# ∩ NetApp

# Manage security-related operations

REST API reference

NetApp
September 09, 2025

# Table of Contents

# Manage security-related operations

## Security endpoint overview

### Overview

You can use this API for various cluster-wide security-related operations.

### "onboard_key_manager_configurable_status" object

Use this API to retrieve details of whether or not the Onboard Key Manager can be configured on the cluster.

&ndash; GET /api/security

&ndash; GET /api/security?fields=onboard_key_manager_configurable_status

### "software_data_encryption" object

Contains software data encryption related information.

The following APIs can be used to enable or disable and obtain default software data at rest encryption values:

&ndash; PATCH /api/security -d '{ "software_data_encryption.disabled_by_default" : true }'

&ndash; PATCH /api/security -d '{ "software_data_encryption.disabled_by_default" : false }'

&ndash; GET /api/security

&ndash; GET /api/security?fields=software_data_encryption

**Platform Specifics**

**Unified ONTAP**

A PATCH request on this API using the parameter "software_data_encryption.conversion_enabled" triggers the conversion of all non-encrypted metadata volumes to encrypted metadata volumes and all non-NAE aggregates to NAE aggregates. For the conversion to start, the cluster must have either Onboard Key Manager or an external key manager set up and the aggregates should either be empty or have only metadata volumes. No data volumes should be present in any of the aggregates. For MetroCluster configurations, the PATCH request will fail if the cluster is in the switchover state.

### "fips" object

Contains FIPS mode information.

A PATCH request on this API using the parameter "fips.enabled" switches the system from using the default cryptographic module software implementations to validated ones or vice versa, where applicable. If the value of the parameter is "true" and unapproved algorithms are configured as permitted in relevant subsystems, those algorithms will be disabled in the relevant subsystem configurations. If "false", there will be no implied change to the relevant subsystem configurations.

&ndash; GET /api/security

&ndash; GET /api/security?fields=fips

&ndash; PATCH /api/security -d '{ "fips.enabled" : true }'

&ndash; PATCH /api/security -d '{ "fips.enabled" : false }'

## "tls" object

Contains TLS configuration information.

A PATCH request on this API using the parameter "tls.cipher_suites" and/or "tls.protocol_versions" configures the permissible cipher suites and/or protocol versions for all TLS-enabled applications in the system. All protocol versions at or above the lowest version level specified are enabled, including those that are not explicitly specified.

&ndash; GET /api/security

&ndash; GET /api/security?fields=tls

&ndash; PATCH /api/security -d '{ "tls" : { "protocol_versions" : ["TLSv1.3", "TLSv1.2"], "cipher_suites" : ["TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384", "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256"] } }'

## "management_protocols" object

Contains Security Protocols information.

This security protocols endpoint is used to retrieve and configure security protocols.

&ndash; GET /api/security

&ndash; GET /api/security?fields=management_protocols

&ndash; PATCH /api/security -d '{ "management_protocols" : { "rsh_enabled" : true } }'

&ndash; PATCH /api/security -d '{ "management_protocols" : { "rsh_enabled" : false } }'

&ndash; PATCH /api/security -d '{ "management_protocols" : { "telnet_enabled" : true } }'

&ndash; PATCH /api/security -d '{ "management_protocols" : { "telnet_enabled" : false } }'

&ndash; PATCH /api/security -d '{ "management_protocols" : { "rsh_enabled" : true, "telnet_enabled" : true } }'

