the cluster.

|===

.Example request
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_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"
      }
    },
    "connectivity": {
      "records": {
        "node": {
          "_links": {
            "self": {
              "href": "/api/resourcelink"
            }
          },
          "name": "node1",
          "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
        },
        "state": "not_responding"
      }
    },
    "server": "keyserver1.com:5698",
    "timeout": 60,
    "username": "admin"
  },
  "onboard": {
    "existing_passphrase": "The cluster password of length 32-256 ASCII
characters.",
    "key_backup": "'-----BEGIN
BACKUP-----
TmV0QXBwIETleSBCbG9iAAEAAAAEAAAAcAEAAAAAAAAAAxBFWWAAAAACEAAAAAAAAA
QAAAAAAAAABzDyyVAAAAALi5Jsjsjvy6gUxnT78KoDKXHYb6sSeraM00quOULY6BeV
n6dMFxuErCD1lbERaOQZSuaYylp8oQHtTEfGMLZM4TYiAAAAAAAAACgAAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAA
IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAAACAAAAAAAAJAGr3tJA/LRzU
QRHwv+1aWvAAAAAAAAAACQAAAAAAAAAgAAAAAAAAADV1Vd/AAAAAMFM9Q229Bhp

```



```

    "code": 346758,
    "message": "No platform support for volume encryption in following
nodes - node1, node2."
  }
}
====

```

== Response

Status: 201, Created

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records

|records
|array[link:#security_key_manager[security_key_manager]]
a|

|===

.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_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-aelc-123478563412"
    },
    "server_ca_certificates": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "uuid": "1cd8a442-86d1-11e0-aelc-123478563412"
    },
    "servers": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "connectivity": {
        "records": {
          "node": {
            "_links": {
              "self": {
                "href": "/api/resourcelink"
              }
            },
            "name": "node1",
            "uuid": "1cd8a442-86d1-11e0-aelc-123478563412"
          },
          "state": "not_responding"
        }
      },
      "server": "keyserver1.com:5698",
      "timeout": 60,
      "username": "admin"
    }
  }
}

```



```

switchover or switchback failure."
    },
    "svm": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "svm1",
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    },
    "uuid": "string",
    "volume_encryption": {
      "code": 346758,
      "message": "No platform support for volume encryption in following
nodes - node1, node2."
    }
  }
}
====

== Error

```

Status: Default

ONTAP Error Response Codes

```

|====
| Error Code | Description

| 65536038
| A maximum of 4 active key servers are allowed.

| 65536214
| Failed to generate cluster key encryption key.

| 65536216
| Failed to add cluster key encryption key.

| 65536310
| Failed to setup onboard key management because the MetroCluster peer is
unhealthy.

| 65536508
| The platform does not support data at rest encryption.

```

| 65536821
| The certificate is not installed.

| 65536822
| Multitenant key management is not supported in the current cluster version.

| 65536823
| The SVM has key manager already configured.

| 65536824
| Multitenant key management is not supported in MetroCluster configurations.

| 65536834
| Failed to get existing key-server details for the SVM.

| 65536852
| Failed to query supported KMIP protocol versions.

| 65536870
| Key management servers already configured.

| 65536871
| Duplicate key management servers exist.

| 65536876
| External key management requires client and server CA certificates installed and with one or more key servers provided.

| 65536878
| External key management cannot be configured as one or more volume encryption keys of the SVM are stored in cluster key management server.

| 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.

| 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.

| 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.

| 65536916

| Onboard key management is only supported for an admin SVM.

| 65536920

| The Onboard Key Manager passphrase length is incorrect.

| 65537240

| The Onboard Key Manager passphrase must be provided when performing a
POST/synchronize operation.

| 65537241

| The Onboard Key Manager existing_passphrase must not be provided when
performing a POST/synchronize operation.

| 65537244

| Unable to sync/create Onboard Key Manager on the local cluster; Onboard
Key Manager is already configured on the cluster.

| 65537245

| Unable to sync/create Onboard Key Manager on the local cluster; Onboard
Key Manager is not configured on the partner cluster.

| 65537246

| Unable to sync/create Onboard Key Manager on local cluster. This cluster
is not part of a MetroCluster configuration.

| 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.
|===

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]

```

```

[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#client_certificate]
[.api-collapsible-fifth-title]
client_certificate

Client certificate

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links

```

```

|link:#_links[_links]
a|

|uuid
|string
a|Certificate UUID

|===

[#server_ca_certificates]
[.api-collapsible-fifth-title]
server_ca_certificates

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|uuid
|string
a|Certificate UUID

|===

[#self_link]
[.api-collapsible-fifth-title]
self_link

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

```

```
|===
```

```
[#node]  
[.api-collapsible-fifth-title]  
node
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name  
|Type  
|Description
```

```
|_links  
|link:#_links[_links]  
a|
```

```
|name  
|string  
a|
```

```
|uuid  
|string  
a|
```

```
|===
```

```
[#key_server_state]  
[.api-collapsible-fifth-title]  
key_server_state
```

The state of the key server for a specific node.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name  
|Type  
|Description
```

```
|node  
|link:#node[node]  
a|
```

```
|state  
|string
```

a|Key server connectivity state

|===

[#connectivity]
[.api-collapsible-fifth-title]
connectivity

This property returns the key server connectivity state on all nodes of the cluster. The state is returned for a node only if the connectivity is not in an available state on that node.

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|cluster_availability
|boolean
a|Set to true when key server connectivity state is available on all nodes of the cluster.

|records
|array[link:#key_server_state[key_server_state]]
a|An array of key server connectivity states for each node.

|===

[#key_server_readcreate]
[.api-collapsible-fifth-title]
key_server_readcreate

[cols=3*,options=header]
|===
|Name
|Type


```

|Description

|_links
|link:#self_link[self_link]
a|

|connectivity
|link:#connectivity[connectivity]
a|This property returns the key server connectivity state on all nodes of
the cluster. The state is returned for a node only if the connectivity is
not in an available state on that node.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.

|server
|string
a|External key server for key management. If no port is provided, a
default port of 5696 is used.

|timeout
|integer
a|I/O timeout in seconds for communicating with the key server.

|username
|string
a|Username credentials for connecting with the key server.

|===

[#external]
[.api-collapsible-fifth-title]
external

Configures external key management

[cols=3*,options=header]
|===
|Name
|Type

```

|Description

|client_certificate

|link:#client_certificate[client_certificate]

a|Client certificate

|server_ca_certificates

|array[link:#server_ca_certificates[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 keyserver per SVM.

|servers

|array[link:#key_server_readcreate[key_server_readcreate]]

a|The set of external key servers.

|===

[#onboard]

[.api-collapsible-fifth-title]

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.

[cols=3*,options=header]

|===

|Name

|Type

|Description

|enabled

|boolean

a|Is the onboard key manager enabled?

|existing_passphrase

|string

a|The cluster-wide passphrase. This is not audited.

```
|key_backup
|string
a|Backup of the onboard key manager's key hierarchy. It is required to
save this backup after configuring the onboard key manager to help in the
recovery of the cluster in case of catastrophic failures.
```

```
|passphrase
|string
a|The cluster-wide passphrase. This is not audited.
```

```
|synchronize
|boolean
a|Synchronizes missing onboard keys on any node in the cluster. If a node
is added to a cluster that has onboard key management configured, the
synchronize operation needs to be performed in a PATCH operation. In a
MetroCluster configuration, if onboard key management is enabled on one
site, then the synchronize operation needs to be run as a POST operation
on the remote site providing the same passphrase.
```

```
|===
```

```
[#status]
[.api-collapsible-fifth-title]
status
```

Optional status information on the current state of the key manager indicating if it is fully setup or requires more action.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|code
```

```
|integer
```

```
a|Code corresponding to the status message. Returns 0 if the setup is
complete. This is an advanced property; there is an added cost to
retrieving its value. The property is not populated for either a
collection GET or an instance GET unless it is explicitly requested using
the `fields` query parameter or GET for all advanced properties is
enabled.
```

```
|message
|string
a|Current state of the key manager indicating any additional steps to
perform to finish the setup. This is an advanced property; there is an
added cost to retrieving its value. The property is not populated for
either a collection GET or an instance GET unless it is explicitly
requested using the `fields` query parameter or GET for all advanced
properties is enabled.
```

```
|===
```

```
[#svm]
[.api-collapsible-fifth-title]
svm
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#volume_encryption]
[.api-collapsible-fifth-title]
volume_encryption
```

```
Indicates whether volume encryption is supported in the cluster.
```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|integer
a|Code corresponding to the status message. Returns a 0 if volume
encryption is supported in all nodes of the cluster.

|message
|string
a|Reason for not supporting volume encryption.

|supported
|boolean
a|Set to true when volume encryption support is available on all nodes of
the cluster.

|===

[#security_key_manager]
[.api-collapsible-fifth-title]
security_key_manager

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|external
|link:#external[external]
a|Configures external key management

```

```

|is_default_data_at_rest_encryption_disabled
|boolean
a|Indicates whether default data-at-rest encryption is disabled in the
cluster.

|onboard
|link:#onboard[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
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

|status
|link:#status[status]
a|Optional status information on the current state of the key manager
indicating if it is fully setup or requires more action.

|svm
|link:#svm[svm]
a|

|uuid
|string
a|

|volume_encryption
|link:#volume_encryption[volume_encryption]
a|Indicates whether volume encryption is supported in the cluster.

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===

```

```

|Name
|Type
|Description

|next
|link:#href[href]
a|

|self
|link:#href[href]
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
|string
a|Error code
```

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
====
```

```
[[ID873aadebe59525a5ac0d22dddc23f8a9]]
= Delete key managers
```

```
[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-
block]#`/security/key-managers/{uuid}`#
```

Deletes a key manager.

== Related ONTAP commands

- * `security key-manager external disable`
- * `security key-manager onboard disable`

== Learn more

* xref:{relative_path}security_key-managers_endpoint_overview.html[DOC


```
/security/key-managers]
```

```
== Parameters
```

```
[cols=5*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|In
```

```
|Required
```

```
|Description
```

```
|uuid
```

```
|string
```

```
|path
```

```
|True
```

```
a|
```

```
|===
```

```
== Response
```

Status: 200, Ok

```
== Error
```

Status: Default

ONTAP Error Response Codes

```
|===
```

```
| Error Code | Description
```

```
| 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.
```

```

| 65536239
| Encrypted volumes are found for the SVM.

| 65536242
| One or more Storage Encryption devices are assigned an authentication
key.

| 65536242
| One or more Storage Encryption devices are assigned an authentication
key.

| 65536800
| Failed to lookup onboard keys.

| 65536813
| Encrypted kernel core files found.

| 65536817
| Failed to determine if key manager is safe to disable.

| 65536822
| Multitenant key management is not supported in the current cluster
version.

| 65536827
| Failed to determine if the SVM has any encrypted volumes.

| 65536828
| External key management is not enabled for the SVM.

| 65536867
| Encrypted volumes are found for the SVM.

| 196608301
| Failed to determine the type of encryption.

| 196608305
| NAE aggregates are found in the cluster.
|===

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```
|error
|link:#error[error]
a|
```

```
|===
```

```
.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
```

```
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

```
== Definitions
```

```
[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[ID5930cede682e5091277952b4dc484ce6]]

```

= Retrieve key managers

```
[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-block]#`/security/key-managers/{uuid}`#
```

Retrieves key managers.

== Expensive properties

There is an added cost to retrieving values for these properties. They are not included by default in GET results and must be explicitly requested using the `fields` query parameter. See [xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Requesting_specific_fields\[DOC Requesting specific fields\]](#) to learn more.

- * `connectivity`
- * `status.message`
- * `status.code`

== Related ONTAP commands

- * `security key-manager show-keystore`
- * `security key-manager external show`
- * `security key-manager external show-status`
- * `security key-manager onboard show-backup`

== Learn more

- * [xref:{relative_path}security_key-managers_endpoint_overview.html\[DOC /security/key-managers\]](#)

== Parameters

```
[cols=5*,options=header]  
|===
```

```
|Name  
|Type  
|In  
|Required  
|Description
```

```
|uuid  
|string
```

```
|path
|True
a|Key manager UUID

|fields
|array[string]
|query
|False
a|Specify the fields to return.

|===

== Response
```

Status: 200, Ok

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|external
|link:#external[external]
a|Configures external key management

|is_default_data_at_rest_encryption_disabled
|boolean
a|Indicates whether default data-at-rest encryption is disabled in the
cluster.

|onboard
|link:#onboard[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
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

|status
|link:#status[status]
a|Optional status information on the current state of the key manager
indicating if it is fully setup or requires more action.

|svm
|link:#svm[svm]
a|

|uuid
|string
a|

|volume_encryption
|link:#volume_encryption[volume_encryption]
a|Indicates whether volume encryption is supported in the cluster.

|===

.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_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"
      }
    },
    "connectivity": {
      "records": {
        "node": {
          "_links": {
            "self": {
              "href": "/api/resourcelink"
            }
          },
          "name": "node1",
          "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
        },
        "state": "not_responding"
      }
    },
    "server": "keyserver1.com:5698",
    "timeout": 60,
    "username": "admin"
  }
},
"onboard": {
  "existing_passphrase": "The cluster password of length 32-256 ASCII
characters.",
  "key_backup": "'-----BEGIN
BACKUP-----
TmV0QXBwIEtleSBGbG9iAAEAAAAEAAAAcAEAAAAAAAAAxBFWWAAAAACEAAAAAAAAA
QAAAAAAAAABzDyyVAAAAALI5Jsjvy6gUxnT78KoDKXHYb6sSeraM00quOULY6BeV
n6dMFxuErCD1lbERaOQZSuaYylp8oQHtTEfGMLZM4TYiAAAAAAAAACgAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAA
IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAAACAAAAAAAAJAGr3tJA/LRzU
QRHwv+1aWvAAAAAAAAAACQAAAAAAAAAGAAAAAAAAADV1Vd/AAAAAMFM9Q229Bhp
mDaTSdqku5DCd8wG+fOZSr4bx4JT5WHvV/r5gJnXDQQAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

```