## GET Examples

### Retrieving information about the security configured on the cluster

The following example shows how to retrieve the 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
},
"software_data_encryption": {
  "conversion_enabled": false,
  "disabled_by_default": false,
  "encryption_state": "unencrypted"
},
"fips": {
  "enabled": false
},
"tls": {
  "cipher_suites": [
    "TLS_RSA_WITH_AES_128_CCM",
    "TLS_RSA_WITH_AES_128_CCM_8",
    "TLS_RSA_WITH_AES_128_GCM_SHA256",
    "TLS_RSA_WITH_AES_128_CBC_SHA",
    "TLS_RSA_WITH_AES_128_CBC_SHA256",
    "TLS_RSA_WITH_AES_256_CCM",
    "TLS_RSA_WITH_AES_256_CCM_8",
    "TLS_RSA_WITH_AES_256_GCM_SHA384",
    "TLS_RSA_WITH_AES_256_CBC_SHA",
    "TLS_RSA_WITH_AES_256_CBC_SHA256",
    "TLS_RSA_WITH_ARIA_128_GCM_SHA256",
    "TLS_RSA_WITH_ARIA_256_GCM_SHA384",
    "TLS_RSA_WITH_CAMELLIA_128_CBC_SHA",
    "TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256",
    "TLS_RSA_WITH_CAMELLIA_256_CBC_SHA",
    "TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256",
    "TLS_DHE_DSS_WITH_AES_128_GCM_SHA256",
    "TLS_DHE_DSS_WITH_AES_128_CBC_SHA",
    "TLS_DHE_DSS_WITH_AES_128_CBC_SHA256",
    "TLS_DHE_DSS_WITH_AES_256_GCM_SHA384",
    "TLS_DHE_DSS_WITH_AES_256_CBC_SHA",
    "TLS_DHE_DSS_WITH_AES_256_CBC_SHA256",
    "TLS_DHE_DSS_WITH_ARIA_128_GCM_SHA256",
    "TLS_DHE_DSS_WITH_ARIA_256_GCM_SHA384",
```

```
"TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA",
"TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA256",
"TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA",
"TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA256",
"TLS_DHE_PSK_WITH_AES_128_CBC_SHA",
"TLS_DHE_PSK_WITH_AES_128_CBC_SHA256",
"TLS_DHE_PSK_WITH_AES_128_CCM",
"TLS_PSK_DHE_WITH_AES_128_CCM_8",
"TLS_DHE_PSK_WITH_AES_128_GCM_SHA256",
"TLS_DHE_PSK_WITH_AES_256_CBC_SHA",
"TLS_DHE_PSK_WITH_AES_256_CBC_SHA384",
"TLS_DHE_PSK_WITH_AES_256_CCM",
"TLS_PSK_DHE_WITH_AES_256_CCM_8",
"TLS_DHE_PSK_WITH_AES_256_GCM_SHA384",
"TLS_DHE_PSK_WITH_ARIA_128_GCM_SHA256",
"TLS_DHE_PSK_WITH_ARIA_256_GCM_SHA384",
"TLS_DHE_PSK_WITH_CAMELLIA_128_CBC_SHA256",
"TLS_DHE_PSK_WITH_CAMELLIA_256_CBC_SHA384",
"TLS_DHE_PSK_WITH_CHACHA20_POLY1305_SHA256",
"TLS_DHE_RSA_WITH_AES_128_CCM",
"TLS_DHE_RSA_WITH_AES_128_CCM_8",
"TLS_DHE_RSA_WITH_AES_128_GCM_SHA256",
"TLS_DHE_RSA_WITH_AES_128_CBC_SHA",
"TLS_DHE_RSA_WITH_AES_128_CBC_SHA256",
"TLS_DHE_RSA_WITH_AES_256_CCM",
"TLS_DHE_RSA_WITH_AES_256_CCM_8",
"TLS_DHE_RSA_WITH_AES_256_GCM_SHA384",
"TLS_DHE_RSA_WITH_AES_256_CBC_SHA",
"TLS_DHE_RSA_WITH_AES_256_CBC_SHA256",
"TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256",
"TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384",
"TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA",
"TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256",
"TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA",
"TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256",
"TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256",
"TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256",
"TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384",
"TLS_ECDHE_ECDSA_WITH_AES_128_CCM",
"TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8",
"TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
"TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA",
"TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
"TLS_ECDHE_ECDSA_WITH_AES_256_CCM",
"TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8",
"TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
```

```
"TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA",
"TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
"TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256",
"TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384",
"TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256",
"TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384",
"TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256",
"TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA",
"TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256",
"TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA",
"TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384",
"TLS_ECDHE_PSK_WITH_CAMELLIA_128_CBC_SHA256",
"TLS_ECDHE_PSK_WITH_CAMELLIA_256_CBC_SHA384",
"TLS_ECDHE_PSK_WITH_CHACHA20_POLY1305_SHA256",
"TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
"TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA",
"TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
"TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
"TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA",
"TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384",
"TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256",
"TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384",
"TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256",
"TLS_PSK_WITH_AES_128_CBC_SHA",
"TLS_PSK_WITH_AES_128_CBC_SHA256",
"TLS_PSK_WITH_AES_128_CCM",
"TLS_PSK_WITH_AES_128_CCM_8",
"TLS_PSK_WITH_AES_128_GCM_SHA256",
"TLS_PSK_WITH_AES_256_CBC_SHA",
"TLS_PSK_WITH_AES_256_CBC_SHA384",
"TLS_PSK_WITH_AES_256_CCM",
"TLS_PSK_WITH_AES_256_CCM_8",
"TLS_PSK_WITH_AES_256_GCM_SHA384",
"TLS_PSK_WITH_ARIA_128_GCM_SHA256",
"TLS_PSK_WITH_ARIA_256_GCM_SHA384",
"TLS_PSK_WITH_CAMELLIA_128_CBC_SHA256",
"TLS_PSK_WITH_CAMELLIA_256_CBC_SHA384",
"TLS_PSK_WITH_CHACHA20_POLY1305_SHA256",
"TLS_RSA_PSK_WITH_AES_128_CBC_SHA",
"TLS_RSA_PSK_WITH_AES_128_CBC_SHA256",
"TLS_RSA_PSK_WITH_AES_128_GCM_SHA256",
"TLS_RSA_PSK_WITH_AES_256_CBC_SHA",
"TLS_RSA_PSK_WITH_AES_256_CBC_SHA384",
"TLS_RSA_PSK_WITH_AES_256_GCM_SHA384",
"TLS_RSA_PSK_WITH_ARIA_128_GCM_SHA256",
"TLS_RSA_PSK_WITH_ARIA_256_GCM_SHA384",
```

```
      "TLS_RSA_PSK_WITH_CAMELLIA_128_CBC_SHA256",
      "TLS_RSA_PSK_WITH_CAMELLIA_256_CBC_SHA384",
      "TLS_RSA_PSK_WITH_CHACHA20_POLY1305_SHA256",
      "TLS_SRP_SHA_WITH_AES_128_CBC_SHA",
      "TLS_SRP_SHA_WITH_AES_256_CBC_SHA",
      "TLS_SRP_SHA_DSS_WITH_AES_128_CBC_SHA",
      "TLS_SRP_SHA_DSS_WITH_AES_256_CBC_SHA",
      "TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA",
      "TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA",
      "TLS_AES_128_GCM_SHA256",
      "TLS_AES_256_GCM_SHA384",
      "TLS_CHACHA20_POLY1305_SHA256"
    ],
    "protocol_versions": [
      "TLSv1.3",
      "TLSv1.2"
    ]
  },
  "management_protocols": {
    "rsh_enabled": false,
    "telnet_enabled": false
  }
}
```

```
'''

== PATCH Examples

=== Enabling software encryption conversion in the cluster

The following example shows how to enable software encryption conversion
in the cluster.

= The API:

PATCH /api/security

= The call

curl -X PATCH "https://+++<mgmt_ip>+++/api/security" -d '{
"software_data_encryption.conversion_enabled" : true }'+++</mgmt_ip>+++

= The response:
```

```
{
 "job": {
     "uuid": "ebcbd82d-1cd4-11ea-8f75-005056ac4adc",
     "_links": {
         "self": {
             "href": "/api/cluster/jobs/ebcbd82d-1cd4-11ea-8f75-
005056ac4adc"
         }
     }
 }
}
```

This returns a job UUID. A subsequent GET for this job UUID returns
details of the job.

= The call

curl -X GET "https://+++<mgmt_ip>+++/api/cluster/jobs/ebcbd82d-1cd4-11ea-
8f75-005056ac4adc"+++</mgmt_ip>+++

= The response:

```
{
"uuid": "ebcbd82d-1cd4-11ea-8f75-005056ac4adc",
"description": "PATCH /api/security",
"state": "success",
"message": "success",
"code": 0,
"start_time": "2019-12-12T06:45:40-05:00",
"end_time": "2019-12-12T06:45:40-05:00",
"_links": {
  "self": {
    "href": "/api/cluster/jobs/ebcbd82d-1cd4-11ea-8f75-005056ac4adc"
  }
}
}
```

[discrete]
=== Enabling FIPS mode in the cluster

The following example shows how to enable FIPS mode in the cluster.

= The API:

PATCH /api/security

= The call