```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBchAgS2V5IEJsb2IA  
AQAAAAMAAAYAQAAAAALgePkcAAAAAIgAAAAAoAAAAAAEOTcr0AAAAA  
AAAAAAAAAACAAAAAJAGr3tJA/LRzUQRHwv+laWvAAAAAAAAACIAAAAAAA  
KAAAAAAAAACIICHZAAAAAAAAAAAAAAAAAgAAAAAQCaFcabsxRXMM7gxhLRzxh  
AAAAAAAAAKAAAAAAIIAAAAAAAAA2JJQBQAAAcT4IqXcNpVggah10axLSn4  
yQjnNVKWY7mANB29042hi7b70DTGCTaVAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAaaaaAwAAAbGBAAAAAA  
7sbaoQAAAAAiAAAAAAACgAAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAAIAAAAAkA  
ave0kd8tHNREfC/7Vpa8AAAAAAAAAIgAAAAAoAAAAAAALOhfWkAAAAA  
AAAAAAAAAACAAAAABAmoI9UxrHOGthQm/CB+EhdAAAAAAAAACQAAAAAA  
gAAAAAAAAACnMmUtAAAAAGVk8AtPzENFgsGdsFvmucmYrlQCsfew0HDSFKazqK6  
W8IEVzbAhPoAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
-----END BACKUP-----'",  
    "passphrase": "The cluster password of length 32-256 ASCII  
characters."  
},  
    "scope": "svm",  
    "status": {  
        "code": 346758,  
        "message": "This cluster is part of a MetroCluster configuration. Use  
the REST API POST method security/key_managers/ with the synchronize  
option and the same passphrase on the partner cluster before proceeding  
with any key manager operations. Failure to do so could lead to  
switchover or switchback failure."  
    },  
    "svm": {  
        "_links": {  
            "self": {  
                "href": "/api/resourcelink"  
            }  
        },  
        "name": "svml",  
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"  
    },  
    "uuid": "string",  
    "volume_encryption": {  
        "code": 346758,  
        "message": "No platform support for volume encryption in following  
nodes - node1, node2."
```

```

    }
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]

```

```

[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#client_certificate]
[.api-collapsible-fifth-title]
client_certificate

Client certificate

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links

```

```

|link:#_links[_links]
a|

|uuid
|string
a|Certificate UUID

|===

[#server_ca_certificates]
[.api-collapsible-fifth-title]
server_ca_certificates

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|uuid
|string
a|Certificate UUID

|===

[#self_link]
[.api-collapsible-fifth-title]
self_link

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

```

```
|===
```

```
[#node]  
[.api-collapsible-fifth-title]  
node
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name  
|Type  
|Description
```

```
|_links  
|link:#_links[_links]  
a|
```

```
|name  
|string  
a|
```

```
|uuid  
|string  
a|
```

```
|===
```

```
[#key_server_state]  
[.api-collapsible-fifth-title]  
key_server_state
```

The state of the key server for a specific node.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name  
|Type  
|Description
```

```
|node  
|link:#node[node]  
a|
```

```
|state  
|string
```

a|Key server connectivity state

|===

[#connectivity]
[.api-collapsible-fifth-title]
connectivity

This property returns the key server connectivity state on all nodes of the cluster. The state is returned for a node only if the connectivity is not in an available state on that node.

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|cluster_availability
|boolean

a|Set to true when key server connectivity state is available on all nodes of the cluster.

|records
|array[link:#key_server_state[key_server_state]]
a|An array of key server connectivity states for each node.

|===

[#key_server_readcreate]
[.api-collapsible-fifth-title]
key_server_readcreate

[cols=3*,options=header]
|===
|Name
|Type

```

|Description

|_links
|link:#self_link[self_link]
a|

|connectivity
|link:#connectivity[connectivity]
a|This property returns the key server connectivity state on all nodes of
the cluster. The state is returned for a node only if the connectivity is
not in an available state on that node.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.

|server
|string
a|External key server for key management. If no port is provided, a
default port of 5696 is used.

|timeout
|integer
a|I/O timeout in seconds for communicating with the key server.

|username
|string
a|Username credentials for connecting with the key server.

|===

[#external]
[.api-collapsible-fifth-title]
external

Configures external key management

[cols=3*,options=header]
|===
|Name
|Type

```

|Description

|client_certificate

|link:#client_certificate[client_certificate]

a|Client certificate

|server_ca_certificates

|array[link:#server_ca_certificates[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[link:#key_server_readcreate[key_server_readcreate]]

a|The set of external key servers.

|===

[#onboard]

[.api-collapsible-fifth-title]

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.

[cols=3*,options=header]

|===

|Name

|Type

|Description

|enabled

|boolean

a|Is the onboard key manager enabled?

|existing_passphrase

|string

a|The cluster-wide passphrase. This is not audited.


```
|key_backup
|string
a|Backup of the onboard key manager's key hierarchy. It is required to
save this backup after configuring the onboard key manager to help in the
recovery of the cluster in case of catastrophic failures.
```

```
|passphrase
|string
a|The cluster-wide passphrase. This is not audited.
```

```
|synchronize
|boolean
a|Synchronizes missing onboard keys on any node in the cluster. If a node
is added to a cluster that has onboard key management configured, the
synchronize operation needs to be performed in a PATCH operation. In a
MetroCluster configuration, if onboard key management is enabled on one
site, then the synchronize operation needs to be run as a POST operation
on the remote site providing the same passphrase.
```

```
|===
```

```
[#status]
[.api-collapsible-fifth-title]
status
```

Optional status information on the current state of the key manager indicating if it is fully setup or requires more action.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|code
```

```
|integer
```

```
a|Code corresponding to the status message. Returns 0 if the setup is
complete. This is an advanced property; there is an added cost to
retrieving its value. The property is not populated for either a
collection GET or an instance GET unless it is explicitly requested using
the `fields` query parameter or GET for all advanced properties is
enabled.
```

```
|message
|string
a|Current state of the key manager indicating any additional steps to
perform to finish the setup. This is an advanced property; there is an
added cost to retrieving its value. The property is not populated for
either a collection GET or an instance GET unless it is explicitly
requested using the `fields` query parameter or GET for all advanced
properties is enabled.
```

```
|===
```

```
[#svm]
[.api-collapsible-fifth-title]
svm
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#volume_encryption]
[.api-collapsible-fifth-title]
volume_encryption
```

```
Indicates whether volume encryption is supported in the cluster.
```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|integer
a|Code corresponding to the status message. Returns a 0 if volume
encryption is supported in all nodes of the cluster.

|message
|string
a|Reason for not supporting volume encryption.

|supported
|boolean
a|Set to true when volume encryption support is available on all nodes of
the cluster.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

```

```

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[ID922daf996f4910464c4adb6e97a2b1a4]]
= Update key managers

[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-
block]#`/security/key-managers/{uuid}`#

```

Updates a key manager.

== Required properties

- * ``onboard.existing_passphrase`` - Cluster-wide passphrase. Required only when synchronizing the passphrase of the Onboard Key Manager.
- * ``synchronize`` - Synchronizes missing Onboard Key Manager keys on any node in the cluster. Required only when synchronizing the Onboard Key Manager keys in a local cluster.

== Related ONTAP commands

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

== Learn more

* `xref:{relative_path}security_key-managers_endpoint_overview.html[DOC /security/key-managers]`

== Parameters

[cols=5*,options=header]

|==

Name
Type
In
Required
Description

uuid
string
path
True
a Key manager UUID

|==

== Request Body

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|external
|link:#external[external]
a|Configures external key management

|is_default_data_at_rest_encryption_disabled
|boolean
a|Indicates whether default data-at-rest encryption is disabled in the
cluster.

|onboard
|link:#onboard[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
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

|status
|link:#status[status]
a|Optional status information on the current state of the key manager
indicating if it is fully setup or requires more action.

|svm
|link:#svm[svm]
a|

|uuid
|string

```

```
a|  
  
|volume_encryption  
|link:#volume_encryption[volume_encryption]  
a|Indicates whether volume encryption is supported in the cluster.
```

```
|===
```

```
.Example request
```

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
```

```
{  
  "_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"  
        }  
      },  
      "connectivity": {  
        "records": {  
          "node": {
```



```

gAAAAAAAAACnMmUtAAAAAGV8AtPzENFgsGdsFvnmucmYrlQCsFew0HDSFKaZqK6
W8IEVzBAhPoAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
-----END BACKUP-----",
  "passphrase": "The cluster password of length 32-256 ASCII
characters."
},
"scope": "svm",
"status": {
  "code": 346758,
  "message": "This cluster is part of a MetroCluster configuration. Use
the REST API POST method security/key_managers/ with the synchronize
option and the same passphrase on the partner cluster before proceeding
with any key manager operations. Failure to do so could lead to
switchover or switchback failure."
},
"svm": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "name": "svm1",
  "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
},
"uuid": "string",
"volume_encryption": {
  "code": 346758,
  "message": "No platform support for volume encryption in following
nodes - node1, node2."
}
}
====

== Response

```

Status: 200, Ok

```
== Error
```

Status: Default

ONTAP Error Response Codes

```
|====
```

Error Code	Description
65536139	The existing passphrase value provided does not match the configured passphrase.
65536150	The new passphrase is same as old passphrase.
65536404	The passphrase does not match the accepted length.
65536406	The change of passphrase failed.
65536407	The passphrase update failed on some nodes.
65536408	The passphrase update failed on some nodes.
65536802	The passphrase does not match the accepted length in common criteria mode.
65536821	The certificate is not installed.
65536822	Multitenant key management is not supported in the current cluster version.
65536828	External key management is not enabled for the SVM.
65536850	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.
65537242	

| The Onboard Key Manager existing_passphrase must be provided when performing a PATCH/synchronize operation.

| 65537243

| The Onboard Key Manager passphrase must not be provided when performing a PATCH/synchronize operation.

| 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.

|===

[cols=3*,options=header]

|===

|Name

|Type

|Description

|error

|link:#error[error]

a|

|===

.Example error

[%collapsible%closed]

====

[source,json,subs=+macros]

{

 "error": {

 "arguments": {

 "code": "string",

```

        "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
}
}
====

```

== Definitions

```

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====

```

```

[#href]
[.api-collapsible-fifth-title]
href

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|href
|string
a|

```

```

|===

```

```

[#_links]
[.api-collapsible-fifth-title]
_links

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|self
|link:#href[href]
a|

```

```

|===

[#client_certificate]
[.api-collapsible-fifth-title]
client_certificate

Client certificate


[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|uuid
|string
a|Certificate UUID


|===


[#server_ca_certificates]
[.api-collapsible-fifth-title]
server_ca_certificates


[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|uuid
|string
a|Certificate UUID

```

```

|===

[#self_link]
[.api-collapsible-fifth-title]
self_link

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#node]
[.api-collapsible-fifth-title]
node

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|

|uuid
|string
a|

|===

[#key_server_state]
[.api-collapsible-fifth-title]

```

key_server_state

The state of the key server for a specific node.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|node
|link:#node[node]
a|

|state
|string
a|Key server connectivity state

|===

[#connectivity]
[.api-collapsible-fifth-title]
connectivity
```

This property returns the key server connectivity state on all nodes of the cluster. The state is returned for a node only if the connectivity is not in an available state on that node.

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|cluster_availability
|boolean
a|Set to true when key server connectivity state is available on all nodes
of the cluster.
```

```

|records
|array[link:#key_server_state[key_server_state]]
a|An array of key server connectivity states for each node.

|===

[#key_server_readcreate]
[.api-collapsible-fifth-title]
key_server_readcreate

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#self_link[self_link]
a|

|connectivity
|link:#connectivity[connectivity]
a|This property returns the key server connectivity state on all nodes of
the cluster. The state is returned for a node only if the connectivity is
not in an available state on that node.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.

|server
|string
a|External key server for key management. If no port is provided, a
default port of 5696 is used.

|timeout
|integer
a|I/O timeout in seconds for communicating with the key server.

|username
|string

```


a|Username credentials for connecting with the key server.

|===

[#external]

[.api-collapsible-fifth-title]

external

Configures external key management

[cols=3*,options=header]

|===

|Name

|Type

|Description

|client_certificate

|link:#client_certificate[client_certificate]

a|Client certificate

|server_ca_certificates

|array[link:#server_ca_certificates[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 keyservers per SVM.

|servers

|array[link:#key_server_readcreate[key_server_readcreate]]

a|The set of external key servers.

|===

[#onboard]

[.api-collapsible-fifth-title]

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.

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|enabled
|boolean
a|Is the onboard key manager enabled?

|existing_passphrase
|string
a|The cluster-wide passphrase. This is not audited.

|key_backup
|string
a|Backup of the onboard key manager's key hierarchy. It is required to
save this backup after configuring the onboard key manager to help in the
recovery of the cluster in case of catastrophic failures.

|passphrase
|string
a|The cluster-wide passphrase. This is not audited.

|synchronize
|boolean
a|Synchronizes missing onboard keys on any node in the cluster. If a node
is added to a cluster that has onboard key management configured, the
synchronize operation needs to be performed in a PATCH operation. In a
MetroCluster configuration, if onboard key management is enabled on one
site, then the synchronize operation needs to be run as a POST operation
on the remote site providing the same passphrase.

|===

[#status]
[.api-collapsible-fifth-title]
status

Optional status information on the current state of the key manager

```

indicating if it is fully setup or requires more action.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|code
```

```
|integer
```

a|Code corresponding to the status message. Returns 0 if the setup is complete. This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```
|message
```

```
|string
```

a|Current state of the key manager indicating any additional steps to perform to finish the setup. This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```
|===
```

```
[#svm]
```

```
[.api-collapsible-fifth-title]
```

svm

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

a|

```
|name
```

```

|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

|===

[#volume_encryption]
[.api-collapsible-fifth-title]
volume_encryption

Indicates whether volume encryption is supported in the cluster.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|integer
a|Code corresponding to the status message. Returns a 0 if volume
encryption is supported in all nodes of the cluster.

|message
|string
a|Reason for not supporting volume encryption.

|supported
|boolean
a|Set to true when volume encryption support is available on all nodes of
the cluster.

|===

[#security_key_manager]
[.api-collapsible-fifth-title]

```

```

security_key_manager

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|external
|link:#external[external]
a|Configures external key management

|is_default_data_at_rest_encryption_disabled
|boolean
a|Indicates whether default data-at-rest encryption is disabled in the
cluster.

|onboard
|link:#onboard[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
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

|status
|link:#status[status]
a|Optional status information on the current state of the key manager
indicating if it is fully setup or requires more action.

|svm
|link:#svm[svm]
a|

|uuid

```

```

|string
a|

|volume_encryption
|link:#volume_encryption[volume_encryption]
a|Indicates whether volume encryption is supported in the cluster.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

```

```

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

:leveloffset: -1

[[IDf273e78aa3bac297100aa8c97a30ea8c]]
= Migrate SVM keys between security key managers

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/key-managers/{source.uuid}/migrate`#

Migrates the keys belonging to an SVM between the cluster's key manager
and the SVM's key manager. This operation can run for several minutes.

== Required properties

* `source.uuid` - UUID of the source key manager.
* `uuid` - UUID of the destination key manager.

== Related ONTAP commands

* `security key-manager migrate`

```

== Parameters

```
[cols=5*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|In
```

```
|Required
```

```
|Description
```

```
|return_timeout
```

```
|integer
```

```
|query
```

```
|False
```

a|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.

```
|return_records
```

```
|boolean
```

```
|query
```

```
|False
```

a|The default is false. If set to true, the records are returned.

```
|source.uuid
```

```
|string
```

```
|path
```

```
|True
```

a|Migration source key manager UUID

```
|===
```

== Request Body

```
[cols=3*,options=header]
```

```
|===
```



```
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|
```

```
|uuid
|string
a|Key manager UUID
```

```
|===
```