```
curl -X PATCH "https://+++<mgmt_ip>+++/api/security" -d '{ "fips.enabled"
: true }'+++</mgmt_ip>+++

= The response:

{
 "job": {
     "uuid": "8e7f59ee-a9c4-4faa-9513-bef689bbf2c2",
     "_links": {
         "self": {
             "href": "/api/cluster/jobs/8e7f59ee-a9c4-4faa-9513-
bef689bbf2c2"
         }
     }
 }
}
```

This returns a job UUID. A subsequent GET for this job UUID returns
details of the job.

```
= The call

curl -X GET "https://+++<mgmt_ip>+++/api/cluster/jobs/8e7f59ee-a9c4-4faa-
9513-bef689bbf2c2"+++</mgmt_ip>+++

= The response:

{
"uuid": "8e7f59ee-a9c4-4faa-9513-bef689bbf2c2",
"description": "PATCH /api/security",
"state": "success",
"message": "success",
"code": 0,
"start_time": "2020-04-28T06:55:40-05:00",
"end_time": "2020-04-28T06:55:41-05:00",
"_links": {
  "self": {
    "href": "/api/cluster/jobs/8e7f59ee-a9c4-4faa-9513-bef689bbf2c2"
  }
}
}
```

[discrete]
=== Configuring permissible TLS protocols and cipher suites in the cluster

The following example shows how to configure the cluster to only allow
TLSv1.3 & TLSv1.2 with selected cipher suites.

```
= The API:

PATCH /api/security

= The call

curl -X PATCH "https://+++<mgmt_ip>+++/api/security" -d '{ "tls" : {
"protocol_versions" : ["TLSv1.3", TLSv1.2"], "cipher_suites" :
["TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384", "TLS_AES_256_GCM_SHA384"] }
}'+++</mgmt_ip>+++

= The response:

{
 "job": {
     "uuid": "b45b6290-f4f2-442a-aa0e-4d3ffefe5e0d",
     "_links": {
         "self": {
             "href": "/api/cluster/jobs/b45b6290-f4f2-442a-aa0e-
4d3ffefe5e0d"
         }
     }
 }
}
This returns a job UUID. A subsequent GET for this job UUID returns
details of the job.

= The call

curl -X GET "https://+++<mgmt_ip>+++/api/cluster/jobs/b45b6290-f4f2-442a-
aa0e-4d3ffefe5e0d"+++</mgmt_ip>+++

= The response:

{
"uuid": "b45b6290-f4f2-442a-aa0e-4d3ffefe5e0d",
"description": "PATCH /api/security",
"state": "success",
"message": "success",
"code": 0,
"start_time": "2021-03-22T08:52:50-05:00",
"end_time": "2021-03-22T08:52:51-05:00",
"_links": {
  "self": {
    "href": "/api/cluster/jobs/b45b6290-f4f2-442a-aa0e-4d3ffefe5e0d"
  }
```

```
   }
  }

[discrete]
=== Enabling security protocols in the cluster

The following example shows how to enable the security protocol rsh in the
cluster.

= The API:

PATCH /api/security

= The call

curl -X PATCH "https://+++<mgmt_ip>+++/api/security" -d '{
"management_protocols" : { "rsh_enabled" : true } }'+++</mgmt_ip>+++

= The response

{
"job": {
"uuid": "2980ba28-adab-11eb-8fa3-005056bbfa84",
"_links": {
  "self": {
    "href": "/api/cluster/jobs/2980ba28-adab-11eb-8fa3-005056bbfa84"
  }
 }
 }
}

= The call:

curl -H "accept: application/hal+json" -X GET "https://+++<mgmt-
ip>+++/api/security/?fields=management_protocols"+++</mgmt-ip>+++

= The response:

{
"management_protocols": {
  "rsh_enabled": false,
  "telnet_enabled": false
},
"_links": {
  "self": {
    "href": "/api/security"
  }
```