.Example request

[%collapsible%closed]

====

[source,json,subs=+macros]

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563434"
}
```

====

== Response

Status: 202, Accepted

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|job
|link:#job_link[job_link]
a|

|===

.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "string"
  }
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

```

```

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#info]
[.api-collapsible-fifth-title]
info

Migration destination key manager UUID


[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|uuid
|string
a|Key manager UUID

|===

[#job_link]
[.api-collapsible-fifth-title]
job_link

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```
|_links
|link:#_links[_links]
a|
```

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

```
|===
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
|string
a|Error code
```

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
====
```

```
[[ID95e96b809cd924b7ea43473ba6c70504]]
= List key servers configured in an external key manager
```

```
[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/key-managers/{uuid}/key-servers`#
```

Retrieves the list of key servers configured in an external key manager.

== Parameters

```
[cols=5*,options=header]
|===
```

```
|Name
|Type
|In
```

```

|Required
|Description

|uuid
|string
|path
|True
a|External key manager UUID


|server
|string
|query
|False
a|Filter by server


|connectivity.cluster_availability
|boolean
|query
|False
a|Filter by connectivity.cluster_availability


|connectivity.records.state
|string
|query
|False
a|Filter by connectivity.records.state


|connectivity.records.node.uuid
|string
|query
|False
a|Filter by connectivity.records.node.uuid


|connectivity.records.node.name
|string
|query
|False
a|Filter by connectivity.records.node.name


|username
|string

```

```
|query
|False
a|Filter by username
```

```
|timeout
|integer
|query
|False
a|Filter by timeout
```

```
|fields
|array[string]
|query
|False
a|Specify the fields to return.
```

```
|max_records
|integer
|query
|False
a|Limit the number of records returned.
```

```
|return_timeout
|integer
|query
|False
a|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
a|The default is true for GET calls.  When set to false, only the number
of records is returned.
```

```
|order_by
|array[string]
|query
```



```
|False
a|Order results by specified fields and optional [asc|desc] direction.
Default direction is 'asc' for ascending.

|===

== Response
```

Status: 200, Ok

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records

|records
|array[link:#key_server[key_server]]
a|

|===

.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
```

```

    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "connectivity": {
      "records": {
        "node": {
          "_links": {
            "self": {
              "href": "/api/resourcelink"
            }
          },
          "name": "node1",
          "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
        },
        "state": "not_responding"
      }
    },
    "password": "password",
    "records": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "connectivity": {
        "records": {
          "node": {
            "_links": {
              "self": {
                "href": "/api/resourcelink"
              }
            },
            "name": "node1",
            "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
          },
          "state": "not_responding"
        }
      },
      "password": "password",
      "server": "keyserver1.com:5698",
      "timeout": 60,
      "username": "username"
    },
    "server": "keyserver1.com:5698",

```

```

    "timeout": 60,
    "username": "username"
  }
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block

```

```

====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|next
|link:href[href]
a|

|self
|link:href[href]
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type

```

|Description

|self

|link:#href[href]

a|

|===

[#node]

[.api-collapsible-fifth-title]

node

[cols=3*,options=header]

|===

|Name

|Type

|Description

|_links

|link:#_links[_links]

a|

|name

|string

a|

|uuid

|string

a|

|===

[#key_server_state]

[.api-collapsible-fifth-title]

key_server_state

The state of the key server for a specific node.

[cols=3*,options=header]

|===

|Name

|Type

|Description

```
|node
|link:#node[node]
a|

|state
|string
a|Key server connectivity state
```

```
|===
```

```
[#connectivity]
[.api-collapsible-fifth-title]
connectivity
```

This property returns the key server connectivity state on all nodes of the cluster. The state is returned for a node only if the connectivity is not in an available state on that node.

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|cluster_availability
|boolean
```

```
a|Set to true when key server connectivity state is available on all nodes
of the cluster.
```

```
|records
|array[link:#key_server_state[key_server_state]]
a|An array of key server connectivity states for each node.
```

```
|===
```

```
[#records]
[.api-collapsible-fifth-title]
```

```

records

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|connectivity
|link:#connectivity[connectivity]
a|This property returns the key server connectivity state on all nodes of
the cluster. The state is returned for a node only if the connectivity is
not in an available state on that node.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.

|password
|string
a|Password credentials for connecting with the key server. This is not
audited.

|server
|string
a|External key server for key management. If no port is provided, a
default port of 5696 is used. Not valid in POST if `records` is provided.

|timeout
|integer
a|I/O timeout in seconds for communicating with the key server.

|username
|string
a|KMIP username credentials for connecting with the key server.

|===

```

```
[#key_server]
[.api-collapsible-fifth-title]
key_server

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|connectivity
|link:#connectivity[connectivity]
a|This property returns the key server connectivity state on all nodes of
the cluster. The state is returned for a node only if the connectivity is
not in an available state on that node.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.

|password
|string
a|Password credentials for connecting with the key server. This is not
audited.

|records
|array[link:#records[records]]
a|An array of key servers specified to add multiple key servers to a key
manager in a single API call. Valid in POST only and not valid if `server`
is provided.

|server
|string
a|External key server for key management. If no port is provided, a
default port of 5696 is used. Not valid in POST if `records` is provided.

|timeout
|integer
```


a|I/O timeout in seconds for communicating with the key server.

|username

|string

a|KMIP username credentials for connecting with the key server.

|===

[#error_arguments]

[.api-collapsible-fifth-title]

error_arguments

[cols=3*,options=header]

|===

|Name

|Type

|Description

|code

|string

a|Argument code

|message

|string

a|Message argument

|===

[#error]

[.api-collapsible-fifth-title]

error

[cols=3*,options=header]

|===

|Name

|Type

|Description

|arguments

|array[link:#error_arguments[error_arguments]]

a|Message arguments

```
|code
|string
a|Error code
```

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
=====
```

```
[[ID489f13338615726541104669f4c956e4]]
= Add primary key servers to an external key manager
```

```
[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/key-managers/{uuid}/key-servers`#
```

Adds key servers to a configured external key manager.

== Required properties

- * `uuid` - UUID of the external key manager.
- * `server` - Key server name.

== Related ONTAP commands

- * `security key-manager external add-servers`

== Parameters

```
[cols=5*,options=header]
|===

|Name
|Type
|In
|Required
|Description

|return_records
|boolean
|query
|False
a|The default is false. If set to true, the records are returned.
```

```
|uuid
|string
|path
|True
a|External key manager UUID
```

```
|===
```

```
== Request Body
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|connectivity
|link:#connectivity[connectivity]
a|This property returns the key server connectivity state on all nodes of
the cluster. The state is returned for a node only if the connectivity is
not in an available state on that node.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.
```

```

|password
|string
a|Password credentials for connecting with the key server. This is not
audited.

|records
|array[link:#records[records]]
a|An array of key servers specified to add multiple key servers to a key
manager in a single API call. Valid in POST only and not valid if `server`
is provided.

|server
|string
a|External key server for key management. If no port is provided, a
default port of 5696 is used. Not valid in POST if `records` is provided.

|timeout
|integer
a|I/O timeout in seconds for communicating with the key server.

|username
|string
a|KMIP username credentials for connecting with the key server.

|===

```

```

.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "connectivity": {
    "records": {
      "node": {

```

```

    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "node1",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "state": "not_responding"
}
},
"password": "password",
"records": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "connectivity": {
    "records": {
      "node": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "node1",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      },
      "state": "not_responding"
    }
  },
  "password": "password",
  "server": "keyserver1.com:5698",
  "timeout": 60,
  "username": "username"
},
"server": "keyserver1.com:5698",
"timeout": 60,
"username": "username"
}
====

== Response

```

Status: 201, Created

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records

|records
|array[link:#key_server[key_server]]
a|

|===

```

```

.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "connectivity": {
      "records": {
        "node": {
          "_links": {
            "self": {

```

```

        "href": "/api/resourcelink"
      },
      {
        "name": "node1",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      },
      "state": "not_responding"
    }
  },
  "password": "password",
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "connectivity": {
      "records": {
        "node": {
          "_links": {
            "self": {
              "href": "/api/resourcelink"
            }
          },
          {
            "name": "node1",
            "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
          },
          "state": "not_responding"
        }
      },
      "password": "password",
      "server": "keyserver1.com:5698",
      "timeout": 60,
      "username": "username"
    },
    "server": "keyserver1.com:5698",
    "timeout": 60,
    "username": "username"
  }
}
====

== Error

```

Status: Default

ONTAP Error Response Codes

|===

| Error Code | Description

| 65536038

| A maximum of 4 active key servers are allowed.

| 65536821

| The certificate is not installed.

| 65536822

| Multitenant key management is not supported in the current cluster version.

| 65536824

| Multitenant key management is not supported in MetroCluster configurations.

| 65536828

| External key management is not enabled for the SVM.

| 65536834

| Failed to get existing key-server details for the SVM.

| 65536852

| Failed to query supported KMIP protocol versions.

| 65536870

| Key management servers are already configured.

| 65536871

| Duplicate key management servers exist.

| 65536921

| The following issues were found. Unable to execute command on KMIP server.

| 66060338

| Unable to establish secure connection to KMIP server due to incorrect server_ca certificates.

| 66060339

| Unable to establish secure connection to KMIP server due to incorrect client certificates.

| 66060340


```
| Unable to establish secure connection to KMIP server due to Cryptsoft  
error.
```

```
| 66060341
```

```
| Unable to establish secure connection to KMIP server due to network  
configuration issues.
```

```
|===
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
====
```

```
[source,json,subs=+macros]
```

```
{  
  "error": {  
    "arguments": {  
      "code": "string",  
      "message": "string"  
    },  
    "code": "4",  
    "message": "entry doesn't exist",  
    "target": "uuid"  
  }  
}
```

```
====
```

```
== Definitions
```

```
[.api-def-first-level]
```

```
.See Definitions
```

```
[%collapsible%closed]
```

```
//Start collapsible Definitions block
```

```
====
```

```

[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#node]
[.api-collapsible-fifth-title]
node

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

```

```
|name
|string
a|
```

```
|uuid
|string
a|
```

```
|===
```

```
[#key_server_state]
[.api-collapsible-fifth-title]
key_server_state
```

The state of the key server for a specific node.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|node
|link:#node[node]
a|
```

```
|state
|string
a|Key server connectivity state
```

```
|===
```

```
[#connectivity]
[.api-collapsible-fifth-title]
connectivity
```

This property returns the key server connectivity state on all nodes of the cluster. The state is returned for a node only if the connectivity is not in an available state on that node.

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query

parameter or GET for all advanced properties is enabled.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|cluster_availability
```

```
|boolean
```

a|Set to true when key server connectivity state is available on all nodes of the cluster.

```
|records
```

```
|array[link:#key_server_state[key_server_state]]
```

a|An array of key server connectivity states for each node.

```
|===
```

```
[#records]
```

```
[.api-collapsible-fifth-title]
```

records

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

a|

```
|connectivity
```

```
|link:#connectivity[connectivity]
```

a|This property returns the key server connectivity state on all nodes of the cluster. The state is returned for a node only if the connectivity is not in an available state on that node.

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```

|password
|string
a|Password credentials for connecting with the key server. This is not
audited.

|server
|string
a|External key server for key management. If no port is provided, a
default port of 5696 is used. Not valid in POST if `records` is provided.

|timeout
|integer
a|I/O timeout in seconds for communicating with the key server.

|username
|string
a|KMIP username credentials for connecting with the key server.

|===

[#key_server]
[.api-collapsible-fifth-title]
key_server

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|connectivity
|link:#connectivity[connectivity]
a|This property returns the key server connectivity state on all nodes of
the cluster. The state is returned for a node only if the connectivity is
not in an available state on that node.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an

```

instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

|password

|string

a|Password credentials for connecting with the key server. This is not audited.

|records

|array[link:#records[records]]

a|An array of key servers specified to add multiple key servers to a key manager in a single API call. Valid in POST only and not valid if `server` is provided.

|server

|string

a|External key server for key management. If no port is provided, a default port of 5696 is used. Not valid in POST if `records` is provided.

|timeout

|integer

a|I/O timeout in seconds for communicating with the key server.

|username

|string

a|KMIP username credentials for connecting with the key server.

|===

[#_links]

[.api-collapsible-fifth-title]

_links

[cols=3*,options=header]

|===

|Name

|Type

|Description

|next

```

|link:#href[href]
a|

|self
|link:#href[href]
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

```

```
|code
|string
a|Error code
```

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
====
```

```
[[ID12345cfca4c60c4d7330ed8a3e8bb7ab]]
= Delete a primary key server
```

```
[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-
block]#`/security/key-managers/{uuid}/key-servers/{server}`#
```

Deletes a key server.

== Related ONTAP commands

* `security key-manager external remove-servers`

== Parameters

```
[cols=5*,options=header]
|===
```

```
|Name
|Type
|In
```



```
|Required
|Description

|uuid
|string
|path
|True
a|

|server
|string
|path
|True
a|
|===

== Response
```

Status: 200, Ok

```
== Error
```

Status: Default

ONTAP Error Response Codes

```
|===
| Error Code | Description

| 65536700
| The key server contains keys that are currently in use and not available
| from any other configured key server in the SVM.

| 65536822
| Multitenant key management is not supported in the current cluster
| version.

| 65536824
| Multitenant key management is not supported in MetroCluster
| configurations.

| 65536828
| External key management is not enabled for the SVM.

| 65536843
```

```
| The key management server is not configured for the SVM.
```

```
|===
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
```

```
{
```

```
  "error": {
```

```
    "arguments": {
```

```
      "code": "string",
```

```
      "message": "string"
```

```
    },
```

```
    "code": "4",
```

```
    "message": "entry doesn't exist",
```

```
    "target": "uuid"
```

```
  }
```

```
}
```

```
=====
```

```
== Definitions
```

```
[.api-def-first-level]
```

```
.See Definitions
```

```
[%collapsible%closed]
```

```
//Start collapsible Definitions block
```

```
=====
```

```
[#error_arguments]
```

```
[.api-collapsible-fifth-title]
```

```
error_arguments
```

```
[cols=3*,options=header]
```

```

|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

```

```
|===
```

```
//end collapsible .Definitions block
```

```
====
```

```
[[ID695773c7065e28a36d121cdfb198ae67]]
```

```
= Retrieve key servers configured in an external key manager
```

```
[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-  
block]#`/security/key-managers/{uuid}/key-servers/{server}`#
```

Retrieves key servers configured in an external key manager.

== Expensive properties

There is an added cost to retrieving values for these properties. They are not included by default in GET results and must be explicitly requested using the `fields` query parameter. See [xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Requesting_specific_fields](#)[DOC Requesting specific fields] to learn more.

* `connectivity`

== Related ONTAP commands

* `security key-manager external show`

* `security key-manager external show-status`

== Parameters

```
[cols=5*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|In
```

```
|Required
```

```
|Description
```

```
|uuid
```

```

|string
|path
|True
a|External key manager UUID

|server
|string
|path
|True
a|Key server configured in the key manager.

|fields
|array[string]
|query
|False
a|Specify the fields to return.

|===

== Response

```

Status: 200, Ok

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|connectivity
|link:#connectivity[connectivity]
a|This property returns the key server connectivity state on all nodes of
the cluster. The state is returned for a node only if the connectivity is
not in an available state on that node.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.

```

```

|password
|string
a|Password credentials for connecting with the key server. This is not
audited.

|records
|array[link:#records[records]]
a|An array of key servers specified to add multiple key servers to a key
manager in a single API call. Valid in POST only and not valid if `server`
is provided.

|server
|string
a|External key server for key management. If no port is provided, a
default port of 5696 is used. Not valid in POST if `records` is provided.

|timeout
|integer
a|I/O timeout in seconds for communicating with the key server.

|username
|string
a|KMIP username credentials for connecting with the key server.

```

```

|===

```

```

.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "connectivity": {
    "records": {
      "node": {
        "_links": {
          "self": {

```

```

        "href": "/api/resourcelink"
    },
    },
    "name": "node1",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
},
"state": "not_responding"
}
},
"password": "password",
"records": {
    "_links": {
        "self": {
            "href": "/api/resourcelink"
        }
    },
    "connectivity": {
        "records": {
            "node": {
                "_links": {
                    "self": {
                        "href": "/api/resourcelink"
                    }
                },
                },
            "name": "node1",
            "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
        },
        "state": "not_responding"
    }
},
"password": "password",
"server": "keyserver1.com:5698",
"timeout": 60,
"username": "username"
},
"server": "keyserver1.com:5698",
"timeout": 60,
"username": "username"
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

```



```

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#node]
[.api-collapsible-fifth-title]
node

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|

|uuid
|string
a|

|===

```

```
[#key_server_state]
[.api-collapsible-fifth-title]
key_server_state
```

The state of the key server for a specific node.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|node
|link:#node[node]
a|

|state
|string
a|Key server connectivity state

|===
```

```
[#connectivity]
[.api-collapsible-fifth-title]
connectivity
```

This property returns the key server connectivity state on all nodes of the cluster. The state is returned for a node only if the connectivity is not in an available state on that node.

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|cluster_availability
```

```

|boolean
a|Set to true when key server connectivity state is available on all nodes
of the cluster.

|records
|array[link:#key_server_state[key_server_state]]
a|An array of key server connectivity states for each node.

|===

[#records]
[.api-collapsible-fifth-title]
records

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|connectivity
|link:#connectivity[connectivity]
a|This property returns the key server connectivity state on all nodes of
the cluster. The state is returned for a node only if the connectivity is
not in an available state on that node.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.

|password
|string
a|Password credentials for connecting with the key server. This is not
audited.

|server
|string
a|External key server for key management. If no port is provided, a

```

default port of 5696 is used. Not valid in POST if `records` is provided.

|timeout
|integer
a|I/O timeout in seconds for communicating with the key server.

|username
|string
a|KMIP username credentials for connecting with the key server.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type

```

|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments


|code
|string
a|Error code


|message
|string
a|Error message


|target
|string
a|The target parameter that caused the error.


|===

//end collapsible .Definitions block
====

[[IDcb643ce725e2f489262bc59b3638a605]]
= Update a primary key server

[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-
block]#`/security/key-managers/{uuid}/key-servers/{server}`#


Updates a key server.

== Related ONTAP commands

* `security key-manager external modify-server`

== Parameters

```

```
[cols=5*,options=header]
|===

|Name
|Type
|In
|Required
|Description

|uuid
|string
|path
|True
a|External key manager UUID

|server
|string
|path
|True
a|Key server configured in the external key manager.

|===
```

== Request Body

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|connectivity
|link:#connectivity[connectivity]
a|This property returns the key server connectivity state on all nodes of
the cluster. The state is returned for a node only if the connectivity is
not in an available state on that node.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.
```

```

|password
|string
a|Password credentials for connecting with the key server. This is not
audited.

|records
|array[link:#records[records]]
a|An array of key servers specified to add multiple key servers to a key
manager in a single API call. Valid in POST only and not valid if `server`
is provided.

|server
|string
a|External key server for key management. If no port is provided, a
default port of 5696 is used. Not valid in POST if `records` is provided.

|timeout
|integer
a|I/O timeout in seconds for communicating with the key server.

|username
|string
a|KMIP username credentials for connecting with the key server.

|===

```

```

.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "connectivity": {
    "records": {
      "node": {

```

```

    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "node1",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "state": "not_responding"
}
},
"password": "password",
"records": {
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "connectivity": {
    "records": {
      "node": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "node1",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      },
      "state": "not_responding"
    }
  },
  "password": "password",
  "server": "keyserver1.com:5698",
  "timeout": 60,
  "username": "username"
},
"server": "keyserver1.com:5698",
"timeout": 60,
"username": "username"
}
====

== 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.
```

```
| 65536824
```

```
| Multitenant key management is not supported in MetroCluster  
configurations.
```

```
| 65536828
```

```
| External key management is not enabled for the SVM.
```

```
| 65536843
```

```
| The key management server is not configured for the SVM.
```

```
| 65536845
```

```
| Missing username.
```

```
| 65536846
```

```
| Missing password.
```

```
|===
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]

```

```

|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#node]
[.api-collapsible-fifth-title]
node

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|

|uuid
|string
a|

|===

[#key_server_state]
[.api-collapsible-fifth-title]
key_server_state

The state of the key server for a specific node.

[cols=3*,options=header]
|===
|Name

```

```
|Type
|Description

|node
|link:#node[node]
a|

|state
|string
a|Key server connectivity state
```

```
|===
```

```
[#connectivity]
[.api-collapsible-fifth-title]
connectivity
```

This property returns the key server connectivity state on all nodes of the cluster. The state is returned for a node only if the connectivity is not in an available state on that node.

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|cluster_availability
|boolean
```

```
a|Set to true when key server connectivity state is available on all nodes
of the cluster.
```

```
|records
|array[link:#key_server_state[key_server_state]]
a|An array of key server connectivity states for each node.
```

```
|===
```

```
[#records]
[.api-collapsible-fifth-title]
records

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|connectivity
|link:#connectivity[connectivity]
a|This property returns the key server connectivity state on all nodes of
the cluster. The state is returned for a node only if the connectivity is
not in an available state on that node.
This is an advanced property; there is an added cost to retrieving its
value. The property is not populated for either a collection GET or an
instance GET unless it is explicitly requested using the `fields` query
parameter or GET for all advanced properties is enabled.

|password
|string
a|Password credentials for connecting with the key server. This is not
audited.

|server
|string
a|External key server for key management. If no port is provided, a
default port of 5696 is used. Not valid in POST if `records` is provided.

|timeout
|integer
a|I/O timeout in seconds for communicating with the key server.

|username
|string
a|KMIP username credentials for connecting with the key server.
```

|===

[#key_server]
[.api-collapsible-fifth-title]
key_server

[cols=3*,options=header]

|===

|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|connectivity
|link:#connectivity[connectivity]

a|This property returns the key server connectivity state on all nodes of the cluster. The state is returned for a node only if the connectivity is not in an available state on that node.

This is an advanced property; there is an added cost to retrieving its value. The property is not populated for either a collection GET or an instance GET unless it is explicitly requested using the `fields` query parameter or GET for all advanced properties is enabled.

|password

|string

a|Password credentials for connecting with the key server. This is not audited.

|records

|array[link:#records[records]]

a|An array of key servers specified to add multiple key servers to a key manager in a single API call. Valid in POST only and not valid if `server` is provided.

|server

|string

a|External key server for key management. If no port is provided, a default port of 5696 is used. Not valid in POST if `records` is provided.

```
|timeout
|integer
a|I/O timeout in seconds for communicating with the key server.
```

```
|username
|string
a|KMIP username credentials for connecting with the key server.
```

```
|===
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
|string
a|Error code
```

```
|message
|string
a|Error message
```

```
|target
|string
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
====
```

= View and update login message configuration

:leveloffset: +1

```
[[IDba221a18c56c8c8db67b4de4b51cc806]]
= Security login messages endpoint overview
```

== Overview

You can use this API to display and manage the login messages configuration. The GET request retrieves all of the login messages in the cluster. GET operations on /security/login/messages/{uuid} retrieve the login messages configuration by UUID. PATCH operations on /security/login/messages/{uuid} update the login messages configuration by UUID.

+


```
'''

== Examples

=== Retrieving all of the login messages in the cluster

'''

----

# The API:
/api/security/login/messages

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

# The response:
{
"records": [
  {
    "uuid": "2581e5aa-9fe3-11e8-b309-005056bbef18",
    "scope": "cluster",
    "banner": "*** WARNING: DO NOT PROCEED IF YOU ARE NOT AUTHORIZED!
****\n",
    "message": "#### Welcome to Cluster X ####\n",
    "show_cluster_message": true,
    "_links": {
      "self": {
        "href": "/api/security/login/messages/2581e5aa-9fe3-11e8-b309-
005056bbef18"
      }
    }
  },
  {
    "uuid": "7b1b3715-9ffa-11e8-a5dd-005056bbef18",
    "scope": "svm",
    "svm": {
      "uuid": "7b1b3715-9ffa-11e8-a5dd-005056bbef18",
      "name": "svm1"
    },
    "message": "#### Welcome to SVM1 ####\n",
    "show_cluster_message": true,
    "_links": {
      "self": {
```

```

        "href": "/api/security/login/messages/7b1b3715-9ffa-11e8-a5dd-005056bbef18"
    }
}
},
{
    "uuid": "8dde11e-a58c-11e8-85e0-005056bbef18",
    "scope": "svm",
    "svm": {
        "uuid": "8dde11e-a58c-11e8-85e0-005056bbef18",
        "name": "svm3"
    },
    "banner": "*** WARNING: This system is for the use of authorized users only. ****\n",
    "_links": {
        "self": {
            "href": "/api/security/login/messages/8dde11e-a58c-11e8-85e0-005056bbef18"
        }
    }
},
{
    "uuid": "f7e41c99-9ffa-11e8-a5dd-005056bbef18",
    "scope": "svm",
    "svm": {
        "uuid": "f7e41c99-9ffa-11e8-a5dd-005056bbef18",
        "name": "svm2"
    },
    "_links": {
        "self": {
            "href": "/api/security/login/messages/f7e41c99-9ffa-11e8-a5dd-005056bbef18"
        }
    }
}
],
"num_records": 4,
"_links": {
    "self": {
        "href": "/api/security/login/messages?fields="
    }
}
}
}
----

'''

```

```

=== Retrieving the login messages configuration at the cluster scope

'''

----

# The API:
/api/security/login/messages

# The call:
curl -X GET "https://<mgmt-
ip>/api/security/login/messages?scope=cluster&fields=*" -H "accept:
application/hal+json"

# The response:
{
  "records": [
    {
      "uuid": "2581e5aa-9fe3-11e8-b309-005056bbef18",
      "scope": "cluster",
      "banner": "*** WARNING: DO NOT PROCEED IF YOU ARE NOT AUTHORIZED!
****\n",
      "message": "#### Welcome to Cluster X ####\n",
      "show_cluster_message": true,
      "_links": {
        "self": {
          "href": "/api/security/login/messages/2581e5aa-9fe3-11e8-b309-
005056bbef18"
        }
      }
    },
  ],
  "num_records": 1,
  "_links": {
    "self": {
      "href": "/api/security/login/messages?scope=cluster&fields=*"
    }
  }
}

----

'''

=== Retrieving the login banner configured at the cluster scope

'''

```

```

-----

# The API:
/api/security/login/messages

# The call:
curl -X GET "https://<mgmt-
ip>/api/security/login/messages?scope=cluster&fields=banner" -H "accept:
application/hal+json"

# The response:
{
  "records": [
    {
      "uuid": "2581e5aa-9fe3-11e8-b309-005056bbef18",
      "scope": "cluster",
      "banner": "*** WARNING: DO NOT PROCEED IF YOU ARE NOT AUTHORIZED!
***\n",
      "_links": {
        "self": {
          "href": "/api/security/login/messages/2581e5aa-9fe3-11e8-b309-
005056bbef18"
        }
      }
    }
  ],
  "num_records": 1,
  "_links": {
    "self": {
      "href": "/api/security/login/messages?scope=cluster&fields=banner"
    }
  }
}
-----

'''

=== Retrieving the login messages configuration of a specific SVM

'''

-----

# The API:
/api/security/login/messages

```

```

# The call:
curl -X GET "https://<mgmt-
ip>/api/security/login/messages?svm.name=svm1&fields=*" -H "accept:
application/hal+json"

# The response:
{
  "records": [
    {
      "uuid": "7b1b3715-9ffa-11e8-a5dd-005056bbef18",
      "scope": "svm",
      "svm": {
        "uuid": "7b1b3715-9ffa-11e8-a5dd-005056bbef18",
        "name": "svm1"
      },
      "message": "#### Welcome to SVM1 ####\n",
      "show_cluster_message": true,
      "_links": {
        "self": {
          "href": "/api/security/login/messages/7b1b3715-9ffa-11e8-a5dd-
005056bbef18"
        }
      }
    },
    ],
    "num_records": 1,
    "_links": {
      "self": {
        "href": "/api/security/login/messages?svm.name=svm1&fields=*"
      }
    }
  }
}
----

'''

=== Retrieving the login messages configuration by UUID, including all
fields

'''

----

# The API:
/api/security/login/messages/{uuid}

```

```

# The call:
curl -X GET "https://<mgmt-ip>/api/security/login/messages/7b1b3715-9ffa-11e8-a5dd-005056bbef18?fields=*" -H "accept: application/hal+json"

# The response:
{
  "uuid": "7b1b3715-9ffa-11e8-a5dd-005056bbef18",
  "scope": "svm",
  "svm": {
    "uuid": "7b1b3715-9ffa-11e8-a5dd-005056bbef18",
    "name": "svm1"
  },
  "message": "#### Welcome to SVM1 ####\n",
  "show_cluster_message": true,
  "_links": {
    "self": {
      "href": "/api/security/login/messages/7b1b3715-9ffa-11e8-a5dd-005056bbef18"
    }
  }
}
----

'''

=== Configuring the login banner in a cluster

'''

----

# The API:
/api/security/login/messages

# The call:
curl -X PATCH "https://<mgmt-ip>/api/security/login/messages?scope=cluster" -H "accept: application/hal+json" -H "Content-Type: application/json" -d '{"banner": "You are entering secure area.\" }'

# The response:
{
  "num_records": 1,
  "_links": {
    "self": {
      "href": "/api/security/login/messages?scope=cluster"
    }
  }
}