```
}
}

'''
```

[[ID46c01f871b2ae21427caca115df8221b]]
= Retrieve information about security configured on the cluster

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

*Introduced In:* 9.7

Retrieves information about the security configured on the cluster.

== Related ONTAP commands

* `security config show`

== Parameters

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

|Name
|Type
|In
|Required
|Description

|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|

|fips
|link:#fips[fips]
a|Cluster-wide Federal Information Processing Standards (FIPS) mode
information.

|management_protocols
|link:#management_protocols[management_protocols]
a|Cluster-wide security protocols related information.

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

|software_data_encryption
|link:#software_data_encryption[software_data_encryption]
a|Cluster-wide software data encryption related information.

|tls
|link:#tls[tls]
a|Cluster-wide Transport Layer Security (TLS) configuration information

|===

.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "_links": {
```

12

```
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "onboard_key_manager_configurable_status": {
      "code": 65537300,
      "message": "No platform support for volume encryption in following
nodes - node1, node2."
    },
    "software_data_encryption": {
      "encryption_state": "string"
    },
    "tls": {
      "cipher_suites": [
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384"
      ],
      "protocol_versions": [
        "string"
      ]
    }
}
====

== Error
```

Status: Default, Error

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

|error
|link:#returned_error[returned_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|

|===


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

Cluster-wide Federal Information Processing Standards (FIPS) mode
information.


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

|enabled
|boolean
a|Indicates whether or not the software FIPS mode is enabled on the
cluster. Our FIPS compliance involves configuring the use of only approved
algorithms in applicable contexts (for example TLS), as well as the use of
formally validated cryptographic module software implementations, where
applicable. The US government documents concerning FIPS 140-2 outline the
relevant security policies in detail.


|===


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

Cluster-wide security protocols related information.


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

```
|Description

|rsh_enabled
|boolean
a|Indicates whether or not security protocol rsh is enabled on the
cluster.


|telnet_enabled
|boolean
a|Indicates whether or not security protocol telnet is enabled on the
cluster.


|===


[#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.
```

```
|===


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

Cluster-wide software data encryption related information.


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

|conversion_enabled
|boolean
a|Indicates whether or not software encryption conversion is enabled on
the cluster. A PATCH request initiates the conversion of all non-encrypted
metadata volumes in the cluster to encrypted metadata volumes and all non-
NAE aggregates to NAE aggregates. For the PATCH request to start, the
cluster must have either an Onboard or an external key manager set up and
the aggregates should either be empty or have only metadata volumes. No
data volumes should be present in any of the aggregates in the cluster.
For MetroCluster configurations, a PATCH request enables conversion on all
the aggregates and metadata volumes of both local and remote clusters and
is not allowed when the MetroCluster is in switchover state.


|disabled_by_default
|boolean
a|Indicates whether or not default software data at rest encryption is
disabled on the cluster.


|encryption_state
|string
a|Software data encryption state.
encrypted &dash; All the volumes are encrypted.
encrypting &dash; Encryption conversion operation is in progress.
partial &dash; Some volumes are encrypted, and others remains in plain
text.
rekeying &dash; All volumes are currently being encrypted with a new key.
unencrypted &dash; None of the volumes are encrypted.
conversion_paused &dash; Encryption conversion operation is paused on one
or more volumes.
```

rekey_paused &dash; Encryption rekey operation is paused on one or more volumes.


|rekey
|boolean
a|

|===



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

Cluster-wide Transport Layer Security (TLS) configuration information


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

|cipher_suites
|array[string]
a|Names a cipher suite that the system can select during TLS handshakes. A list of available options can be found on the Internet Assigned Number Authority (IANA) website.


|protocol_versions
|array[string]
a|Names a TLS protocol version that the system can select during TLS handshakes. The use of SSLv3 or TLSv1 is discouraged.


|===



[#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



|===


[#returned_error]
[.api-collapsible-fifth-title]
returned_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
====



[[ID1a5d3038b88973c1fbe3a75939de16e8]]
= Update the software FIPS mode or enable conversion of non-encrypted
metadata volumes non-NAE aggregates

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

*Introduced In:* 9.8

Updates the software FIPS mode or modifies software data encryption.

== Platform Specifics

== Unified ONTAP

The PATCH request can be used to enable conversion of non-encrypted
metadata volumes to encrypted metadata volumes and non-NAE aggregates to
NAE aggregates.

== Related ONTAP commands

* `security config modify`


== 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
* Max value: 120
* Min value: 0

|===

== Request Body


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

|fips
|link:#fips[fips]
a|Cluster-wide Federal Information Processing Standards (FIPS) mode
information.


|management_protocols
|link:#management_protocols[management_protocols]
a|Cluster-wide security protocols related information.


|software_data_encryption
|link:#software_data_encryption[software_data_encryption]
a|Cluster-wide software data encryption related information.


|tls
|link:#tls[tls]
a|Cluster-wide Transport Layer Security (TLS) configuration information


|===

```
.Example request
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "software_data_encryption": {
    "encryption_state": "string"
  },
  "tls": {
    "cipher_suites": [
      "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384"
    ],
    "protocol_versions": [
      "string"
    ]
  }
}
====
```

== Response

Status: 200, Ok

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

|job
|link:#job_link[job_link]
a|

|===


.Example response
[%collapsible%closed]
====
[source,json,subs=+macros]
{
  "job": {
    "uuid": "string"
  }
}
====

== Response
```

Status: 202, Accepted

```
== Error
```

Status: Default

```
ONTAP Error Response Codes

|===
| Error Code | Description

| 5636142
| This operation is not supported in a mixed-release cluster.

| 5636145
| This operation is not supported when cluster security is configured with
FIPS mode.
```

| 52428817
| SSLv3 is not supported when FIPS is enabled.

| 52428824
| TLSv1 is not supported when FIPS is enabled.

| 52428830
| Cannot enable FIPS-compliant mode because the configured minimum
security strength for certificates is not compatible.

| 52428832
| TLSv1.1 is not supported when FIPS is enabled.

| 52559974
| Cannot enable FIPS-compliant mode because a certificate that is not
FIPS-compliant is in use.

| 65536987
| One or more key servers are unavailable.

| 196608047
| Operation is not allowed when volume move is in progress.

| 196608070
| Key manager is not configured on the cluster. Configure either an
external Key Management Server or an onboard key manager.

| 196608081
| Cannot start software encryption conversion while there are data volumes
in the cluster.

| 196608082
| The operation is not valid when the MetroCluster is in switchover mode.

| 196608368
| Failed to perform the requested operation. One or more data volume in
offline state.

| 196608369
| Conversion cannot be enabled because the cluster contains read-only or
primordial logical data-protection volumes. Retry the patch operation
after deleting those volumes.

| 196608370
| The PATCH request to enable conversion failed because one or more
volumes are already queued for the encryption conversion operation.

| 196608372
| An automated ONTAP update is in progress, retry the PATCH request after it is completed.

| 196608373
| Unable to perform the encryption operation because of a mixed-release cluster. Complete the upgrade or revert operation, then try the PATCH request again.

| 196608374
| Failed to perform the requested operation. One or more SVMs not in admin running state.

| 196608375
| Failed to perform the requested operation. One or more volume is of temporary type.

| 196608376
| Internal error. Could not get volume encryption information.

| 196608377
| Internal error. The Volume Location Database (VLDB) is inconsistent. Contact support personnel to resolve this issue.

| 196608378
| Failed to perform the requested operation. Data SVM Key manager configuration is in mixed state.

| 196608379
| Internal error. The encryption metadata for the volume is inconsistent. Contact technical support for assistance.

| 196608380
| Failed to perform the requested operation. Wafliron is currently active.

| 196608381
| Failed to perform the requested operation. A clone split operation is in progress.

| 196608382
| Failed to perform the requested operation. A volume rehost operation is in progress.

| 196608383
| Failed to perform the requested operation. The cluster contains one or more SnapLock volume.

| 196608384
| The PATCH request to start rekey failed because the cluster contains one or more plain text volumes. Retry the PATCH request after converting the existing plain text volumes to encrypted volumes.

| 196608385
| Failed to perform the requested operation. Keystore configuration is being switched. Wait until the keystore is in the active state and then try the PATCH request again.

| 196608386
| Failed to perform the requested operation. Rekey operation for one or more SVMs is in progress. Wait until the keystore is in the active state and then try the PATCH request again.

| 196608387
| "software_data_encryption.conversion_enabled" cannot be set to "false" in a PATCH request.

| 196608388
| Both "software_data_encryption.conversion_enabled" and "software_data_encryption.disabled_by_default" cannot be set to "true" in a single PATCH request.

| 196608389
| Both "software_data_encryption.conversion_enabled" and "software_data_encryption.rekey" cannot be set to "true" in a single PATCH request.

| 196608390
| "software_data_encryption.rekey" cannot be set to "false" in a PATCH request.

| 196608391
| Both "software_data_encryption.rekey" and "software_data_encryption.disabled_by_default" cannot be set to "true" in a single PATCH request.

| 196608392
| The PATCH request for cluster level rekey requires an effective cluster version of 9.16.1 or later.

| 196608393
| The PATCH request for cluster level rekey is not supported on this platform.
|===