```

```

}
----

'''

=== Configuring the message of the day (MOTD) in a cluster

'''

----

# The API:
/api/security/login/messages

# The call:
curl -X PATCH "https://<mgmt-
ip>/api/security/login/messages?scope=cluster" -H "accept:
application/hal+json" -H "Content-Type: appplication/json" -d "{
\"message\": \"Welcome to Cluster X\", \"show_cluster_message\": true }"

# The response:
{
  "num_records": 1,
  "_links": {
    "self": {
      "href": "/api/security/login/messages?scope=cluster"
    }
  }
}
----

'''

=== Clearing the login banner and message of the day (MOTD) in a cluster

'''

----

# The API:
/api/security/login/messages

# The call:
curl -X PATCH "https://<mgmt-
ip>/api/security/login/messages?scope=cluster" -H "accept:
application/hal+json" -H "Content-Type: appplication/json" -d "{
\"banner\": \"\", \"message\": \"\" }"

```

```

# The response:
{
  "num_records": 1,
  "_links": {
    "self": {
      "href": "/api/security/login/messages?scope=cluster"
    }
  }
}
----

'''

=== Configuring the login messages for a specific SVM

'''

----

# The API:
/api/security/login/messages

# The call:
curl -X PATCH "https://<mgmt-
ip>/api/security/login/messages?svm.name=svm1" -H "accept:
application/hal+json" -H "Content-Type: application/json" -d "{
  \"banner\" : \"AUTHORIZED ACCESS ONLY\" }, \"message\": \"WELCOME!\" }"

# The response:
{
  "num_records": 1,
  "_links": {
    "self": {
      "href": "/api/security/login/messages?svm.name=svm1"
    }
  }
}
----

'''

=== Configuring the login messages by UUID

'''

----

# The API:

```



```
/api/security/login/messages/{uuid}
```

```
# The call:
```

```
curl -X PATCH "https://<mgmt-ip>/api/security/login/messages/7b1b3715-9ffa-11e8-a5dd-005056bbef18" -H "accept: application/hal+json" -H "Content-Type: application/json" -d "{ \"banner\" : \"AUTHORIZED ACCESS ONLY\" }, \"message\": \"WELCOME!\" }"
```

```
----
```

```
'''
```

```
== Clearing the login messages configuration by UUID
```

```
'''
```

```
----
```

```
# The API:
```

```
/api/security/login/messages/{uuid}
```

```
# The call:
```

```
curl -X PATCH "https://<mgmt-ip>/api/security/login/messages/7b1b3715-9ffa-11e8-a5dd-005056bbef18" -H "accept: application/hal+json" -H "Content-Type: application/json" -d "{ \"banner\": \"\", \"message\": \"\" }"
```

```
----
```

```
'''
```

```
[[ID15893ba78c3516b9b6ea706928b2c4e6]]
```

```
= Retrieve login banner and messages of the day
```

```
[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-block]#`/security/login/messages`#
```

Retrieves the login banner and messages of the day (MOTD) configured in the cluster and in specific SVMs.

```
== Learn more
```

```
* xref:{relative_path}security_login_messages_endpoint_overview.html[DOC
/security/login/messages]
```

```
== Parameters
```

```
[cols=5*,options=header]
|==
```

```
|Name
|Type
|In
|Required
|Description
```

```
|svm.uuid
|string
|query
|False
a|Filter by svm.uuid
```

```
|svm.name
|string
|query
|False
a|Filter by svm.name
```

```
|show_cluster_message
|boolean
|query
|False
a|Filter by show_cluster_message
```

```
|banner
|string
|query
|False
a|Filter by banner
```

```
|message
|string
|query
|False
```

a|Filter by message

|scope

|string

|query

|False

a|Filter by scope

|uuid

|string

|query

|False

a|Filter by uuid

|fields

|array[string]

|query

|False

a|Specify the fields to return.

|max_records

|integer

|query

|False

a|Limit the number of records returned.

|return_timeout

|integer

|query

|False

a|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

a|The default is true for GET calls. When set to false, only the number of records is returned.

```

|order_by
|array[string]
|query
|False
a|Order results by specified fields and optional [asc|desc] direction.
Default direction is 'asc' for ascending.

|===

== Response

```

Status: 200, Ok

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records

|records
|array[link:#login_messages[login_messages]]
a|

|===

.Example response
[%collapsible%closed]
=====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },

```

```

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

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====

```

```

[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type

```

```

|Description

|next
|link:#href[href]
a|

|self
|link:#href[href]
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#svm]
[.api-collapsible-fifth-title]
svm

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#login_messages]
[.api-collapsible-fifth-title]
login_messages
```

The login banner and message of the day (MOTD) configuration.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|banner
|string
a|The login banner text. This message is displayed during SSH and console
device
login just before the password prompt displays. When configured, a
cluster-level
login banner is used for every incoming connection. Each data SVM can
override
the cluster-level banner to instead display when you log into the SVM. To
restore
the default setting for a data SVM, set the banner to an empty string.
New lines are supplied as either LF or CRLF but are always returned as LF.
Optional in the PATCH body.
```

```
|message
|string
a|The message of the day (MOTD). This message appears just before the
clustershell
prompt after a successful login. When configured, the cluster message
```


displays first. If you log in as a data SVM administrator, the SVM message is then printed. The cluster-level MOTD can be disabled for a given data SVM using the "show_cluster_message" property. New lines are supplied as either LF or CRLF but are always returned as LF. Optional in the PATCH body.

```
|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".
```

```
|show_cluster_message
|boolean
a|Specifies whether to show a cluster-level message before the SVM message
when logging in as an SVM administrator.
This setting can only be modified by the cluster administrator.
Optional in the PATCH body.
```

```
|svm
|link:#svm[svm]
a|
```

```
|uuid
|string
a|The unique identifier (ID) of the login messages configuration.
```

```
|===
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
=====

```

```
[[IDb67e9435ff4b1a19cc29c9272b418c69]]
```

= Retrieve login messages configuration by UUID

```
[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-block]#`/security/login/messages/{uuid}`#
```

Retrieves the login messages configuration by UUID.

== Learn more

* xref:{relative_path}security_login_messages_endpoint_overview.html[DOC /security/login/messages]

== Parameters

```
[cols=5*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|In
```

```
|Required
```

```
|Description
```

```
|uuid
```

```
|string
```

```
|path
```

```
|True
```

```
a|Login messages configuration UUID
```

```
|fields
```

```
|array[string]
```

```
|query
```

```
|False
```

```
a|Specify the fields to return.
```

```
|===
```

== Response

Status: 200, Ok

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|banner
|string
a|The login banner text. This message is displayed during SSH and console
device
login just before the password prompt displays. When configured, a
cluster-level
login banner is used for every incoming connection. Each data SVM can
override
the cluster-level banner to instead display when you log into the SVM. To
restore
the default setting for a data SVM, set the banner to an empty string.
New lines are supplied as either LF or CRLF but are always returned as LF.
Optional in the PATCH body.

|message
|string
a|The message of the day (MOTD). This message appears just before the
clustershell
prompt after a successful login. When configured, the cluster message
displays first. If you log in as a data SVM administrator, the
SVM message is then printed. The cluster-level MOTD can be disabled
for a given data SVM using the "show_cluster_message" property.
New lines are supplied as either LF or CRLF but are always returned as LF.
Optional in the PATCH body.

|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

|show_cluster_message
|boolean
a|Specifies whether to show a cluster-level message before the SVM message

```

when logging in as an SVM administrator.
This setting can only be modified by the cluster administrator.
Optional in the PATCH body.

```
|svm
|link:#svm[svm]
a|
```

```
|uuid
|string
a|The unique identifier (ID) of the login messages configuration.
```

```
|===
```

.Example response

[%collapsible%closed]

====

[source,json,subs=+macros]

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

====

== Error

Status: Default, Error

[cols=3*,options=header]

```

|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#svm]
[.api-collapsible-fifth-title]
svm

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

```

|===

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
```

|===

```
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

|===

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
```

|===

```
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
|string
a|Error code
```



```

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[IDf2854f30b2ae62b3351a6c49a38efa26]]
= Update login messages configuration

[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-
block]#`/security/login/messages/{uuid}`#

Updates the login messages configuration.
There are no required fields. An empty body makes no modifications.

== Learn more

* xref:{relative_path}security_login_messages_endpoint_overview.html[DOC
/security/login/messages]

== Parameters

[cols=5*,options=header]
|===

|Name
|Type
|In
|Required
|Description

|uuid

```

```
|string
|path
|True
a|Login messages configuration UUID
```

```
|===
```

```
== Request Body
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|banner
```

```
|string
```

a|The login banner text. This message is displayed during SSH and console device

login just before the password prompt displays. When configured, a cluster-level

login banner is used for every incoming connection. Each data SVM can override

the cluster-level banner to instead display when you log into the SVM. To restore

the default setting for a data SVM, set the banner to an empty string.

New lines are supplied as either LF or CRLF but are always returned as LF. Optional in the PATCH body.

```
|message
```

```
|string
```

a|The message of the day (MOTD). This message appears just before the clustershell

prompt after a successful login. When configured, the cluster message

displays first. If you log in as a data SVM administrator, the

SVM message is then printed. The cluster-level MOTD can be disabled

for a given data SVM using the "show_cluster_message" property.

New lines are supplied as either LF or CRLF but are always returned as LF. Optional in the PATCH body.

```

|scope
|string
a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to
"cluster".

|show_cluster_message
|boolean
a|Specifies whether to show a cluster-level message before the SVM message
when logging in as an SVM administrator.
This setting can only be modified by the cluster administrator.
Optional in the PATCH body.

|svm
|link:#svm[svm]
a|

|uuid
|string
a|The unique identifier (ID) of the login messages configuration.

|===

.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "scope": "svm",
  "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 codes | Description

| 10225636
| Only a cluster administrator can modify the `show_cluster_message`
property.
|===
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
====
```

```
[source,json,subs=+macros]
```

```
{
  "error": {
    "arguments": {
```

```

        "code": "string",
        "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
}
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]

```

```

a|

|===

[#svm]
[.api-collapsible-fifth-title]
svm

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|name
|string
a|The name of the SVM.

|uuid
|string
a|The unique identifier of the SVM.

|===

[#login_messages]
[.api-collapsible-fifth-title]
login_messages

The login banner and message of the day (MOTD) configuration.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]

```

a|

|banner

|string

a|The login banner text. This message is displayed during SSH and console device

login just before the password prompt displays. When configured, a cluster-level

login banner is used for every incoming connection. Each data SVM can override

the cluster-level banner to instead display when you log into the SVM. To restore

the default setting for a data SVM, set the banner to an empty string.

New lines are supplied as either LF or CRLF but are always returned as LF. Optional in the PATCH body.

|message

|string

a|The message of the day (MOTD). This message appears just before the clustershell

prompt after a successful login. When configured, the cluster message

displays first. If you log in as a data SVM administrator, the

SVM message is then printed. The cluster-level MOTD can be disabled

for a given data SVM using the "show_cluster_message" property.

New lines are supplied as either LF or CRLF but are always returned as LF. Optional in the PATCH body.

|scope

|string

a|Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster".

|show_cluster_message

|boolean

a|Specifies whether to show a cluster-level message before the SVM message when logging in as an SVM administrator.

This setting can only be modified by the cluster administrator.

Optional in the PATCH body.

|svm

|link:#svm[svm]

a|

```
|uuid
|string
a|The unique identifier (ID) of the login messages configuration.
```

```
|===
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments
```

```
|code
```



```

|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

```

```

|===

```

```

//end collapsible .Definitions block
====

```

```

:leveloffset: -1

```

```

= Manage security roles

```

```

:leveloffset: +1

```

```

[[ID0919dd3799c78d7ad1cf2c176a8c5b4f]]
= Security roles endpoint overview

```

```

== Overview

```

ONTAP supports Role Based Access Control (RBAC) wherein a user account must be associated with a role and the role defines the privileges and rights for that user account. A privilege defines the access level of the API as either "none", "readonly", or "all". This specifies whether the user account can perform only a GET operation or POST, PATCH, and DELETE operations as well. A role can comprise of multiple tuples and each tuple consists of the REST API and its access level.

For example, "role1" might be a role that has a tuple

{"access":"all","path":"/api/storage/volume"}, which means that a user account with "role1" can perform all GET, POST, PATCH, and DELETE requests

on the `_api/storage/volume_` API or derived APIs which have `_api/storage/volume_` as the prefix.

In cases where a role has tuples with multiple APIs having the same prefix, the highest match wins out.

For example, if "role1" has the following tuples:

```
{"access": "readonly", "path": "/api/cluster"} and  
{"access": "all", "path": "/api/cluster/schedules"}, then only a GET request  
is allowed on APIs with _api/cluster_ as the prefix; while POST, PATCH and  
DELETE requests are possible on the _api/cluster/schedules_ API.
```

=== Predefined (built-in) roles

Related REST APIs are used to form predefined cluster-scoped and SVM-scoped roles, such as: "admin", "backup", "readonly" for cluster and "vsadmin", "vsadmin-backup", "vsadmin-protocol" for SVMs.

These can be retrieved by calling a GET request on `_/api/security/roles_` API and can be assigned to user accounts. See the examples for `_api/security/accounts_`.

These predefined roles cannot be modified or deleted.

=== Mapped roles

Before REST APIs, the RBAC roles (legacy roles) were defined to contain the CLI commands and their access levels. Now, almost all REST APIs map to one or more CLI commands. When a role is created using a POST request on `_/api/security/roles_`, a mapped legacy role is created. This legacy role has the same access level (as that of the REST API) for the mapped CLI commands. However, if a legacy role with the same name already exists, the POST operation fails and you need to choose a unique name for the role. The legacy roles cannot be managed using the REST endpoint `_/api/security/roles_` or its derivatives. Legacy roles are managed using the CLI commands "security login role <create \| modify \| delete> -role +++<rolename>+++ ".
+++</rolename>+++

Note that the mapped legacy role (for the REST API role created) cannot be manipulated using the CLI.

The reverse case is not true; the creation of a legacy role will not create a mapped role with equivalent REST APIs.

=== API restrictions

Numerous APIs are scoped for the cluster level only. This results in an access error if assigned to an SVM-scoped role. For example, `_api/cluster/nodes_` does not work when added as a tuple entry for an SVM-

scoped role.

A number of APIs allowed for an SVM-scoped role might have restrictions on the access level. For example, `_/api/network/ethernet/ports_` cannot have an access level of "all" for an SVM-scoped role; this results in an access error when a POST or PATCH request is made.

Roles created with a REST API path prefix which is common to many APIs might have restrictions based on the scope of the role; cluster or SVM. For example, `{"access":"all","path":"/api/security"}` might be a tuple entry for an SVM role. Any GET, POST, PATCH, or DELETE operation fails on API `_/api/security/accounts_` while the same on `_/api/security/login/messages_` succeeds. However, a role with exactly the same tuple when created at the cluster-scope level allows the operations.