```
Also see the table of common errors in the
xref:{relative_path}getting_started_with_the_ontap_rest_api.html#Response_
body[Response body] overview section of this documentation.


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

Cluster-wide Federal Information Processing Standards (FIPS) mode
information.


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

|enabled
```

|boolean
a|Indicates whether or not the software FIPS mode is enabled on the
cluster. Our FIPS compliance involves configuring the use of only approved
algorithms in applicable contexts (for example TLS), as well as the use of
formally validated cryptographic module software implementations, where
applicable. The US government documents concerning FIPS 140-2 outline the
relevant security policies in detail.


|===


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

Cluster-wide security protocols related information.


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

|rsh_enabled
|boolean
a|Indicates whether or not security protocol rsh is enabled on the
cluster.


|telnet_enabled
|boolean
a|Indicates whether or not security protocol telnet is enabled on the
cluster.


|===


[#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.


|===


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

Cluster-wide software data encryption related information.


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

|conversion_enabled
|boolean
a|Indicates whether or not software encryption conversion is enabled on
the cluster. A PATCH request initiates the conversion of all non-encrypted
metadata volumes in the cluster to encrypted metadata volumes and all non-
NAE aggregates to NAE aggregates. For the PATCH request to start, the
cluster must have either an Onboard or an external key manager set up and
the aggregates should either be empty or have only metadata volumes. No
```

data volumes should be present in any of the aggregates in the cluster.
For MetroCluster configurations, a PATCH request enables conversion on all
the aggregates and metadata volumes of both local and remote clusters and
is not allowed when the MetroCluster is in switchover state.


|disabled_by_default
|boolean
a|Indicates whether or not default software data at rest encryption is
disabled on the cluster.


|encryption_state
|string
a|Software data encryption state.
encrypted &dash; All the volumes are encrypted.
encrypting &dash; Encryption conversion operation is in progress.
partial &dash; Some volumes are encrypted, and others remains in plain
text.
rekeying &dash; All volumes are currently being encrypted with a new key.
unencrypted &dash; None of the volumes are encrypted.
conversion_paused &dash; Encryption conversion operation is paused on one
or more volumes.
rekey_paused &dash; Encryption rekey operation is paused on one or more
volumes.


|rekey
|boolean
a|

|===


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

Cluster-wide Transport Layer Security (TLS) configuration information


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

```
|cipher_suites
|array[string]
a|Names a cipher suite that the system can select during TLS handshakes. A
list of available options can be found on the Internet Assigned Number
Authority (IANA) website.


|protocol_versions
|array[string]
a|Names a TLS protocol version that the system can select during TLS
handshakes. The use of SSLv3 or TLSv1 is discouraged.


|===


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

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

|fips
|link:#fips[fips]
a|Cluster-wide Federal Information Processing Standards (FIPS) mode
information.


|management_protocols
|link:#management_protocols[management_protocols]
a|Cluster-wide security protocols related information.


|software_data_encryption
|link:#software_data_encryption[software_data_encryption]
a|Cluster-wide software data encryption related information.


|tls
|link:#tls[tls]
a|Cluster-wide Transport Layer Security (TLS) configuration information
```

```
|===


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

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

|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


|===


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

```
returned_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


<<<
*Copyright information*

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S. No
part of this document covered by copyright may be reproduced in any form
or by any means—graphic, electronic, or mechanical, including
```

*Trademark information*