Numerous APIs have restrictions on the objects that can be operated on based on the context of the SVM or cluster. For example, a POST request on `_/api/security/authentication/password_` API changes the password for a user account. If executed in the context of an SVM (POST request on an SVM interface), only the password of the user executing the POST can be modified, and attempts to modify the password of any other user results in an access error. However, if a POST request is performed by a cluster administrator account, the password for any user account (cluster or SVM) can be modified.

== Examples

=== Creating a cluster-scoped custom role

Specify the role name and the tuples (of REST APIs and their access level) in the body of the POST request. The `owner.uuid` or `owner.name` are not required to be specified for a cluster-scoped role.

The API:

POST `"/api/security/roles"`

The call:

```
curl -X POST "https://<mgmt-ip>/api/security/roles" -d
'{"name":"cluster_role", "privileges" :
[{"access":"readonly","path":"/api/cluster/jobs"}, {"access":"all","path":"/api/application/applications"}, {"access":"readonly","path":"/api/application/templates"}]}'
```

=== Creating an SVM-scoped custom role

For an SVM-scoped role, specify either owner.name or owner.uuid in the request body along with other parameters for the role. These correspond to the name or UUID of the SVM for which the role is being created and can be obtained from the response body of the GET request performed on the `_api/svm/svms_` API.

The API:

POST "/api/security/roles"

The call:

```
curl -X POST "https://<mgmt-ip>/api/security/roles" -d '{"owner": {"uuid": "9f93e553-4b02-11e9-a3f9-005056bb7acd"}, "name": "svm_role", "privileges": [{"access": "readonly", "path": "/api/cluster/jobs"}, {"access": "all", "path": "/api/application/applications"}, {"access": "readonly", "path": "/api/application/templates"}]}'
```

=== Retrieving the configured roles

All of the roles or a filtered list of roles (for example by name, predefined, and so on) can be retrieved.

The API:

GET "/api/security/roles"

The call to retrieve all the roles configured in the cluster:

```
curl -X GET "https://<mgmt-ip>/api/security/roles"
```

The response:

```
{
  "records": [
    {
      "owner": {
        "uuid": "2903de6f-4bd2-11e9-b238-0050568e2e25",
        "name": "cluster1",
        "_links": {
          "self": {
            "href": "/api/svm/svms/2903de6f-4bd2-11e9-b238-0050568e2e25"
          }
        }
      }
    }
  ]
}
```

```

    },
    "name": "admin",
    "privileges": [
      {
        "path": "/api",
        "access": "all",
        "_links": {
          "self": {
            "href": "/api/security/roles/2903de6f-4bd2-11e9-b238-0050568e2e25/admin/privileges/%2Fapi"
          }
        }
      }
    ],
    "builtin": true,
    "scope": "cluster",
    "_links": {
      "self": {
        "href": "/api/security/roles/2903de6f-4bd2-11e9-b238-0050568e2e25/admin"
      }
    }
  },
  {
    "owner": {
      "uuid": "aaef7c38-4bd3-11e9-b238-0050568e2e25",
      "name": "svml",
      "_links": {
        "self": {
          "href": "/api/svm/svms/aaef7c38-4bd3-11e9-b238-0050568e2e25"
        }
      }
    },
    "name": "vsadmin",
    "privileges": [
      {
        "path": "/api/application/applications",
        "access": "all",
        "_links": {
          "self": {
            "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/vsadmin/privileges/%2Fapi%2Fapplication%2Fapplications"
          }
        }
      }
    ],
  },
  {

```

```

    "path": "/api/application/templates",
    "access": "readonly",
    "_links": {
      "self": {
        "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/vsadmin/privileges/%2Fapi%2Fapplication%2Ftemplates"
      }
    }
  },
  {
    "path": "/api/cluster",
    "access": "readonly",
    "_links": {
      "self": {
        "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/vsadmin/privileges/%2Fapi%2Fcluster"
      }
    }
  },
  {
    "path": "/api/svm/svms",
    "access": "readonly",
    "_links": {
      "self": {
        "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/vsadmin/privileges/%2Fapi%2Fsvm%2Fsvms"
      }
    }
  },
  {
    "path": "/api/svms",
    "access": "readonly",
    "_links": {
      "self": {
        "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/vsadmin/privileges/%2Fapi%2Fsvms"
      }
    }
  }
],
"builtin": true,
"scope": "svm",
"_links": {
  "self": {
    "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/vsadmin"
  }
}

```


Retrieves a list of roles configured in the cluster.

== Related ONTAP commands

* `security login rest-role show`

== Learn more

* xref:{relative_path}security_roles_endpoint_overview.html[DOC
/security/roles]

== Parameters

[cols=5*,options=header]
|==

|Name
|Type
|In
|Required
|Description

|scope
|string
|query
|False
a|Filter by scope

|owner.uuid
|string
|query
|False
a|Filter by owner.uuid

|owner.name
|string
|query
|False
a|Filter by owner.name

|builtin


```
|boolean
|query
|False
a|Filter by builtin
```

```
|name
|string
|query
|False
a|Filter by name
```

```
|privileges.path
|string
|query
|False
a|Filter by privileges.path
```

```
|privileges.access
|string
|query
|False
a|Filter by privileges.access
```

```
|fields
|array[string]
|query
|False
a|Specify the fields to return.
```

```
|max_records
|integer
|query
|False
a|Limit the number of records returned.
```

```
|return_records
|boolean
|query
|False
a|The default is true for GET calls. When set to false, only the number
of records is returned.
```

```

|return_timeout
|integer
|query
|False
a|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.

|order_by
|array[string]
|query
|False
a|Order results by specified fields and optional [asc|desc] direction.
Default direction is 'asc' for ascending.

|===

== Response

```

Status: 200, Ok

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records

|records
|array[link:#role[role]]
a|

|===

```

```

.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "admin",
    "owner": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "svm1",
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    },
    "privileges": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "access": "readonly",
      "path": "/api/storage/volumes"
    },
    "scope": "cluster"
  }
}
====

== Error

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name

```

```

|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|next
|link:href[href]
a|

|self
|link:href[href]
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:href[href]
a|

|===

```

```
[#owner]
[.api-collapsible-fifth-title]
owner
```

Owner name and UUID that uniquely identifies the role.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#role_privilege]
[.api-collapsible-fifth-title]
role_privilege
```

A tuple containing the REST endpoint and the access level assigned to that endpoint.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
```

```

a|

|access
|string
a|Access level for the REST endpoint.

|path
|string
a|REST URI/endpoint

|===

[#role]
[.api-collapsible-fifth-title]
role

A named set of privileges that defines the rights an account has when it
is assigned the role.

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|builtin
|boolean
a|Indicates if this is a built-in (pre-defined) role which cannot be
modified or deleted.

|name
|string
a|Role name

|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the role.

```

```
|privileges
|array[link:#role_privilege[role_privilege]]
a|The list of privileges that this role has been granted.
```

```
|scope
|string
a|Scope of the entity. Set to "cluster" for cluster owned objects and to
"svm" for SVM owned objects.
```

```
|===
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```
|===
```

```
[#error]
[.api-collapsible-fifth-title]
error
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
```



```

|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments


|code
|string
a|Error code


|message
|string
a|Error message


|target
|string
a|The target parameter that caused the error.


|===

//end collapsible .Definitions block
====

[[ID998d7f94d595a0c6f7eacdec3d95a887]]
= Create a new cluster-scoped or SVM-scoped role

[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-
block]#`/security/roles`#


Creates a new cluster-scoped role or an SVM-scoped role. For an SVM-scoped
role, specify either the SVM name as the owner.name or SVM UUID as the
owner.uuid in the request body along with other parameters for the role.
The owner.uuid or owner.name are not required to be specified for a
cluster-scoped role.


== Required parameters

* `name` - Name of the role to be created.

```

* ``privileges`` - Array of privilege tuples. Each tuple consists of a REST API path and its desired access level.

== Optional parameters

* ``owner.name`` or ``owner.uuid`` - Name or UUID of the SVM for an SVM-scoped role.

== Related ONTAP commands

* ``security login rest-role create``

== Learn more

* `xref:{relative_path}security_roles_endpoint_overview.html[DOC /security/roles]`

== Parameters

[cols=5*,options=header]

|===

|Name

|Type

|In

|Required

|Description

|return_records

|boolean

|query

|False

a|The default is false. If set to true, the records are returned.

|===

== Request Body

[cols=3*,options=header]

|===

|Name

|Type

|Description

```

|_links
|link:#_links[_links]
a|

|builtin
|boolean
a|Indicates if this is a built-in (pre-defined) role which cannot be
modified or deleted.

|name
|string
a|Role name

|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the role.

|privileges
|array[link:#role_privilege[role_privilege]]
a|The list of privileges that this role has been granted.

|scope
|string
a|Scope of the entity. Set to "cluster" for cluster owned objects and to
"svm" for SVM owned objects.

|===

.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "name": "admin",
  "owner": {
    "_links": {

```

```

    "self": {
      "href": "/api/resourcelink"
    },
    "name": "svml",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "privileges": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "access": "readonly",
    "path": "/api/storage/volumes"
  },
  "scope": "cluster"
}
====

== Response

```

Status: 201, Created

```

== Error

```

Status: Default

ONTAP Error Response Codes

```

|====
| Error Code | Description
|
| 5636129
| Role with given name has not been defined.
|
| 5636143
| Vserver admin cannot use the API with this access level.
|
| 5636144
| Invalid value specified for access level.
|
| 5636169
| Invalid character in URI.

```

```
| 5636170
| URI does not exist.

| 5636171
| Role already exists in legacy role table.

| 13434890
| Vserver-ID failed for Vserver roles.

| 13434891
| UUID lookup failed for Vserver roles.

| 13434892
| Roles is a required field.

| 13434893
| SVM does not exist.
|===
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
```

```
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

```

    }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#owner]
[.api-collapsible-fifth-title]

```

owner

Owner name and UUID that uniquely identifies the role.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|name
```

```
|string
```

```
a|The name of the SVM.
```

```
|uuid
```

```
|string
```

```
a|The unique identifier of the SVM.
```

```
|===
```

```
[#role_privilege]
```

```
[.api-collapsible-fifth-title]
```

```
role_privilege
```

A tuple containing the REST endpoint and the access level assigned to that endpoint.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|access
```

```
|string
a|Access level for the REST endpoint.
```

```
|path
|string
a|REST URI/endpoint
```

```
|===
```

```
[#role]
[.api-collapsible-fifth-title]
role
```

A named set of privileges that defines the rights an account has when it is assigned the role.

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|builtin
|boolean
a|Indicates if this is a built-in (pre-defined) role which cannot be
modified or deleted.
```

```
|name
|string
a|Role name
```

```
|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the role.
```

```
|privileges
```



```

|array[link:#role_privilege[role_privilege]]
a|The list of privileges that this role has been granted.

|scope
|string
a|Scope of the entity. Set to "cluster" for cluster owned objects and to
"svm" for SVM owned objects.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments

```

```
|array[link:#error_arguments[error_arguments]]
```

```
a|Message arguments
```

```
|code
```

```
|string
```

```
a|Error code
```

```
|message
```

```
|string
```

```
a|Error message
```

```
|target
```

```
|string
```

```
a|The target parameter that caused the error.
```

```
|===
```

```
//end collapsible .Definitions block
```

```
====
```

```
:leveloffset: -1
```

```
= View or delete a role
```

```
:leveloffset: +1
```

```
[[IDcaea97dec75565e5a5ec8565bbe836e2]]
```

```
= Security roles owner.uuid name endpoint overview
```

```
== Overview
```

This API is used to retrieve or delete a role. The role can be SVM-scoped or cluster-scoped.

Specify the owner UUID and the role name in the URI path. The owner UUID corresponds to the UUID of the SVM for which the role has been created and

can be obtained from the response body of a GET call performed on one of the following APIs:

- `_api/security/roles_` for all roles
- `_api/security/roles/?scope=svm_` for SVM-scoped roles
- `_api/security/roles/?owner.name=\{svm-name}_` for roles in a specific SVM

This API response contains the complete URI for each role that can be used for retrieving or deleting a role.

NOTE: The pre-defined roles can be retrieved but cannot be deleted.

== Examples

=== Retrieving a role configuration

The API:

GET "/api/security/roles/{owner.uuid}/{name}"

The call:

curl -X GET "https://<mgmt-ip>/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/secure_role"

The response:

```
{
  "owner": {
    "uuid": "aaef7c38-4bd3-11e9-b238-0050568e2e25",
    "name": "svm1",
    "_links": {
      "self": {
        "href": "/api/svm/svms/aaef7c38-4bd3-11e9-b238-0050568e2e25"
      }
    }
  },
  "name": "secure_role",
  "privileges": [
    {
      "path": "/api/security",
      "access": "all",
      "_links": {
        "self": {
          "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/secure_role/privileges/%2Fapi%2Fsecurity"
        }
      }
    }
  ]
}
```

```

],
"builtin": false,
"scope": "svm",
"_links": {
  "self": {
    "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-
0050568e2e25/secure_role"
  }
}
}
}
----

```

=== Deleting a custom role

The API:

```
DELETE "/api/security/roles/{owner.uuid}/{name}"
```

The call:

```
curl -X DELETE "https://<mgmt-ip>/api/security/roles/aaef7c38-4bd3-11e9-
b238-0050568e2e25/svm_role1"
```

```
[[IDece338f52a74cfb4df61af6a6c200f53]]
```

= Delete a role

```
[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-
block]#`/security/roles/{owner.uuid}/{name}`#
```

Deletes the specified role.

== Required parameters

- * `name` - Name of the role to be deleted.
- * `owner.uuid` - UUID of the SVM housing the role.

== Related ONTAP commands

- * `security login rest-role delete`

== Learn more

```
*
xref:{relative_path}security_roles_owner.uuid_name_endpoint_overview.html[
DOC /security/roles/{owner.uuid}/{name}]
* xref:{relative_path}security_roles_endpoint_overview.html[DOC
/security/roles]
```

== Parameters

```
[cols=5*,options=header]
|===
```

```
|Name
|Type
|In
|Required
|Description
```

```
|owner.uuid
|string
|path
|True
a|
```

```
|name
|string
|path
|True
a|
|===
```

== Response

Status: 200, Ok

== Error

Status: Default

ONTAP Error Response Codes

```
|===
| Error Code | Description
```

```
| 5636172
| User accounts detected with this role assigned. Update or delete those
accounts before deleting this role.
```

```
| 5636173
| Features require an effective cluster version of 9.6 or later.
```

```
| 13434890
| Vserver-ID failed for Vserver roles.
```

```
| 13434893
| The SVM does not exist.
|===
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|error
|link:#error[error]
a|
```

```
|===
```

```
.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
```

```
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====
```

```

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string

```

a|Error code

|message

|string

a|Error message

|target

|string

a|The target parameter that caused the error.

|===

//end collapsible .Definitions block

====

[[ID0fc3b1b2d94177217531b3dbb6a3c7c3]]

= Retrieve the details of a role

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-block]#`/security/roles/{owner.uuid}/{name}`#

Retrieves the details of the specified role.

== Related ONTAP commands

* `security login rest-role show`

== Learn more

*

xref:{relative_path}security_roles_owner.uuid_name_endpoint_overview.html[DOC /security/roles/{owner.uuid}/{name}]

* xref:{relative_path}security_roles_endpoint_overview.html[DOC /security/roles]

== Parameters

[cols=5*,options=header]


```

|===

|Name
|Type
|In
|Required
|Description

|fields
|array[string]
|query
|False
a|Specify the fields to return.

|owner.uuid
|string
|path
|True
a|Role owner UUID

|name
|string
|path
|True
a|Role name

|===

== Response

```

Status: 200, Ok

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer

```

a|Number of records

|records
|array[link:#role[role]]
a|

|===

.Example response
[%collapsible%closed]

====

[source,json,subs=+macros]

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    },
    "name": "admin",
    "owner": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      },
      "name": "svm1",
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    },
    "privileges": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      },
      "access": "readonly",
```

```

    "path": "/api/storage/volumes"
  },
  "scope": "cluster"
}
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]

```

```

//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|====
|Name
|Type
|Description

|href
|string
a|

|====

[#\_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|====
|Name
|Type
|Description

|next
|link:#href\[href\]
a|

|self
|link:#href\[href\]
a|

|====

[#\_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|====
|Name

```

```
|Type
|Description
```

```
|self
|link:#href[href]
a|
```

```
|===
```

```
[#owner]
[.api-collapsible-fifth-title]
owner
```

Owner name and UUID that uniquely identifies the role.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|name
|string
a|The name of the SVM.
```

```
|uuid
|string
a|The unique identifier of the SVM.
```

```
|===
```

```
[#role_privilege]
[.api-collapsible-fifth-title]
role_privilege
```

A tuple containing the REST endpoint and the access level assigned to that endpoint.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|access
|string
a|Access level for the REST endpoint.
```

```
|path
|string
a|REST URI/endpoint
```

```
|===
```

```
[#role]
[.api-collapsible-fifth-title]
role
```

A named set of privileges that defines the rights an account has when it is assigned the role.

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|_links
|link:#_links[_links]
a|
```

```
|builtin
|boolean
a|Indicates if this is a built-in (pre-defined) role which cannot be
modified or deleted.
```

```

|name
|string
a|Role name

|owner
|link:#owner[owner]
a|Owner name and UUID that uniquely identifies the role.

|privileges
|array[link:#role_privilege[role_privilege]]
a|The list of privileges that this role has been granted.

|scope
|string
a|Scope of the entity. Set to "cluster" for cluster owned objects and to
"svm" for SVM owned objects.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

```

```

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

:leveloffset: -1

= Manage role privilege details

:leveloffset: +1

```



```
[[ID276793f94177f5287f0aa7e864dfc455]]
```

= Security roles owner.uuid name privileges endpoint overview

== Overview

This API is used to configure the role privileges (tuples of REST URI path and its access levels). It also retrieves all of the privilege tuples for a role and can add a tuple to an existing role.

The role can be SVM-scoped or cluster-scoped.

Specify the owner UUID and the role name in the URI path. The owner UUID corresponds to the UUID of the SVM for which the role has been created and can be obtained from the response body of a GET request performed on one of the following APIs:

`_/_api/security/roles_` for all the roles

`_/_api/security/roles/?scope=svm_` for SVM-scoped roles

`_/_api/security/roles/?owner.name=+++<svm-name>+++</i>` for roles in a specific SVM This API response contains the complete URI for each role and can be used after suffixing it with `_"privileges"_.+++</svm-name>+++_`

NOTE: The pre-defined roles can be retrieved but cannot be updated.

== Examples

=== Adding a privilege tuple for an existing custom role

The API:

POST `"/security/roles/{owner.uuid}/{name}/privileges"`

The call:

`curl -X POST "https://<mgmt-ip>/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_role1/privileges" -d`

`'{"access":"readonly","path":"/api/protocols"}'`

=== Retrieving all the privilege tuples for a role

The API:

GET `"/api/security/roles/{owner.uuid}/{name}/privileges"`

```

# The call:
curl -X GET "https://<mgmt-ip>/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_role1/privileges"

# The response:
{
  "records": [
    {
      "path": "/api/application",
      "access": "all",
      "_links": {
        "self": {
          "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_role1/privileges/%2Fapi%2Fapplication"
        }
      }
    },
    {
      "path": "/api/protocols",
      "access": "readonly",
      "_links": {
        "self": {
          "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_role1/privileges/%2Fapi%2Fprotocols"
        }
      }
    }
  ],
  "num_records": 2,
  "_links": {
    "self": {
      "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_role1/privileges"
    }
  }
}
----

[[ID5fd9866dab88282d3bc5c0724f3f9c46]]
= Retrieve privilege details of the specified role

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-

```

```
block]#`/security/roles/{owner.uuid}/{name}/privileges`#
```

Retrieves privilege details of the specified role.

== Related ONTAP commands

* `security login rest-role show`

== Learn more

*

xref:{relative_path}security_roles_owner.uuid_name_privileges_endpoint_overview.html[DOC /security/roles/{owner.uuid}/{name}/privileges]

* xref:{relative_path}security_roles_endpoint_overview.html[DOC /security/roles]

== Parameters

[cols=5*,options=header]

|===

|Name

|Type

|In

|Required

|Description

|fields

|array[string]

|query

|False

a|Specify the fields to return.

|max_records

|integer

|query

|False

a|Limit the number of records returned.

|return_records

|boolean

|query

```

|False
a|The default is true for GET calls. When set to false, only the number
of records is returned.

|return_timeout
|integer
|query
|False
a|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.

|order_by
|array[string]
|query
|False
a|Order results by specified fields and optional [asc|desc] direction.
Default direction is 'asc' for ascending.

|owner.uuid
|string
|path
|True
a|Role owner UUID

|name
|string
|path
|True
a|Role name

|===

== Response

```

Status: 200, Ok

```

[cols=3*,options=header]
|===
|Name
|Type

```

```

|Description

|_links
|link:#_links[_links]
a|

|num_records
|integer
a|Number of records


|records
|array[link:#role_privilege[role_privilege]]
a|

|===

.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "access": "readonly",
    "path": "/api/storage/volumes"
  }
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

```

```

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|next
|link:href[href]
a|

|self
|link:href[href]
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:href[href]
a|

|===

[#role_privilege]

```

[.api-collapsible-fifth-title]

role_privilege

A tuple containing the REST endpoint and the access level assigned to that endpoint.

[cols=3*,options=header]

|===

|Name

|Type

|Description

|_links

|link:#_links[_links]

a|

|access

|string

a|Access level for the REST endpoint.

|path

|string

a|REST URI/endpoint

|===

[#error_arguments]

[.api-collapsible-fifth-title]

error_arguments

[cols=3*,options=header]

|===

|Name

|Type

|Description

|code

|string

a|Argument code

|message

|string


```

a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[ID65a27bd91ff7e01e9c7beb7344966642]]
= Add a privilege tuple to an existing role

```

```
[.api-doc-operation .api-doc-operation-post]#POST# [.api-doc-code-block]#`/security/roles/{owner.uuid}/{name}/privileges`#
```

Adds a privilege tuple (of REST URI and its access level) to an existing role.

== Required parameters

- * `owner.uuid` - UUID of the SVM that houses this role.
- * `name` - Name of the role to be updated.
- * `path` - REST URI path (example: "/api/storage/volumes").
- * `access` - Desired access level for the REST URI path (one of "all", "readonly" or "none").

== Related ONTAP commands

* `security login rest-role create`

== Learn more

*

xref:{relative_path}security_roles_owner.uuid_name_privileges_endpoint_overview.html[DOC /security/roles/{owner.uuid}/{name}/privileges]
* xref:{relative_path}security_roles_endpoint_overview.html[DOC /security/roles]

== Parameters

```
[cols=5*,options=header]  
|==
```

```
|Name  
|Type  
|In  
|Required  
|Description
```

```
|return_records  
|boolean  
|query  
|False
```

a|The default is false. If set to true, the records are returned.

```

|owner.uuid
|string
|path
|True
a|Role owner UUID

|name
|string
|path
|True
a|Role name

|===

== Request Body

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|access
|string
a|Access level for the REST endpoint.

|path
|string
a|REST URI/endpoint

|===

.Example request
[%collapsible%closed]
=====
[source,json,subs=+macros]
{

```

```
"_links": {
  "self": {
    "href": "/api/resourcelink"
  }
},
"access": "readonly",
"path": "/api/storage/volumes"
}
====

== Response
```

Status: 201, Created

```
== Error
```

Status: Default

ONTAP Error Response Codes

```
|===
| Error Code | Description

| 5636129
| A role with given name has not been defined.

| 5636143
| A Vserver admin cannot use the API with this access level.

| 5636144
| The value specified for the access level is not valid.

| 5636169
| A character in the URI is not valid.

| 5636170
| The URI does not exist.

| 5636173
| This feature requires an effective cluster version of 9.6 or later.

| 5636175
| Vserver admin cannot have access to given API.

| 13434890
```

```
| Vserver-ID failed for Vserver roles.

| 13434891
| UUID LookUp failed for Vserver roles.

| 13434892
| Roles is a required field.

| 13434893
| The SVM does not exist.
|===
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|error
```

```
|link:#error[error]
```

```
a|
```

```
|===
```

```
.Example error
```

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
```

```
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

```
=====
```

```
== Definitions
```

```
[.api-def-first-level]
```

```
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|href
|string
a|
```

```
|===
```

```
[#_links]
[.api-collapsible-fifth-title]
_links
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|self
|link:href[href]
a|
```

```
|===
```

```
[#role_privilege]
[.api-collapsible-fifth-title]
role_privilege
```

A tuple containing the REST endpoint and the access level assigned to that endpoint.

```
[cols=3*,options=header]
```

```

|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|access
|string
a|Access level for the REST endpoint.

```

```

|path
|string
a|REST URI/endpoint

```

```

|===

```

```

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

```

```

[cols=3*,options=header]

```

```

|===

```

```

|Name
|Type
|Description

```

```

|code
|string
a|Argument code

```

```

|message
|string
a|Message argument

```

```

|===

```

```

[#error]
[.api-collapsible-fifth-title]

```

```

error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments


|code
|string
a|Error code


|message
|string
a|Error message


|target
|string
a|The target parameter that caused the error.


|===


//end collapsible .Definitions block
====


:leveloffset: -1


= Manage role privilege path


:leveloffset: +1


[[IDb14e1ffea9cbb92bca7b997be6e7828f]]
= Security roles owner.uuid name privileges path endpoint overview

```


== Overview

A role can comprise of multiple tuples and each tuple consists of the REST API path and its access level. These APIs can be used to retrieve and modify the access level or delete one of the constituent REST API paths within a role.

The role can be SVM-scoped or cluster-scoped.

Specify the owner UUID and the role name in the URI path. The owner UUID corresponds to the UUID of the SVM for which the role has been created and can be obtained from the response body of a GET request performed on one of the following APIs:

`_/api/security/roles_` for all roles

`_/api/security/roles/?scope=svm_` for SVM-scoped roles

`_/api/security/roles/?owner.name=+++<svm-name>+++</i>` for roles in a specific SVM This API response contains the complete URI for each tuple of the role and can be used for GET, PATCH, or DELETE operations.+++</svm-name>+++_

NOTE: The access level for paths in pre-defined roles cannot be updated.

== Examples

=== Updating the access level for a path in the privilege tuple of an existing role

The API:

PATCH `"/api/security/roles/{owner.uuid}/{name}/privileges/{path}"`

The call:

```
curl -X PATCH "https://<mgmt-ip>/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_role1/privileges/%2Fapi%2Fprotocols" -d '{"access":"all"}'
```

=== Retrieving the access level for a path in the privilege tuple of an existing role

The API:

GET `"/api/security/roles/{owner.uuid}/{name}/privileges/{path}"`

```
# The call:
curl -X GET "https://<mgmt-ip>/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_role1/privileges/%2Fapi%2Fprotocols"
```

```
# The response:
{
  "owner": {
    "uuid": "aaef7c38-4bd3-11e9-b238-0050568e2e25"
  },
  "name": "svm_role1",
  "path": "/api/protocols",
  "access": "all",
  "_links": {
    "self": {
      "href": "/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_role1/privileges/%2Fapi%2Fprotocols"
    }
  }
}
-----
```

=== Deleting a privilege tuple from an existing role

```
# The API:
DELETE "/api/security/roles/{owner.uuid}/{name}/privileges/{path}"
```

```
# The call:
curl -X DELETE "https://<mgmt-ip>/api/security/roles/aaef7c38-4bd3-11e9-b238-0050568e2e25/svm_role1/privileges/%2Fapi%2Fprotocols"
-----
```

```
[[ID7edcde80ad5a5a8fa2e708f0940286c3]]
= Delete a privilege tuple from the role
```

```
[.api-doc-operation .api-doc-operation-delete]#DELETE# [.api-doc-code-block]#`/security/roles/{owner.uuid}/{name}/privileges/{path}`#
```

Deletes a privilege tuple (of REST URI and its access level) from the

role.

== Required parameters

- * `owner.uuid` - UUID of the SVM which houses this role.
- * `name` - Name of the role to be updated.
- * `path` - Constituent REST API path to be deleted from this role.

== Related ONTAP commands

- * `security login rest-role delete`

== Learn more

*
xref:{relative_path}security_roles_owner.uuid_name_privileges_path_endpoint_overview.html[DOC
/security/roles/{owner.uuid}/{name}/privileges/{path}]
* xref:{relative_path}security_roles_endpoint_overview.html[DOC
/security/roles]

== Parameters

[cols=5*,options=header]
|===

Name	Type	In	Required	Description
------	------	----	----------	-------------

owner.uuid	string	path	True	a
------------	--------	------	------	---

name	string	path	True	a
------	--------	------	------	---

path	string			
------	--------	--	--	--

```
|path
|True
a|
|===

== Response
```

Status: 200, Ok

```
== Error
```

Status: Default

ONTAP Error Response Codes

```
|===
| Error Code | Description

| 5636172
| User accounts detected with this role assigned. Update or delete those
accounts before deleting this role.

| 5636173
| This feature requires an effective cluster version of 9.6 or later.

| 13434890
| Vserver-ID failed for Vserver roles.

| 13434893
| The SVM does not exist.
|===
```

```
[cols=3*,options=header]
```

```
|===
|Name
|Type
|Description
```

```
|error
|link:#error[error]
a|
```

```
|===
```

```
.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
=====
```

== Definitions

```
[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
=====
```

```
[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments
```

```
[cols=3*,options=header]
|===
|Name
|Type
|Description
```

```
|code
|string
a|Argument code
```

```
|message
|string
a|Message argument
```

```

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[ID995ed77d4ea3b724d0a34eddbd283b30]]
= Retrieve the access level for a REST API path or command/command
directory path for a role

[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/roles/{owner.uuid}/{name}/privileges/{path}`#

```

Retrieves the privilege level for a REST API path for the specified role.

== Related ONTAP commands

* `security login rest-role show`

== Learn more

*

xref:{relative_path}security_roles_owner.uuid_name_privileges_path_endpoint_overview.html[DOC
/security/roles/{owner.uuid}/{name}/privileges/{path}]
* xref:{relative_path}security_roles_endpoint_overview.html[DOC
/security/roles]

== Parameters

[cols=5*,options=header]
|===

|Name
|Type
|In
|Required
|Description

|fields
|array[string]
|query
|False
a|Specify the fields to return.

|owner.uuid
|string
|path
|True
a|Role owner UUID

|name
|string
|path

```
|True
a|Role name

|path
|string
|path
|True
a|REST API path

|===

== Response
```

Status: 200, Ok


```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|access
|string
a|Access level for the REST endpoint.
```

```
|path
|string
a|REST URI/endpoint
```

```
|===
```

```
.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "access": "readonly",
  "path": "/api/storage/volumes"
}
====

== Error
```

Status: Default, Error

```
[cols=3*,options=header]
|===
|Name
```

```

|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string

```

```

a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message
|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]

```

```

error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

[[ID9fb9f02fca200bea5644d498f0fb9253]]
= Update the access level for a REST API path or command/command directory
path

[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-
block]#`/security/roles/{owner.uuid}/{name}/privileges/{path}`#

Updates the privilege level for a REST API path.

```

== Required parameters

- * `owner.uuid` - UUID of the SVM that houses this role.
- * `name` - Name of the role to be updated.
- * `path` - Constituent REST API path whose access level has to be updated.
- * `access` - Access level for the path (one of "all", "readonly", or "none")

== Related ONTAP commands

- * `security login rest-role modify`

== Learn more

*
xref:{relative_path}security_roles_owner.uuid_name_privileges_path_endpoint_overview.html[DOC
/security/roles/{owner.uuid}/{name}/privileges/{path}]
* xref:{relative_path}security_roles_endpoint_overview.html[DOC
/security/roles]

== Parameters

[cols=5*,options=header]
|===

|Name
|Type
|In
|Required
|Description

|owner.uuid
|string
|path
|True
a|Role owner UUID

|name
|string
|path
|True
a|Role name

```
|path
|string
|path
|True
a|REST API path
```

```
|===
```

```
== Request Body
```

```
[cols=3*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|Description
```

```
|_links
```

```
|link:#_links[_links]
```

```
a|
```

```
|access
```

```
|string
```

```
a|Access level for the REST endpoint.
```

```
|path
```

```
|string
```

```
a|REST URI/endpoint
```

```
|===
```

```
.Example request
```

```
[%collapsible%closed]
```

```
=====
```

```
[source,json,subs=+macros]
```

```
{
```

```
  "_links": {
```

```
    "self": {
```

```
      "href": "/api/resourcelink"
```

```
    }
```

```
  },
```

```
  "access": "readonly",
```

```
  "path": "/api/storage/volumes"
```

```
}  
====  
  
== Response
```

Status: 200, Ok

```
== Error
```

Status: Default, Error

```
[cols=3*,options=header]  
|===  
|Name  
|Type  
|Description  
  
|error  
|link:#error[error]  
a|  
  
|===  
  
.Example error  
[%collapsible%closed]  
====  
[source,json,subs=+macros]  
{  
  "error": {  
    "arguments": {  
      "code": "string",  
      "message": "string"  
    },  
    "code": "4",  
    "message": "entry doesn't exist",  
    "target": "uuid"  
  }  
}  
====  
  
== Definitions  
  
[.api-def-first-level]  
.See Definitions
```

```
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#role_privilege]
[.api-collapsible-fifth-title]
role_privilege
```

A tuple containing the REST endpoint and the access level assigned to that endpoint.

```
[cols=3*,options=header]
|===
```



```

|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|access
|string
a|Access level for the REST endpoint.

```

```

|path
|string
a|REST URI/endpoint

```

```

|===

```

```

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

```

```

[cols=3*,options=header]
|===

```

```

|Name
|Type
|Description

```

```

|code
|string
a|Argument code

```

```

|message
|string
a|Message argument

```

```

|===

```

```

[#error]
[.api-collapsible-fifth-title]
error

```

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

:leveloffset: -1

= Manage SSH server

:leveloffset: +1

[[ID6247744df0a26069f2fefa467e938bb5]]
= Security SSH endpoint overview

```

== Overview

ONTAP supports SSH server that can be accessed from any standard SSH client. A user account needs to be associated with SSH as the application (refer the documentation for `_api/security/accounts_xref:{relative_path}security_accounts_endpoint_overview.html[DOC /security/accounts]` . Upon connecting from a client, the user is authenticated and a command line shell is presented.

This endpoint is used to retrieve or modify the SSH configuration at the cluster level. The configuration consists of SSH security parameters (security algorithms and maximum authentication retry attempts allowed before closing the connection) and SSH connection limits.

The security algorithms include SSH key exchange algorithms, ciphers for payload encryption, and MAC algorithms. This configuration is the default for all newly created SVMs; existing SVM configurations are not impacted. The SSH connection limits include maximum connections per second, maximum simultaneous sessions from the same client host, and overall maximum SSH connections at any given point in time. The connection limits are per node and will be the same for all nodes in the cluster.

== Examples

=== Updating the SSH security parameters

Specify the algorithms in the body of the PATCH request.

The API:

PATCH "/api/security/ssh"

The call:

```
curl -X PATCH "https://<mgmt-ip>/api/security/ssh" -d '{ "ciphers": [
"aes256_ctr", "aes192_ctr" ], "key_exchange_algorithms": [
"diffie_hellman_group_exchange_sha256", "diffie_hellman_group14_sha1" ],
"mac_algorithms": [ "hmac_sha2_512_etm", "umac_128_etm" ],
"max_authentication_retry_count": 3 }'
```

=== Updating the SSH connection limits

Specify the connection limits in the body of the PATCH request.

```

# The API:
PATCH "/api/security/ssh"

# The call:
curl -X PATCH "https://<mgmt-ip>/api/security/ssh" -d '{
"connections_per_second": 8, "max_instances": 10, "per_source_limit": 5 }'
----

=== Retrieving the cluster SSH server configuration

----

# The API:
GET "/api/security/ssh"

# The call:
curl -X GET "https://<mgmt-ip>/api/security/ssh"

# The response:
{
  "ciphers": [
    "aes256_ctr",
    "aes192_ctr"
  ],
  "key_exchange_algorithms": [
    "diffie_hellman_group_exchange_sha256",
    "diffie_hellman_group14_sha1"
  ],
  "mac_algorithms": [
    "hmac_sha2_512_etm",
    "umac_128_etm"
  ],
  "max_authentication_retry_count": 3,
  "connections_per_second": 8,
  "max_instances": 10,
  "per_source_limit": 5,
  "_links": {
    "self": {
      "href": "/api/security/ssh"
    }
  }
}
----

```

```
[[IDe0715e9e254f380648ea766baf92deeb]]
= Retrieve cluster SSH server ciphers, MAC algorithms, key exchange
algorithms, and connection limits
```

```
[.api-doc-operation .api-doc-operation-get]#GET# [.api-doc-code-
block]#`/security/ssh`#
```

Retrieves the cluster SSH server ciphers, MAC algorithms, key exchange algorithms, and connection limits.

== Related ONTAP commands

- * `security ssh`
- * `security protocol ssh`

== Learn more

- * xref:{relative_path}security_ssh_endpoint_overview.html[DOC /security/ssh]

== Response

Status: 200, Ok

```
[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|ciphers
|array[string]
a|Ciphers for encrypting the data.

|connections_per_second
|integer
```

a|Maximum connections allowed per second.

|key_exchange_algorithms
|array[string]
a|Key exchange algorithms.

|mac_algorithms
|array[string]
a|MAC algorithms.

|max_authentication_retry_count
|integer
a|Maximum authentication retries allowed before closing the connection.

|max_instances
|integer
a|Maximum possible simultaneous connections.

|per_source_limit
|integer
a|Maximum connections from the same client host.

|===

.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
 "_links": {
 "self": {
 "href": "/api/resourcelink"
 }
 },
 "ciphers": [
 "aes256_ctr",
 "aes192_ctr",
 "aes128_ctr"
],
 "key_exchange_algorithms": [

```

    "diffie_hellman_group_exchange_sha256",
    "diffie_hellman_group14_sha1"
  ],
  "mac_algorithms": [
    "hmac_sha1",
    "hmac_sha2_512_etm"
  ]
}
====

== Error

```

Status: Default, Error

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

```

```

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type
|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type

```


|Description

|code

|string

a|Argument code

|message

|string

a|Message argument

|===

[#error]

[.api-collapsible-fifth-title]

error

[cols=3*,options=header]

|===

|Name

|Type

|Description

|arguments

|array[link:#error_arguments[error_arguments]]

a|Message arguments

|code

|string

a|Error code

|message

|string

a|Error message

|target

|string

a|The target parameter that caused the error.

|===

```
//end collapsible .Definitions block
```

```
====
```

```
[[IDdf2a1cb4786ab7a5c984962ddbfe9e7b]]
```

```
= Update the SSH server setting for a cluster
```

```
[.api-doc-operation .api-doc-operation-patch]#PATCH# [.api-doc-code-  
block]#`/security/ssh`#
```

Updates the SSH server setting for a cluster.

== Optional parameters

- * `ciphers` - Encryption algorithms for the payload
- * `key_exchange_algorithms` - SSH key exchange algorithms
- * `mac_algorithms` - MAC algorithms
- * `max_authentication_retry_count` - Maximum authentication retries allowed before closing the connection
- * `connections_per_second` - Maximum allowed connections per second
- * `max_instances` - Maximum allowed connections per node
- * `per_source_limit` - Maximum allowed connections from the same client host

== Related ONTAP commands

- * `security ssh`
- * `security protocol ssh`

== Learn more

- * xref:{relative_path}security_ssh_endpoint_overview.html[DOC /security/ssh]

== Parameters

```
[cols=5*,options=header]
```

```
|===
```

```
|Name
```

```
|Type
```

```
|In
```

```

|Required
|Description

|return_records
|boolean
|query
|False
a|The default is false. If set to true, the records are returned.

|===

== Request Body

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|ciphers
|array[string]
a|Ciphers for encrypting the data.

|connections_per_second
|integer
a|Maximum connections allowed per second.

|key_exchange_algorithms
|array[string]
a|Key exchange algorithms.

|mac_algorithms
|array[string]
a|MAC algorithms.

|max_authentication_retry_count
|integer

```

a|Maximum authentication retries allowed before closing the connection.

|max_instances

|integer

a|Maximum possible simultaneous connections.

|per_source_limit

|integer

a|Maximum connections from the same client host.

|===

.Example request

[%collapsible%closed]

====

[source,json,subs=+macros]

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "ciphers": [
    "aes256_ctr",
    "aes192_ctr",
    "aes128_ctr"
  ],
  "key_exchange_algorithms": [
    "diffie_hellman_group_exchange_sha256",
    "diffie_hellman_group14_sha1"
  ],
  "mac_algorithms": [
    "hmac_sha1",
    "hmac_sha2_512_etm"
  ]
}
```

====

== Response

Status: 200, Ok

== Error

Status: Default

ONTAP Error Response Codes

|===

Error Code	Description
------------	-------------

10682372	
----------	--

| There must be at least one key exchange algorithm associated with the SSH configuration.

10682373	
----------	--

| There must be at least one cipher associated with the SSH configuration.

10682375	
----------	--

| Failed to modify SSH key exchange algorithms.

10682378	
----------	--

| Failed to modify SSH ciphers.

10682399	
----------	--

| Key exchange algorithm not supported in FIPS enabled mode.

10682400	
----------	--

| Failed to modify SSH MAC algorithms.

10682401	
----------	--

| MAC algorithm not supported in FIPS enabled mode.

10682403	
----------	--

| There must be at least one MAC algorithm with the SSH configuration.

10682413	
----------	--

| Failed to modify maximum authentication retry attempts.

10682413	
----------	--

| Failed to modify maximum authentication retry attempts.

10682418	
----------	--

| Cipher not supported in FIPS enabled mode.

|===

```

[cols=3*,options=header]
|===
|Name
|Type
|Description

|error
|link:#error[error]
a|

|===

.Example error
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
====

== Definitions

[.api-def-first-level]
.See Definitions
[%collapsible%closed]
//Start collapsible Definitions block
====
[#href]
[.api-collapsible-fifth-title]
href

[cols=3*,options=header]
|===
|Name
|Type

```

```

|Description

|href
|string
a|

|===

[#_links]
[.api-collapsible-fifth-title]
_links

[cols=3*,options=header]
|===
|Name
|Type
|Description

|self
|link:#href[href]
a|

|===

[#cluster_ssh_server]
[.api-collapsible-fifth-title]
cluster_ssh_server

[cols=3*,options=header]
|===
|Name
|Type
|Description

|_links
|link:#_links[_links]
a|

|ciphers
|array[string]
a|Ciphers for encrypting the data.

|connections_per_second
|integer

```

```

a|Maximum connections allowed per second.

|key_exchange_algorithms
|array[string]
a|Key exchange algorithms.

|mac_algorithms
|array[string]
a|MAC algorithms.

|max_authentication_retry_count
|integer
a|Maximum authentication retries allowed before closing the connection.

|max_instances
|integer
a|Maximum possible simultaneous connections.

|per_source_limit
|integer
a|Maximum connections from the same client host.

|===

[#error_arguments]
[.api-collapsible-fifth-title]
error_arguments

[cols=3*,options=header]
|===
|Name
|Type
|Description

|code
|string
a|Argument code

|message

```



```

|string
a|Message argument

|===

[#error]
[.api-collapsible-fifth-title]
error

[cols=3*,options=header]
|===
|Name
|Type
|Description

|arguments
|array[link:#error_arguments[error_arguments]]
a|Message arguments

|code
|string
a|Error code

|message
|string
a|Error message

|target
|string
a|The target parameter that caused the error.

|===

//end collapsible .Definitions block
====

:leveloffset: -1

```

:leveloffset: -1

:leveloffset: -1

<<<

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 [link:http://www.netapp.com/TM](http://www.netapp.com/TM)^[http://www.netapp.com/TM^] are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.